CYBER DEFENSE MAGAZINE

eMAGAZINE

DECEMBER 2022

In This Edition

Largest Data Breaches Of 2022 - Protect Data With Deep Packet Inspection

Data, Privacy, And the Future of Artificial Intelligence

The Great Resignation, The Quiet Resignation - Five Security Awareness Countermeasures to Security Threats Derived from these Workforce Trends

...and much more...

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the

Publisher…

Dear Friends,

Looking back over the year, and ahead to the next, from the Publisher's desk we see many things have changed but data breaches and ransomware attacks have become even more pervasive this year. As a result, there is a heightened concern with cybersecurity, and cyber safety is the top priority.

As readers will know, Cyber Defense Media Group offers various ways to recognize and promote providers of cybersecurity solutions. As we near the beginning of a new year, this is the perfect time to showcase your solution worldwide. However, there are thousands of cybersecurity companies worldwide.

The question is **"How Will You Stand Out?"**

Apply for the ***Global Infosec Awards 2023*** to help you stand out among your competitors!

We have now launched the Global Infosec Awards nomination opportunities for 2023 at www.cyberdefenseawards.com. We are looking for the best and the brightest in the innovators who are changing this shape and scope of the Cyber Defense landscape, to help us get one step ahead of the next threat.

We also wish to bring to the attention of our readers the opening of our Women In Cybersecurity Scholarship Fund for 2023. More information on applying is posted at https://cyberdefenseawards.com/women-in-cybersecurity-scholarship-fund-for-2023/

As always, the view from the Publisher's desk continues to focus on the immediacy of threats to our national and international cybersecurity. The current news often focuses on the cyber attacks which have become the war zone of today.

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, CISSP®, fmDHS
CEO, Cyber Defense Media Group
Publisher, Cyber Defense Magazine

P.S. When you share a story or an article or information about CDM, please use #CDM and @CyberDefenseMag and @Miliefsky – it helps spread the word about our free resources even more quickly

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

EDITOR-IN-CHIEF

Yan Ross, JD

yan.ross@cyberdefensemagazine.com

ADVERTISING

Marketing Team

marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451

http://www.cyberdefensemagazine.com

PUBLISHER

Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
http://www.cyberdefensemagazine.com/about-our-founder/

10 YEARS OF EXCELLENCE!

Providing free information, best practices, tips, and techniques on cybersecurity since 2012, Cyber Defense magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group:

CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE TV RADIO AWARDS

PROFESSIONALS VENTURES WEBINARS

CYBERDEFENSECONFERENCES

Welcome to CDM's December 2022 Issue

From the Editor-in-Chief

As we complete this eventful year in the practice of cybersecurity, we face a landscape of cyber threats growing in both magnitude and complexity. These attacks are launched against government, critical infrastructure, private organizations (both for profit and non-profit), academic institutions, and even individual consumers. By every indication, they will continue to grow.

Among cybersecurity professionals, this presents both a threat and an opportunity. Success will be based on capabilities, current knowledge, and the ability to make and deliver on promises of minimizing risks of cyber incursions.

In this December issue of Cyber Defense Magazine, we are pleased to provide dozens of relevant articles on cybersecurity practice responding to this array of cyber challenges. We believe that in the marketplace of ideas and capabilities, Cyber Defense Magazine offers the most comprehensive and valuable forum for cybersecurity professionals.

As always, we are delighted to receive both solicited and unsolicited proposals for articles. Please remember to submit all articles on the Cyber Defense Magazine writer's kit template, which incorporates the major terms and conditions of publication. We make every effort to close out acceptance of articles by the 15th of each month for publication in the following month's edition.

Wishing you all success in your cybersecurity endeavors,

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & U.S. Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him by e-mail at yan.ross@cyberdefensemagazine.com


SPONSORS

CionSystems

Next Generation Enterprise Identity Management (EIM)™

THE SECRETS OF HARDENING ACTIVE DIRECTORY

• Deploy. • Manage. • Tune up. • Audit. • Defend. Report.

GET YOUR FREE eBook

Get https://cionsystems.com/

STOP BEING REACTIVE. START BEING PROACTIVE.

Get the Zero Trust endpoint security solution that offers a unified approach to protecting your business, users, networks, and devices against the exploitation of zero-day vulnerabilities.

Visit our website, or speak to a Cyber Hero to learn more about how the ThreatLocker® solution can help you better protect your business.

THREATLOCKER

threatlocker.com

NIGHTDRAGON

***"NightDragon** Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"*

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

ACCELERATE

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

www.nightdragon.com

HERJAVEC GROUP

Celebrating Over 15 Years of Cybersecurity Operations Excellence

At Herjavec Group, information security is what we do.

You may know me from making deals on television, but my passion lies in innovating technology - yes, cybersecurity.

Over 15 years ago we started the business selling commercial firewalls to IT buyers. Over time we've seen a monumental shift towards what we are all familiar with - the cybercrime epidemic. Now our customers are challenged to address compliance requirements, incident response plans, nation state threats, security awareness, malware detection…the list goes on. In response, we have advanced our cyber capabilities and attracted world class talent.

Today, Herjavec Group is a global leader in cybersecurity with expertise in comprehensive security services including **Managed Security Services** (SOC Operations, Threat Detection, Security Technology Engineering) & **Professional Services** (Advisory Services, Identity Services, Technology Implementation, Threat Management & Incident Response). Herjavec Group is over 300 people strong, with offices and Security Operations Centers across the United States, United Kingdom, Canada and India. At Herjavec Group, we realize that in cybersecurity change is constant, but we are driven by a steadfast goal: to make enterprises around the world more secure.

To your success,

Robert Herjavec
Black Unicorn Awards Judge (Emeritus)
Star of ABC's Shark Tank
Founder & CEO of Herjavec Group

Recognized Industry-Wide

MOST INNOVATIVE IAM PROVIDER
Cyber Defense Magazine Global Awards 2018 WINNER

SECURITY SERVICES LEADER
IDC Analyze the Future

LEADER IN MANAGED SECURITY SERVICES
Cyber Defense Magazine Global Awards 2018 WINNER

SECURITY COMPANY OF THE YEAR
CDM Cyber Defense Magazine

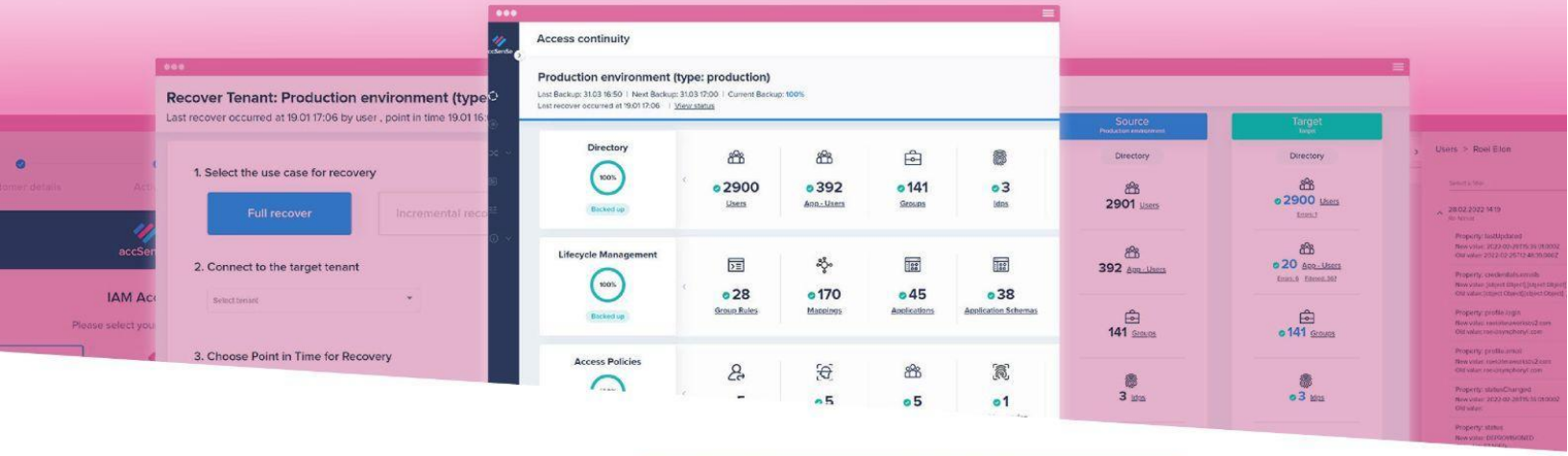
#1 ON THE
Cyber Security 500 — World's Hottest Security Companies

TOP 10 ON THE
2018 TOP 100 MSSPs — MSSPAlert.com/Top100


2001
2022
ALLEGIS CYBER CAPITAL
The first dedicated cybersecurity venture firm in the world.
AN INTEGRATED GLOBAL, STAGE-AGNOSTIC CYBERSECURITY INVESTMENT PLATFORM SPANNING SEED THROUGH GROWTH.
For 20 years, AllegisCyber Capital has offered a proven investment platform that actively engages with the most promising entrepreneurs in cyber and delivers the market access, team building, and operating experience essential to their success.
BUILDING AND FUNDING THE MOST INNOVATIVE COMPANIES IN CYBER
Signifyd
SAFEGUARD CYBER
ELISITY
panaseer
Synack
SkyHive
cyber GRX
DRAGOS
CONCEAL
varmour
ALLEGISCYBER CAPITAL
www.allegiscyber.com

accSenSe

A complete protection and recovery solution for your organization's most critical SaaS.
(Your IAM WF and CIAM)



The Road To Quick And Easy Recovery Starts With accSenSe and Okta

- Complete protection for your Okta tenant, which gives you full visibility to configuration and data history.
- The ability to recover means you can reduce RTO during a disaster, keeping your business running and financial loss to a minimum.
- Stay compliant with SOC2 & SOX. The audit capabilities mean you can easily control system changes.

With accSenSe you can rest secure knowing your Cloud Identity and Access Management system is fully protected and recoverable, no matter what tomorrow brings.

monday.com GLASSBOX bright data fiverr.

After running through endless Cloud Identity Access Management system implementation use-cases and disasters, the accSenSe team decided to solve the most significant problem of modern organizations relying on SaaS solutions.

We developed a platform to manage and protect cloud Identity and Access Management system to ensure business as usual isn't just a phrase.

START A 30-day TRIAL >>

https://accsense.io


DATATRIBE
CYBER STARTUP FOUNDRY
Forging dominant companies from nation-state domain expertise
CAPITAL | RESOURCES | GUIDANCE | SUCCESS
HOME TO THE WORLD'S FASTEST GROWING CYBERSECURITY AND DATA SCIENCE COMPANIES
quickcode
DRAGOS
ENVEIL
INERTIALSENSE
PREVAILION
the cyberwire
Ntrinsec
SIXMAP
STRIDER
CONTRAFORCE
BLACKCLOAK
SightGain
JOIN THE TRIBE
DATATRIBE.COM

i2Chain

Ready, set, Chain.

Convert MS Office, Adobe, images, and design document into non-fungible, traceable, hack-proof artifacts.

Encrypted store and compliant share using i2Chain APIs.

Preventing Tomorrow's Malware

Today.

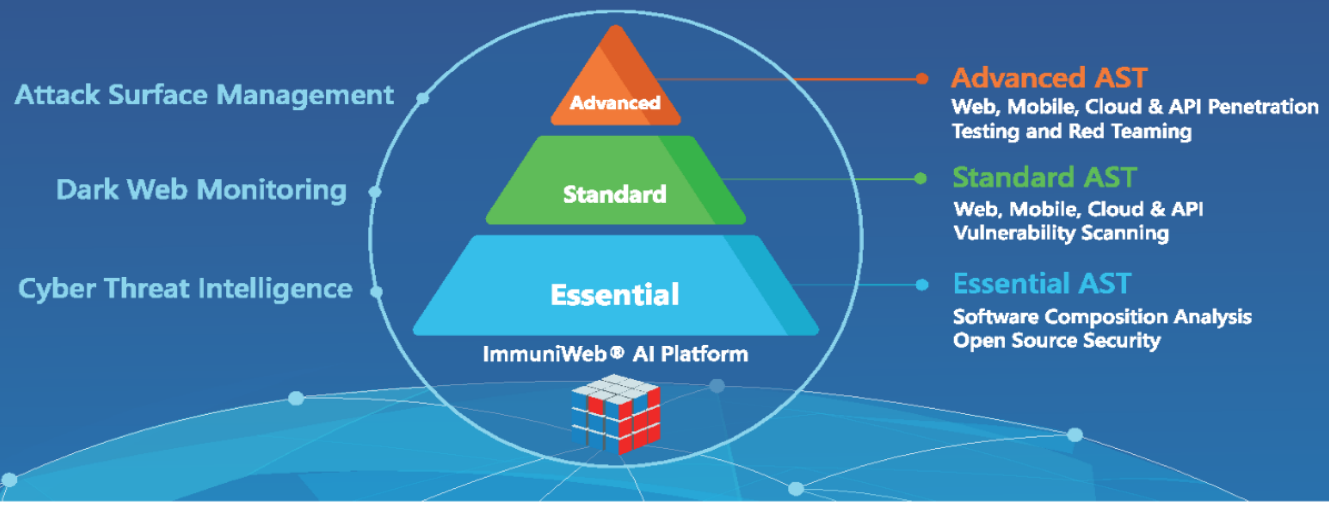
www.cythereal.com

ImmuniWeb®

AI for Application Security

We Simplify, Accelerate, and Reduce Costs of Application Penetration Testing, Protection, and Compliance

Risk-Based and Threat-Aware Application Security Testing (AST)



ImmuniWeb® Discovery

ImmuniWeb® Discovery leverages OSINT and our award-winning AI technology to illuminate attack surface and Dark Web exposure of a company. The non-intrusive and production-safe discovery is a perfect fit both for continuous self-assessment and vendor risk scoring to prevent supply chain attacks.

ImmuniWeb® Neuron

ImmuniWeb® Neuron unleashes the power of Machine Learning and AI to take traditional web vulnerability scanning to the next level. While detecting more vulnerabilities compared to automated web scanners, every web vulnerability scan by Neuron is equipped with a contractual zero false positives SLA.

ImmuniWeb® On-Demand

ImmuniWeb® On-Demand leverages our award-winning Machine Learning technology to accelerate and enhance web penetration testing. Every pentest is easily customizable and provided with a zero false positives SLA. Unlimited patch verifications and 24/7 access to our security analysts are included into every project.

ImmuniWeb® MobileSuite

ImmuniWeb® MobileSuite leverages our award-winning Machine Learning technology to accelerate and enhance mobile penetration testing. Every pentest is easily customizable and provided with a zero false positives SLA. Unlimited patch verifications and 24/7 access to our security analysts are included into every project.

ImmuniWeb® Continuous

ImmuniWeb® Continuous monitors your web applications and APIs for new code or modifications. Every change is rapidly tested, verified and dispatched to your team with a zero false positives SLA. Unlimited 24/7 access to our security analysts for customizable and threat-aware pentesting is included into every project.

One Platform. All Needs.
www.immuniweb.com

Email: sales@immuniweb.com
Phone:+41 22 560 6800

SCawards EUROPE Winner — Best Usage of Machine Learning and AI

AIFINTECH 100

Gartner peer insights
4.8 out of 5

HORNETSECURITY

ALL-INCLUSIVE SECURITY FOR MICROSOFT 365

- SPAM FILTER & ADVANCED EMAIL SECURITY
- SIGNATURE & DISCLAIMER

TOTAL PROTECTION
ENTERPRISE BACKUP

- EMAIL ARCHIVING, ENCRYPTION & CONTINUITY
- BACKUP & RECOVERY

FROM EMAIL SECURITY TO BACKUP & RECOVERY

ALL IN ONE SOLUTION!

START YOUR FREE 30-DAY-TRIAL

WWW.HORNETSECURITY.COM

Gain control of your Attack Surface with a Cybersecurity Co-pilot

Headless
We embed directly to your platform, any SIEM, or ticketing Solution.

Agentless
Easy to onboard all known and unknown client assets.

Auto-Remediate
Triggers to protect unknown assets for management.

Get started with a demo at lucidum.io/request-demo

LUCIDUM
ATTACK SURFACE MANAGEMENT

CYBLE

Is Your Organization Protected Against External Threats?

GENERATE YOUR ORGANIZATION'S EXTERNAL THREAT PROFILE REPORT AND OBTAIN

01 Overview of vulnerabilities in your digital risk footprint

02 Risk assessment of your attack surface and threat landscape

03 Unique Risk Score as per your darkweb exposure

04 Critical information about your leaked data and security posture

SCAN ME

TO GET THE REPORT!

Phylum

The Software Supply Chain Security Company

Stop Software Supply Chain Risk at the Source

Automate software supply chain security to block new risks, prioritize existing issues and only use open-source code that you trust.

Protect the Organization

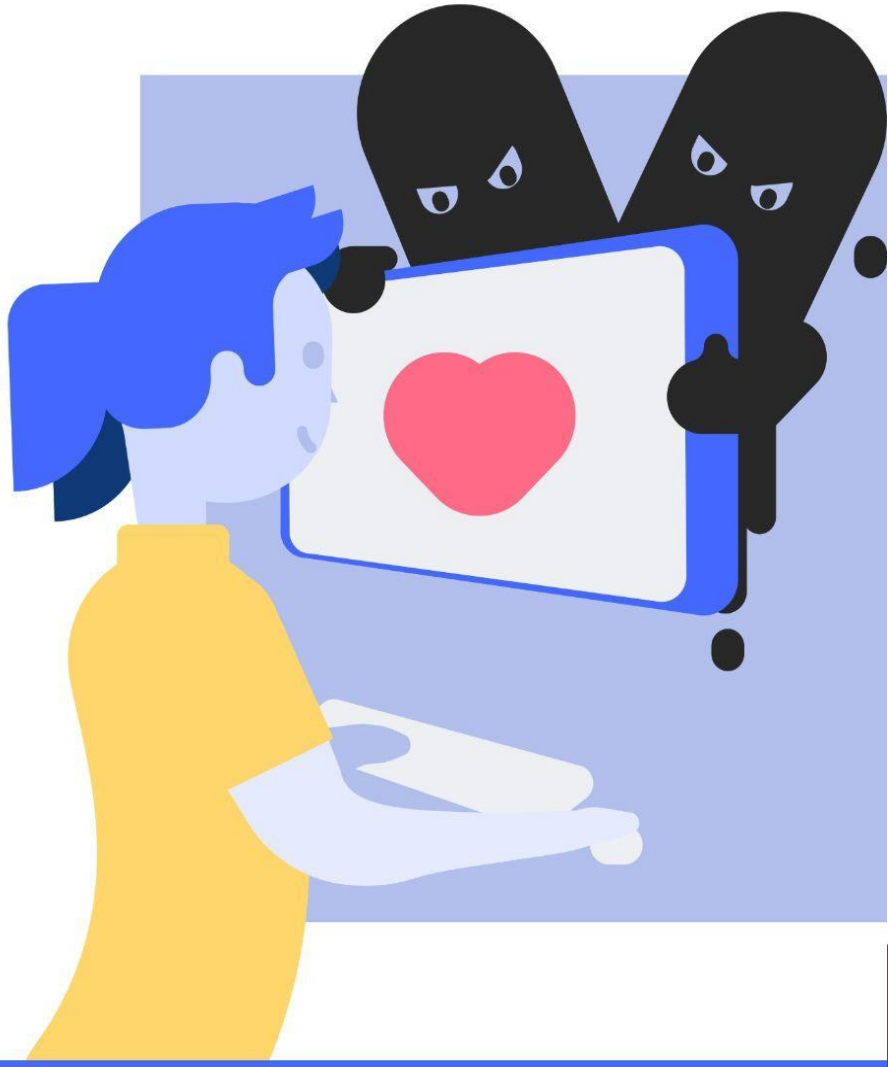
- Proactive OSS Risk Management
- Policy Standardization & Enforcement
- Improved Signal : Noise
- Modern Attack Prevention

Secure Innovation

- Developer-First Approach to Security
- Reduced Organizational Friction
- Accelerated Release Cycles
- Uninterrupted Developer Workflows

YOUR WEBSITE LOOKS GREAT!

BUT WHAT'S HAPPENING BEHIND THE SCENES?



reflectiz

Reflectiz maps all 1st, 3rd and 4th party risks, including compliance violations, web skimming attempts, and external domain threats.

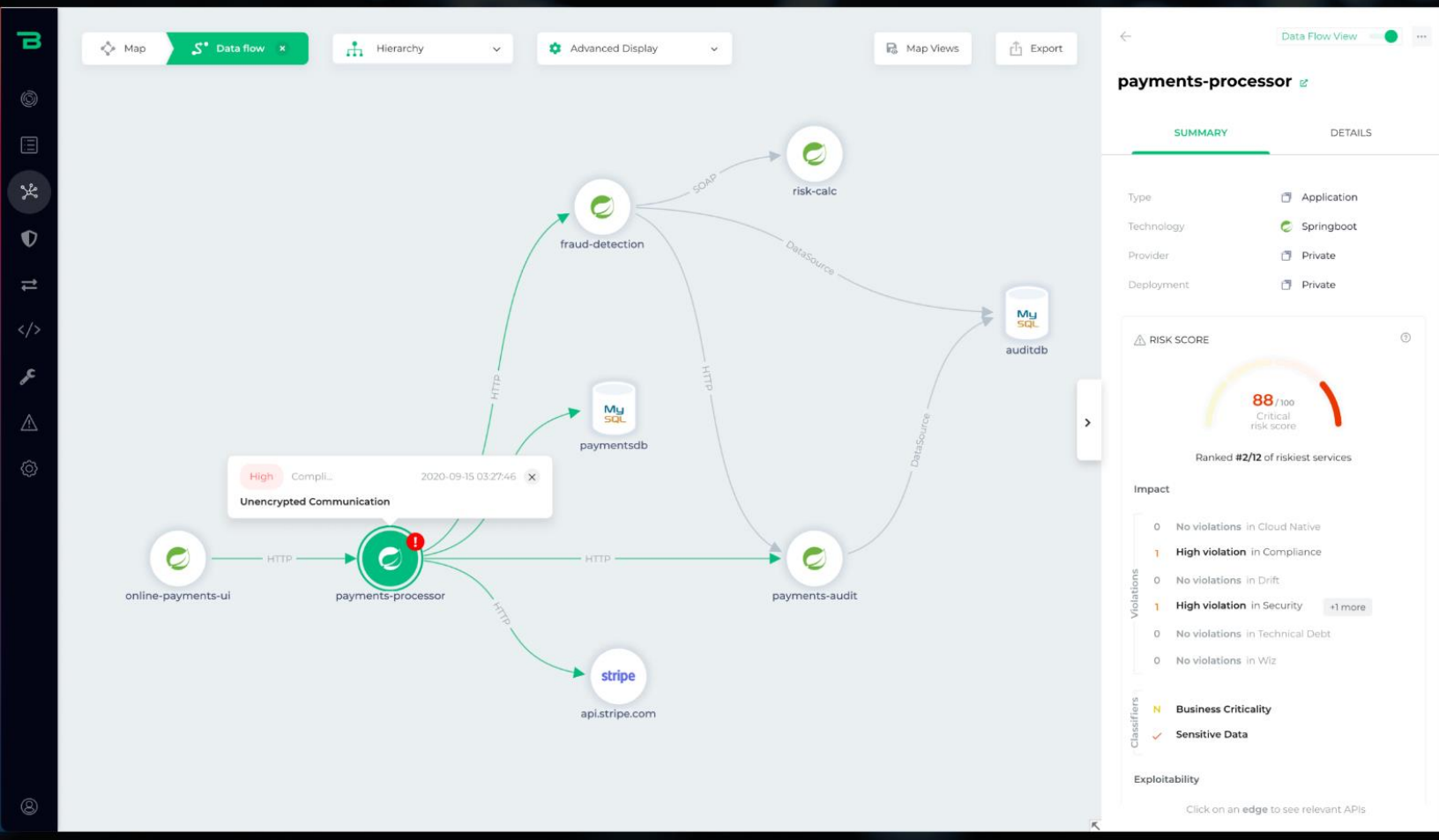
Get in touch for a quick PCI assessment.
www.reflectiz.com

BIONIC

ASPM

Application Security Posture Management

Make applications secure and resilient to significantly reduce business risk.



Start reducing business risk of apps today

www.bionic.ai

Phosphorus

Secure the Enterprise xIoT Attack Surface

FIND, FIX, and MONITOR every IoT, OT, and Network device.

See how Phosphorus can bring enterprise xIoT security to every cyber-physical Thing in your enterprise

xIoT Attack Surface Management + **xIoT Hardening & Remediation** + **xIoT Detection & Response**

Across all xIoT devices

- Enterprise IoT Devices
- Operational Technology Devices
- Smart Buildings & Cities
- Network & Cloud Connected Devices
- Industrial Internet of Things
- Internet of Healthcare Things
- Smart Ships
- Internet of Battlefield Things

Automated bot protection with 24/7 adult supervision.

From the **Top Infosec Innovator Award** winner.

TOP INFOSEC INNOVATOR
CYBER DEFENSE MAGAZINE
2022

DATADOME

datadome.co

Ditch the SEG.

Get twice the protection for half the cost.

Give your modern workforce the advantage against multi-channel threats with **SlashNext Integrated Cloud Communication Security Platform**. Stop sophisticate, fast moving phishing and malware threats in Microsoft 365, Zoom, SMS, LinkedIn, WhatsApp and other messaging channels.

www.slashnext.com

SLASHNEXT

Protect Email, Mobile, Web, and Brand

plainID
THE AUTHORIZATION COMPANY

Power of the Policy

Move to an Identity-First Security paradigm.

Download the eBook

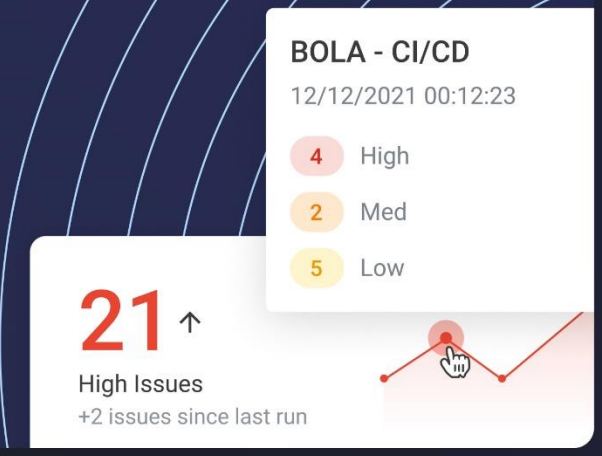
noname

The Complete, Proactive API Security Platform

nonamesecurity.com >

Shift Left with **API Security Testing**

Industry-leading posture managment, runtime security and API security testing




ARTICLES

Largest Data Breaches Of 2022 - Protect Data With Deep Packet Inspection

By Randy Reiter CEO of Don't Be Breached

There were many massive Data Breaches in 2022. Don't be a member of this group in 2023. Data breaches are occurring now on almost a daily basis. They result in confidential data such as credit card numbers, email addresses, passwords, social security numbers and other private personnel or organization data being exposed.

Since this data is always maintained in centralized databases these databases are high profile targets for Hackers and Rogue Insiders. Experian has reported that 31% of data breach victims have their identity later stolen.

Largest Data Breaches in 2022

- **November 7**, 2022. Medibank the largest health insurance provider in Australia was publicly threatened by an unidentified Hacker. The Hacker claimed to have stolen the data on 9.7 million customers. Medibank confirmed that 500,000 health claims had been stolen in the data breach.
- **September 19**, 2022. Kiwi Farms forum was hacked. Emails, IP addresses and passwords were stolen. The Hacker obtained the administrator credentials to the website via session hijacking.

- **September 16**, 2022. American Airlines disclosed a data breach that had occurred in July of 2022. Approximately 1,700 employees and customers data was exposed in the breach as a result of a phishing attack.
- **September 15**, 2022. Uber's private Slack channel was breached by the Lapsus$ group that has successfully compromised companies such as Microsoft, Nvidia and Samsung. The Hackers gained full access to Uber's internal databases and source code. They were able to successfully get pass Uber's multi-factor authentication.
- **September 12**, 2022. U-Haul informed customers of a data breach that included customer names and drivers licenses. The Hackers gained access to rental contracts from November 2021 to April 2022.
- **July 19, 2022**. Hacker posted data for sale on 69 million Neopets users. Stolen data included date of birth, email address, name, zip code and much more. Other Hackers in the past have also accessed Neopets databases.
- **June, 2022**. Flagstar Bank in Michigan was breached. The social security numbers of 1.5 million customers were stolen. The attack occurred in December 2021 and was discovered in June 2022.
- **April, 2022**. Block (formerly Square) disclosed their Cash App was breached by a former employee. Brokerage numbers, customer names, portfolio value, stock trading info and other data was stolen.
- **March, 2022**. Okta an authentication company was breached. Approximately 2.5% of their customers data was exposed. Hackers gained access via a 3rd-party customer support provider.
- **February, 2022**. GiveSendGo a Christain fundraising website was hacked. The personal details on 90,000 people were posted by the hackers.

Conventional approaches to cyber security may NOT prevent Data Exfiltration and Data Breaches. In 2020 the DHS, Department of State, U.S. Marine Corps and the Missile Defense Agency recognized this and all issued requests for proposals (RFP) for network full packet data capture for Deep Packet Inspection analysis of network traffic. This is an important step forward protecting confidential database data and organization information.

Zero-day vulnerabilities that allow hackers to gain system privileges are a major threat to all organizations encrypted and unencrypted confidential data. Confidential data includes: credit card, tax ID, medical, social media, corporate, manufacturing, trade secrets, law enforcement, defense, homeland security, power grid and public utility data. This confidential data is almost always stored in DB2, Informix, MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL and SAP Sybase databases.

How to Stop Data Exfiltration and Data Breaches with Deep Packet Inspection

Protecting encrypted and unencrypted confidential database data is much more than securing databases, operating systems, applications and the network perimeter against Hackers, Rogue Insiders, Government-backed Hacking Teams and Supply Chain Attacks.

Non-intrusive network sniffing technology can perform a real-time Deep Packet Inspection of 100% of the database activity from a network tap or proxy server with no impact on the database servers. The database SQL activity is very predictable. Database servers servicing 1,000 to 10,000 end-users typically

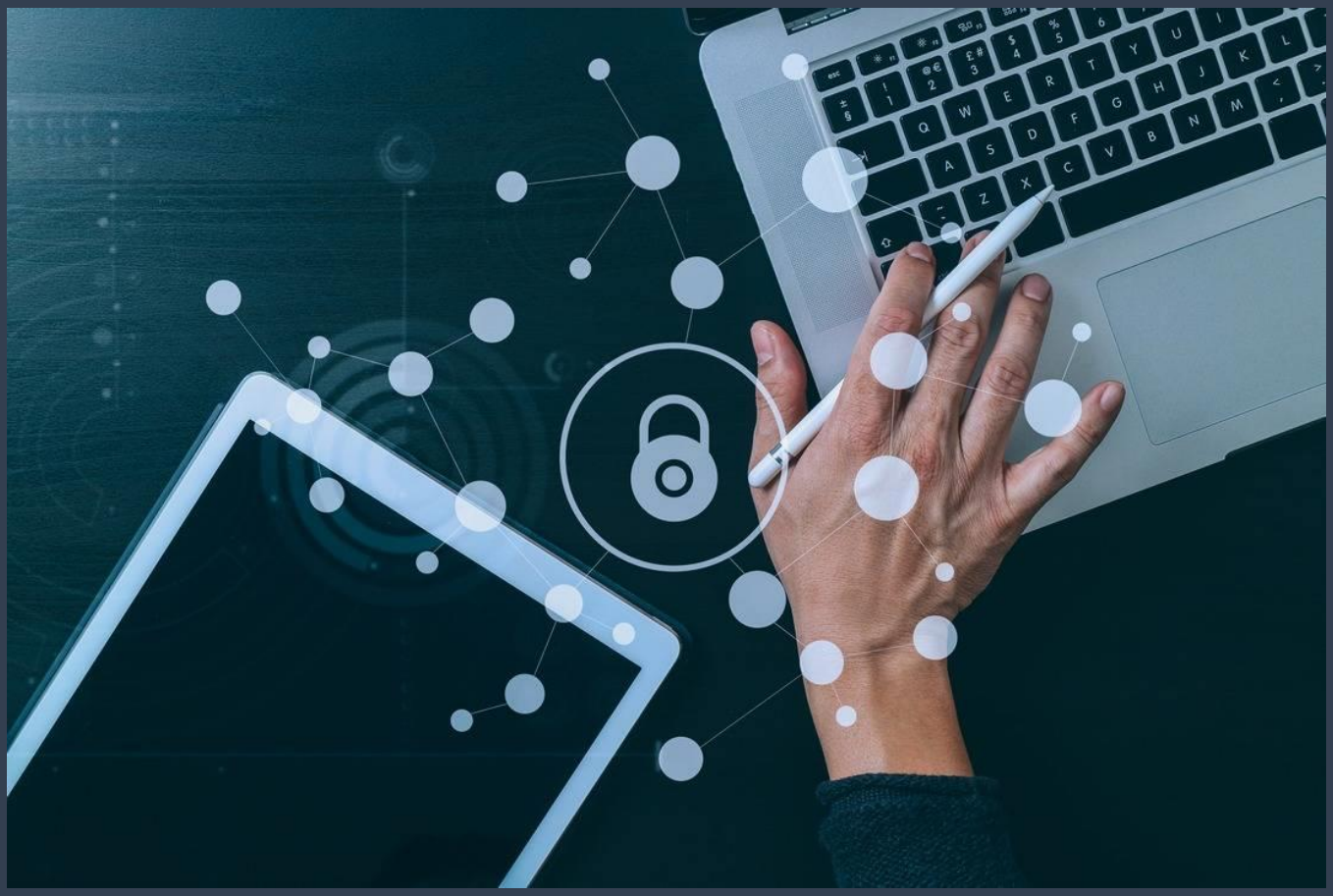
process daily 2,000 to 10,000 unique queries or SQL commands that run millions of times a day. Deep Packet Analysis does not require logging into the monitored networks, servers or databases. This approach can provide CISOs with what they can rarely achieve. Total visibility into the database activity 24x7 and 100% protection of confidential database data.

Advanced SQL Behavioral Analysis from Deep Packet Inspection Prevents Data Breaches

Advanced SQL Behavioral Analysis of 100% of the real-time database SQL packets can learn what the normal database activity is. Now the database query and SQL activity can be non-intrusively monitored in real-time with Deep Packet Inspection and non-normal SQL activity immediately pinpointed. This approach is inexpensive to setup and has a low cost of operation. Now non-normal database activity from Hackers, Rogue Insiders and Supply Chain Attacks can be detected in a few milli seconds. The Security Team can be immediately notified and the Hacker session terminated so that confidential database data is not stolen, ransomed or sold on the Dark Web.

About the Author

Randy Reiter is the CEO of Don't Be Breached a Sql Power Tools company. He is the architect of the Database Cyber Security Guard product, a database Data Breach prevention product for DB2, Informix, MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL, and SAP Sybase databases. He has a Master's Degree in Computer Science and has worked extensively over the past 25 years with real-time network sniffing and database security. Randy can be reached online at rreiter@DontBeBreached.com, www.DontBeBreached.com and www.SqlPower.com/Cyber-Attacks.



Data, Privacy, And the Future of Artificial Intelligence

By Michael G. McLaughlin, Associate, Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Data privacy and protection have become both central and increasingly restrictive for businesses in the United States and Europe. At the same time, innovators at the cutting edge of Artificial Intelligence (AI) research are continuously seeking more and better datasets to develop breakthrough technologies to solve the most challenging problems facing humanity. However, with the expanding data privacy regulatory landscape, Western technology companies more and more find themselves at a disadvantage to their Chinese counterparts, whose authoritarian goals and ethics stand in stark contrast with those of the democratic states.

Nearly every person on Earth has a unique digital fingerprint. This fingerprint identifies us through innumerable datapoints and becomes more detailed through each interaction we have with the inescapable technology that surrounds us. From the mobile devices and smart-watches we carry and wear, to the social media profiles and accounts we log into for work and leisure, to the cars we drive and the things we buy—the amount of digital exhaust we create every day is staggering.

Each minute, Internet users spend $443,000 on Amazon, post 347,000 Tweets, share 1.7 million pieces of content on Facebook, and upload over 500 hours of video to YouTube, according to Domo. Each of those millions of transactions is comprised of multiple datapoints—IP addresses, credit card information, geographic location, language and grammar, gender, skin tone, biometrics—the list goes on. By 2025, the total amount of data that will be created, copied, or consumed will reach 181 zettabytes. For reference, the typed letter "a" is one byte. One zettabyte is roughly the equivalent of a typed letter "a" for every grain of sand on all the beaches on earth. The Library of Congress contains 16 petabytes of information. There are 1 million petabytes in a zettabyte.

Every action we take online enlarges the boundless diaspora of data uniquely attributable to each of us. And while data privacy and protection have become the subject of much legal scrutiny recently, few people understand just how important their data really is. It has become tiresome to hear the trite phrase: "*if you are not paying for a product, you are the product*." With the technological advancements in AI looming large on the horizon, perhaps it is more accurate to say, "your *data* is the product."

Free social media platforms, such as Facebook, Twitter, and TikTok all use their mobile applications to harvest geolocational data, photos and videos, contacts, device and browser type, likes, tweets, posts, even how long users pause on particular posts or advertisements as they scroll through their feeds. TikTok also collects biometrics and anything copied to a device's clipboard—including usernames and passwords from other applications. And Google scans the content of every email a Gmail user sends and receives.

The portrait tech companies are able to paint about individual users is astounding. In a 2014 study, researchers from Stanford University and the University of Cambridge found that Facebook needs 10 likes to know a user better than their co-worker, 70 likes to surpass a friend, and 300 likes to know someone more personally than their spouse. Given Moore's law, stating that computing power doubles every two years, social media platforms very likely know their users far more intimately today with far fewer engagements.

Regulators and privacy advocates are staunchly opposed to the unchecked and nonconsensual collection of personal information, whether indirectly through third-party cookies or directly by social media platforms, online retailers, or other service providers. Many regulatory bodies and legislatures have established legal frameworks to try and curb the collection and monetization of personal information due to privacy concerns. Europe's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and Virginia's Consumer Data Protection Act (VCDPA) are all examples of legislation that limit data collection and sales. The regulatory logic is that for individuals to unknowingly cede their digital fingerprint to major technology companies who aggregate data from every conceivable online activity constitutes unreasonable and intrusive surveillance that poses a risk in individual privacy.

However, while the collection of significant amounts of personal data does pose privacy concerns, over-regulation of data collection and sharing could have significant adverse effects on America's future economic and national security. Though huge swaths of data collected and aggregated by tech giants are used for targeted advertising and enhancing user experience, they are also being used to develop the data-driven technologies that will determine the future of America's standing on the world stage—namely, Artificial Intelligence.

To realize the benefits of AI—that is, simulated human inferences and decision-making processes—developers require large quantities of high-quality data to *train* the AI. Training data is used by machine learning algorithms to "self-teach" AI to perform specific tasks. For instance, whenever Gmail requires its users to authenticate their accounts by selecting pictures of a stoplight or when Google Maps directs a

driver to take a “short cut” down a side street, Google is creating a dataset of training data to enable the development of autonomous vehicles.

The development of AI is patently different from the development of any other modern technology. Where most modern technologies rely on basic if/then decision trees, AI creates a neural network of innumerable datapoints to mathematically calculate the best solution to any problem. For this neural network to function, the AI must be “taught” to make connections across a vast universe of data. And unlike many technologies, the success of a particular AI will be determined by the quality and quantity of data it can access.

You are already seeing AI at play when you turn on Amazon Prime and have custom video content queued up based upon the genre of your recent book purchases, or the political videos appearing in your Facebook feed after you view the election results on MSNBC. Soon, this type of data-driven personalized experience could apply to every part of your life.

Take healthcare, for instance—

With access to quality data, in the not-too-distant future, health monitoring AI would be able to identify and diagnose the onset of illness and disease in ways modern medicine is simply not capable of. Smartwatches and mobile devices will be able to work in concert to identify imperceptible symptoms such as irregular breathing, sleep patterns, heartrate, and a change of gait. These symptoms would be flagged as anomalous against a health data baseline created from years of 24/7 monitoring from your devices. It would also be checked against the baselines of millions of other people of a similar age and demographic worldwide. The AI at the backend of this platform would incorporate datapoints from your genetic code, as well as your medical history and the medical histories of your immediate and extended family. Using location data from a mesh network of mobile devices, the AI could also determine who in your recent proximity might have exhibited similar symptoms. Based on near-instantaneous analysis of your personal data as well as a thorough understanding of the entire compendium of medical studies and research, the AI could diagnose ailments at the earliest possible moment and request that your doctor approve a recommended prescription available for immediate delivery to your location.

You wouldn’t necessarily know why the AI is making the decisions it is making, but it would create a decision web from millions of datapoints to achieve the best outcome for your wellbeing. Expanding this web to the Internet-of-Things, your home and office thermostats could lower the ambient temperature to account for the coming fever; your office calendar could automatically reschedule the next morning’s meetings; and your refrigerator could order Pedialyte, Tylenol, and chicken soup. Before you know you’re sick, you could already be on the path to recovery.

A future like this is predicated on technology developers being able to access immense quantities of both high-quality training data for AI development and the sharing of data collected by multiple sources to create the necessary digital neural networks. However, in the United States and other Western democracies, much of the data required to achieve the level of personal automation in the above scenario is currently neither centralized nor shared freely across organizations, who prize this data for its commercial value. Moreover, some of the data is also governed by regulations—such as the Health Insurance Portability and Accountability Act (HIPAA), CCPA, and GDPR—which prohibit or significantly limit the type of collection and disclosure that would allow for the development of such AI.

Presently, the United States and China are locked in a race as the world’s two competing AI superpowers. The United States is ahead, but the lead is narrowing. Americans value privacy and enjoy the protections they are afforded by the Fourth Amendment and other regulations, but the importance of privacy should be weighed against future economic and national security interests. Where American AI developers are

increasingly brushing against various sectoral data privacy regulations, Chinese developers face no such restrictions. Beyond having access to the world's largest population of 1.4 billion people, China's leading AI developers also benefit from legal and regulatory frameworks designed to advance Beijing's technological ambitions. These frameworks collectively require all data collected about Chinese citizens be stored within the geographic borders of China and compels the sharing of that data with the Chinese government.

The applicable data is not limited to Chinese citizens. Whenever TikTok users worldwide upload their videos, ByteDance—TikTok's parent company—adds to its dataset material for training its facial recognition, voice recognition, and deep-fake technologies. Whenever cities in Africa or Asia install HikVision cameras or Huawei servers as part of China's "Safe City" products, the foreign data collected add diverse inputs to China's AI training datasets. Whenever women from around the globe provide blood samples to China's BGI Group for neonatal testing, the company harvests genetic sequences of millions of women and children worldwide.

While the U.S. and other techno-democracies seek to use AI to advance societal interests, China is plumbing the depths of the dark side of AI.

According to *The Washington Post*, Chinese security services are currently using the fruits of its data collection to develop and deploy AI to identify, detain, and persecute its Uyghur Muslim population. So-called "predictive policing," China's Ministry of Public Security leverages access to data about individual Uyghur's hobbies, occupations, familial ties, travel history, social media activities, and other traits to predict acts of terrorism. Utilizing data collected from worldwide sources, Chinese technology companies have developed facial recognition, gait recognition, and behavioral identifiers that are incorporated into its nationwide surveillance system to identify Uyghurs assessed to pose a threat. As though taken from the script of *Minority Report*, Chinese law enforcement use AI to identify and arrest Uyghurs their algorithms predict will commit acts contrary to state interests. These individuals are then rounded up and summarily sent to "re-education" camps.

The two uses of AI detailed in this article are intended to illustrate the crossroads the world faces. Authoritarian systems of government readily lend themselves to mass surveillance, collection, and data aggregation. Democratic systems, by contrast, place a premium on privacy and are generally resistant to most forms of government surveillance. In the age of AI, where access to data will determine both economic success and national security, this distinction places democracies at a disadvantage. As regulators, lawmakers, and tech giants in democratic nations seek to develop the foundations for ethical uses of AI, lawmakers and regulators need to establish a regulatory environment that gives western AI developers access to sufficient data to compete with their Chinese counterparts.

For techno-democracies to thrive in the age of Artificial Intelligence, lawmakers and regulators should seek to balance individual privacy with the society's need to develop advanced technologies. Further, regulations need to be established that enable companies that collect large and diverse datasets—from personal information to genetic data—to share that data with AI developers in such a way that protects privacy while encouraging innovation. Otherwise, the United States will cede AI superiority to China.

About the Author

Michael McLaughlin is a cybersecurity and data privacy attorney with Baker Donelson in Washington, D.C., and the former Senior Counterintelligence Advisor for United States Cyber Command. His forthcoming book, Battlefield Cyber: How China and Russia Are Undermining our Democracy and National Security, is available for pre-order on Amazon. He can be reached at mgmclaughlin@bakerdonelson.com and via the Baker Donelson website at https://www.bakerdonelson.com/.

The Great Resignation, The Quiet Resignation - Five Security Awareness Countermeasures to Security Threats Derived from these Workforce Trends

By Omer Taran, CTO & Co-Founder, CybeReady

According to Fortune Magazine, 40% of U.S. employees are considering an exit from their current place of business. This trend, which has been termed "The Great Resignation," creates instability within organizations. High employee turnover increases security risks, making companies more vulnerable to attacks as human infrastructure becomes fragmented, leaving gaps that very often expose an organization. This problem is compounded by the "Quiet Resignation" or quiet quitting - a trend of employees who feel overworked because of additional responsibilities placed on their shoulders, due in large to today's employee shortage. This trend has employees choosing to not go above and beyond in their jobs, such as not checking email in off-hours, passing on assignments outside of their normal duties, and limiting their compliance with security rules and practices.

Because of this employee exodus, the influx of untrained employees, and general malaise, the deployment of a successful security awareness program can be more challenging than ever for security

teams. With new employees entering the organization at every level, the extent of cultural dissonance increases, creating instability. Security professionals need to act quickly in response to security concerns caused by this instability to protect their organizations during these volatile times.

Issues that commonly arise as employees transition out and enter the organization include the following:

- **Potential data leaks** - When employees leave, there's a high risk of sensitive data leaks. Poor off-boarding processes and lurking emails may lead to data loss.
- **Need for educational leveling** - When new employees join the organization, even if security training is well conducted, they are usually not on par with their peers. Unknown security habits may put the organization at risk, requiring the need for supplemental training.
- **Security oversight by employees** - With fewer staff, employees are overburdened and pressured. Security may be "forgotten" or neglected in the process.
- **Lack of support for remote work** –To support rapid employee recruitment, working at home is a must. Remote work flexibility helps to attract and retain new employees.
- **Training mobility** – Remote work requires securing remote devices and dealing with new employee behavior for inherent distractions - on the go and at home.

With these challenges confronting organizations, security teams should consider deploying the following strategies:

1. **Continuous Training** – All employees are needed to protect against sophisticated phishing threats and this has become even more complicated in light of The Great Resignation. Because of the fractured and less-trained employee base, companies are at much greater risk. To mitigate that risk, training needs to be frequent - at least once a month and short – to not add additional burden to already burned-out employees. The training must also be positive so employees are motivated to get actively involved in the cybersecurity effort.

2. **Prioritize New Employees** - Security depends on employee help and cooperation. Therefore, it is important to establish best practices in the workplace. New employees with unknown cybersecurity habits pose a high risk for the organization and need to level up their awareness fast. Start with low difficulty, create a foundation, then continually promote learning to the next level.

3. **Implement data-driven Training** - For a cyber awareness training program to be successful, security teams must plan, operate, evaluate and adapt the training continuously. With data-driven platforms, security teams can monitor campaign performance to fine-tune employee defenses and build custom high-intensity training campaigns for high-risk groups, while also adapting the training per employee locale - to optimize learning results.

4. **Maintain Vigilance** - Security itself is a full-time job. Keeping the training unpredictable to maintain employee vigilance is an essential part of the process, such as surprising simulation campaigns in a continuous cycle with the idea of catching employees off-guard – which deliver

the best learning experience. To create high engagement, ensure training content is relevant to daily actions. Use short, frequent, and intriguing content in the employees' own language. Tailor the training content to local references and current news.

5. **Promote long-term results** - Take advantage of the 'golden moment' of failure to generate a meaningful learning experience. Instead of random enforcement training which can often be irrelevant to employees, make a lasting impression right when mistakes happen. Ensuring that training uses this limited window of time is also known as 'just-in-time learning and is the key to the most effective results and behavior change.

Comprehensive integration of the latest security know-how into everyday work is a must to counter the new risks of The Great Resignation and related workforce trends, making it more important than ever for every employee to get up to speed for high cyber resilience quickly. Until the current state of affairs shifts in a direction more favorable to a stable and secure environment, IT professionals must be proactive in their security awareness training approach.

About the Author

Omer Taran is the Co-Founder and CTO of CybeReady. As Co-Founder, Omer serves as the company's technologist-in-residence. His vision for CybeReady drives him to build out a product roadmap that serves a variety of enterprise customers by blending best practices in learning with tech innovation. He's known for bringing ideas to life quickly and precisely.

5 Ways to Protect Your Workplace from Cybersecurity Threats

By Nicole Allen, Senior Marketing Executive, Salt Communications.

The cybersecurity environment is rapidly evolving. Meanwhile, technological advancements are steadily improving the ability for cyber criminals and hackers to exploit data security flaws. The ever-increasing scope of data breaches and cybersecurity threats should be a major source of concern for all types of organisations.

No one could have predicted the holes in network security postures that the 2020 coronavirus pandemic has revealed with the increase of employees working from home. Unsecured home networks, BYOD (bring-your-own-device) policies, and compartmentalised operations turned previously evident hazards on corporate networks into invisible, hidden threats on a wider range of networks. As a result of the increasing attack surface even more than usual phishing, vishing, and ransomware assaults were launched. So in this article Salt Communications are going to explain five ways to protect your workplace from cybersecurity threats.

1. Increase enterprise security protection

Mobile workplaces can boost productivity and access to work-related resources, but they also raise the danger of data leaks due to apps and services like email, social media, and cloud access. Maintaining a more secure organisation while enabling mobile productivity requires creating a safer environment for employees to work remotely.

The risks to organisations from actions or inactions of employees come from a wide range of factors: such as human error – this can include sending sensitive information or personal data to the wrong person by accident. There's also the issue of system misconfiguration, which can lead to unauthorised

access if sensitive data isn't adequately secured, encrypted, or password protected. It's also crucial to consider the loss of sensitive information-containing devices or documents.

Many businesses do not take data security as seriously as it should be. They have weak passwords, important files that aren't encrypted, and servers that aren't configured correctly. More than 4 billion data records containing sensitive information were allegedly compromised in the first six months of the year in 2021 as a result of this negligent attitude.

2. Enable secured collaboration for business communications

Since the recent crisis-forced transition to remote work, there has been an increase in the use and reliance on communication tools. Employees across organisations are looking for an effective, secure approach to continue collaborating throughout the business now that they are dispersed in various remote locations. Migration to business communication platforms as a replacement for in-person and other technical communication has become a major goal for a business's digital transformation.

Companies become more vulnerable to major security concerns when more communication – and business-critical information – is shared across cloud platforms likeZoom and Teams. As we saw with COVID-19, there has been an increase in hacks, including targeted Teams attacks using impersonating Teams notifications and GIFs vulnerabilities.

With the likes of Teams in terms of external vulnerabilities, federated access to external users is enabled by default when Teams is implemented out of the box. This means that anyone in the world can send an email to a user, request to chat with them, or exchange files with them, exposing the individual, and hence their entire organisation, to messages that are frequently hostile in nature.

Whereas, if an organisation uses a closed communications platform such as Salt they don't leave themselves open to these types of threats. Salt Communications recognises that encryption alone isn't enough to keep an organisation's data safe. Salt delivers a highly secure platform that gives the same convenient user experience as consumer apps, but in a safer and more secure manner, allowing the business to maintain complete, centralised management of the system at all times and therefore ensure complete control.

3. Ensure you are reducing malware exposure

Malware infections are frequently linked to user mistakes. Phishing and spoofing schemes have advanced to the point where they can trick users into downloading innocuous-looking apps that contain hidden attacks by sending them fake emails from trusted brands. These emails lure users in with fake news stories, or very personalised offers, which leaves themselves and their companies open to attack. As well as this in the past year there has been an increase in 'smishing' attacks which are threatening

businesses worldwide. Smishing is a form of 'phishing' using SMS or text messages instead of emails to entice recipients to click on fake links which downloads malware onto their device.

On their own devices, users cannot be prevented from surfing the web, utilising social media, or accessing personal email. How can you assist them in performing these routine duties in a safer manner? Request that all staff read basic instructions and/or participate in training that covers common malware attack strategies.

Employers should also teach users to double-check URLs in emails to ensure they are accurate, relevant, and trustworthy. Also, think about deploying email security solutions that can help prevent malware and phishing attacks from reaching employees' inboxes. It makes no difference if you have the world's most secure security system. It only takes one inexperienced employee to be deceived by a phishing attempt and hand up the information you've worked so hard to safeguard. Make sure you and your staff are both aware of these specific email phishing examples, as well as all of the warning indicators of a phishing attempt.

4. Back everything up regularly

What if your organisation already has a backup system in place? First and foremost, kudos on a job well done; but, the task does not end there. It's critical to test your backup recovery process on a frequent basis. It's pointless to back up data if you can't recover it. You'll know if your backup procedure is working properly if you run that test on a frequent basis. It's not uncommon for a backup drive to run out of disc space for no one to notice.

Performing a proper backup can be a challenging task. Therefore, backups should be included in your business continuity plan. A business continuity plan, according to Travelers Insurance, is "*a proactive plan to avoid and manage risks associated with a disruption of operations.*"

It outlines the measures that must be performed before, during, and after an event in order for an organisation's financial viability to be maintained. That implies that if your business systems are affected, whether by a fire or flood in the office or, more recently, a cyber attack, you'll have a plan in place to minimise the impact on business performance. Backing up your company's data could mean the difference between surviving a cyber attack and going out of business.

5. Manage all organisational devices

Security concerns are growing as the Bring Your Own Device (BYOD) trend rises and the use of Software-as-a-Service (SaaS) applications spreads. Organisations can begin with user education on devices is a simple but crucial step in securing them. It guarantees that every employee in your company is informed of the best procedures for safeguarding your data. While it starts with onboarding, teaching your staff how to safeguard their devices is a continuous activity.

Mobile security should be at the top of any company's cybersecurity priority list, especially in an era where remote working has become the standard and isn't going away anytime soon. Many of the companies and organisations in which Salt Communications works have experienced a surge in mobile usage for communications and day-to-day tasks. Often, businesses will consider creating a mobile security policy that outlines what users should and should not do while using their mobile devices. Other businesses have implemented MDM/UEM systems to lock down devices and add an extra layer of security to company-issued devices that employees use.

Allowing employees to be flexible does not have to mean jeopardising the security of your cybersecurity, mobile security and corporate communications. You can provide your employees the freedom to work anywhere, anytime with adequate planning, the correct tools, and education while avoiding risk. Our team of professionals have worked with a variety of organisations to assist them in dealing with cybersecurity issues.

To discuss this article in greater detail with the team, or to sign up for a free trial of Salt Communications contact us on info@saltcommunications.com or visit our website at saltcommunications.com.

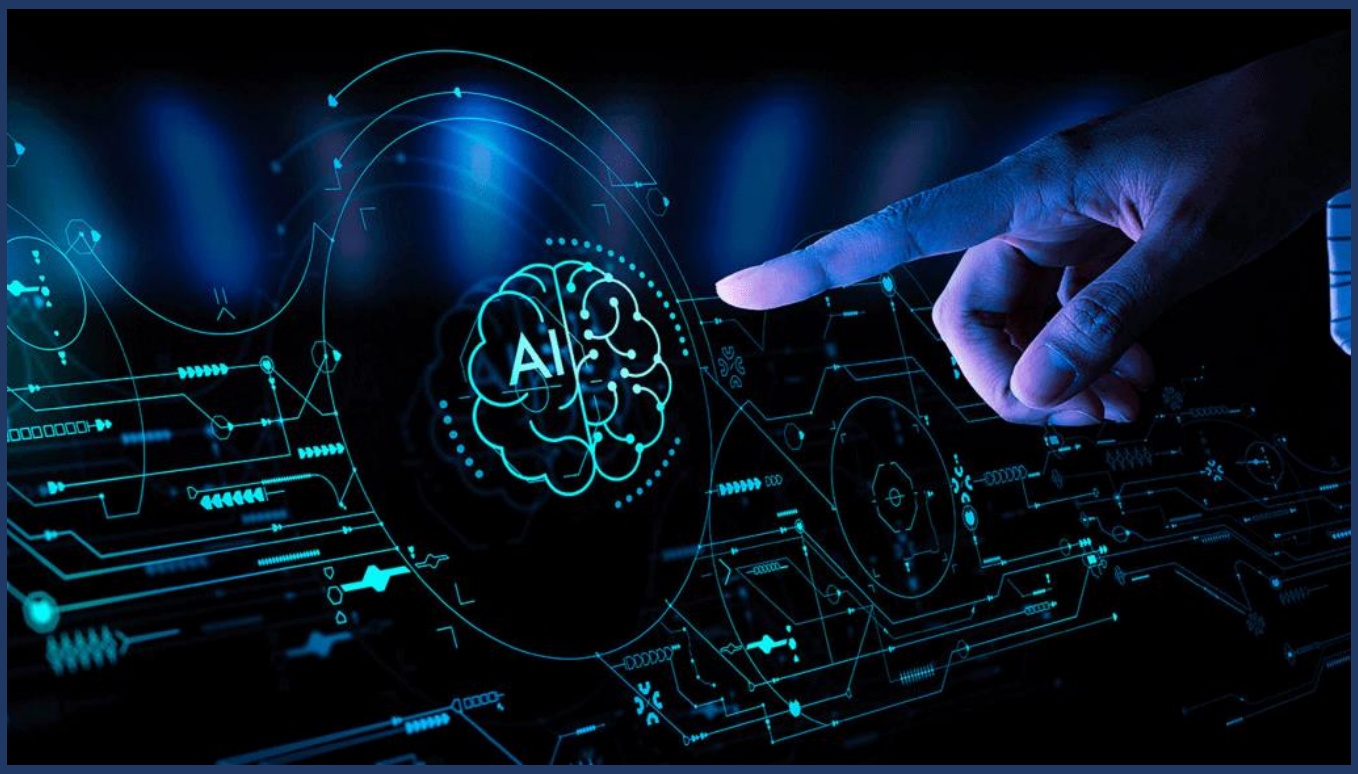
About Salt Communications

Salt Communications is a multi-award winning cyber security company providing a fully enterprise-managed software solution giving absolute privacy in mobile communications. It is easy to deploy and uses multi-layered encryption techniques to meet the highest of security standards. Salt Communications offers 'Peace of Mind' for Organisations who value their privacy, by giving them complete control and secure communications, to protect their trusted relationships and stay safe. Salt is headquartered in Belfast, N. Ireland, for more information visit Salt Communications. .

About the Author

Nicole Allen, Senior Marketing Executive at Salt Communications. Nicole has been working within the Salt Communications Marketing team for several years and has played a crucial role in building Salt Communications reputation. Nicole implements many of Salt Communications digital efforts as well as managing Salt Communications presence at events, both virtual and in person events for the company.

Nicole can be reached online at (LINKEDIN, TWITTER or by emailing nicole.allen@saltcommunications.com) and at our company website https://saltcommunications.com/



AI Is the Answer To Modern Cybersecurity Threats

Why embracing AI solutions is key to combatting evolving cyber threats across many sectors.

By Ralph Chammah, CEO, OwlGaze

With cyber threats becoming increasingly diverse in how they strategically cripple organisations, the cybersecurity landscape is under increasing pressure to bolster its technology and defence methods. Cyber-attacks have only become more frequent year-on-year, with the costs to an unprepared business only increasing with them. Data breaches can harm not only your organisation's wallet but also your reputation. It is therefore imperative that businesses branch out when it comes to data protection, and AI could indeed be the answer cyber operatives need to detect and prevent threats before they can do any damage.

No industry is safe

Cyber-attacks are not limited to one sector. As we have witnessed throughout this year, no industry is safe. In the healthcare industry alone, doctors continue to struggle to cope with the fallout of a major ransomware attack on NHS software supplier, Advanced, which took place in early August. Cyber actors target hospitals and healthcare providers increasingly to access sensitive patient data, leading to critical consequences for patients, the NHS and other national health systems globally. Ransomware attacks can be particularly deadly – France suffered an attack on the Centre Hospitalier Sud Francilien (CHSF)

late last month which totalled over £90 million in damages. Cyber actors have no remorse; therefore, it is crucial that organisations keep their cybersecurity up to date, especially when lives could potentially be on the line.

Similarly for telcos, the UK government has begun cracking down on employing cybersecurity rules across all mobile and broadband providers. In an effort to protect Britain's broadband and mobile networks from potential threats, CSPs need to be more vigilant in their cybersecurity, or else risk fines of up to £100,000 per day should they fail to comply. With governments realising the importance of investing in modern technology for data protection, businesses across all sectors can benefit from updating their systems, or else risking a healthy pay-out.

It is predicted that, by 2025, cyber-crimes could cost over £9 trillion annually across the world. This estimation is based on growing figures, including factors such as the damage and destruction of data, theft of intellectual and financial property, and also post-attack disruption of business and reputational harm. In the UK alone, Ramsac reported that costs could reach £27 billion annually across all sectors. Organisations must start prioritising identifying and preventing complex cyber-attacks before they occur – something that is impossible if remaining with a legacy system.

Challenges with the legacy software

For businesses relying on traditional reactive security monitoring software (such as with legacy SIEM solutions), they have access to basic analysis and aggregation of log data for detecting cyber incidents. Unfortunately, this can be limited, as most solutions only focus on the alert mechanisms to trigger once a previously known attack pattern has transpired. With the dynamically changing threat landscape, a legacy system often does not offer enough organisation-wide visibility and scalability to truly prevent attacks should they occur.

Cyber criminals have access to the best software available, meaning even the most advanced security software can be bypassed. Criminals are able to hide their activity in the hundreds of gigabytes of data collected from various log sources, as legacy systems do not have the capacity to learn and differentiate them from common user behaviour. When alerts are triggered, these also often are false positives, leading to actual threats slipping through the cracks and going ignored entirely.

Updating legacy systems is therefore imperative. Investing in modern technologies such as cloud-based artificial intelligence (AI) and machine learning (ML) based threat detection can help IT managers and security operations center (SOC) analysts to be far more proactive in monitoring and preventing any cyber threats, by automatically predicting the behaviour of highly complex healthcare IT networks and systems.

Being proactive in threat detection

Businesses that remain holding on to legacy cybersecurity systems rather than updating and modernising their technology only grow increasingly ineffective in preventing threats. In relying on being able to resolve issues after the damage has already happened, they are simply allowing otherwise preventable attacks from being perpetrated.

With the right AI system in place, next generation SIEM solutions can contextualise information to predict cyber threats, rather than just detecting them at the impact stage. Further still, multiple AI models can be used in sequence to optimise the threat detection output to detect early signs of an attack. By integrating with automated data and web scrapers to incorporate the latest contextual threat intelligence for organisations, AI-driven solutions provide near real-time adjustment ability to reflect real exposure from vulnerabilities, compromised credentials, malicious domain spotting within the context, and risk exposure of any client. Further still, alerts can be prioritised and adjusted based on the potential impact to the organisation, putting the most serious alerts at the top of the agenda.

Embracing AI in threat detection is critical

Predictive threat detection using the potential of AI is critical in ensuring businesses avoid the cost of potentially damaging attacks. Dynamically changing threats have to be combatted with an equally complex and reactive prevention system – something companies must realise quickly to ensure customer data remains safe and protected. AI solutions also help business leaders keep their own peace of mind – less focus or worry about the threat of a destructive cyber-attack, and instead more time and money focussed on business development.

About the Author

Ralph Chammah is the Chief Executive Officer at OwlGaze. After serving as the lead Cyber Director of the analytics practice with Deloitte in Canada and Hong Kong, Ralph noticed an opportunity segment that was not being met in the current cybersecurity software market and decided to fill that need. Since starting OwlGaze, Ralph has kept himself and his team laser-focused on meeting that goal, and as CEO, he plays a crucial role in defining the vision and direction of the company. Ralph holds a degree in electrical engineering from Concordia University in Canada.

First Name can be reached online at https://www.linkedin.com/in/ralphchammah/ and at our company website www.owlgaze.com.

Automated Patch Management Can Protect Your Business from A Data Disaster

By Sami Mäkiniemelä, Chief Security Officer, Miradore

It's easy to identify security needs from physical threats we can see. For example, the aviation industry prohibits guns or knives on planes and has a system in place with metal detectors and scanning devices to make sure they aren't allowed on board. But when it comes to the digital threats in the world of cybersecurity, these are usually invisible making them much harder to identify and eliminate. That means businesses need to be constantly scanning for threats to protect their vital business systems from an unwanted data disaster.

Automated systems are key to accomplishing this goal. In a cybersecurity context, one of the most impactful examples of this is automated patch management (APM). This is a process in which code changes, or patches, are automatically deployed to devices to fix or update the operating system or installed software products. APM is the easiest way to fix known vulnerabilities caused by outdated software. According to the Ponemon Institute, 57% of cyberattack victims report that their breaches could have been prevented by installing an available patch. And 52% of respondents say their organizations are at a disadvantage in responding to vulnerabilities because they use manual software patching processes.

Unpatched software is a real cybersecurity risk which can result in data breaches that have severe monetary and reputational consequences. Some of the largest breaches in history were a result of unpatched software. Equifax was forced to pay a settlement of $425 million to victims of their data breach caused by a known, unpatched software vulnerability. And this weakness continues to serve as an easy avenue for attackers to breach a businesses' data. In 2021, unpatched software vulnerabilities were one of the most common attack vectors for hackers. A recent study by Ponemon Institute and ServiceNow showed that nearly 50% of the respondents reported having one or more data breaches in the last two years, and 60% of breached companies stated those attacks may have occurred due to an unpatched vulnerability.

Yet because of the focus on the huge corporations and the major implications of attacks on them, small- and medium-sized businesses have been lured into a false sense of security that they're not at risk because they're not as big a target. The reality is that these types of attacks can happen to any company, big or small. That means it's essential for all businesses to develop resources to defend themselves against this pervasive and growing threat. A challenge for smaller companies is they often have less financial resources available for cybersecurity. If a business has a limited IT budget and needs to focus on one area of digital security, they should focus on APM which can provide a solution that secures a company's critical digital assets at minimal cost.

Here are three main reasons why APM is the best solution out there today to protect companies large and small from digital vulnerabilities:

1–APM is better than manual patch management

Info Security Magazine reported that more than 18,000 common vulnerabilities and exposures (CVEs) were published last year — that's an average of around 50 CVEs a day, making it nearly impossible to keep track of every one manually. By using APM, you'll always be up-to-date with the latest patches for operating systems and applications. So even if your company is managing a small fleet of computers, APM is the best option as it precludes the possibility of forgetting to check for updates or installing a patch incorrectly due to human error.

2–APM mitigates risk for employees

Because APM automatically installs new updates, IT managers don't have to rely on their device end users to install patches on their own. It's also convenient, making it easy to centrally monitor the patching status of your IT environment with every device running APM available in one online portal. This allows you to upload and install all necessary patches to your devices automatically, so your IT manager doesn't have to manually search for new patches every time.

3–APM means better productivity

Devices running the most up-to-date versions of software will have better performance overall. That means productivity increases as your device users don't have to struggle with performance issues or bugs. Both employees and IT managers will spend far less time worrying about keeping software up to date as well, leading to even more increased productivity.

Many smaller-sized businesses might think, “Well, this all sounds great, if we could afford it.” The good news is APM is more affordable than managers might expect. Also, APM software is often integrated into a mobile device management (MDM) platform that has a wide variety of additional asset management functionality, like online device inventories. Online device inventories make both automated and manual patch management much easier because the technical specifications for every device, including versions for all installed software, are stored in a central repository for convenient reference by a company’s IT staff.

MDM also gives smaller businesses the ability to significantly streamline IT operations by automating device setup and maintenance tasks, leaving your IT department with more time to assist employees with pressing/complex issues. In fact, use of an MDM platform has been found to save some IT departments up to 30 hours per month. That can translate into a lot of increased productivity, especially for smaller businesses with minimal IT staff.

In today’s digital environment with ever-increasing threats, now is the time for companies to be leveraging APM to ensure they are providing the safest possible network, devices, and other infrastructure to their employees, vendors, and customers. And it also helps allocate the valuable time of their IT professionals for other, more demanding purposes. While there is some cost associated with implementing these technologies, it’s not nearly as great as it would be if a patch failure caused your company to be the subject of the next Yahoo!- or Facebook-sized data breach. APM is the easiest, most efficient way for companies of all sizes to mitigate unpatched vulnerabilities, ensuring all their computers and digital devices are safe and performing optimally.

About the Author

Sami Mäkiniemelä is the Chief Security Officer at Miradore, a software company that offers MDM services. Sami can be reached online via LinkedIn. You can learn more about the benefits of patch management and mobile device management on Miradore’s website.

Common Vulnerabilities of Enterprise Web Security That Demands Your Attention

By Eden Allen, Cyber Security Educator, CheapSSLWeb

Years ago, the way leading enterprise-level concerns were viewed differed from how it is viewed today. As enterprise companies started taking on the latest technologies for their business, it paved the way for digital attacks and exposed them to additional network vulnerabilities that attackers can easily exploit. Thus, '**enterprise web security**' has become one of the crucial considerations for enterprises while they are looking to expand their digital venture.

Enterprise web security must efficiently control the network's threats to avoid any chance of financial or reputational damage usually associated with a data breach. Therefore, prioritizing web security as an active part of the enterprise risk management solution will help organizations secure their confidential digital assets.

Before we get into the vulnerable areas of enterprise web security, let us understand what it is:

What is Enterprise Security?

If we talk about holistic enterprise risk management programs, enterprise security is one of its most crucial components. It comprises systems, processes, and controls in an organized manner for securing IT systems and critical data.

As companies continue to depend on cloud-based infrastructures, there is an increase in data privacy and compliance regulations globally. Thus, they need to undertake relevant measures to secure their crucial assets.

Now, have a look at the common cyber vulnerabilities that large-scale companies face:

What are the Common cyber vulnerabilities of Enterprise Organisations?

Cybersecurity has become one of the leading concerns for companies across all industries, thanks to the constantly increasing data breach.

Take a look at these common vulnerabilities to stay alert:

- **Missing or Weak Data Encryption**

With a missing or weak encryption cover, it becomes convenient for cyber attackers to access the data of the end user's and central server communications. An unencrypted data exchange becomes a hot, rather easy target of attackers for accessing the crucial data and injecting malicious files onto a server.

Malware files can severely damage a company's efforts towards cyber security adherence, leading to fines from regulatory authorities. Organizations usually have multiple subdomains, so using a multi-domain SSL certificate is ideal. They can secure the main domain and multiple domains using a single certificate.

- **Zero-day Vulnerabilities**

Some particular software vulnerabilities that an attacker has caught wind of but is yet to be found by an organization can be defined as zero-day vulnerabilities.

When we talk about zero-day vulnerability, there is no available solution or fix as the vulnerability is yet to be notified or detected by the system vendor. There is no defense against such vulnerabilities until the attack has taken place, so naturally they are quite dangerous.

The least you, as an organization, can do is stay cautious and regularly track systems for vulnerabilities to minimize, if not stop, zero-day attacks. Apart from this, organizations can equip themselves with comprehensive endpoint security solutions to stay ready for damaging occurrences.

- **Social Engineering Attacks**

Malicious actors launch social engineering attacks to bypass verification and authorization security protocols. It is a widely used method for getting access to a network.

'Social engineering' can be defined as all the malicious activities that are done through human interactions. It is done by psychological manipulation to trick web users into making security mistakes or accidentally sharing confidential data.

In the last five years, the network vulnerability has significantly increased, making it a lucrative business for hackers. Since Internet users are not quite aware of internet security, they (though not deliberately) can pose a security risk to an organization. They accidentally download malicious files, and as a result, they cost significant damage.

Some of the common social engineering attacks include:

- Phishing emails
- Spear phishing
- Whaling
- Vishing
- Smishing
- Spam
- Pharming
- Tailgating
- Shoulder surfing
- Dumpster diving

- **System Misconfigurations**

Accidentally exposing an organization's internal servers or network to the Internet has proven to be one of the most significant threats to an organization. Upon exposure, threat actors can spy on the company's web traffic, risk their network, or steal data for malicious purposes.

Network assets with vulnerable settings or contrasting security controls can result in system misconfigurations. Cybercriminals usually check networks to find system misconfigurations and leverage them to exploit data. As the digital transformation progresses, network misconfigurations have also increased.

To eliminate this, organizations often leverage 'firewalls' in the demilitarized zone. It acts as a buffer between the internal network and the Internet, thus acting as the first line of defense. So, it tracks all the outbound and inbound traffic and decides to limit or allow traffic depending on a set of rules.

- **Out-of-date or Unpatched Software**

Typically, software vendors release upgraded versions of applications to patch up known and significant vulnerabilities or incorporate new feature (s) or vulnerability (s). Outdated or unrepaired software becomes a convenient target for smart cyber criminals. Such vulnerability can be easily exploited.

Though software updates might come with crucial and valuable security measures, organizations are obligated to update their network and each endpoint (s). However, there is a good chance that various software application updates might be released every day.

This becomes overwhelming for the IT team, so sometimes they might fall behind on patching or updates. The situation paves the way for a ransomware attack, malware, and several security threats.

These are some of the common vulnerabilities of enterprise web security. So take up relevant measures to combat these threats.

- **Ending Thoughts**

As malicious actors try to find different ways of exploiting and gaining access to the system, network vulnerabilities are always at risk of being compromised. Furthermore, with networks becoming more cumbersome, there is a dire need to actively manage cyber security vulnerabilities.

Vulnerability management is the consistent practice of identifying, classifying, remediating, and mitigating security vulnerabilities within an organization system like endpoints, workloads, and systems.

Since enterprises potentially have several cybersecurity vulnerabilities within their IT environment, a robust vulnerability management program is necessary. It deploys threat intelligence and IT and business operations knowledge to emphasize risks and find all cybersecurity vulnerabilities in no time.

About the Author

Eden Allen is a Cyber Security Educator and Tutor at CheapSSLWeb. She has over 14 years of experience in the field of Encryption and Cybersecurity. With all her experience and knowledge, she started sharing it to people to make them aware of Cyber security, encryption, malware, threats, etc. First Name can be reached online at twitter @TutorEden and at our company website https://cheapsslweb.com/.

Cyber Threats Driving Insurance Claims Activity

By Scott Sayce, Global Head of Cyber and Group Head of the Cyber Centre of Competence at Allianz Global Corporate & Specialty (AGCS)

Cyber Threats Driving Insurance Claims Activity

In response to the challenging loss environment of recent years, the insurance industry is more diligently assessing clients' cyber risk profiles and clarifying coverage areas in a bid to incentivize companies to improve cyber security and risk management controls.

Our experience shows a number of companies still need to improve their frequency of IT security training, cyber incident response plans and cyber security governance. Incident response is critical as the cost of a claim quickly escalates once business interruption kicks in.

It is clear that organizations with good cyber maturity are better equipped to deal with incidents. It is not typical for us to see companies with strong cyber maturity and security mechanisms suffer a high frequency of 'successful' attacks. Even where they are attacked, losses are usually less severe.

Ransomware threat continues to help drive elevated cyber claims activity

In recent years AGCS has experienced elevated levels of cyber insurance claims, driven in part by the growth of the cyber insurance market, but also by an overall rise in incidents, including notifications of ransomware attacks, which are among the biggest drivers of cyber insurance losses. During 2020 and 2021, AGCS received more than 1,000 cyber-related claims per year overall and while claims activity has stabilized, driven by a more diligent underwriting approach and better risk dialogue with companies, 2022

has the potential to be another year of high claims frequency, as cyber claims historically have occurred predominantly in the third and fourth quarters of the year.

Despite the efforts of law enforcement agencies, the frequency of ransomware attacks remains high, as does related claims activity. Ransomware attacks hit a record 623 million in 2021, double the number in 2020 and a 232% increase since 2019. Despite a 23% reduction in frequency at the start of this year, the number of ransomware attacks globally in the first half of 2022 still exceeded full-year totals of 2017, 2018 and 2019, according to SonicWall's Cyber Threat Report, while Europe actually recorded a 63% surge in ransomware attacks in the first half of 2022. Meanwhile, ransomware is forecast to cause $30bn in damages to global organizations by 2023, remaining the top cyber threat to enterprises as well as governments, according to cyber protection industry estimates.

There is no denying that cyber extortion, and ransomware, has become big business. Ransomware-as-a-service (RaaS), which gives cyber criminals access to ransomware tools and support services, has lowered the barriers to entry and enabled criminals to scale up their efforts and ramp up their attacks. With average ransom demands in 2021 in the millions and RaaS kits costing as little as $40 per month, cyber criminals can make huge returns with little investment or technical expertise from ransomware attacks.

On a positive note, there are some signs, however, that risk management actions taken by insured companies are beginning to take effect, yet overall the frequency and severity of ransomware and cyber extortion claims for AGCS has increased significantly in recent years.

Rising severity: Double extortion is now the norm

The severity of ransomware claims continues to rise year-on-year as gangs employ increasingly sophisticated attack tools and extortion techniques. The value of ransomware claims globally has increased significantly since 2019, accounting for well over 50% of all cyber claims costs that AGCS has been involved in together with other insurers over the past two years and remains a significant cost driver through 2022 to date. Business interruption, restoration costs and expert fees are the main loss drivers in a ransomware event.

In a traditional ransomware attack, criminals infiltrate a network and use malware to encrypt files, demanding a ransom in return for its restoration. A double extortion attack, however, also involves the theft of sensitive data, which is then used as leverage for extortion. By exfiltrating data, criminals can make ransom demands of companies even if they successfully restore data from backups.

Triple extortion goes one step further, with criminals making extortion demands of business partners, customers, or suppliers that may be affected by data stolen in the initial attack. Double and triple extortion adds to the cost of a ransomware attack, as well as introducing an element of third-party liability.

Ransomware severity is likely to remain a key threat for businesses, fuelled by the growing sophistication of ransomware gangs and rising inflation, which is reflected in the increased cost of IT and cyber security specialists.

Action on ransom payments on the horizon

High profile disruptive cyber-attacks, such as the 2021 Colonial Pipeline incident, have put ransomware on the political agenda, sparking a redoubling of law enforcement efforts. Attention has also turned to the payment of ransom demands, with new rules and potential bans on the horizon.

Ransom demands continue to rise. According to the Paloalto Ransomware Threat Report, ransom demands increased by 144% in 2021, while the average payments rose 78%. Some 46% of companies paid ransoms in order to get data restored, according to Sophos.

The payment of ransom demands is a contentious topic. Critical service providers, such as hospitals or power companies, may have little option other than to pay a ransom demand in order to avoid crippling disruption. On the other hand, paying extortion demands may encourage further ransomware attacks. Sanction rules and terrorism regulations may also bar payment of ransoms to certain states, groups or individuals, including cyber groups.

Potential legal changes around ransom payments are unlikely to 100% solve the problem of ransomware, but they might help improve the maturity level of companies. Longer term, cyber criminals are likely to consolidate and change tactics as ransomware attacks become less lucrative, and as easy targets are harder to find.

Small and mid-sized companies an increasing sweet spot for hackers

All companies, across all sectors, are now exposed to ransomware attacks, although small and mid-sized companies are proving a more attractive target for cyber criminals as larger companies beef up their cyber security.

Cyber security, rather than sector focus, is now the key driver for cyber-attacks. The most attractive targets for cyber criminals traditionally have been large organizations, where they can get the most financial gain for reasonable effort. With these organizations investing heavily in security, the focus is gradually shifting to small and mid-sized firms. The current real sweet spot is a mid-sized business with weak controls, risk management and cyber security in place. That is what cyber criminals like most."

Large companies are better positioned to mitigate the growing threat landscape than smaller companies, which often lack the resources to invest in cyber security and risk management. Small to medium sized companies see their risks increasing with digitalization, but typically would not carry out impact analysis linked to cyber security and the value of the business.

Even larger companies can have vulnerabilities and blind spots**.** In around 80% of AGCS cyber insurance claims, involving companies with an annual turnover in the triple digit millions, a significant flaw in the security of the insured led, or contributed, to the eventual loss.

The good news is that insurance companies are now seeing a very different conversation on the quality of cyber risk than we were a few years ago and are therefore gaining much better insights as the cyber insurance market matures. Insurers have a role that goes beyond pure risk transfer, helping clients adapt to the changing risk landscape and raising their protection levels.

About the Author

Scott Sayce is the Global Head of Cyber and Group Head of the Cyber Centre of Competence.

Scott can be reached online at scott.sayce@allianz.com.

Cyberattacks Remain on the Rise – How Can the Corporate World Remain Proactive?

By Geoffrey Lottenberg

Imagine a swarm of termites secretly and incessantly feeding on your home. In relative silence, your home is under attack, 24 hours a day. By the time you detect the bugs, your door frames have turned to dust and your joists have failed. Cybercriminals are like termites. Relentless. Sure, you can repair the house after the walls crumble down, but what if you had detected the infiltration earlier and prevented catastrophic failure? This is the key question modern cybersecurity professionals are asking themselves every day.

The Common Foe

It has been recently reported that only 10-20% of American hospitals have a meaningful cybersecurity program – a scary thought given hospitals process an enormous amount of financial and personal health information. For other industries outside of the tech industry, this number is likely far worse. Many

business owners question the motives of cybercriminals and do not necessarily see themselves as a potential target, which is a mistake. The single prevailing motive for cybercriminals attacking businesses is financial gain. Financial gain is typically derived from ransoms, trafficking in stolen personal and financial data, or corporate espionage. The latter – corporate espionage – has seen a significant uptick since COVID-19, as businesses were pushed deeper into the Cloud. Many of these attacks are "inside jobs," perpetrated by outside criminals given access credentials or other information about a company's system.

Layers of Security

Preventing cyberattacks in the corporate world requires a multi-faceted approach. Businesses must simultaneously mobilize their information technology, human resources, and legal departments.

Information technology and data security departments need more time, personnel, and a more extensive equipment and software budget to implement necessary changes to prevent and redress cybercrime. Advanced firewall and encryption technology become an absolute must – two-factor authentication is often not enough. Incident response plans will need to be reviewed and updated quarterly to provide specific guidelines on how to respond to the latest cybercrime techniques. After changes and upgrades are implemented, businesses should engage third-party cybersecurity companies to run independent cybersecurity audits and penetration testing so that weakness can be exposed before an actual security incident occurs (insurance companies may require such testing, or offer discounts if testing meets certain standards).

An essential advancement for IT professionals is the implementation of AI-enabled infiltration detection software. Machine learning has been proven a key development in meeting cyberattacks head-on because as infiltration techniques change and improve, so does the AI engine of the detection software. There are many AI solutions on the marketplace – enough to fit virtually any use case from SMEs all the way to Enterprise-level. Not to sound like the "SkyNet" alarms – but AI-enabled cybersecurity detection software can go a long way to solving the relative unavailability of qualified cybersecurity and IT professionals in today's market.

Businesses should also have in-house counsel or experienced outside counsel review, update company data and privacy policies, and engage in critical analysis and education to develop an in-depth understanding of current and proposed state, federal, and international law regarding cybercrime, reporting, and response obligations on a business entity should an attack occur. Cybersecurity insurance policies should be procured or updated to meet increased exposure.

HR departments must implement and improve company-wide cybersecurity and data privacy training for all employees. This means both technical training to understand how to securely use new systems and compliance training to understand where data and/or privacy breaches can occur and how to spot and redress potential security breaches.

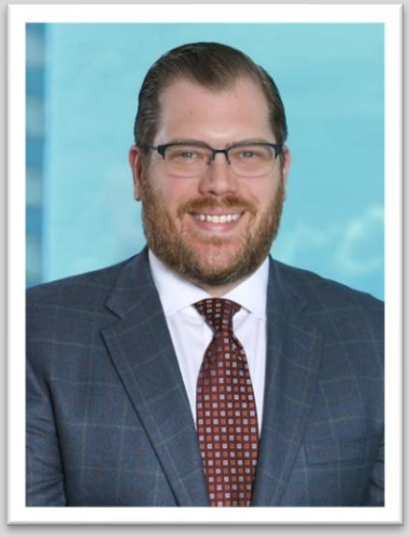
Sleeping with the Enemy

HR departments must also pay significant attention to their hiring and retention practices, implement fail-safes to avoid hiring potentially disloyal employees, and detect unusual activity indicating that an active employee may be misappropriating sensitive information, including feeding it to would-be cybercriminals. A standard vetting process would include multiple interviews (including live, in-person interviews, even for remote positions), in-depth background searches as to financial, employment, and criminal histories and an investigation into the candidates' Internet and social media presence. These practices must be implemented in compliance with applicable state and federal employment practices – so consult your local employment attorney.

Human resource managers and hiring partners must work cohesively with information technology and security departments to develop and implement safer employment practices. Proper data controls must be in place to identify and designate data with the appropriate level of secrecy, tier and compartmentalize access to that data, and track the use and transfer of that data internally and externally. Most enterprise-level file management software includes this functionality, and these resources' cost has decreased significantly over the past several years.

From a legal perspective, failure to take reasonable precautions to prevent cyberattacks – a standard that varies with the type and size of the business, can expose a business to significant liability under state and federal law in the event of a cyberattack. As noted above, cybersecurity insurance may help, but it is not a silver bullet and only matters *after* an attack has occurred. Much of the focus now needs to be placed on the front end with prevention, testing, education, and compliance measures working together to stop the house from turning into dust.

About the Author



Geoffrey Lottenberg is partner and lead of Berger Singerman's intellectual property practice and co-manager of the firm's Dispute Resolution Team, Geoff handles a wide variety of matters, including IP procurement and enforcement, business and technology law, and complex commercial litigation. With a calculated approach, Geoff regularly litigates patent, trademark, and copyright disputes in Federal Court throughout the United States. He also handles a variety of technology-related commercial litigation matters including disputes over software contracts, non-compete agreements, and trade secrets.

As a Registered Patent Attorney armed with a background in mechanical engineering, Geoff prosecutes domestic and foreign patents and renders opinions on a variety of cutting-edge technologies, including automation, facial recognition technology, medical devices, emergency communication devices, software-based systems, and energy devices. Geoff also has hundreds of federal trademark applications and registrations under his belt.

Geoff is also an experienced transactional lawyer who works on broad array of corporate intellectual property matters including negotiating and preparing license agreements, software contracts, manufacturing and distribution agreements, and intellectual property asset transfers. Geoff is a key member of our firm's mergers and acquisitions team and provides support in restructuring and work out matters.

Geoff can be reached online via his LinkedIn (https://www.linkedin.com/in/geoffreylottenberg/) and on his company website (https://www.bergersingerman.com/).

DevSecOps and Digital Transformation: Bridging the Security Gap

How DevSecOps Ensure Security in Development Lifecycle?

By Sudeep Srivastava, CEO, Appinventiv

The Covid-19 pandemic has accelerated digital transformation to a staggering speed. However, for most organizations going digital has also posed a considerable challenge at times. To ensure both longevity and success, organizations require a combination of the right people, the right tools, and the right skill sets.

Nevertheless, digital transformation brings new scopes like databases, digital assets, cloud computing services, applications, and websites, thereby increasing the need to secure the organization. Therefore, it is vital to deploy a complete security approach in the form of DevSecOps to avoid security breaches, protect the company's goodwill, and maintain the customer's connection.

As per Statista, 47% of companies are now leveraging the DevOps or DevSecOps methodology for the software development process. This practice aims for timely delivery while ensuring high software quality and shortened development cycle period. Reasons, why businesses are choosing the DevOps or DevSecOps methodology for software development are faster time to market, code qualities, security, and improved collaboration among the developers.

What is DevSecOps?

DevSecOps is an excellent solution for organizations that requires the immediate adoption of security and improvise their productivity level. DevSecOps is positioned as one of the top security controls in the development process, and it operates at every level of the product development life cycle stage. If implemented properly, DevSecOps can train employees, automate security checks and ensure the development of a great product.

DevSecOps is the seamless integration of security protection and testing, right from software development to the deployment stage. The goal is to incorporate security into the CI/CD workflow in both pre and post-production environments.

Is DevOps Different From DevSecOps?

For accelerating the development and delivery of the software product, the modern software development process utilizes an agile SDLC process. DevOps and DevSecOps utilize the agile framework for various purposes. DevOps mainly focuses on the speed of the application delivery, whereas DevSecOps too focuses on speed but ensures the complete security of the deployed application. The goal of DevSecOps is to promote a faster development process with a secured code base.

DevSecOps is all about integrating security at every level of the software development life cycle stage. In DevSecOps, security is the stakeholder's shared responsibility in the DevOps value chain. In short, DevOps focuses on speed, while DevSecOps maintains velocity without compromising security.

How Does DevSecOps Work?

By integrating automated security checks into the software development pipeline, organizations can verify the security of both their application infrastructure and the application itself before it is tested with real users. These types of security checks can come in the form of container scanning, code analysis, infrastructure configuration validation, and peer reviews.

Developers can directly identify the problems that were previously established in the CI/CD workflow and fix them rather than waiting for security audits to process after all the work has been done. This helps in embedding security hygiene into the company's digital culture, thereby increasing the security level while reducing the scope of failure. Various software development companies are now offering DevOps services, taking care of their client's end-to-end DevOps needs to ensure the deployment of a robust product.

How DevSecOps Helps in Bridging the Security Gaps

Adopting DevSecOps into your software development lifecycle unifies the development process security and the entire operations. Let's have a look at how DevSecOps has benefited organizations along with bridging the security gaps.

Faster Product Delivery

Security issues often bog down the developers with the time-consuming bug-fixing processes. By adopting DevSecOps, things become easier as the developers can now resolve the bugs and glitches easily. DevSecOps, thus, eliminates or minimizes such bottlenecks and streamlines the security of a particular product development process.

Increased Vulnerability Patching and Code Coverage

By utilizing automated processes, DevSecOps improvises overall security through wider and increased code coverage and vulnerability patching. In doing so, it analyzes and resolves security vulnerabilities more quickly.

Proactive and Improvised Security

DevSecOps inculcate the best cybersecurity practice throughout the software development lifecycle and delivery stage. By channelizing audits, code reviews, QA tests, and scanning for security vulnerabilities, problems are detected and addressed in a lean process. With DevSecOps, fixing bugs has become easier and more cost-effective.

Builds an Adaptive Security Process

DevSecOps encourages a kind of work culture where security is constantly applied throughout the product development life cycle environment. DevSecOps, as a process is capable of transforming and adapting to new requirements.

Advantages of Adopting the DevSecOps

With modern technologies like dynamic apps, flexible cloud computing, shared storage, data analytics, and containerization, businesses have seen huge changes in their IT integrity in the last few years. DevSecOps has the capability of elevating your mission-critical application’s speed, performance, and functionality, scaling it to new heights of success.

However, due to the lack of solid security and compliance, these applications are lately deployed. This is where DevSecOps comes to the scene. DevSecOps ensures that all the security measures are in place and no malware gets injected into the application during the development process. Here a some of the following advantages of adopting DevSecOps in your digital transformation projects.

- Continuous security checks and monitoring
- Reduced compliance cost
- Quicker deployment of applications
- Enhanced project transparency from the start to the end
- Faster recovery time in the event of an unwanted security breach
- Automated security throughout

Wrapping it Up

The purpose of every business in the era of digital transformation is to offer the best products to their customers that are free of security threats and hacks. DevSecOps is a technique that is cost-effective and proactive. The adoption of DevSecOps helps developers to employ the best security precautions in an established atmosphere where security begins right at the outset of development.

Integrating DevOps and security into the software development life cycle doesn't just make the product more secure but also provides it a competitive advantage. Partner with the best DevSecOps service provider today, who can optimize your development processes efficiently and help you achieve the best business outcomes.

About the Author

Sudeep Srivastava is the CEO of mobile app development company "Appinventiv", is someone who has established himself as the perfect blend of optimism and calculated risks, a trait that has embossed itself in every work process of Appinventiv. Having built a brand that is known to tap the unexplored ideas in the mobile industry, he spends his time exploring ways to take Appinventiv to the point where technology blends with lives.

Sudeep can be reached online at https://twitter.com/sudeepsriv?s=20 and at our company website https://appinventiv.com/

Doenerium: When Stealing from Thieves Is Also a Crime

By Igal Lytzki, Incident Response Analyst, Perception Point

Over the past few weeks our team of 'white hat' cyber threat experts uncovered a particularly worrying and sophisticated phishing attack that posed a unique, twofold threat to its unsuspecting victims.

The attack used a malware called Doenerium to harvest victims' personal data through open-source code left lingering on Github – including crypto wallets, as well as browser data such as cookies, passwords, history, and bookmarks. But what made this malware unique was a hidden backdoor within the attack code. Any information that a hacker gleaned while using Doenerium was secretly and automatically made available to the malware's initial author. The victims' data, stolen first by a hacker, would immediately be scooped up by the creator of Doenerium as well, to grow his own crypto mining operation.

The model of hacked data-sharing is not new – hackers have long sold stolen data to the highest bidder. But with Doenerium, the hackers themselves were made unsuspecting victims: the hackers that utilize this malware to steal sensitive data are actually being hacked themselves by the malware author.

Here are the key components that make this attack and the malware's capabilities so dangerous, as well as best practices for individuals and organizations looking to avoid its consequences.

Part One: Illicit Business as Usual

This attack, like so many others, begins with an email titled, “Important Windows Defender Update!” formatted in a believable faux-Windows Defender template replete with official-looking graphics and MSL logos. The recipient is warned that Windows Defender has recently detected malicious software on the user’s computer and is then prompted to download additional software for removing the malware. After clicking the link, the recipient is then redirected to a spoofed landing page for the malware itself.

The landing page offers links to two fictitious ‘software removal tools,’ one for a 32-bit system and the second one for a 64-bit system. Both links yield the same malicious results, but present two further options in order to establish legitimacy, which fools users into continuing the process.

These links lead to a shared drive containing a ZIP archive with two files inside: first, a README.txt file that, when opened, explains how to use the tool, and second, the actual malware, a 64 bit C++ PE, compiled using Node.js with the size of 102mb. When running the malware, analysts searched for unique strings and found an unusual one:

<==========[t.me/doenerium]>==========>

The unusual string is actually a short URL to a Telegram server, which leads to a Github repository called doenerium created by the user doener2323. This is but one of many instances of malware being hosted on Github.

Because the user’s profile remained available for some time, with the malware publicly available, we were able to review its source code and analyze the malware. In this instance, the malware had two main capabilities – harvesting individuals’ personal data and mining their crypto wallets.

It does so by first identifying the CPU of the victim’s computer – information found in the victim’s profile – that is sent to the hacker’s Discord server. The malware then creates an exfiltration folder on the victim’s computer, which is saved in the TEMPdirectory. Every directory entry contains the victim’s computer name concatenated with an underscore and “36 char UUID” (universally unique identifier).

The malware then searches for crypto wallets housed in the victim’s computer and creates a folder called “Wallets” within the exfiltration folder to store any crypto wallets discovered. Additionally, it creates a small text file that summarizes the findings.

Next, the malware hunts for Discord tokens, decrypts them, and tries to validate them before finally harvesting the rest of the browser data to look for passwords, cookies, bookmarks, history, autofill, and more.

After the malware has harvested all the data, it creates a complete virtual profile for the victim, which is archived and uploaded to gofile.io – a free file sharing and storing platform. The malware author leverages gofile.io to host the archive and share it with the hacker.

Part Two: The Backdoor Twist

Further research into the attack revealed that doener2323, the malware author, had also created a second Github repository called 1337wtf1337. Both accounts were linked using a technique known as "Dual Hooking" – in addition to the webhook that the hacker applies to the malware (where exfiltrated data is copied), the malware contains an additional Discord webhook associated with doener2323.

In other words, everything a hacker achieved using this malware was automatically shared with doener2323.

The dual hook was removed on September 3, 2022, but not before Doener created a separate, completely obfuscated javascript file. When decoded, this file led to an open Discord server for sharing the active hackers' profits and updating the users about new features and fixes.

Initially, Doener2323 and their partners weren't shy about informing other Discord users about their goal. They openly explained that the purpose was monetization and that the webhook was part of a bigger crypto mining operation for Doener2323, which infects any victims that are lured by active hackers using Doenerium.

When other users started catching on, Doener became less enthusiastic about the possibility that they might share in the spoils, and removed them from the Discord chat.

Recommendations

This attack (and its double-crossing backdoor) teaches us that nothing comes free – not even the stolen fruits of malware. The hackers who utilized this publicly accessible malware to steal sensitive data were ultimately themselves hacked in turn by a malware author growing their own crypto mining operation.

Like many dangerous phishing attacks, this sophisticated attack began with a simple email. Considering about 1 in 5 phishing attempts evade Microsoft's default security offering and actually get to users' inboxes, it is integral that security leaders ensure that their organizations are provided with the most advanced safeguards.

The first line of defense for protecting against this type of attack must be user education around email security – regular email security drills can help employees better identify genuine suspicious content and remind them not to open strange files, links, or attachments and double-check the identity of the sender. Organizations should also establish a standardized process for employees to follow when they receive a suspicious email or link.

Security teams would do well to deploy an advanced email security solution that prevents phishing emails from reaching users; without this, any business could be destroyed by ransomware, and sensitive information can be stolen.

Publicly outing suspicious behavior alerts bad actors that their misdeeds do not go unnoticed. Several weeks after we shed light on the campaign, Doener realized that threat detection teams were catching onto their ruse. By November 5, 2022, Doener had purged the Discord server previously used to communicate with other hackers using Doenerium malware, and also removed the link to the malware from the official Github repository. Despite this, a few weeks still allows ample time for hackers to win big, further demonstrating the need for advanced email security solutions that will stamp out threats instantly.

In the nefarious world of cybercrime, there are no Robin Hoods - only robbers. As these bad actors continue to push the envelope, we must all be able to recognize the difference between good email and bad email, even before they arrive in our inboxes.

About the Author

Igal Lytzki is currently a Cybersecurity Analyst on Perception Point's Incident Response team. Prior, he served as a Commander in the Israeli Air Force's Iron Dome division. With his background in programming and cyber, Igal has become an expert on all thing's malware, his interest fueled by the curiosity of understanding hackers and their methods. In his spare time Igal can be found on Twitter @0xToxin hunting malware.

Igal can be reached online at https://www.linkedin.com/in/igal-lytzki-99bb0721a/ or https://twitter.com/0xToxin at our company website https://perception-point.io/

Five Ways to Keep Endpoint Protection Simple

By Ashley Leonard, CEO, Syxsense

Endpoint security continues to be more challenging and complex as workplace environments hybridize and evolve. In fact, research shows that 68% of organizations have experienced one or more endpoint attacks that compromised data and/or their IT infrastructure. The same percentage of organizations also found a rise in frequency of endpoint attacks over the last year. These statistics show not only the growth in attacks, but also that the variance and complexity of these attacks are rapidly changing year over year. As a result, it's never been more critical to manage and secure your endpoints. But with everyone talking about complexity (of attacks and solutions), what are some steps you can take to simplify the process?

Endpoints are the gateway that attackers use to access company data. Leaving them unprotected exposes your organization to risk and potential attack, not to mention financial, reputational, and legal consequences. Creating an endpoint security strategy starts with adopting consistent approaches to protection. While the best way to achieve that is with continuous threat monitoring, detection, and automation of critical endpoint security tasks, there are some simple steps you should be taking – with or without an endpoint security solution in place. Let's dive in.

1. ABP = Always Be Patching

Managing software updates — and specifically patching endpoints — helps secure an organization from known threats. A recent study showed that 60% of breach victims cited a known but unpatched vulnerability, where the patch was available but had not been applied, as the reason for a breach. This lack of action often stems from the sheer volume of emerging attacks combined with the large number of patches being released across today's IT ecosystem, and a lack of a comprehensive patching strategy.

The appearance of new endpoint types, such as Internet of Things (IoT), Bring Your Own Device (BYOD), and other operating system and software vulnerabilities, has resulted in a tidal wave of patch releases over the last 5 years. Staying ahead of threat actors means patching all the time.

2. Seek Out All Endpoints

Think about a company network and how many endpoint devices there are. Hundreds? Thousands? Tens of thousands? Endpoint compromise accounts for most of today's security breaches. In fact, estimates put the number around 70 percent. If you can't identify and track these devices, how can you secure them? The easiest way to do so is with a comprehensive discovery and configuration compliance audit. This process can have multiple steps, but it typically involves:

- Discovering and taking a thorough inventory of all hardware, such as servers, laptops, virtual machines, mobile and networking devices.
- Ensuring all systems are configured in line with applicable compliance standards and internal security policies.
- Continuously monitoring those configurations for inappropriate or unwanted changes and mitigating configuration drift.

Ensuring you have a running tally of your endpoints is critical to securing them.

3. Stay Current on Innovations

Hackers and threat actors are constantly upgrading their technology and approaches. To stand against them, you and your organization must do the same. Whether utilizing patching, compliance, or security solutions (or better yet, all of those in a single platform), it's important to regularly evaluate new technology innovations. Advancements around automation, machine learning and more, are streamlining endpoint security, reducing the false positive rates, and enabling IT and security teams to do more with less resource.

4. Be Active

All quality security programs require both a proactive and reactive approach to endpoint vulnerabilities. One key proactive approach is the continual active scanning of network devices to identify weak points,

misconfigurations, and vulnerabilities. This means testing for vulnerabilities from both outside and inside the network to ensure robust visibility, which can expose open ports, disabled firewalls, or issues with antivirus. This is also important for companies that need to meet government and industry compliance or regulatory policies.

Once vulnerabilities are detected (e.g., missing patches, faulty configuration, or out-of-compliance devices) they must be remediated quickly. Finding an endpoint security solution that integrates with a SOAR (Security, Orchestration, Automation and Response) solution can enable process remediation for large groups of devices without the typical manual workload.

5. Make It a Priority

Endpoint security should be a priority – dare we say even higher priority than the "protect the perimeter" firewall strategy? In many ways, individual endpoints have become the perimeter of the network. But for many organizations it's not. Endpoint security doesn't just protect a business — it preserves their reputation, reassures customers, and streamlines business processes. Without the necessary prioritization that cybersecurity demands, your endpoint security endeavors will likely fall short. Need executive buy-in? Consider running these facts by leadership:

- 81% of businesses experienced an endpoint attack involving some form of malware.
- 79% of people traveling for business have connected their devices to a public USB port or charging station.
- One in three US employees (33%) uses a personal computer or smartphone to work remotely.
- Only 47% of organizations monitor their networks 24/7.

These are just a few simple steps and insights to help get your organization on track with endpoint security. As consolidation continues across the security industry, solutions are emerging that deliver comprehensive endpoint security, patch management, and compliance, in a single platform. To truly protect against the rising endpoint threat, organizations must look to leverage these powerful new solutions.

About the Author

Ashley Leonard is the President and CEO of Syxsense—a global leader in Unified Security and Endpoint Management (USEM). Ashley is a technology entrepreneur with over 25 years of experience in enterprise software, sales, marketing, and operations, providing critical leadership during the high-growth stages of well-known technology organizations.

Ashley manages U.S., European, and Australian operations in his current role, defines corporate strategies, oversees sales and marketing, and guides product development. Ashley has worked tirelessly to build a robust, innovation-driven culture within the Syxsense team while delivering returns to investors.

Ashley has founded several successful technology companies, including NetworkD Inc., with operations in 7 countries. NetworkD made several strategic international acquisitions and then completed a successful exit to Sparxent in 2008. In 2012 he founded Verismic Software and launched Syxsense in 2019.

Ashley serves on several boards and acts as a mentor to up-and-coming technology CEOs through his membership in the Young Presidents Organizations (YPO). He served as Orange County chair for two years. Ashley also served as Area Chair for YPO Pacific Region and was host city partnership chair for the 2020 YPO Global EDGE conference in San Diego, CA, welcoming over 3,000 of the world's top CEOs.

Ashley was a finalist for Ernst & Young's "Entrepreneur of The Year" and AeA's "Outstanding Private

How 5G Networks Are Secured and Enabled By SASE

By Kelly Ahuja, Versa Networks CEO

As more organizations consider their own 5G MEC (Multi-Access Edge Computing) roll outs and environments, there are important deployment and security considerations. While still a fairly new technology, adoption rates of 5G have increased significantly, currently at three times that of 4G. The buzz has been growing around 5G for some time, as the new networking standard promises faster speeds, greater bandwidth, and optimized mobility.

The technology has quickly gone from concept to reality as the demand for an enhanced digital experience, along with the increase in personal and IoT devices, as well as workload transition to cloud, have driven the need for 5G.

With 5G, it is extremely important for organizations to consider security solutions that can enforce consistent security posture across public cloud, hybrid cloud, and on-premises environments, or any combination of these environments. 5G introduces a whole host of security threats and vulnerabilities, such as kernel bypass, DDOS attacks on 5G service interfaces, and exploitation of software or hardware vulnerabilities leading to zero-day exploits.

5G and Potential Security Risks

5G network edges are designed to support various use cases that will prove extremely important to organizations across the board, including video analytics, location services, Internet of Things (IoT), Augmented Reality (AR), optimized local content distribution, and more.

It is well documented that 5G comes with promising advancements of greater speeds, higher bandwidth, improved connectivity, and lower latency, all while handling millions to billions of devices. However, along with these advantages 5G also introduces new security challenges. 5G not only increases the *number* of devices but *types* of devices to protect, including IoT devices, sensors, cameras, virtual assistants, etc. This expands the network's attack surface, resulting in more network vulnerabilities and holes for attackers to exploit.

SASE is Crucial to 5G Succeeding

Secure Access Service Edge (SASE) is crucial to a successful 5G environment, since it enables improved services and performance, increased security, and faster infrastructure rollout and management. SASE delivers end-to-end security, visibility, and telemetry for 5G infrastructure and services; and enforces compliance through a consistent security posture across public cloud, hybrid cloud, on-premises and MEC.

SASE interworks with 5G network slicing to guarantee aggressive 5G SLAs with end-to-end security and enables flexible implementation of Gi-LAN services in various form factors.

Secure SD-WAN, a SASE component, combined with network slicing guarantees that Service Level Agreements are met, and provides end-to-end security, including UTM, IDS/IPS, Anti-Virus, and more.

SASE can also enable automated 5G rollout of thousands of devices with true zero-touch provisioning using a SASE orchestrator, and leverages elastic auto-scaling and network intelligence to meet real-time capacity demands.

5G Deployment and Environmental Considerations

Preparing for and supporting 5G networks can seem daunting. With the right tools in place, including Secure SD-WAN and other SASE functions, organizations are prepared to best take advantage of all the benefits 5G has to offer, while addressing new security threats.

Organizations can dramatically lower CAPEX and OPEX of their 5G networks by choosing:

A multi-tenant uCPE architecture. One of the key use cases for 5G is to enable multiple virtual network operators' (MVNOs') use of a shared 5G infrastructure. This is done to provide differentiated services based on the application requirement (or network slice requirement) while keeping overall costs low. This approach delivers advantages of centralized management, reducing appliance sprawl and improving adaptability. One of the core components to its success is multi-tenancy. Each tenant can have multi-

level RBAC (role-based access control) to manage the network based on the roles and responsibilities with full segmented security. Advanced solutions deliver complete segregation of control-plane, data-plane, and management-plane for each of its tenants.

A solution with options for software and hardware-accelerated encryption and decryption capabilities that provide faster processing and tamper-resistant key storage. The solutions should also support chaining the services that are running on different nodes, including third-party service functions. All of these directly tie into the 5G vision of providing unparalleled application and user performance without any compromise in security.

A single pass parallel architecture for maximum performance and lowering latency. As seen above, 5G comes with very aggressive SLA demands and organizations must change their current infrastructure to meet these demands. In a traditional mobile architecture, there are silos of point and dedicated appliances that have different functions. However, this type of fragmented architecture simply can't scale in the new era of 5G.

A single pass architecture ensures that the majority of services are performed in the same cloud-service stack, at the same location, and at the same time. This approach has the advantage of needing to decrypt a data packet only once, which is important for optimal security. This is important because the requirement to open, parse, re-encrypt and forward traffic happens only once. This also avoids expensive, high-latency packet copying, and service inconsistency, therefore ensuring that 5G SLAs are adhered to.

A solution with a single management interface to manage, configure and monitor complete 5G and SASE services, such as Secure SD-WAN and the host of additional security services mentioned above.

For all organizations, security breaches, power outages, or any accidents resulting in down-time can be extremely costly. Whether it’s a school, manufacturing facility, or a large global enterprise, ensuring a rapid 5G rollout is crucial for agile IT and meeting the new networking and security requirements of users. 5G solutions built with automation capabilities such as zero-touch provisioning can help enable rapid deployment.

About the Author

Kelly Ahuja, CEO of Versa Networks is a seasoned industry veteran with more than 20 years of experience in networking and telecommunications. He currently serves on the board of directors for two startups in Silicon Valley. Kelly spent 18 years at Cisco rooted in the design and deployment of telecommunications networks. He was most recently SVP of Service Provider Business, Products and Solutions at Cisco where he was responsible for developing and managing the service provider segment strategy and portfolio. Kelly held several other senior executive roles at Cisco, including SVP and GM of the Mobility Business Group, Chief Architect for the Service Provider business, and SVP and GM of the Service Provider Routing Technology Group.

Earlier in his career, Kelly served as VP of Marketing at optical networking startup BlueLeaf Networks and product management leader at Stratacom. He also managed the design and deployment of data and voice networks for AT&T Canada, Bank of Canada and Telesat Canada. Kelly holds a Bachelor of Science in Electrical Engineering from the University of Calgary.

https://www.linkedin.com/in/kelly-ahuja-5820772

https://twitter.com/kahuja

Company website: https://versa-networks.com/

How Does a Botnet Attack Work?

By Zac Amos, Features Editor, ReHack

Keeping up with cybercriminals is a full-time job, as new attack types appear daily. Cybersecurity analysts must consider botnet attacks among classic ransomware and phishing schemes.

How new and common are these cybersecurity threats, and how do they compete against other methods concerning the danger to companies and individuals? No matter the novelty of cyberthreats, there are always ways to reinforce prevention and prepare for breaches.

What Are Botnet Attacks?

Hackers create infected groups of devices connected to the internet, known as the botnet. They can make these machines run bots using command and control (C&C) software, and they perform everything from ransomware to distributed denial-of-service attacks (DDoS) to infect networks. Since one of the first

botnet attacks in 2004 — called Bagle — botnets have taken advantage of internet relay channel (IRC) protocols to instigate infection.

The architecture evolved as botnets advanced to disguise their activity in a few ways. They began to use fake IP addresses and HTTP protocols instead of IRC because hackers masked it as typical internet usage. This client-based system was risky since it relied on connectivity to a server connected to the herder to issue orders.

That worry dissipates with peer-to-peer (P2P) botnets since the bots can communicate with each other to perform tasks instead of being connected to a client. This decentralized nature makes them more challenging to detect.

Creating a botnet is advantageous for hackers since these groups are profitable in more ways than one. The bot herder — the hacker behind the botnet — can instigate potentially lucrative attacks and rent out the net to other cybercriminals to use for whatever purposes they desire. The botnet can stay in operation for a long time without detection, so others may find value in the network a hacker built.

How Do They Work?

Botnets initiate the same way many attacks do — they find a vulnerability. The goal is to exploit that exposure without the target knowing. They first start by creating what some analysts call a zombie army. The first objective of the botnet is to increase the number of infected devices with any method, like spam and trojan horses. Then, the herder can initialize commands to steal data or install malware.

Popular botnets have thrived for over a decade. One of the most well-known is called Zeus or Zbot. It had over 3.6 million devices in its network in 2009, but eventually, it had to rebrand and switch to a decentralized architecture to stay hidden.

Another is Mirai, which exposed the vulnerabilities of IoT-connected devices. Mirai overtook sensors and security systems to perform bricking attacks — deleting a device's firmware. To demonstrate the accessibility of botnet attacks, college students created Mirai to hack the popular internet game Minecraft — not a Fortune 100 corporation. They saw how much a Minecraft server could make a month and decided to capitalize on that as a side hustle that unfortunately went awry.

Other botnets seek to do more than just attack unsuspecting devices. Bot herders can also automate them to mine cryptocurrency, like Sysrv, especially since the prices are constantly in flux. It provides herders stability despite volatile prices if they can keep mining. This is problematic, especially since the nature of cryptocurrency is anonymous, giving botnets an extra layer of protection from identification.

What Protections Can People Take?

Technology isn't defenseless against botnets despite their durability. This is especially true since almost all causes of botnet attacks — including phishing and brute force hacks — are problems analysts must

prepare for daily. They are all considered, so they are a part of risk management programs and business continuity plans. However, nobody can ignore the impartial nature of cyberattacks — everyone and anyone should prepare, regardless of if someone is a solopreneur or a multimillion-dollar enterprise.

The ideal action is to shut down the server connecting the infected devices. This may not be effective if the herders have multiple C&C servers, but it's a great place to start in the event of an attack. Severing the tie can allow teams to scan and potentially reformat devices if necessary to remove all instances of infection.

However, the best way to protect is through preventive measures. Here are some of the top tips to safeguard any number of internet-connected devices:

- Keep systems and programs updated, including firewalls and antivirus software
- Train on best cybersecurity hygiene, like strong password creation and email management
- Stay informed on recent trends and attack methods
- Implement measures for access and permissions like zero-trust infrastructure
- Install an intrusion detection system (IDS)
- Enable two-factor authentication (2FA)

Botnet Attacks in Cybersecurity

Botnet attacks don't occur as frequently as other kinds of cyberthreats, but they often have the facade of another type of source. They can send out phishing emails or DDoS attacks, so it isn't easy to know if it's part of a botnet.

Fortunately, only a few new measures need to be implemented to respond to or protect against botnet attacks. The best protection is awareness — knowing they exist as a potential threat can help create a more comprehensive protection plan for every kind of device for the future.

About the Author

Zac Amos is the Features Editor at ReHack, where he covers cybersecurity and the tech industry. For more of his content, follow him on Twitter or LinkedIn.

How To Reduce Rising Cyber Insurance Costs When You Have a Remote Workforce

By Raul Popa, CEO & Co-Founder, TypingDNA

Like other types of insurance, Cybersecurity Insurance protects businesses in case of a rainy day. But as breaches become commonplace, insurers are running for shelter — becoming pickier about who they'll insure, and what premium they'll charge based on perceived risk.

When it comes to cyber insurance… the name of the game is risk mitigation. Insurers reward companies who take steps to mitigate risk and reduce the likelihood of payout for damages. On the flip side, many insurance providers are increasing premium prices and turning away the most vulnerable prospects.

Similarly to driving a car. If you wreck it once, your premium will jump. If you wreck it repeatedly and don't take precautionary steps to mitigate risk, you'll no longer be able to get insurance. In the long-term though, this approach is actually a good thing for all parties involved. Businesses will take steps to be

more secure — resulting in fewer data breaches and sensitive customer data spills — while insurers will have fewer incidents to pay out.

Risk mitigation pays off, for everyone.

What To Do Before Negotiating Your Cyber Insurance Premium

When it comes to negotiating the cost of your cyber insurance premium, it comes down to a simple question of preventative measures. What steps did you take to mitigate the risk of cyber breach?

A robust security structure takes time. There are a myriad of things you can do in the long term, but your remote workforce is out there TODAY. Not to worry, below are immediate steps you can take to improve your security posture — ultimately, putting you in a stronger position to negotiate your cybersecurity insurance premium.

Keep in mind, the actual cost savings from implementing the advice below will vary depending on your industry, company size, annual revenue, and the insurance carrier, among other factors. It will be important for you and your carrier to customize an insurance policy to your particular industry, business risks, and identified vulnerabilities. This is not one-size-fits-all advice. Yet, implementing cybersecurity best practices and remaining compliant with industry standards will lower your premiums with many carriers.

So what can you do to reduce the risk of a cybersecurity breach?

Perform A Risk Assessment

One of the first questions cybersecurity insurers ask is what data is at risk and what steps you've done to safeguard these assets. Analyze what may be impacted by a cyber attack or data breach, and the potential fallout from damages. Consider the cyber criminal's desire for:

- Customer data
- Financial data
- Employee data
- Proprietary company data and intellectual property
- Credentials and access

One of the key determining factors in the cost of your cyber insurance policy is the number of records you store, access, and transfer on a normal basis. One easy way to keep your insurance premium down is to tightly control the volume of records you deal with, and the access controls that protect that data.

Educate Your Workforce On Security Best Practices

The efforts of your cybersecurity team will go a long way; but they can only do so much. If your workforce is not well-educated on security protocol, or doesn't take their security training seriously, the chances of a breach are significantly higher. Take the time for ongoing security training for every team member in your company. Continue to do compliance, security, phishing, social engineering, and privacy training to ensure your employees and contractors are all aware of how to keep sensitive data out of harm's way. This is especially crucial for remote employees and the security issues that arise from insecure work-from-home environments.

Implement A Strong Password Security Policy

Weak Passwords = Big Trouble. If your employee leaves their computer at a cafe, you want to make sure it can't be easily accessed with a predictable password. Many insurers will outright refuse to insure you if you don't have a strong password policy in place. Everyone online today has heard of the dangers of identity theft, hacking, and cyber fraud, yet we consistently hear that the two most commonly used passwords are "123456" and "password." At minimum, strong passwords are at least 8 characters, do not contain words that are found in the dictionary and include a combination of lowercase and uppercase letters, numbers and symbols, and are frequently updated.

Have A Strong 2FA

A phrase we hear often: "Attackers aren't breaking in, they're logging in." Compromised credentials are the root cause of cyber breaches. And with 65% of people reusing the same password across multiple websites — including their company logins — it's easy to see why cyber insurers are nervous. With so many remote workers now either working remotely or in a hybrid manner, it is not enough to focus on firewalls or enhanced passwords – today, robust MFA must be part of every login scenario.

Least Privilege Access Control

Every team member doesn't need access to every file. Give your workforce only the access they need to perform their particular job and complete their job-related tasks. No more, no less. One of the key determining factors in the cost of your cyber insurance policy is the number of records you access, store, and transfer on a normal basis. An easy way to keep your insurance premium down is to tightly control the volume of records you deal with. The other is limiting who actually has access to those records.

Continuous Endpoint Authentication On Every Device

Cyber insurers want to mitigate the risk of a data breach. But when employees work remotely, device sharing may actually be your company's biggest threat. To reduce your premium — in addition to the tips above, you'll need to prove to your insurer that you're taking precautionary steps to ensure that only authorized employees are accessing the company laptop and the sensitive information that lives on it at all times.

Companies from highly regulated industries such as healthcare, finance, legal, customer service, and human resources have to follow strict standards to safeguard customer and company data. Educate your workforce on the dangers of device sharing. Company devices should never be left unattended, especially in a public place like a coffee shop. But even in the comfort of their homes, employees must know that sharing their company laptop with an unauthorized user is never okay — even if it's for something "innocent" like letting your kid watch Netflix on your device. One wrong click and you're risking a phishing scam, accidental file deletion, or violating compliance regulations like HIPAA, PCI DSS, GDPR, and SOC2.

Unfortunately, relying on your employees alone is more of a "hope & pray" strategy. Security teams must implement continuous endpoint authentication solutions that constantly verify an employee's identity in the background throughout the day without being a burden.

Want To Lower Your Cyber Insurance Premium? Mitigate Risk.

In a work-from-anywhere environment, company devices are more vulnerable than ever before. The biggest thing you can do to lower your cyber insurance premiums is to reduce your overall risk. While it takes time to build a truly robust security infrastructure, taking the steps we covered above like Education, Strong password policy, 2FA/MFA, Least privilege, and most importantly protecting your devices with continuous endpoint authentication will immediately improve your security posture — giving you more leverage to negotiate and reduce your cybersecurity premium.

About the Author

Raul Popa is the CEO, Co-Founder, and Data Scientist at TypingDNA — an award-winning cybersecurity startup that authenticates people by the way they type on computers and mobile devices. Typing biometrics technology is currently being used in our suite of Continuous Authentication and 2FA products. Raul and TypingDNA have won multiple awards and were featured in TechCrunch, Forbes, VentureBeat, TheNextWeb, ProductHunt, FinancialTimes, and other top publications. Raul was recognized in the Top 60 AI Influencers from Eastern Europe and was featured in the Top 100 New Europe list of influencers. As a tech innovator Raul speaks about AI, Biometrics, Identity Access Management and entrepreneurship at global events such as TEDx, Applied Machine Learning Days, World Summit AI, International Biometrics Summit, Future of AI (at European Parliament), How To Web, TechFest, any many others. Connect with Raul on LinkedIn and Twitter, or at https://www.typingdna.com/

Infrastructure-as-Code Security: a Critical Responsibility

By Thomas Segura, Technical Content Writer, GitGuardian

By large, software is still in its adolescence compared to other large-scale industries. Although its principles have been established for over half a century, it is still undergoing powerful transformations that regularly expand how it can be used. Recently, enterprises have experienced such a move with the advent of cloud computing. Moving large swaths of their IT operations to the cloud has been a massive opportunity for them to deliver new products faster. The cloud offers an unprecedented level of agility when it comes to allocating or deallocating computing resources on the fly.

But on closer inspection, we find that most of the power of the cloud relies on infrastructure capabilities. Cloud assets, cloud services, and resources, as well as orchestrators like Kubernetes, and even policies, are not managed in real-time by human operators. They are software-controlled and defined in code. Welcome to the era of Infrastructure-as-Code, or IaC!

Democratizing cloud resources

IaC is the new abstraction layer offering DevOps engineers, SRE, and developers a common language to declare what the IT infrastructure should look like: the number of servers, storage, databases, network topology, and all the basic configurations (DNS entries, firewalls, etc..).

Infrastructure is not just about production workloads. It is something required to support the entire development process. The great thing about IaC is that everyone can specify what resources are needed at every stage of the SDLC: spawn a few isolated environments at the development stage, replicate the production conditions for testing, etc. IaC is the standard language for describing these resources and how they should be configured.

This yields incredible benefits for go-to-market strategies: infrastructure becomes as flexible as the software it supports and faster to execute thanks to reusable modules, and more consistent at the same time. Maintenance costs are lowered, as is the risk of human error when done right.

Of course, as requirements become more complex, so do IaC declarations. But this is where this technology shines: having a textual "single source of truth" (meaning what's written in the files corresponds at all times to what is deployed and how it is configured), version-controlled (allowing people to inspect changes and collaborate easily) saves engineers a lot of time and headaches.

This paradigm has a name: GitOps. It allows faster and more reliable cloud-native deployments by using the same approach for managing infrastructure configuration files as for software source code. Teams collaborate more effectively on infrastructure changes and vet configuration files with the same rigor as software code. Infrastructure definitions are stored in git repositories, are incrementally modified and reviewed pull or merge requests, and finally tested and applied via CI/CD pipelines.

Since engineers are working directly with code, IaC has made infrastructure workflows shift left.

But as with everything, this comes at a cost. In this case, it is the need to shift cloud security left as well.

Securing the infrastructure with code

Regarding security, IaC has some interesting features: first, it can be used to automate the provisioning of security controls. This means that you can enforce security policies more consistently and efficiently.

Second, IaC can help you to manage your security posture more effectively. By automating the provisioning of security controls, you can more easily track and monitor your infrastructure for security issues. It can help you to identify and resolve any potential security problems quickly.

Finally, IaC can also help you to improve your incident response capabilities. You can more quickly and easily deploy countermeasures in a security incident. This can help minimize the impact of a security incident and get infrastructure back up and running as soon as possible.

But protecting the infrastructure is a considerable challenge. By blurring the line between application and infrastructure security, IaC adoption raises a big question: who should be responsible for it?

Infrastructure-as-Code is a new responsibility

It goes without saying that infrastructure security is paramount. Traditionally, specialized operations teams supervised this attack surface with many tried and tested tools. But when code manages

infrastructure, uncaught mistakes can result in sneaky security vulnerabilities. A single misconfiguration in an IaC manifest can impact runtime or network security: for instance, traffic can be left unrestricted to a resource or data mistakenly exposed to the exterior.

Not only that, but static vulnerabilities need to be specifically addressed as well: hard-coded credentials are the most critical. No matter the level of awareness about the importance of **not** storing plaintext credentials in configuration files, mistakes still happen on a frequent basis.

In fact, misconfigurations are one of the top ten vulnerabilities identified by OWASP. Therefore, it is logical to anticipate potential vulnerabilities by setting up the right guardrails to ship clean code from the start. This responsibility, part quality, part security, should be shared to implement a genuine DevSecOps philosophy. Failing to do so could mean a potentially costly security failure is around the corner.

Infrastructure-as-Code responsibility is at the crossroads between DevOps, AppSec, and CloudOps engineers. Enabling their collaboration from source to deployment is the only way for an organization to shield itself from future threats. Tools are starting to emerge to cater to this new paradigm.

Since IaC has reached new heights in the realm of automation, it is evident that automation is part of the answer. Bringing automated scanning for misconfigured vulnerabilities and hard-coded credentials will strengthen organizations' overall security posture. More than that, it will also participate in raising awareness about IaC security best practices and common mistakes.

Conclusion

Infrastructure-as-code is here to stay. The benefits it brings are entirely transforming the software development cycle and opening new doors for automation and innovation. While its advantages have been praised for some time, its associated threats are becoming more apparent. Security needs to fully embrace this new paradigm centered around the dynamism and ephemerality of the underlying resources offered by the cloud. Bridging the gap between security, operations, and development activities, leveraging automation to build efficient security solutions, will be essential for organizations to raise the bar of their security posture. The first step in that direction must be to protect their cloud infrastructure at the source code level as early in the SDLC as possible.

About the Author

Thomas has worked both as an analyst and as a software engineer consultant for various big French companies. His passion for tech and open source led him to join GitGuardian as technical content writer. He focuses now on clarifying the transformative changes that cybersecurity and software are going through.

Thomas can be reached online at LinkedIn, TWITTER, and at our company website https://www.gitguardian.com/

Managing Cybersecurity for Critical National Infrastructure

General guidelines and realities of managing a cybersecurity program for critical national infrastructure

By Juan Vargas, Cybersecurity and Engineering Consultant, Artech, LLC

What's the reality of managing a cybersecurity program for critical national infrastructure? Twenty years ago, we had no idea. Companies didn't have to get serious about protecting infrastructure until the North American Electric Reliability Corporation (NERC), in the wake of the attacks on 9/11, forced power companies into mandatory compliance with its Critical Infrastructure Protection (CIP) standards. Or an early version of them. But that change effectively created an entire ecosystem of products and services for the world of Operational Technology (OT) we didn't we needed.

While the definition of critical infrastructure may change in the future- it's been circulating in the news that the United States may expand the definition to include water plants- my background is where it all started- in power generation. Over many years I've witnessed many organizational iterations to keep up with the ever-changing nature of regulation. And it is only fair for new people to have a proper introduction to what has worked and what hasn't.

A common misconception about managing an OT cybersecurity program is that it is mostly about choosing the right software. Or the newest software. Or the most powerful software. While the software

tools have gotten significantly better, cheaper, and more effective, the biggest challenge has been managing and executing highly advanced programs with the existing talent pool. A workforce that we didn't train to use or understand IT software and executives that don't see the return on investment of these types of initiatives.

Painful as it has been, the NERC CIP standards have been widely successful in their goal to help protect critical infrastructure. The subject of how safe power plants are may be up for a deeper analysis in the future, but at least it is safer than before and gets better with every iteration. It has been so successful that it has become an international reference for others to follow. Canada and Mexico have adopted it, as well as several parts of Europe and many countries in Central and South America. It's a great starting point for any nation seeking to improve its resilience and reliability. And given that NERC revises the standards frequently for improvements, the trend will likely continue in years to come. But how does this translate into actions for a program manager to avoid the growing pains?

Understanding the usual challenges of a program manager

Let's start with what seems logical. A newly hired program manager gets support from management to roll out a program using a limited budget. The program manager knows he needs software to make it work, so he walks into a store with every possible cybersecurity software on the market. He thinks of the easiest possible solution to the problem. Can he buy cutting-edge software and ask his IT team to install and support it at the power plant? Sure. But that's a big mistake. Who is going to support it? Does IT know how the control system works? Will the control system vendor support you when things break? As it turns out, support is the keyword here and is crucial for your program's success because, otherwise, you are on your own. And soon after, you will have to become an expert in things you should not be an expert on. This approach rarely works in OT because it is very slow and costly. The program manager relies too heavily upon their ability to quickly become subject matter experts and get and retain top talent to create a customized program that works. The reality is that IT methods don't translate well into the OT world, vendors won't support your decisions, and your program will suffer greatly each time an employee leaves for a better job.

We have learned that the least expensive and most effective way to manage a cybersecurity program is by having a long-term relationship with key vendors and learning to develop three internal competencies that scale well for power plants. Those competencies follow three career paths in compliance, engineering, and operations.

Why working with vendors is important

To expand further, you are not looking for the lowest price when working with OT vendors. Instead, you are looking for a reputable cybersecurity strategy, guaranteed integration to your control system, and phenomenal customer support to get your teams the support they need. Having a long-term relationship with vendors will also help alleviate issues of talent attrition or training needs. Lastly, unlike IT vendors, OT ones have experience with power plant personnel and their operational realities.

The role of the compliance analyst

You meet your compliance needs with the help of compliance analysts. They are typically company employees, preferably people who are very comfortable with extracting and manipulating data from various sources. You also want them to be good at coding. And if someone has to know the NERC requirements is them. They may go to the plant for a few days now and then, but the bulk of their work is back at the office or perhaps at home. They aim to avoid NERC fines by generating evidence that the power plants comply with CIP standards. And you will also use the compliance data to develop your Key Process Indicators (KPIs) for upper management, and you will also use it to inform your engineering team's decisions when they do maintenance.

If your program is new and you are hiring an inexperienced (but technically sound) analyst, then the best strategy is to let them work at a single site first. Let them get acquainted with the compliance requirements and the tools available at the plant until they figure out a way to automate the extraction of this data and can do multiple sites simultaneously. Many times power companies have merged the roles of compliance analysts and engineers, but the results have not been great because often, the analyst and the engineers have conflicting interests. Conversely, a well-trained compliance analyst could easily oversee five or more plants as his methods improve. They can also train new hires, reducing the learning curve once the program is underway.

Engineers provide routine maintenance

Cybersecurity engineers are typically a rotating workforce traveling to different sites for maintenance. The right engineer will know computer systems very well and be confident troubleshooting for hours until they find a solution. Recruiting IT professionals have not yielded as good results as hiring former control engineers. Smaller companies that don't see it economically viable to employ full-time engineers can outsource these roles to vendors. They install software patches, update antivirus definitions and various software packages, and troubleshoot common issues. A trained engineer can typically complete their tasks in about one week per site. Patching every plant once a month is too costly and resource-intensive for most companies, so most power plants tend to complete these tasks at a slower frequency, for example, once every three months. Under extraordinary circumstances, NERC allows for exceptions. But in general, it is not ideal to rely on exceptions as the risk of non-compliance is higher.

The goal of the engineers is to provide a working system for compliance analysts to extract their data from and to provide company employees with the tools to protect their systems. When a change is needed, the engineers are the people that know the software intimately to make the changes. However, engineers are not the end users of most tools they help maintain.

Who are the end-users?

Letting local employees at a power plant run the day-to-day cybersecurity operations can be a controversial decision. It is the norm in the IT world to have a dedicated (read "trusted") team to handle computer security concerns and relieve employees from any responsibilities regarding configuring their

computers. However, in the OT world, your operations team has to be co-responsible for information security because they will eventually need to enable or disable features to complete their work. Install new software. Work with vendors. In general, experience has shown that relying on external engineers results in security gaps, long waiting times, and a lack of oversight and accountability.

Here's a thought experiment we can use to frame it in terms of what we already know. Most employees have no medical training, and it stands to reason that it would be dangerous for them to make medical decisions for themselves or others. However, it is a well-established practice to train employees to provide CPR and a series of first-response techniques to care for others while medical professionals get on their way. Similarly, we have to teach a subset of the power plant employees on first-response procedures to keep their systems safe because we have limited resources. The same reason we don't have doctors sprinkled around the office. That is not to say that every employee has the same level of access. Operators, I&C Technicians, and DCS Engineers may all have different access levels. And some features, like access to the firewall configuration, may not be accessible to anyone at the site. You give access to people based on what they can protect.

What does the Program Manager do?

Finally, the program manager's role is to understand the big picture. Allocate capital resources to keep the program running. Find the right talent- which is a tremendous challenge- and communicate to them what the team's vision is so they can go out and do their jobs. Also, program managers will negotiate with vendors over time to compensate for temporary talent gaps and customize their software offering to reflect changing realities. Awareness of these realities leads to another very tough challenge for the program manager: to be realistic about what the cybersecurity program can accomplish for the organization.

That last idea is often left unexplored. As advanced as your cybersecurity program may be, a great manager understands that there are many moving parts that a sophisticated attacker could exploit in ways we can't even imagine. For example, they know that they cannot have engineers deploy patches in real-time. There is a lag. And end-users can be sloppy from time to time. And no one in their organization may have the tools or expertise necessary to block or even detect a zero-day exploit. Hence it is vital to enable event logging, often to an external server, and have a contingency plan. The logs will be your black box to help you write a post-mortem and work with vendors to understand what happened. And the contingency plan will help you contain a problem as soon as it is detected. Sometimes the contingency plan is as simple as an identified uplink cable to the firewall that plant operators disconnect in an emergency to isolate the control network.

Conclusion

We've come a long way. Many companies are still trying to figure out the roles for their employees, and many are still writing exceptions because they can't keep up with patching even once a year. A few still believe they can merge OT into IT. And several others are taking advantage of the opportunities presented by the Biden administration to improve their cybersecurity programs in new ways. Some

others, mainly unregulated utilities, don't yet have a cybersecurity program. As a spectator of different strategies, I see the value of witnessing these organizational experiments and providing insight into what appears to be working best.

About the Author

Juan Vargas, a Cybersecurity and Engineering Consultant at Artech, LLC.

A graduate of Carnegie Mellon University, he started his career doing data analysis at Intel Corp before focusing on automation and control systems at Emerson Electric and finally becoming a cybersecurity expert for those systems. He has worked with most control systems in power generation and on various projects for all of the Top 10 utility companies in the United States.

Juan can be reached on Twitter @JuanVargasCMU.

Moola Market Manipulation

Why Liquidity Matters for Lending Protocols

By Professor Ronghui Gu, Co-Founder, CertiK

On October 18, 2022, Moola Market – a non-custodial liquidity protocol operating on the Celo blockchain – suffered a loss of approximately $8 million. The incident was the result of an attacker manipulating the price of the platform's native $MOO token, which allowed them to use the inflated price of their $MOO collateral to borrow additional tokens from the platform.

The attack flow was nearly identical to the Mango Markets incident that occurred the week prior, in which an attacker also borrowed the illiquid native token of the lending platform, manipulated the price higher, and then used this newly inflated value of their collateral to borrow an outsized amount of the protocol's assets.

In both cases, the attacker returned most of the funds they had obtained. Moola Markets negotiated with the attacker, who returned 93.1% of the funds in return for a $500,000 bounty payment. While this prevented Moola liquidity providers from being as negatively impacted as they could have been, DeFi

platforms cannot rely on retroactive bounties from attackers who decide to adopt the role of a white hat hacker after the fact.

The market liquidity of a token should be a primary consideration when deciding which assets can be used as collateral on a lending platform. Illiquid tokens introduce a much greater risk of being manipulated in a way that breaks the intended functioning of the platform. In the case of the Moola incident, the attacker only required approximately $133k worth of $CELO to pump the price of $MOO from $0.018 to a peak of $3.58, representing a gain of nearly 20,000%.

In deeper, more liquid markets, the cost of such an attack increases dramatically. It would take an astronomic amount of money to manipulate the price of blue-chip assets by the same magnitude.

This was a flaw in the design of the protocol. It was not the result of an error in the platform's smart contract, but rather a lack of foresight when choosing which assets could be used as collateral. While it remains unclear who the perpetrator of the Moola Market manipulation was, they would likely defend their actions not as an attack on the protocol but rather as a "highly profitable trading strategy," to use the words of the Mango Markets exploiter.

Lending platforms want to incentivize the usage of their token, and allowing it to be used as a collateral asset is one way of doing so. However, if liquidity is insufficient to prevent attacks such as these, this ends up being a short-sighted strategy, as there is unlikely to be any demand for the token of a broken platform that opened its users up to potentially devastating losses.

In addition to the careful selection of collateral assets, DeFi platforms have a range of tools at their disposal to protect their protocols and its users. On-chain monitoring services such as Skynet that continuously scan the blockchain for suspicious activity can raise the alarm minutes before an attack can be carried out.

Careful design choices, pre-deployment auditing, and post-deployment monitoring can all combine to raise a protocol's level of security to the highest possible standard. A meaningful commitment to security is not just the right thing to do, it's also a no-brainer from a business standpoint. DeFi protocols that take security seriously demonstrate to potential users that they intend to be around for the long term, which is crucial when it comes to attracting the liquidity and day-to-day usage that makes a platform thrive.

DeFi's transparency is one of its greatest strengths. It means on-chain security incidents can be quickly diagnosed and addressed, not just by the team behind a platform that suffered the exploit but also by the developers of other platforms that may share similar vulnerabilities. But these lessons are not always learned as quickly as they should be, which leads to DeFi's transparency becoming one of its greatest liabilities. Copycat attacks are trivial to carry out when the exact attack flow of a previously successful exploit is permanently written into the chain.

The fact that Moola Markets suffered the same fate as Mango Markets did just a week prior is illustrative of this conundrum. In order to make transparency a powerful strength rather than a critical weakness, DeFi and Web3 projects need to move quickly to address vulnerabilities and mitigate risks as soon as they appear. Security does not end after a project is deployed. It needs to be integrated into all steps of the process, from design, to deployment, and beyond.

About the Author

Professor Gu is the Tang Family Assistant Professor of Computer Science at Columbia University. He holds a Ph.D. in Computer Science from Yale University and a bachelor's degree from Tsinghua University. He is the primary designer and developer of CertiKOS and SeKVM. Gu has received: an SOSP Best Paper Award, a CACM Research Highlight, and a Yale Distinguished Dissertation Award. Prof. Gu is on Twitter at @guronghuieric and CertiK's company website is http://certik.com/

Remote Workers Face Growing Threats from Phishing Attacks

Analysis Shows Phishing Strikes Up 61% Over 2021, With a 50% Increase on Mobile Devices

By Patrick Harr, CEO, SlashNext

Hybrid offices and BYOD policies have reorganized the workplace forever, and this shift has also amplified the risks of phishing attacks on remote workers. Security teams need to protect against phishing gangs that increasingly breach organizations through clever social engineering scams on employees' personal devices, or through private messaging apps such as SMS texts, Slack, and WhatsApp.

Cyber attackers employ nefarious social engineering techniques such as spoofed websites or fake links to deceive people into giving away sensitive data by mistake. The attackers can then use the breach entry point to install malware on an organization's infrastructure, such as encrypted ransomware for extortion purposes.

The recently released SlashNext State of Phishing Report analyzed billions of link-based URLs, attachments, and natural language messages sent by email, mobile, and browser channels over six

months in 2022. The in-depth analysis identified more than 255 million phishing attacks in 2022, or a jaw-dropping 61% increase over 2021.

In addition, the detailed analysis revealed a 50 percent increase in attacks on mobile devices, with scams and credential thefts topping the list of payloads. This disturbing growth trend seems to highlight that prior security strategies – including secure email gateways, firewalls, and proxy servers – are no longer adequate to prevent the latest phishing threats.

At this point, the cybercriminals know that most email systems have at least some phishing protections in place. They also know that more employees are using their personal mobile devices for work purposes. This transition has greatly increased the number of attacks targeting mobile devices and other communication channels.

Even more alarming, the bad guys have updated their strategies to launch more phishing attacks from trusted services and messaging apps. In fact, the threats from trusted services such as Microsoft, Amazon Web Services, and Google are up 80% this year, with nearly one-third of all threats (32%) now being hosted on such trusted services.

For many businesses, this increase in mobile phishing and credential harvesting has incurred costly data losses, harmed brand reputations, and hurt the bottom line. And as the phishing landscape continues to evolve and expand, the cybercriminals have become even more sophisticated in their use of software automation and AI technologies to launch zero-day threats.

Such zero-day threats are designed to make the biggest impact and wreak the most havoc before security controls can detect and block them. In turn, more than half of all threats now detected (54%) are defined as zero-day threats, marking a 48% rise over the prior year. This uptick reveals how the hackers have shifted to more real-time technologies to improve their success rates.

The Easiest Phishing Targets Are Distracted Employees

Fallible people continue to be the most vulnerable attack surface for phishing breaches. The attackers have adjusted their fraudulent methods to meet targets wherever they use digital devices for both work and personal purposes. One of the most damaging problems involves credential harvesting from an unwitting employee's personal account on a mobile device.

Such threats can be launched through link-based attacks, malicious attachments, or natural language conversations that are highly personalized to trick the victim. Someone posing as an internal IT technician can catch a distracted employee off-guard with an urgent request for logins to perform troubleshooting, and that may be all it takes to breach the entire system.

Yet the crooks require less time and effort to launch such personalized attacks today, due to the growing use of automation and machine learning. Cybercriminals can now send out thousands of targeted spear-phishing attacks to detailed lists of targets, creating highly unique and customized lures. This technique enables the bait to bypass many threat detection engines for hours and sometimes even days, giving the attackers a huge advantage.

Providing cybersecurity training to employees should always be part of the solution, but training alone cannot stop the speed, scale, and sophistication of never seen, zero-day attacks. Furthermore, many

current security tools and processes – such as reputation-based and relationship-graph technologies – can no longer keep pace with many of these newest attack vectors.

Armed with stolen logins and passwords, the hackers can then penetrate an organization laterally. Once a user's credentials have been compromised, the threat can be devastating to an enterprise. The effects may include the loss of critical business data, customer information, and intellectual property, resulting in lawsuits, financial payouts, and reductions in shareholder value.

New phishing safeguards should be deployed wherever employees communicate today, whether for personal or work reasons. This includes collaboration apps such as Outlook, Gmail, LinkedIn, WhatsApp, Telegram, Slack, Microsoft Teams and more. To stay protected, organizations must move from traditional practices and last-generation tools to a more modern security strategy.

The adoption of real-time, cloud-based AI phishing controls that can address all types of attacks will be essential, along with multi-layered protections that preemptively hunt for threats and scan for breaches in real-time. This is the only way for security teams to keep their remote workers protected from zero-day threats across all potential attack vectors, including email, mobile, and web messaging apps.

About the Author

Patrick Harr, Chief Executive Officer, SlashNext. As CEO of SlashNext, Patrick Harr directs a workforce of security professionals focused on protecting people and organizations from phishing anywhere. Before SlashNext, Patrick was CEO of Panzura, which he transformed into a SaaS company, grew ACV 400%, and led to successful acquisition in 2020. He has held senior executive and GM positions at Hewlett-Packard Enterprise, VMware, BlueCoat and was CEO of multiple security and storage start-ups, including Nirvanix (acquired by Oracle), Preventsys (acquired by McAfee), and Sanera (acquired by McDATA).

Patrick can be reached by email at patrick.harr@slashnext and on Twitter at @patrickharr and at our company website https://www.slashnext.com/.

Secure APIs to Drive Digital Business

By Mourad Jaakou, General Manager Amplify at Axway

Back in 2010, API Evangelist blogger Kin Lane posited that application programming interfaces (APIs) are driving the Internet and our economy. A decade later, we are seeing the prescience of that statement everywhere. From users to bots and applications, to a myriad of cloud services, everyone is leveraging APIs to implement a wide and growing range of functionality to serve our modern digital infrastructure.

But the rise of APIs and the benefits they provide also brings with it the risk of data exposure, which can jeopardize business continuity and user trust. Consider how an issue involving the ODdata API on the Microsoft Power Apps portal compromised sensitive data from large U.S. companies and various government agencies in summer of 2021. In addition, the IBM Security X-Force Cloud Threat Landscape 2021 report suggests that APIs would be involved in two-thirds of the cybersecurity incidents examined.

Meanwhile, in the era of digital transformation and API development, Zero-Trust Architecture (ZTA) has emerged as a critical approach to maintaining the security of enterprise infrastructure. The Cybersecurity Executive Order signed by President Biden last year required this type of "Zero Trust" architecture within some jurisdictions. As a result of the executive order, many companies have also included the implementation of this type of architecture in their roadmap. In this context, the combination of API-based technologies and ZTA could be decisive in the fight against relentless cyberattacks.

Addressing API vulnerabilities

Until now, organizations have often approached security by placing their trusted infrastructure and applications within a defined perimeter, with a key priority of protecting the company's assets and networks from unauthorized external access. Unfortunately, just because the hosts that share a trust zone are nominally protected from hackers outside the enterprise does not mean they are sufficiently protected from each other.

In fact, systems were left at greater risk of attack as intruders posed as internal users to breach perimeter security and then move freely across the network. A hacker could then access the victim's internal resources and steal information. The perimeter is no longer an effective barrier to intrusion, whether it's due to resources being increasingly moved to the cloud or the widespread use of telecommuting.

APIs are major entry points into systems and will continue to be key elements of data access management. But their usual defense mechanism - the use of API keys to limit access to a certain API - has shown its limitations, particularly because the keys can be stolen or are already in circulation. This weakness, now identified, makes it more difficult to validate the true identity of the caller when submitting an API.

Reduce the security perimeter to protect individual assets

To ensure enterprise security, strong authentication techniques and ensuring proper API configuration have become essential. And the ZTA approach can provide just that extra layer of protection.

However, it is critical to remember that a ZTA is not a standalone IT infrastructure architecture. It is an approach that recognizes that attacks can come from both inside and outside the network and, therefore, no one can be trusted, not even bots.

The "Zero Trust" approach includes a set of best practices to strengthen security through more sophisticated protection of corporate assets. For science fiction fans, you could think of it as force fields around each asset: in this case, it makes more sense to consider individual protection than to try to protect the whole spaceship.

Accessibility must remain an essential consideration

Implementing a ZTA infrastructure means that internal and external entities are treated the same. Neither can access resources until they have been validated and have proven to be who they say they are, according to the company's rules. This rigor applies to all resources and communications, which must be governed by well-defined access restrictions. Applications and services must constantly authenticate any entity attempting to access a resource.

Organizations must therefore focus on certain key considerations, such as whether it is acceptable for each person to access a particular piece of information from a given location, regardless of where they are located. Can this microservice accept data from another microservice?

The ZTA approach has a basic two-step method for establishing and governing policies for these decisions: on the one end, policy decision points (PDPs) are used to model and govern the policies. On the other, policy enforcement points (PEP) enforce those decisions.

Organizations that use many APIs can do this most effectively with an API gateway (or, as frequently happens in larger organizations, multiple gateways) – but a truly universal approach to API governance is needed for the most accurate view.

Universal governance doesn't mean adding more gateways; different teams may want to keep their API gateways from different vendors or with different configurations. Rather, it is a governance layer that offers greater control over security and compliance for all APIs. Teams should be able to keep their flexibility, and the organization gets the final say in what is exposed or not.

Observability is key: only a complete, centralized overview of all APIs, regardless of where they are – vendor-agnostic, multi-cloud, on-prem, hybrid – can bring all of an organization's APIs securely into view.

If you rely on an API gateway to accelerate ZTA efforts, be sure to adopt a token-based API access and authorization solution (e.g., OAuth or OpenID Connect) if you don't already. By combining the two – universal API governance and a token-based strategy for API access and authorization – it is possible to implement the strategy of least privilege, a security concept that limits a user's level of access to only the task at hand.

A secure foundation gives organizations the confidence to open up

To meet complex enterprise security requirements and adapt to the future, ZTA infrastructure that uses APIs, token-based access, and authorization in addition to API gateways, can be customized through distributed policy enforcement.

In the era of multi-cloud, on-premises, and distributed installations, these capabilities will prove increasingly important for anyone looking to improve API security in the short and long term. But ultimately, the true value in API development is realized when they are adopted, not when they are built or secured.

A recent study on API adoption found that 96% of IT decision makers are prioritizing securing digital experience in their API initiatives right now. But just as many of them (97%) are also seeking to improve customer experience, and 84% hope to enter new markets with their APIs.

A secure foundation gives enterprises the confidence to unlock the true value of API products by exposing them on an API marketplace. By bringing them into one place for better adoption, management, and security, it is possible to fulfill the true potential of APIs to drive faster digital business outcomes.

About the Author

Mourad Jaakou is the General Manager Amplify at Axway.

Axway helps companies move forward faster and create brilliant digital experiences using our Amplify API Management Platform and proven MFT and B2B integration solutions. Mourad's mission is to support and accompany customers to succeed in their digital transformation. After a degree in network engineering and early experience as an enterprise application integration (EAI) consultant, Mourad joined Axway in 2007 where he held various positions as EAI consultant and Senior Project Manager before joining and leading the EMEA Presales Consulting team. Strong with his 13 years of Presales experience managing and supporting large customers, a robust understanding of APIs, and a willingness to help companies to grow their business, Mourad was appointed General Manager of the Amplify offering in 2022.

Mourad can be reached online and at our company website https://www.axway.com/en

Security in gaming: How to Recognize and Prevent Social Engineering Attacks in Gaming

What is social engineering?

By Jenna Greenspoon, Head of Parenting, Kidas

As an avid internet user, it's likely that at some point, you received an intriguing email with a subject that says "Congratulations, you have won a…". This is a scam used by exploiters to make you click on a link that then introduces malware to your computer. It's called social engineering.

Social engineering is when an exploiter takes advantage of human behaviors and natural tendencies. By analyzing how users interact when faced with an everyday scenario, social engineering occurs by exploiting human psychology to manipulate people into making security mistakes and giving away confidential information. While this has been happening on the internet for decades, it's now happening to gamers, many of which are too young to decipher the dangers.

First let's take a look at how a social engineering attack happens. It's more than just the click of a link, and happens long before the first click.

- First, the potential victims are identified. Next, a lot of background research is done on the potential victim. They find out how they can best be exploited psychologically and then they select their attack method.
- The attacker then starts attempting to psychologically take control of the victim by engaging with them. They spin a story and then begin taking control of the interaction.
- Over time, they start executing the attack using the information they gained from the victim.

- After the victim performs the expected response, the intruder takes the confidential information by sabotaging the system, and when they are done, they remove any trace of evidence and close all conversations.

Types of social engineering attacks in gaming

Phishing

When it comes to gaming, phishing is used to gain users' credentials to take over gaming accounts. This is the most common type of social engineering attack in gaming. Here, the attacker makes the victim feel a sense of urgency or fear that tricks them into sharing confidential information. Phishing scams include fake websites that have an in-game money generator or enter to win type games. To use it, gamers have to login with their gaming account credentials. Once the credentials are shared, scammers are able to access sensitive information related to the gaming account and the victim.

Gaming scams have become much more advanced. In games such as CS:GO, scammers have created fraudulent stores where players go to buy weapons for the game. These stores look very real and deceive gamers to take over their accounts and steal their money.

Baiting

Baiting is when the attacker sends a fake offer as bait and takes advantage of the user's interest or curiosity. This may be done through offers to earn free Robux or V-bucks, in-game currencies. An example of this is an offer for a free gift card or free software which then gives the opening for malware to be downloaded onto their computer.

Cheat programs

Gamers everywhere want to achieve the best score or the best time, even when they aren't formally competing. Many gamers use cheat programs to improve their scores, however, they can get cheated themselves. Cybercriminals create fake cheat programs which do the opposite of what the gamer believes they were built to do. The fake cheat programs steal players' data and can negatively affect computer performance.

Malware & Unwanted software

Cybercriminals frequently distribute malware and unwanted software, most often on multiplayer gaming platforms. Since a large number of gamers on multi-player gaming platforms are kids and teens, it's important that they're educated on cybersafety. Scareware is an example of unwanted software. While it has no benefit to the user, after being bombarded by 'danger' popups on their computer, the victim is

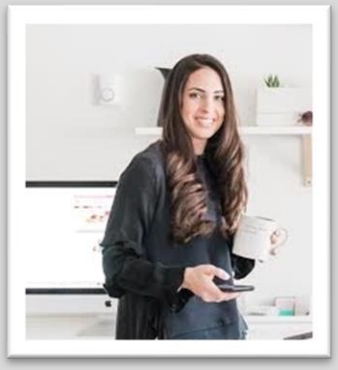
enticed to click the download button to “protect” their computer. At this point, they are redirected to malicious sites or they download the malware directly onto their computer.

How to prevent social engineering attacks

In order to prevent social engineering attacks while gaming, it is important to be very attentive in discerning a real offer from a fake one. Here’s how to do so.

1. Use a unique, strong password for all of your gaming accounts. Ensure that each account has a different username and password so that if one password is stolen, it can’t be used on every other account.
2. Download games from safe sites and official stores whenever possible. Read reviews before you download.
3. Do not open or click on any links that come from an unknown source, a pop-up or an unsolicited message. Pay close click attention to the website address if you end up on a website you were directed to. If it doesn’t feel right, it likely isn’t.
4. Don’t download cheats or any other illegal content. The repercussions are not worth it.
5. Avoid sharing personal information. If you receive an email or text message asking for your gaming credentials or other personal information, ensure that you thoroughly verify the sender’s identity before sharing any information.
6. Watch out for tempting offers! If you feel it is too good to be true, it likely is. You can always check its validity by searching on google. Don’t be fooled by a too-good-to-be-true offer. Pay close attention to the website link of the offer. If it doesn’t look legitimate, it likely isn’t.
7. Use multi-factor authentication. This is a great safety precaution that we highly recommend for all gaming accounts. By using multi-factor authentication, your login credentials will be verified by more than one means.
8. If you are gaming on a computer, install an antimalware solution and keep your operating system software up to date. This will keep you on top of any security issues.
9. Be careful about what private and personal information you share on social media or in other public forums like gaming chats. Sharing personal information makes it easier for attackers to gain access to information about you.
10. If your child is a gamer, keep the lines of communication with them open and educate them about cybersafety. Set up their gaming accounts with them and remind them the importance of asking for help if someone sends them a link, sends them an offer or asks them for personal information.

About the Author



Jenna Greenspoon is the Head of Parenting at Kidas, a technology company focused on developing anti-cyberbullying and predator protection software for PC games. Jenna was an educator and administrator in the education system working with both students and their families.

Jenna can be reached online at jenna@getkidas.com and at our company website www.getkidas.com.

Table Stakes Security Services for 2023

By Jim Mundy, Director of Security Operations, Segra

Most business owners may be aware of cybersecurity defenses such as firewall, DDoS prevention, or various endpoint protection solutions, and assume some form of each may be included in the security package sold to them by a carrier or managed IT service provider. However, due to the advancement of IoT, a more remote workforce, and increases in the sheer number and complexity of cyberattacks, there are next generation versions of each of these forms of protection available to owners and IT leaders that are now table stakes security services to protect their business.

Last year, 61% of small to medium sized businesses admitted they experienced a cyberattack, according to Verizon's 2022 Data Breach Investigations report. As we enter 2023, small and medium sized businesses will need to make sure they (and their stakeholders, customers, etc.) are protected against traditional attacks such as DDoS and phishing along with more current and sophisticated attacks such as ransomware.

General Firewall vs Next Generation Firewall

When we are talking about cyber security in a business, people think about a firewall. Firewall has gone from a simple box that essentially did much what a router did in the past, plus some extra security features, but the industry has now moved to a more robust solution called next generation firewall.

Next generation firewall picks up some additional functionality that can happen in the device or firewall service including web filtering, antivirus services, and intrusion prevention, which are all cybersecurity solutions that any business would need.

Web Filtering: This function gives business owners the ability to block websites or allow them with some limitations. Categories can also be included to filter out the types of content allowed. Web filtering was a separate box in the past but now it's functioning inside the next generation firewall.

Network Antivirus: Another function that the next generation firewall can perform is the antivirus protection. In most cases people are used to using software such as Norton or McAfee separately. These security applications live on the end user's device or the network server. The problem with this is that these antivirus solutions only target things that arrive at the device after traversing the network. An example of this would be if someone was to open a web page and click something leading to a virus. Network antivirus will monitor the network traffic as it enters the firewall, detect the virus, and stop it. This firewall-based network antivirus feature does not replace antivirus software running on devices but rather compliments it.

Intrusion Prevention: In this case, a firewall would block the same way it would a virus but instead of a specific virus file targeting a machine, it goes after attacks that are targeted to a particular operating system or application that lives on one's network. If there is a main file server that lives in one's office and it runs a certain version of a program that's known to have a vulnerability, this is where intrusion prevention would be helpful. As traffic comes in, intrusion prevention looks at what appears to be an effort to exploit a vulnerability, detects and stops it.

When looking at web filtering, network antivirus, or intrusion prevention services, it's important to remember that these threats change constantly. Protection should not be purchased only once because a single installation of software won't provide a stream of constant updates. What will allow updates are subscribing to more evergreen, managed services solutions such as hosted or cloud-based firewall capabilities delivered as a service.

Physical vs Hosted/Cloud Based Firewall Capabilities

Firewall is essentially available in two formats. One is a physical box that is placed into a location that would typically sit between the internet and the rest of someone's network. The hosted or cloud-based firewall sits in the cloud, taking the internet with it.

Cloud firewall can be built with geodiversity, where multiple cloud-based firewall platforms operate and allow continued secure connection to the internet even if one of the cloud platforms should suffer a connectivity or device failure. If a company with many locations were headquartered in Charlotte and had a physical firewall at that data center, and there was an issue with the fiber going into that data center, all the offices that are connected would be down because the Internet lived at the corporate headquarters. This level of diversity and availability is difficult to duplicate with a premise-based firewall solution.

Cloud-based firewall solutions are particularly beneficial for businesses and enterprises with multiple locations, as they eliminate the need for multiple boxes and receive constant updates if the firewall is hosted on the cloud. Cloud-based firewalls bring multiple capabilities such as not worrying about the capital expenditures of buying a box, having high availability, and geodiversity.

DDoS Protection vs Carrier-based DDoS Solutions

The next table stakes security issue is paying attention to DDoS attacks, which is an attack from multiple locations around the internet all coming into a central point with the goal to overwhelm the protection that sits there, the firewall at the end, or to overwhelm a web or application server. DDoS attacks usually intend to either take a company out of service or for some type of a political statement.

A firewall itself can prevent DDoS, but if the firewall is busy worrying about throwing away the trash that's coming in with an attack, it would become overwhelmed, causing the end goal of a DDoS attack to be achieved since the firewall stops doing its primary function.

The best way to combat a DDoS attack is to let a carrier deploy protection in their network, preferably at the very edges of a network, which is known as carrier-based DDoS solutions. The value of that is if multiple businesses are located in the same general market and one of those is attacked, it could impact everyone, not just the targeted business due the overall network being overwhelmed. By pushing that mitigation of the attack as far out as possible, such as to the edge, nobody sees it and the attack is prevented by the carrier.

DDoS protection should be considered regardless, but the more optimal way to deploy it would be to use carrier-based DDoS solutions as they gain the benefits of being able to push it out to the edge.

A carrier deployed DDoS protection solution may also benefit from threat intelligence related to attacks around the country or the globe. This intelligence allows an attacker’s signature to be known even before the attack spreads to the carrier’s edge.

Endpoint Protection vs Holistic Endpoint Protection Solutions

The next thing that would be considered table stakes is protection of the end points in a network, known as endpoint protection or EPP. When you go online to a secure website, such as an online banking login page, you would most likely see that little lock on the left side of the address bar, which basically means that traffic is being encrypted.

Encryption is a good thing, but as more and more Internet traffic becomes encrypted, firewall itself can't see what's going on as traffic passes through, so threats are going to get through to the end user's computer. Something may look normal to the user but could contain a virus or malware.

And just like the firewall needs to have those regular updates, it's terribly critical that endpoint protection software is updated continuously, also. Buying EPP individually and putting it on individual computers is good, but it's not ideal. What you want is a holistic endpoint protection solution for a company. A holistic

approach could allow business owners to apply the company policies down to the computers, be alerted when someone's computer is faulty or get an alert to quarantine a threat.

Zero Trust Access Policy

As attackers get more sophisticated and are able to hide in a network and impersonate legitimate users it is table stakes to implement a zero trust solution. The solution is not a single device or application but applying the zero trust principal to all users and all traffic. This principle states that no user or network connection should be allowed access to a network or application without first confirming who is connecting, what their role is, and if their role had a need and the authority to access the network or resource. Zero trust policy is implemented in firewalls, network devices, applications, and end point protection.

Overall, downtime due to data breaches or non-compliance can cripple a business, causing financial issues and impacting one's business operations. Relying on firewalls and antivirus software is no longer enough to protect an organization against threats – a holistic approach to cybersecurity needed. The solutions mentioned above will help provide a well-rounded approach for small and medium sized business owners to have a more effective and safer network by looking for threats at the endpoint, firewall, or out into the edge of the carrier's network.

About the Author

Jim Mundy is the Director, Security Operations at Segra. Jim leads the security operations center team of cyber security engineers and analysts who are responsible for the full lifecycle of Segra managed security from policy review and implementation, upgrades and changes, and repair support for Segra's customers. The SOC team at Segra also manages the daily care and sustainment of the firewall platforms and security applications used to deliver the managed security services. Jim and the team are actively involved in the development and roll out of new cyber security services and continuous improvement of the products and processes within the area of customer managed security.

Prior to joining Segra, Jim worked as a Sales Engineer, Sales Engineering Manager and Product Manager for companies in the telecommunications and managed service provider space. Jim is a Certified Information Systems Security Professional (CISSP) and has recently held Cisco professional level network and voice certifications. Jim has also worked as an entrepreneur - starting PaxNet, an ISP in Greenville South Carolina, which he later sold to NewSouth Communications. Jim began his telecommunications career in a family-owned cable television company and has more than 20 years of experience in the industry.

For more information about Segra, go to www.segra.com.

The 'New Cold War' Continues To Mark Urgency For Organisations To Bolster Cyber-Resilience

By Dave Adamson, Chief Technology Officer at Espria encourages businesses to re-claim authority over their networks, thereby enhancing cyber-resilience in the wake of current geopolitical conflicts.

It's no secret that the consequences of the Russia-Ukraine war are widespread, impacting the world in ways no one could have foreseen. As the tension continues, organisations have noticed a sharp increase in cyber-attacks. According to Bridewell Consulting's research, 86% of organisations have reported an increased number of cyber-attacks since the start of the Ukraine war and 69% worry their systems are vulnerable to attack. With sustained attacks including DDoS, new data wipers, phishing campaigns and malware on government organisations, businesses across the globe are in danger of being caught in the cyber-crossfire.

The cyber threats are particularly concerning for critical infrastructure where IT and OT/ICS are highly interconnected. In these circumstances, a compromise may have a domino effect leading to potentially devastating consequences. While nation-state hackers may display a sense of focus and restraint, an ad-hoc army of freelance hackers is more unpredictable, leading to new vulnerabilities for both people and businesses.

This surge in cyber-attacks creates a unique sense of vulnerability for businesses. With heightened cyber-risks, there is an urgent need for organisations to become cyber-resilient. The Government department for Digital, Culture, Media & Sport (DCMS), along with Julia Lopez MP has urged businesses and charities to strengthen their cyber security practices now. This comes at a time when the National Cyber Security Centre has published guidance on the steps organisations can take when the cyber threat is heightened.

It's imperative for businesses to focus their attention on their cyber security efforts, starting with what has failed in the past and seeking solutions to address these failures. This will allow businesses to learn from previous mistakes and take ownership of their own network security, or risk being collateral damage in the cyber crossfire.

Aligning digital transformation with cyber-resilience

Many businesses fast-tracked their approach to digital transformation during the Covid-19 pandemic. As such, organisations were forced to ease security procedures to help staff adjust to remote working, creating a variety of security issues. The emerging all-digital lifestyle and work-from-home environment will continue to complicate cyber security and give criminals new vulnerabilities to attack.

In Deloitte's recent article on the impact of Covid-19 on cyber security, it highlights a Swissinfo.ch report of figures from the NCSC (National Cyber Security Center) for June 2020. These figures indicated individuals working at home do not have the same level of inherent protection/deterrent measures compared to an office working environment.

Reimagining traditional password security

The main reason criminals easily gain access and command over a network is due to the inherent weaknesses apparent in the traditional approach to network security. In the office workspace, organisations distribute passwords to their employees directly, rather than having an employee craft a key themselves. The power lies in the hands of the business, rather than the individual.

But when companies went digital, they flipped that process around. Suddenly, they let their employees create their own keys to every system, transferring ownership and control of access to them. From that moment, organisations no longer knew or had control over when, where, and how employees would share, lose, or reuse passwords.

The ability for employees to share, lose, and reuse their passwords without their organisation knowing, leads to tactics such as phishing, social engineering, credentials stuffing and password spraying to allow cyber criminals to get past unsuspecting users.

Cyber criminal's access points

Loosening the security rules and regulations on staff to support remote work, continues to cause several security issues.

For instance, it has proven to be problematic to blindly give untrained staff permission to connect their personal devices to the enterprise network or use employer-supplied computers for personal use. Doing so can create various problems, even something as simple as clicking on a phishing link within a personal email, can cause enormous disruption, if only to the work flow of the IT team tasked with resolving the issue.

The problem is compounded as employees increase the chances of a threat through their personal Wi-Fi networks that have no security policies in place. Once connected they're often using a VPN, granting open-ended authorisations to access entire suites of corporate files and data, without background verification checks or security reviews.

Regain control of your network, before it's too late

Businesses should invest to secure their networks. They should adopt a high-bandwidth network infrastructure, upgrade security protocols, establish internal policies giving guidelines on how employees should protect company data and information, and improve password protection by enforcing multifactor authentication.

Faced with the increased risk of getting caught in the cyber crossfire, it is not too late for organisations to take responsibility for the security of their networks and make their digital infrastructure cyber-resilient.

About the Author

Dave Adamson, Chief Technology Officer at Espria. He is a gifted IT professional with extraordinary breadth and depth of knowledge. Dave is a creative problem solver who remains calm under pressure and his ability to understand, translate and fluently communicate complex technical concepts across audiences is impressive. He can be reached online at Enquiries@espria.com

The Benefits of eBPF for API Security

By Sanjay Nagaraj, Co-Founder & CTO of Traceable AI

You might hear the term “eBPF” mentioned when chatting to DevOps and DevSecOps folks about network, infrastructure or security management. eBPF (extended Berkeley Packet Filter) is based on a Linux kernel technology and opens the possibilities of monitoring and other capabilities to be done on top of the operating systems used mostly for the cloud. As developers continue to learn to utilize eBPF capabilities, the potential to radically advance infrastructure, application and security tools is immense. This definitely is the case as it relates to API security.

What is eBPF?

eBPF is a technology with origins in the Linux kernel that has been shipped since 2014, which was also when the first Kubernetes commit was made. In contrast to most of the developer code that is written in user space, employing eBPF necessitates writing code in the kernel, which has clear benefits in terms of performance and resource usage.

Teams that work in high-performance environments frequently use eBPF. For instance, Facebook has roughly 40 eBPF programs active on every server with an additional 100 eBPF programs spawned and

terminated as needed, compared to Netflix, which has about 15 eBPF applications operating on each server instance.

The Value of eBPF

eBPF is crucial for businesses that are seeking high-performance security requirements. Think of it as a [web]space telescope that offers businesses performance benefits while providing previously unattainable views into their APIs.

Three areas in how eBPF brings value include:

-Non-invasive observability of system and workloads

-Efficient virtual networking

-Enables innovation around the core of the operating system – vast untapped potential

Why is eBPF Important?

Two areas where eBPF really shines regarding API security are observability and monitoring:

1) Observability - When filtering network packets, eBPF was first applied to improve observability and security. It has, however, evolved into a means of making the use of user-supplied code safer, more practical and more effective over time. eBPF is presently utilized in numerous applications due to its growing popularity. The use of eBPF enables major cloud providers like Netflix, Facebook, AWS, Google, and Microsoft to offer new cloud tools and capabilities. To get the application data, eBPF helps with:

· Metrics

· Tracing

· Logs

· Exception

2) Monitoring - Deep API traffic data, such as request/response headers and bodies/payloads, can be displayed using the eBPF-based data collection for both North-South and East-West traffic. Because it operates at the kernel level, this data collecting is out-of-ban, non-intrusive, quick, and extremely efficient. Additionally, this high eBPF efficiency produces a nearly negligible overhead (difference in latency of less than 1ms) on instrumented applications.

How Does it Work?

With the help of eBPF, programmers can run code in the kernel's privileged environment and see how the kernel responds to specified triggers such as system calls, network events, kernel tracepoints and

function entries. The ability for user space applications to read and respond to data from kernel activities is effectively enabled by eBPF in this case. eBPF ensures the safety of the kernel and other processes running on it by requiring validation before it runs programs in a kernel sandbox. The eBPF framework is already widely used, particularly in cloud-based applications and is native to all contemporary Linux kernels and is also accessible in Windows.

Advantages of eBPF

The biggest advantage of eBPF comes from its ability to pull deep data from the application environment. When this is combined with the right security solution can give a 360-degree view of observability and visibility into all API activity. This provides visibility into how an API is working. This allows unprecedented insight into security incidents, which can assist in prevention by seeing where issues might arise. Another advantage is how APIs can be built on top of eBPF, which can more easily achieve isolation of services when under attack.

The list of innovations will expand and change as eBPF continues to draw more extensive and mainstream attention and as the industry learns more about how to build value on top of it. Infrastructure, application, and security management will have a bright and exciting future thanks to eBPF. That is why we must continue to leverage eBPF to increase the effectiveness and efficiency of API security. End of article.

About the Author

Sanjay Nagaraj is Co-Founder & CTO of Traceable AI and an entrepreneur and a silicon valley engineering leader.

Sanjay believes in building products and teams that are obsessed with customer's success. Prior to co-founding Traceable, he was VP Engineering for AppDynamics/Cisco. At AppDynamics he was responsible for product teams for Application Performance Management and Database Monitoring products. He was responsible for scaling teams across different geographic locations. The innovation that he and his team built was critical in helping DevOps teams to lead the digital transformation at many of fortune 100 companies. The customer obsession of his team and the products at AppDynamics he was responsible for generated over half a billion dollars in revenue during his tenure.

As a senior engineering leader, he has been building complex enterprise software solutions for over 20 years. Sanjay received his BS in Computer Science from University of Mysore. Prior to AppDynamics, Sanjay worked at various companies including Hyperion Solutions (Oracle) and Philips. Sanjay is an inventor credited with 10+ US Patents.

https://www.traceable.ai/

The Importance To Provide Buyers And Sellers Secure, Convenient, And Frictionless Payment Experiences

By Héctor Guillermo Martínez, President GM Sectec

The COVID-19 pandemic accelerated the adoption of digital payments globally and especially in Latin America and the Caribbean, as buyers and sellers continue to expand their use of contactless, on-line and remote payment capabilities. The use of the Internet is increasingly present in people's daily lives and financial institutions are exposed to constant security threat vectors. This situation has led to an increase in the number of cyber-attacks and the need to reinforce the security of transactions made through digital channels. Every 11 seconds, a successful cyber or ransomware attack occurs, while for organizations the average cost per cyber-attack can reach $13 million.

It is interesting to see that companies are open to expand various forms of payment capabilities, and one example is presented by the 6th edition of Visa's Global Back to Business study that finds that 73% of small businesses surveyed said accepting new forms of digital payments is fundamental to growth in 2022. 59% of small businesses surveyed said they already are, or plan to, only use digital payments within the next two years – largely in step with 41% of consumers surveyed who said the same. 90% of small businesses surveyed with an online presence said they attributed pandemic survival to increased efforts to sell online.

These figures show the importance of companies implementing an effective cybersecurity strategy that allows them to continue to grow, while offering secure shopping experiences to their customers. The

recent partnership between GM Sectec, global leader in cybersecurity, and Visa, global leader in digital payments, will facilitate the implementation of fraud prevention, cyber defense and cybersecurity best practices in the Latin America and Caribbean region. Both organizations are committed to continue to inform the financial ecosystem on the topic of cybersecurity and further support the development and implementation of solutions to mitigate threats, safeguarding the integrity of their systems and protecting consumers.

One of the biggest concerns for businesses and organizations of all types, sizes and industries is how to protect the personal data and sensitive information of hundreds and thousands of users, customers and consumers who rely on them to conduct their daily transactions through various channels and platforms, many of them digital. The strengthening of this partnership, will allow organizations of all types across the payment system to engage cyber defense best practices with the support of a trusted cyber defense leader, bringing a unique support in PCI validation services, cybersecurity consulting, and fraud prevention assessments.

Companies need to understand their true cyber risk and be able to respond quickly and efficiently to strengthen their position.

Not only have large corporations understood that their cybersecurity systems need to be updated, but Latin American governments have understood that cybersecurity must be regulated and become a mandatory standard to be applied.

Cybersecurity must be a team effort involving the collaboration of persons, companies and governments. Cybersecurity should not be an option but the norm.

From left to right: Eduardo Coello, Regional President, Visa Latin America and the Caribbean, Héctor Guillermo Martínez, Presidente GM Sectec, and Eduardo Pérez, Regional Risk Officer, Visa, Latin America and the Caribbean.

About the Author

Héctor Guillermo Martínez is President and Board Member at GM Sectec. Héctor is responsible for the growth, vision, and execution of the company. GM Sectec creates innovative tailored solutions that help accelerate business breakthroughs in the areas of cyber defense, managed detection and response services, digital forensics, multi-tenancy, business continuity, information security, automation and process orchestration with the goal of ultimately delivering outstanding cost efficiencies to customers and partner community.

International Experience in both mature and emerging markets; particular focus and core competency in North America, Asia Pacific/Japan and Latin American geographies. Developed a specialty over the years of implementing 'made for market' technologies, with a particular focus on innovative 'tailored' solutions.

Héctor Guillermo can be reached online at Linkedin and Twitter. Our company website is https://www.gmsectec.com/

The Psychology Behind Spear Phishing Scams

By Dr. Yvonne Bernard, CTO, Hornetsecurity

Criminals are increasingly using fake emails to exploit their victims for financial gain and are using spear phishing takes the well-known social engineering scam to a new dimension. Employees training needs to encompass both fast and slow thinking systems to combat this cyber-attack.

Social engineering has been practiced for many decades, if not centuries! At its core, it's always the same thing. Fraudsters try to worm their way into gaining the trust of their victims to get them to hand over money or other assets. A prominent example is the con artist Frank Abagnale, whose story was made into the 2002 crime comedy "Catch Me If You Can." To obtain cash, he disguises himself as a security guard and sets himself up at the airport next to a locking system where funds from the ticket counter are deposited. When Abagnale pins the note "Out of order - please leave with security guard," his uniform seems so confidence-inspiring that people press the bills into his hand by the dozen.

First: Indiscriminate shipping to many recipients

With the advent of the Internet, new social engineering methods were established, with fraudsters making contact via fake emails. In classic phishing, large volumes of electronic messages are sent indiscriminately to countless recipients. The aim of the senders is to trick the addressees into disclosing confidential information, opening harmful links and attachments, or making payments to third-party

accounts. One example involves the deceptively genuine-looking PayPal emails that contain a link to an imitation website, asking recipients to verify or update their login information there. If they comply with this request, their data ends up directly in the hands of the scammers. Phishing emails can be produced very easily and without much effort. Even if only a few recipients bite, the effort pays off for the attackers.

Now: Threats tailored to specifically to the intended victim

Cybercriminals are more sophisticated when it comes to spear phishing, a form of phishing that specifically targets certain users. Their main target group is company employees, since that is where most of the money is to be made.

First, the fraudsters take a lot of time to scour social media and other Internet sources for information about their potential victims. This data can then be used to create emails that are precisely tailored to the recipient. Disguised as superiors, colleagues, or business partners, the attackers try to trick their victims with seemingly plausible prompts or cleverly designed lures.

In addition to feigning insider knowledge, hackers rely on psychological tricks to trick their victims. They skillfully target the recipients' emotions to get them to do what is asked of them without thinking about it. Here is a small selection of the most important psychological influencing factors:

- **Deference to authority:** For example, the scammers forge an email in the name of a board member. In it, the employee is asked to make an urgent payment to a supplier. Large sums of money can end up in foreign accounts in this way. The chances of recovering these sums are usually slim.
- **Willingness to help**: The alleged acquaintance of a colleague contacts the employee about a problem. The email contains a file attachment, which the employee opens immediately - maybe the employee had the information needed and can help. The file contains malware that infects the computer and the system unnoticed.
- **Time pressure:** In a deadline-critical project, the scammers pretend to be the department head. They demand that the employee send security-relevant information and urges the employee to hurry. Since there is no time for a more detailed check, the recipient reveals the requested information in good faith.
- **Curiosity:** In the name of the management, the hackers inform the recipient about important structural and personnel changes in the administration. The mail contains a link that supposedly leads to an updated organizational chart with the new distribution of responsibilities. If the employee clicks on the link, he or she plays into the scammers' hands.
- **Fear:** The alleged superior asks about an invoice for a service that was not ordered. The employee is afraid of being suspected of embezzlement and therefore hastily clicks on the link to the invoice - and thereby opens the door to hackers. Not infrequently, the loophole is also used as an opportunity to penetrate the entire corporate network.

Worldwide fraud gangs raking in millions

Spear phishing is one of the most dangerous and most common cyber-attack method today. These attacks are increasingly being carried out by international fraud gangs and can cost companies a fortune. The best-known examples include the German automotive supplier Leoni, which lost around 40 million euros through CEO fraud in 2016, while the Austrian-Chinese aerospace supplier FACC lost 50 million euros in this way.

Alarmed by recurrent stories of this sort in the media, many companies naturally want to make their employees aware of the dangers posed by spear phishing. One common method they resort to is security awareness training, which focuses on classroom training, e-learning and webinars. These provide participants with theoretical knowledge of how spear phishing attacks work, how to recognize forged mails and how to behave in the event of an attack. This is certainly important to know, but it is not enough to effectively arm users against attackers' psychological tricks.

Two highly different systems of thought

The reason for this lies in the two different human thought systems, as described by psychologist and Nobel Prize winner Daniel Kahnemann in his bestseller "Thinking, Fast and Slow". According to this, system 1 - fast thinking - is guided by subjective feelings and empirical values and tends to make impulsive decisions "based on gut instinct". System 2, on the other hand - slow thinking - takes objective data into account and proceeds systematically, rationally and logically when making decisions.

By imparting objective knowledge about spear phishing methods, conventional security trainings target the second - slow - thinking system. In doing so, they neglect the first thinking system, which is responsible for spontaneous clicks on incoming emails. Therefore, training urgently needs to be supplemented with learning content that promotes employees' fast thinking and intuitive decisions.

Simulated attacks strengthen awareness

This can be achieved with spear phishing simulations. These use real company and employee information to fake attacks. If an employee is taken in by a fraudulent email, he or she is immediately taken to an explanation page. Here, they receive information about the features that would have enabled them to recognize the mail as fake on closer inspection: from misspellings in the sender address to the use of subdomains and suspicious-looking links.

Phishing simulations are a proven method to sustainably increase employees' security awareness. This is because they take advantage of the "teachable moment," when a user is most receptive to new lessons. Since the employee's error is immediately made clear to him or her, they will be more careful with incoming emails in the future. To keep the employee on guard, it is advisable to repeat spear phishing simulations regularly and adapt them to the attackers' ever-changing methods. The goal here must not be to monitor or trick employees - instead, the focus must be on training. For this to succeed, the use of security awareness training must be communicated correctly.

Humans remain the weakest link

Effective security awareness training should combine e-learning with realistic phishing simulations. It is important that the training is tailored to the personal learning needs of each individual employee. It should also allow for metrics-based measurement of their learning progress.

Although IT departments can already intercept many spear phishing emails using the right email security solutions, humans still remain the biggest vulnerability. Companies should make this clear to their employees not as something demeaning, but to motivate them to participate in security awareness training. As well as relying on the IT security technology used by their employers, users must understand that they too have an essential part to play: They are the most important lever for successful defense, through their own self-efficacy. Only those organizations that can convince their employees of this will remain one step ahead of spear phishing attackers in the future.

About the Author

Dr Yvonne Bernard is CTO at Hornetsecurity, the global Cloud Security, Compliance and Backup Pioneer founded in Hannover, Germany. With a Ph.D. in Computer Science, she has a technical background and is responsible for strategic and technical development in the areas of Product Management, Software Development, Innovation & Research, Security Lab and Cloud Infrastructure. Yvonne can be reached online at https://www.linkedin.com/in/dr-yvonne-bernard-b3388a25/ and at our company website http://www.hornetsecurity.com/

The Quantum Threat: Our Government Knows More Than You Do

By Skip Sanzeri, COO and Founder, QuSecure, Inc.

Quantum computers are extremely powerful machines that utilize subatomic properties providing amazing potential to change the way that we process information and to improve our world. However, in addition to quantum computers running applications that will generate world-changing capabilities, they will be used as weapons by our adversaries.

One such weaponization will materialize through quantum computers breaking the existing cybersecurity the world uses today. The Department of the Defense's (DoD) primary concern is that a weaponized quantum computer could be used to break the encryption that protects sensitive government data and communications. In short, quantum computers will threaten our data and privacy to the extent that this will force the largest technology upgrade cycle in computer history.

Fortunately, the U.S. government has recognized this critical issue, and is now dealing with this threat. *What they know that you don't* is that adversarial nation-states are spending tens of billions of dollars, and deploying thousands of computer scientists, PhDs and quantum programmers to build a quantum computer that will break all the world's current encryption. These same nation-states are harvesting data today at amazing rates via listening devices around the world in order to decrypt that data when they have quantum capability.

Currently encryption is difficult to break with standard computers. However, via Shor's algorithm it has been proven that quantum computers will be able to decrypt this stolen information. So by building a powerful quantum computer, these nation-states will be able to decrypt data that may still have 25, 50 or even 75 years of value remaining. Think in terms of military secrets, banking information, healthcare information and other personal information that has been stolen. Much of this information needs decades of secrecy and if decrypted, it could be used for great harm.

The fact is our government, led by our intelligence organizations and communities, knows that these huge quantum computing investments of resources by our adversaries provide a clear and present danger. *Our government just knows more than you do*. This is evidenced by the warnings that have come out in the past eight months with increasing velocity, where the U.S. State Department and other federal agencies have mandated quantum cyber upgrade policies. The State Department issued two separate memos, and NIST (the National Institute of Standards and Technology) finalized algorithm choices for post-quantum cybersecurity (PQC) just this past July.

Then on Aug. 24, the Cybersecurity and Infrastructure Security Agency (CISA) raised the red flag regarding the quantum computing threat by releasing a paper providing updated advice on how any organization with critical infrastructure and data should get ready for security risks from quantum computers. It is now no longer a matter of if the U.S. needs to upgrade its federal agency systems to PQC, but only a matter of when. According to the U.S. Secretary of Homeland Security, Alejandro Mayorkas, “The transition to post-quantum encryption algorithms is as much dependent on the development of such algorithms as it is on their adoption. While the former is already ongoing, planning for the latter remains in its infancy. We must prepare for it now to protect the confidentiality of data that already exists today and remains sensitive in the future.”

All of this has been done to address the quantum threat which, based on findings from the intelligence community, could be only a few years away. According to Britain's MI6 Chief Richard Moore, "Our adversaries are pouring money and ambition into mastering artificial intelligence, quantum computing and synthetic biology because they know...this will give them leverage." Governments and commercial organizations that are responsible for securing sensitive data should not underestimate the threat of quantum computers. The science to support quantum computing is well-founded and quantum computers may be a single breakthrough away from cracking modern cryptography. Quantum computing is not a question of if, but when.

Some believe that building a quantum computer powerful enough to break encryption is a decade or more away. No one knows for sure, however nation-states are finding clever ways of stringing quantum computers together to enable processing via an aggregate number of systems, instead of relying on a single developed quantum computer, enabling the quantum systems to operate in a parallel fashion.

China has proven they can entangle sub-atomic particles and maintain that entanglement over 12.5 kilometers, which means two different quantum computers could share the same state. This capability would enable decentralized operation of quantum computers, which would utilize distributed design with the same quantum computer transmitting information from one quantum computer to another as needed. This means that we could be closer to more quantum power and the subsequent associated threats to standard encryption than expected.

It is advisable that federal agencies, commercial organizations and other infrastructure providers begin to immediately assess potential vulnerabilities in their current encryption and cybersecurity practices, and start planning for post-quantum encryption. Post-quantum resilience is needed today.

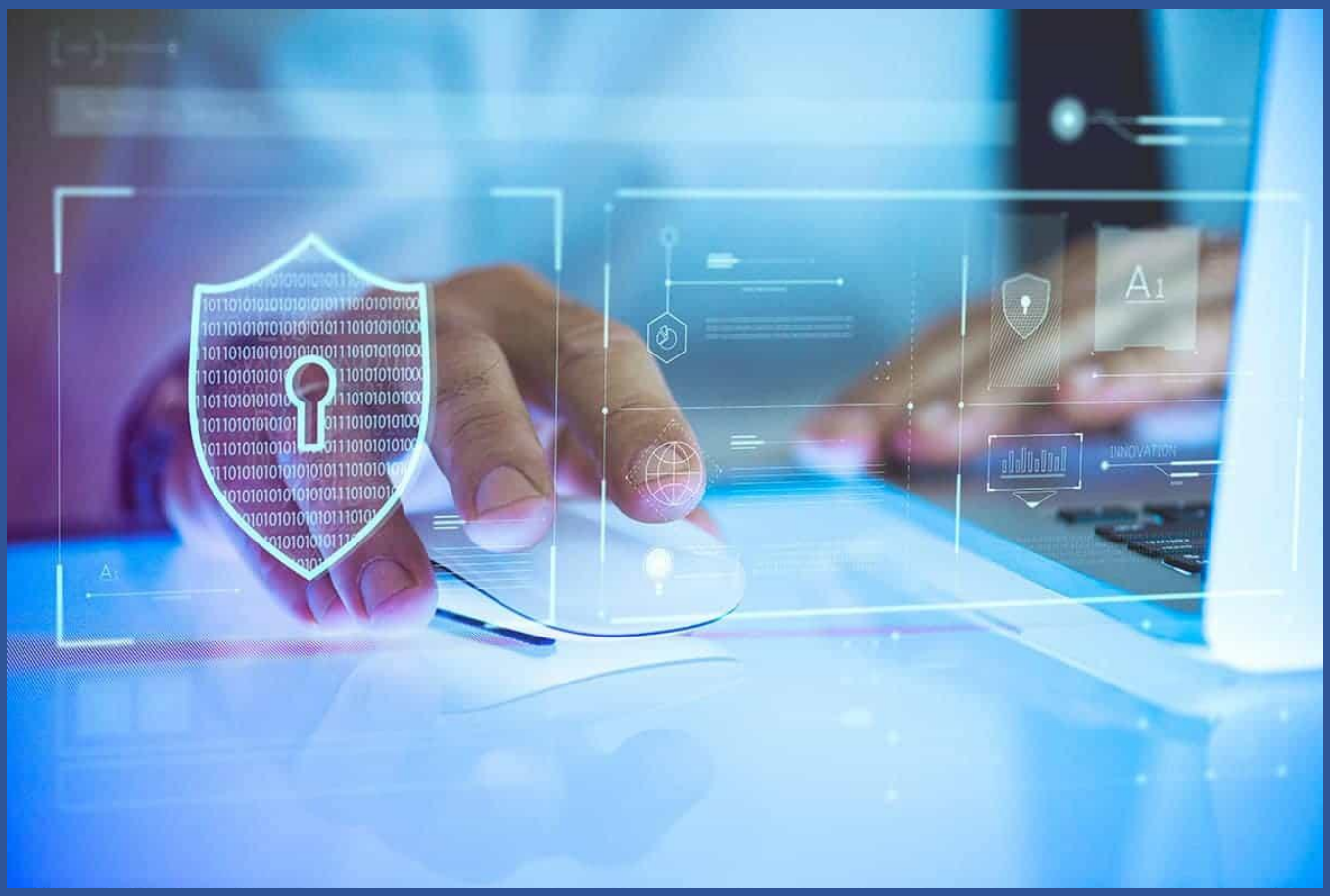
About the Author

Skip Sanzeri has been an entrepreneur since 1986 and currently is the Founder, Board Chair, and COO at QuSecure, a top post-quantum cyber-security company using post-quantum cryptography to help secure the US military, government and commercial businesses. Founder and Board Chair Quantum Thought a leading venture studio focused on quantum computing applications and is also the Founder and Partner at Multiverse Capital. Skip is a co-author of "Quantum Design Sprint: A Workbook for Designing a Quantum Computing Application and Disruptive Business Model". Skip started his entrepreneurial career at age 26 when he founded, funded and built 6 Gold's Gyms, re-branded as California Athletic Clubs which were later acquired by 24 Hour Fitness. After that, Skip joined Quote.com (backed by Sequoia Capital), which was subsequently bought by Lycos.

https://www.linkedin.com/in/skipsanzeri

Twitter - @sanzeri

Main website: https://www.qusecure.com/



The Top 10 Predictions For The Cybersecurity Industry In 2023

By Christopher Prewitt, Chief Technology Officer, Inversion6

Technology never stops moving forward. Each new year brings changes which create downstream effects on how we are attacked and how we defend against those attacks.

As the IT and cybersecurity industry pushes to be less reactive, predicating what's coming in the next year has become more and more popular. Here are my top 10 trends that will be most important in 2023.

1. Active response will likely become the default defense posture.

The industry has learned proper preventive controls, yet there is still room for improvement. Some responders have not been as timely as needed, which should lead to more automation, self-assessments

and more real-time responses. Account lockouts, password resets and network contained systems will likely be some of the methods used to reduce the impact of a data breach.

Should responders continue to waste time, we will see a shift from default configurations to more auto-responses. Our end customers will have to change with the times and understand the value of the disruption.

2. Zero trust models are going to have a massive impact on security.

We've seen a shift in organizations migrating to the cloud and abandoning their internally hosted data centers. With the shift will come an increase in the reliance on zero trust models to improve security.

This could change how we perform penetration testing, secure our networks and may even remove the need for significant network security for some organizations. The perimeter network edge is all but dissolved, zero trust may help to finish it off. We will still have a need for internal segmentation in many industries that rely on local computer resources.

3. Government regulations are going to balloon.

We can predict there will be changes to the current international privacy requirements. These new security regulations will likely come from the SEC. On top of these changes, additional executive orders and Congressional committee meetings will be coming down the pipeline next year.

I expect most of these regulations to lack real teeth. The fines and penalties likely won't be sizable enough to implement real change. The FTC stands out with some regulations that have significant teeth to them.

4. Hacktivism is increasing.

The ongoing conflict in Ukraine has been the first war to prompt large scale cyberattacks from nonmilitary citizens of other nations.

The Ukrainian army's offensive cyber-operations are now attacking Russian infrastructure as both a hobby and a political statement. We can foresee these types of offensive operations across borders to become more conventional in the coming year.

5. Governments will be more direct on attribution.

This past year we saw multiple public reports of US espionage efforts in China. This does not come as a shock given our government's recent trend of outing its own cybersecurity enemies by name.

As China, Iran, North Korea and others continue to increase their defensive capabilities, we will hear further communications about attribution of attacks and our own cyber operations.

6. Attackers will continue to stay away from the weaponization of artificial intelligence and machine learning.

Effortless attacks are here to stay. Attackers have no use for advanced methods. Look at the recent attacks against Uber, Twitter and others for proof. While there are ways to generate attacks against multi-factor authentication, simple supply chain-based approaches still get the job done. Now that we are locking the door more consistently, it's almost as easy to walk right in when you have the keys.

7. 5G won't help decrease cyber attacks.

5G can allow for private networks, which can prevent direct internet access to their fleet of devices. This amplifies technology providers' security abilities, by reducing the attack surface. The increase in bandwidth is still no match for the skills of cyber criminals.

Given the influx of new devices, 5G will likely provide an even larger opportunity for attacks with most providers not taking advantage of private secured networks.

8. The next big hack likely won't target a hyperscaler/cloud-provider.

As organizations migrate workload and servers to the cloud, these providers may indeed be hacked. I don't anticipate it to be large-scale, more so an increase in risk. There are considerable risks for organizations, especially if an attacker can gain tenant level access to your assets. While we may see large outages, it is unlikely that we'll have some catastrophic level security breach.

9. Cyber insurance won't help more companies cope with uncertainty.

We saw a rise in cyber insurance rates in 2022. With carriers becoming more restrictive, many customers will likely face more coverage requirements in 2023.

The cyber insurance market will continue to provide some options to small and medium-sized businesses. The downside to these heightened measures is the increase in organizations abandoning their policy renewals for 2023 and choosing to self-insure.

10. **Mobile devices still could be targeted by attackers.**

In this space we see and hear about the expensive zero days that few companies and many nation states have access to. Attacks against these platforms aren't occurring the way experts have predicted. While phishing, smishing and other social engineering attacks are still present, they don't traditionally attack the phone's operating system.

Apple and Google do a great job securing their devices. Individuals that upgrade to a new phone every two years limit the exposure risk that comes with running an old device. So, much of the risk here is limited to social engineering unless you are one of a very few nation states.

About the Author

Christopher Prewitt s CTO at Inversion6, responsible for helping develop security-related products and services for customers. Over the past 20+ years, he has acquired extensive experience in end-to-end planning and execution of robust, large-scale security, privacy, compliance, and risk management systems/solutions in Fortune 500 and 1000 environments, supported by strong customer service and technical issue resolution. He excels in designing and optimizing cutting-edge enterprise security systems and data center architectures. Chris can be reached online at https://www.linkedin.com/in/cprewitt/ and at our company website www.inversion6.com.

Typical Cybersecurity Methods Aren't Enough to Support the Modern Workforce

By Gee Rittenhouse, CEO, Skyhigh Security

It's time to adopt a zero-trust approach. Organizations in all sectors are adopting the hybrid workforce model, and this is forcing a shift in cybersecurity practices. Employees, contractors and other third parties demand rapid and secure access to the web, cloud and private applications to support global collaboration transparently and without disruption.

It's no longer network security as usual. Traditional or perimeter network security mainly concerns itself with keeping attackers out of the network with technologies like firewalls, VPNs, access controls, intrusion detection systems (IDS), intrusion prevention systems (IPS), security information and event management (SIEM) and email gateways. Now that remote work and the widespread use of cloud apps and services are the common workforce model, perimeter security is rendered nearly obsolete.

One of the most important steps you can take to secure your entire hybrid estate is to implement a zero-trust architecture, which is based on the tenet of "never trust, always verify." Zero trust challenges the users and devices to prove they are authorized to access resources, even if they are within the walls of the network perimeter. In other words, zero trust treats all traffic as potentially hostile until the identity of the device or user is authenticated according to a strict set of criteria.

To properly and fully protect your evolving hybrid environment, you need to implement a zero-trust architecture, which includes cloud-native security and an understanding of the limitations of network perimeter security. Let's look at some of the ways you can benefit from this approach:

1. **Shrink the attack surface:** Your users connect directly to SaaS or private apps and other resources they need to do their jobs, but less frequently to the network. As such, there's little risk of lateral attacks or compromised devices infecting other resources, but still a risk of data being exfiltrated. By diminishing the attack surface, zero trust curtails the impact and severity of attacks, which reduces the time and costs associated with response and remediation.

2. **Improve threat detection:** All data-sharing and data-access activity must be continually monitored and compared to baselines built on analytics and historical trends to identify anomalous behavior and traffic. With this combination of monitoring user behaviors, granular policies and rules and security analytics, you'll find it easier to discover internal and external threats.

3. **Prevent data breaches:** Since everything in zero trust is assumed to be risky, every access request is inspected and authenticated before "trust" is granted. Even when trust is established, it's continually reassessed in terms of context, such as changes in the user's location or the type of data that is being accessed. A zero-trust model or architecture provides secure access to everything and everyone.

4. **Reduce business risk:** Zero trust provides better visibility and control over what and who is on your network—users, devices, components and workloads—and how they are communicating. It also enables you to manage and enforce data protection and web access policy company-wide.

The ideal solution of a zero-trust architecture is a unified Security Service Edge (SSE) architecture that converges and integrates data and threat protection technologies and acceptable use control across private apps, shadow IT, SaaS apps and web traffic. The most comprehensive single-vendor SSE solutions bring together a cloud access security broker (CASB), secure web gateway (SWG) and zero trust network access (ZTNA). SSE provides you with visibility across your infrastructure, making it easy to create, manage and enforce policies in one place.

The right SSE also gives you powerful, cloud-native protection for any device anywhere—whether managed and agent-based or personal and agentless. A truly effective, data-aware SSE integrates data loss prevention (DLP) scanning, antimalware technology and remote browser isolation (RBI)—an ideal trio for protecting the internal and remote workforce.

SSE also provides a single-pane-of-glass management platform that enables you to apply unified policies across cloud platforms, endpoints, the web, SaaS and private apps, regardless of whether your data is at rest or in motion. Consistent policy is applied corporate-wide and moves with the user and data instead of being tied to each access technology.

Now is the time to level up your cybersecurity approach and meet the future of digital transformation confidently.

About the Author

Gee Rittenhouse is the CEO of Skyhigh Security. Gee is a recognized innovation leader whose passion is creating technology solutions that empower people. Gee joined Skyhigh Security in January 2022 to help organizations thrive by providing a simpler way to secure their data. Before stepping into the role of CEO, Gee was the Senior Vice President and General Manager of Cisco's Security Business Group and previously served as Vice President and General Manager of Cisco's Cloud and Virtualization Group, helping shape the company's cloud and virtualization strategy. Before Cisco, Gee was President of Bell Labs famous for Noble Prize-winning innovations.

As a technology thought leader and veteran in the security industry, he has published numerous articles, holds more than a dozen patents, and has appeared before the U.S. Congress, U.S. FCC, European Presidential Commission, and World Economic Forum. Gee has a Ph.D. degree in electrical engineering and computer science from the Massachusetts Institute of Technology.

Gee can be reached online on LinkedIn and at our company website at www.skyhighsecurity.com.

Understand And Reduce The Sap Attack Surface

By Christoph Nagy, CEO & Co-Founder, SecurityBridge

Knowing the attack surface in today's world is very important to reduce the risk of exploitation of the so-called unknown-unknown. Zero days are vulnerabilities that have not been patched and are also not widely known. Organizations need to assume that any application, also the enterprise-critical solutions from SAP, contains a severe vulnerability that can't be patched since no patch is available. Waiting for the moment the vulnerability gets published and patched by the software vendor may not be a safe bet, since threat actors may already know and exploit the open loophole.

Security firms interact with partners and customers to understand their risk appetite and to engender a solution to mitigate the unacceptable risks. One of the first questions is the following: Do you know your attack surface?

What is the attack surface?

The attack surface is the sum of all possible entry points, or attack vectors, where an unauthorized attacker can access a system or application to e.g. extract data or manipulate sensitive information. The smaller the attack surface, the easier it is to protect.

Why is the SAP attack surface so important?

Organizations must constantly monitor their attack surface to identify and block potential threats as quickly as possible. They also must try to minimize the attack surface area to reduce the risk of cyberattacks succeeding. In the context of SAP, the Internet Communication Manager (ICM) or Internet Communication Framework (ICF) available via SAP transaction SICF, and also the remote function call connection setup, is prone to overexposing services to the outside.

SAP customers with SAP security in mind need to continuously assess and inventory the exposed services (SOAP, WebService, API's). Any service that is not used or does not serve a specific SAP business scenario should be deactivated to reduce the attack surface and thus also to minimize the risk of exploitation.

Furthermore, a close tab needs to be kept on those services that are not requiring authentication. In SAP they exist in the /sap/public/ namespace that can be found in transaction SICF. Services like /sap/public/info are the number one touchpoint for threat actors to gather information in the exploration phase of an attack.

Effective counter measures against SAP Zero-Day exploitation?

Just to remind, a zero-day is a vulnerability that is not yet widely known, and no patch exists. Hence patching is not an option. This does not mean that regular and timely patching is not one of the most effective exercises to protect against exploitation - on the contrary. Any second Tuesday of a month SAP customers expect to see another SAP Security Patch Day – a day when SAP publishes the new security patches. This event starts the race between attackers and defenders, who can only win by installing the patch before the exploitation.

SAP sponsors bug bounty programs to support bug hunters and security researchers. There are various individual researchers but also entire research labs that analyze standards software for vulnerabilities, however, even with a combined effort zero-days can't be eliminated.

Patch Management solutions can inform you once a new patch has been published that is relevant for your specific system installation to reduce effort and lead time before patching. Additionally, SAP security firm product teams can instantly issue signature updates that allow customers to monitor for potential exploits of yet unpatched vulnerabilities.

However, as no patch is available for a zero-day, there are a few other things that you need to consider:

1. Inventory of Attack Vectors

Knowing your attack surface overall is important and serves as the foundation for further countermeasures. It also helps organizations to understand their individual risk situations.

2. **Reduce the Attack Vectors**

Any connection point such as the previously mentioned SAP Internet Communication Framework (ICF) services that are not used or needed, shall be deactivated. Also, ensure to sufficiently harden all touchpoints with untrusted networks or the public internet.

3. **Software Components**

Software components that do not serve a distinct purpose shall be uninstalled or at least deactivated. Most of the SAP customers still run at least one SAP NetWeaver system where the client 066 exists, which is not needed anymore but until recently was shipped with the standard installation.

4. **Surveillance of Change**

Whenever a new service is enabled or introduced, there are security considerations to make. A SAP security firm can help customers to monitor any change to the attack surface. Those changes are immediately reflected in the overall SAP security posture.

5. **Threat detection**

The recent Log4j incident but also the somewhat older RECON release have impressively proven that vulnerabilities can exist for a long period of time without being noticed. Detection of malicious and monitoring of action with impacts to the SAP system security are key elements to protect against severe damage.

6. **Layered security**

Introduce additional security layers. Besides precise hardening, patching, and monitoring it is beneficial to consider adding intrusion prevention systems and network segmentation based on your individual risk situation.

How to reduce the SAP attacker surface?

This is not an easy task and especially becomes difficult for SAP organizations that expand their digital footprint and embrace new technologies. Reducing means:

- Deactivation of services of SAP Internet Communication Framework (ICF) and Internet Communication Manager (ICM)
- Deinstallation of unused software components
- Deletion of unused or obsolete RFC Destination and service endpoints. Those in use need to be sufficiently hardened
- Elimination of trusting (SMT1), which is not needed
- Deletion of SAP clients that are not used
- Governance and tracking of SSL certificate handling in SAP (STRUST)
- And many more…

It may be a fine line between accepting the risk and fulfilling the business department's wish for a new service. This is especially true if the new service only adds additional comfort but comes with a very

specific risk. And this already describes the one challenge to master – many SAP experts do not have the classification of benefit versus SAP security impact at hand – the moment they evaluate a request for change. An SAP security firm can provide the missing piece of information by a sophisticated classification system that puts the likelihood of exploitation in perspective.

The previously described scenario applies to a particular change, and mainly connects to the security governance model that needs to be in place to ensure the attack surface of SAP does not increase. Taking a step back and looking at the overall surface of an existing system or an entire landscape is a lot more complex. It typically requires an extensive assessment phase before dependencies and other environment-specific considerations, like the existence of additional security layers, can be made. Additional security layers can be introduced by network segmentation, intrusion prevention systems contained in intelligent firewalls.

Conclusion

Every second Tuesday of a month, SAP customers will see new security patches. It is very likely that some of the security updates released will again force you to patch severe vulnerabilities within your enterprise critical SAP applications.

If services are impacted that are deactivated, the risk of exploitation is typically reduced – hence often the deactivation of an impacted service is mentioned as a workaround for those that can't install the patch.

Log4j has hit many organizations and also SAP customers unprepared. Be aware this can happen at any time again, and better yet assume that this will happen and develop your security strategy adequately.

About the Author

Christoph Nagy has 20 years of working experience within the SAP industry. He has utilized this knowledge as a founding member and CEO at SecurityBridge–a global SAP security provider, serving many of the world's leading brands and now operating in the U.S. Through his efforts, the SecurityBridge Platform for SAP has become renowned as a strategic security solution for automated analysis of SAP security settings, and detection of cyber-attacks in real-time. Prior to SecurityBridge, Nagy applied his skills as a SAP technology consultant at Adidas and Audi. Christoph can be reached online at christoph.nagy@securitybridge.com and at https://securitybridge.com/.

Unwitting Insider Threats Remain A Challenge As Security Solutions Struggle To Keep Up

By Chip Witt, Vice President of Product Management

Ransomware continues to be a rising and persistent threat to organizations, with research showing that 50% of organizations have been hit with ransomware attacks anywhere from two to five times in 2022, compared to 33.5% in 2021.

The rise of these attacks, and evolving tactics and targets, led some IT leaders to seek upgrades and tack on newer cybersecurity tools to current protections to thwart such intrusions.

According to SpyCloud's 2022 Ransomware Defense Report, which surveyed 310 IT security practitioners across North America and the UK, 90 percent of respondents reported that their organization was affected by at least one ransomware attack last year — up from 72.5 percent a year prior — and with 77.7 percent claiming they have been hit multiple times.

As a result, confidence in existing ransomware mitigation tools has dipped over the past year, with more organizations seeking either capability upgrades or new technologies.

But while new tools can help combat ransomware attacks, organizations may be overlooking fundamental gaps that will allow attackers to bypass their expanding security stacks.

Ransomware remains top of mind for organizations

The fallout, and possible damage to an organization's reputation, from a ransomware attack, remains a top concern for organizations when addressing their security operations.

This fear, combined with an expectation that ransomware will eventually successfully impact their networks, has led organizations to divide their focus between defending against intrusions and extenuating their effects.

That has included an increased focus on recovery efforts, such as companies purchasing cyber insurance to mitigate potential losses or opening cryptocurrency accounts as a preparedness measure to pay the ransoms that attackers may demand.

These efforts come alongside organizations' desire to mount a more robust defense to reduce their risk of a ransomware attack, adding new tools to their technology stack. However, while pursuing new solutions may offer organizations new capabilities, they may not reduce risk if foundational cybersecurity practices remain overlooked.

Threat vectors such as unmonitored devices accessing the network and malware-stolen session cookies that can enable session hijacking can be as damaging as traditional ransomware entry points like unpatched software or phishing emails.

Implementing new solutions without first addressing the core issue can leave organizations with critical security gaps that make them more vulnerable to ransomware attacks and are ultimately a band-aid on a bullet wound when it comes to a true defense program.

The attacker is already inside the house

As attackers already have access to an organization's data before deploying ransomware, IT security professionals must be able to prevent potential breaches through solutions like endpoint protection, credential monitoring, user and entity behavior analytics, software patching, and other best practices.

But even with those steps in place, organizations face vulnerabilities from third-party and partner applications that may sidestep cybersecurity tools. The risk of a third party-based cyberattack was ranked as the top concern for organizations when reflecting on their cybersecurity plans, coming ahead of the sophistication of ransomware attacks and the frequency and severity of malware.

However, one of the most impactful issues facing organizations fell to fourth in the report, despite its potential to fuel future ransomware attacks: the severity of data breaches.

After the significant disruption of an initial ransomware attack, it is easy for organizations to view subsequent intrusions as standalone events, each compartmentalized in its circumstances and highlighting yet another vulnerability that new tools need to solve.

It's more likely that these ransomware attacks are recurring from data taken in the initial breach that has become a force multiplier of new intrusions. Without organizations having full visibility into what data has been compromised, they may be subject to a feedback loop of new ransomware attacks resulting from data taken in the initial breach.

At its foundation, the full mitigation of a ransomware attack is still a challenge for organizations. Even with a percentage of organizations able to retrieve their stolen data post-attack, that doesn't mean that data wasn't already shared more widely for other follow-on attacks, as the multiple attack data may indicate.

With current endpoint solutions only accounting for the initial infection on a device and not the additional applications or tools that may have been impacted, a big part of the post-infection remediation is missing for most organizations to truly be free of exposure.

The post infection remediation approach

Remediating malware infection usually begins and ends with re-imaging the infected machine, but as we've seen from recaptured data, criminal activity usually lives well beyond the scope of an initial malware infection.

Post-infection remediation, rather than focusing just on the machine, requires exploring what information was exposed and then remediating that exposure to its furthest reaches.

A machine's infection is not fully remediated until the exposure of the user and the user's impacted applications are known and accounted for. This means taking the appropriate steps to re-image the infected machine and researching the impacts of that infection concurrently to prevent new attacks from materializing.

Factoring post-infection remediation into an enterprise's cybersecurity plan helps prevent attackers from re-accessing a network through malware-harvested credentials, stolen session cookies, and other data exposed from an infostealer infection.

While wiping malware-infected devices is the first step, organizations also need full visibility into the devices, applications and users that may have been compromised by an infection. Without all that compromised data being remediated, the enterprise remains at risk for follow-on attacks including ransomware.

Prevention and remediation can help promote resilience

Tools to identify and prevent ransomware and other cyberattacks continue to evolve, but organizations are unlikely to outpace the ingenuity of their attackers. While layered defense built with cutting-edge technology can help identify potential attacks, organizations must also focus on identifying workforce and implementation challenges and obtaining full visibility of any compromised data.

By strengthening detection and prevention tools, organizations can make themselves a smaller target, and with thorough post-infection remediation, they can ensure a swift recovery from any potential breach or malware infection and be better prepared to limit the damage.

About the Author

Chip Witt has over twenty years of diverse technology experience, including product management and operations leadership roles at Hewlett Packard Enterprise, Webroot, VMware, Alcatel, and Appthority. He is currently the Vice President of Product Management at SpyCloud, where he drives the company's product vision and roadmap. Chip works closely with field intelligence teams specializing in OSINT and HUMINT tradecraft, actor attribution and underground monitoring. Chip can be reached online at https://www.linkedin.com/in/chipwitt/ and at SpyCloud's company website, https://spycloud.com/.

Upskilling And Automation The Keys To Cyber Resilience For Businesses

Why investing in cybersecurity measures is more important than ever, despite challenging economic times

By Achi Lewis, Area VP EMEA, Absolute Software

At a time where cybercrime is on the rise with an increased attack surface in our work from anywhere world, as well as the heightened cyber threat from the Russian invasion of Ukraine, investing in cybersecurity is more important than ever.

With an economic downturn on the horizon, businesses will be looking to tighten budgets and make cuts where possible. Ensuring a strong cybersecurity posture is in place should be treated as essential when allocating where funds should be spent.

The UK Government's Cyber Security Breaches Survey 2022 revealed that 82 per cent of UK business boards and senior management rank cybersecurity as a high priority, while the Security Priorities Study whitepaper shows that 90 per cent of respondents believe their organization is failing to appropriately address cyber risks.

Upskilling, automation, and outsourcing are all options that organizations can, and should, be deployed to create a resilient cybersecurity posture on a budget.

The need for upskilling and training

The digital skills gap is an ongoing problem and one that is being felt heavily throughout the technology industry. This problem extends to cybersecurity, however, the effects of this could be reduced if IT teams were to be upskilled with cyber training.

The 2022 Cybersecurity skills gap report from Fortinet found that 64 per cent of organizations worldwide have experienced some form of security breach, linking 80 per cent of those attacks to the cybersecurity skill gap. Furthermore, non-malicious user error has been cited as the top cause of security incidents. This highlights the gap in awareness and understanding around cyber-attacks by current employees and the need to improve education around threats, both for cybersecurity and non-cybersecurity staff.

Through regular training and upskilling, organizations will be able to equip their staff with the knowledge that will enable them to act effectively to protect against attacks, as well as understand what to do to recover once a successful attack does occur.

Additionally, there are many untapped pools of individuals that can be drawn on to plug the gap. For example, women are largely unrepresented in the technology world, with just 19 per cent of the tech industry being made up of females. Thinking outside the box when looking for talent is one-way organizations can extend the talent pools available to them, with no extra costs.

While training staff, finding talent, and eliminating human error is not an easy task, it is it a relatively small expense in comparison to the financial, time, and reputation costs of stolen data.

Why automated technology is the way forward

Training and upskilling current employees is one way to minimize cyber risk, but eradicating human error indefinitely is almost impossible without the right technology. Automation technology can strengthen and compliment the efforts of employees, and with only 45 per cent of companies currently using automated cybersecurity solutions to prevent and recover from attacks, the value is not being fully realized.

Resilient Zero Trust is one effective solution, monitoring an organization's endpoint devices and applications for suspicious activity. If a device logs on from an unfamiliar location, or accesses a restricted application, an alert can be sent to a centralized IT team who have the power to freeze or shut off a device to prevent a potential breach. The goal with this technology is for employees to remain operational, rather than simply cutting them off at the first opportunity, whilst also helping to automate threat detection.

The number of Zero-Trust architectures deployed by businesses rose by 8 per cent between 2021 and 2022 as this technology offers a cost-effective way of bolstering cyber defenses.

Self-healing technologies can also strengthen an organization's security portfolio, repairing and recovering compromised devices automatically, reducing the risk of reinfection and allowing businesses to continue using their existing enterprise devices.

Being appropriately prepared to respond to a security incident takes the number one spot when looking at key security priorities, and having automated technology in place that helps with response and recovery will allow organizations to comfortably work without the looming worry of a cyber-attack.

Outsourcing to service providers

Outsourcing is another low-cost solution businesses can utilize to improve their cybersecurity posture. With time and money an important factor, 83% of IT leaders that currently use an in-house security team are now considering outsourcing.

Delegating security tasks to skilled professionals outside your organization can compensate for a lack of accessible digital talent whilst still bolstering cyber defenses.

Outsourcing is a cost effective solution, which at a time when budgets are tight, is a huge incentive. Organizations will not need to worry about the training and salary of full-time staff, but instead outsource to services that are simply cheaper.

Cybersecurity must remain a priority and difficult economic conditions cannot be an excuse. With several low-cost approaches available to help improve cyber resilience, organizations should look to re-thinking their processes to capitalize upon the resources available to them.

By deploying a mixture of upskilling, automating, and outsourcing organizations will be able to build a strong cybersecurity portfolio to protect against incoming threats and help them to recover and respond to attacks effectively.

About the Author

Achi Lewis is the Area VP EMEA of Absolute Software. He is a veteran of the cybersecurity industry with decades of experience in enterprise security, overseeing Absolute's go-to-market strategy in EMEA, establishing relationships with key customers and growing its partner network.

Achi can be reached online at @absolutecorp and at our company website https://www.absolute.com

User Behavior Analytics in Case Management

By Milica D. Djekic, Independent Researcher from Subotica, the Republic of Serbia.

Abstract: Some criminology studies suggest crime can be committed by coping with some schemes, plans or patterns as such an action leaves a lot of findings and evidence behind itself providing an option to the law enforcement to open a case once being reported about such an incident. On the other hand, an active policing goes ahead of the crime trying to uncover any incident happening within communities either if being reported or not. The modern time is an era of the emerging technologies and literally everyone over the globe has become a part of the cyber environment. In a cyber defense, there is recognized a user behavior on the web and truly once well-analyzed those findings can give a full picture about someone's habits as the Police in such a sense can be supported with the real clues serving in a lawful resolving of the investigation. The crime areas have remained a very colorful ecosystem, but even if a criminal actor copes with the common cell phone there will be some footage with such an information-communication infrastructure which means a plenty of so can be applied in an intelligence gathering manner. The user behavior analytics is a well-developed and studied field within high-tech security and the most obvious thing with so is once all pieces of the puzzle are collected a complete mosaic can be interpreted dealing with an increasing level of the accuracy and objectiveness. This effort demonstrates some reviewing and analytical insights into such a topic attempting to indicate a significance of the well-researched cyber defense theory and practice, so far.

Keywords: cyber defense, intelligence, technology, analytics, risk, etc.

Introduction

Accuracy is an attribute of the natural sciences as it seeks some methodologies to explain some occurrence in a truly quantitative fashion. In other words, in such a sense it is important to precisely measure outcomes of any event in an observed environment in order to understand and potentially develop some mathematical model which can lead into mastering some engineering concepts. In the past, it was sufficient to find two witnesses which would make a same statement as there were no ways to confirm if that witnessing was true or false because the world was at a lower technological level and no one could apply, say, a polygraph in order to check out if those persons were honest or dishonest. Also, such investigations were supported with the legal regulation which would literally send someone in a prison treating those investigation evidence collecting procedures as fully lawful.

With a rapid technological progress there have appeared some real methodologies for estimating an honesty of some claims as a case itself became helped with something which could be assumed as trusted. The criminology is not yet an exact science, but it deeply relies on some products of the technical advancements, as well as certain achievements of the other natural sciences and practices. Also, the entire laws and legal guidelines demonstrate some kind of the support to such a social and technological tendency putting into a case management doctrine that kind of the approaches.

Indeed, there were some reasons why such a policing paradigm was in a use before as anyone being dishonest with the authorities could be punished for providing some fake statements during an interview with the investigators, so far. Even today many communities are warned about the consequences of being dishonest with the law enforcement or the other community members as in this time it's possible to prove that kind of the criminality. In addition, a modern technology is well-developed, but not completely powerful for a reason there will always be some holes in the system which bad guys can exploit and good guys need to find some methods to patch once reported about them not letting a crime to get forcing and threaten anyone within some society.

Anytime, the accuracy has meant an advantage as anyone dealing with the accurate findings can make a lead over the rest of the actors. The 4th industrial revolution has provoked a mass usage of the high-tech technologies even in an everyday life as many of so are web-based and it's well-known an internet service is very cheap anywhere across the globe. That means the modern world belongs to the same network and a plenty of those actions must be adjusted to such dynamic and complicated ecosystem.

On the other hand, the majority of the emerging systems can be traceable and those are still in hands of a legal side of the community. It has been mentioned in this effort that the crime must cope with some rules meaning a successfully prepared criminal scheme which must be investigated and proved with the law enforcement case maintainace as a role of the ongoing policing is to bring to the justice those who disobey a society. Apparently, the investigators are required to offer a deep capacity, as well as some huge capabilities regarding their tasks as the security is a branch which is such a demanding to get delivered via those being in need.

The main reason why is such insisted on the accuracy in the case management is in such a manner there could appear a fair condition to all and the justice would be brought in a more exact and deeply honest way. The tendencies show that so many law enforcement agencies worldwide look for new methods to assure policing being better innovative and probably with a true pragmatism, so far. The world of the knowledge is all around the humankind and as many would agree an only certain thing in the future is a change. For such a reason, the entire case management will need to cope with such a trending as there are yet a plenty of the ideas and innovations which will impact an environment where some community belongs.

Being in position to determine a quantity of something is a true imperative of any scientific methodology as the real science deals with some measurement techniques that are applied in order to improve a result of some scientific research. Indeed, a modern criminology gives a lot of attention to an analytics as a method to increase an accuracy of the Police activities. It seems the entire defense community just accepts well-researched and interpreted results which are covered with a great mathematics getting a role to through numbers and values serve in an evidence collecting procedure.

In an essence, only measurable findings are good enough to make some case and explain what happened in a reality offering such outcomes as clues on the court. In such a sense, it is feasible to prove someone's guiltiness or at least a responsibility regarding any violation or criminal justice offense. Indeed, an ongoing policing is well-modernized and trained to apply an advantage of the novel technological solutions, but it also appears that coping with the best practice in the case management can provide a heap of the opportunities to use some benefits of such a conceptualized investigation practice or in other words, a nowadays policing is very capable to take a step ahead of the arising threats and literally there will be a space to provide more outlets, as well as improve a current best practice in the case management, so far.

It looks like a tomorrow will bring an age of the options and it will be possible to choose between a dozen of the opportunities in order to select something which can give a concrete result. In addition, already there are some concepts in a business which recommend a result-driven approach in order to move up productivity and provide certain advancements in competitiveness on the marketplace counting on a better profit to such an enterprise. At a present time, it seems many want to make a progress and even in the business surroundings that competition will be more than obvious as business organizations will significantly contribute to an economy dictating trends and tendencies among a number of the communities. The law enforcement must cope with such a situation as they would have an adequate response to any unlawful event in some environment serving hard to assure their communities and provide an effective and accurate service at a national, regional and international stage.

Background Overview

The criminal justice case is something that has challenged the law enforcement through the history. The incidental situations can appear anytime and anywhere as a criminal landscape is such a vivid area of the activities. Some of those events are well-known to the authorities either being shared via a community support or uncovered applying some crime prevention program. As the global ecosystem has progressed the Police have become more and more professional developing a strong capacity to tackle any kind of

the offense. At a today's stage, the criminology seems as well-developed and organized machinery which can literally smash anything illegal within some communities.

Indeed, it's a time of the arising threats, but the case management obviously demonstrates some sort of the superiority as an ongoing best practice is capable to deal with the biggest policing challenges. The only thing which should be better improved is an evidence collecting procedure as it might take a lot of time to prove someone's unlawful responsibility. In other words, if that section of the investigation would be more effective, some true results could be just more far reaching, so far. It appears the modern law enforcement strictly relies on an identity management in order to accurately determine who committed a crime either that person or the entire group used some counterfeited documents or the genuine ones.

In other words, something which was a problem yesterday is a capacity nowadays as under today's conditions the majority of the criminal justice offenses can be uncovered and successfully resolved on a behalf of the currently approved best practice in the case management. The modern tendencies suggest a widely applied concept in the criminology is an intelligence-led investigation that can provide a much deeper understanding of the case as in such a scenario it is feasible to in compliance with the laws offer some rigid evidence which if the case is well-investigated can lead to a great epilog on the court judging those who are guilty and supporting the victims, witnesses or the other participants in the investigation.

The most obvious aim of the good policing is to understand how the criminal mind works and even presently coping with some intelligence it is possible to uncover and explain such a question. Apparently, in order to produce some intelligence it's needed to collect some information and put them through some analysis in order to gain an answer to such a remark which habits, behavior models and patterns are typical to some criminal actors. In committing some offense the criminal and terrorist organizations must cope with some rules being known as their schemes pushing aside their personal needs and putting everything below their professional demands which must be met in order to remain in such a business.

The professional criminals operate for a profit, while a terrorist threat is simply an asymmetric concern being used to intimidate the civilians interfering with their private and working lives. The ongoing time is a true Pandora's Box which brought many evils and left some hope to everyone. These days, the world is experiencing a lot of heavy lessons as the asymmetric risk took advantage over their web services to deliver some psychological campaigns, propaganda and brainwashing programs deeply impacting a mental wellbeing, as well as some physical security of many.

The point is those defense challenges are capable to find some vulnerabilities with community just recruiting such careless young men and women to become the soldiers in their rows. Also, in many sections across the globe there are some areas which cannot offer any outlet – only a terrorism and in such a case anyone being born there has no option to choose what to do in own life, but a good portion of the youth goes under such a jihadist program getting selected as so young and powerless to be produced into the most dangerous threats of the modern times. Indeed, those children will not get provided with any schooling as an alternative, but mostly a terrorist training in order to since their childhood grow into killing machines and such merciless warriors for some ideology, belief or mission, so far.

As mentioned in this research, everyone has adopted some kind of the dependability about the cutting-edge technologies and in such a sense it is clear the modern humans leave a lot of so within some grid,

asset or infrastructure. It's an age of the technological boom and many found as enjoyable using some benefits to communicate or control their devices via so quick and suitable internet signal. This tendency is available on the both sides of the law and literally everyone has created some account on the web, as well as has some experience with applying peer-to-peer connecting possibilities.

In a high-tech defense, there are a dozen of the developed techniques, methodologies and practices in maintaining a security in the cyberspace and as it is well-known; anyone coping with such a network leaves a track which can be prevented, monitored and responded at any single moment. Some cyber footage can serve as a good starting point in uncovering who dealt with the infrastructure, what such accurate identity could be and using some tracking capacities where that person's whereby is. In other words, it's feasible to literally catch any activities within cyber systems as no one more can escape from such a technically designed environment.

It looks like the emerging technologies are an outcome of the positive selection providing some highly accurate findings to those who serve with cyber defense. That means if the modern technological landscape can offer a great level of the accuracy such indications and evidence can be considered as very trusted. If those are applied in the case management they can affect the entire investigation providing highly reliable clues which need to get lawfully interpreted and explained.

Such demand seeks form the law enforcement to invest into education, training and some learning programs in order to transfer some skill to their officers that need to make a case or at this stage; prepare a Police story which can correlate all those updates and in some sense; re-construct the events happened regarding the committed offense. The criminal justice case is difficult for tackling and some innovative approaches have shown certain pluses in combating a crime and bringing those bad actors to the justice. In addition, it seems that a present hard situation imposed much higher requirements to an entire defense community as the majority of the law enforcement members significantly improved their capacities to think in a deeply innovative and rational way dealing with a linkage that is better than ever, so far.

User Activities are Traceable

In order to open up and apply a user account within some asset or conduct hacking operation through some infrastructure such cyber facilities remain with the information how, when and from where those activities are done. In other words, everything being delivered via cyberspace is traceable and good forensic detectives can find some clues which can lead to an arrest of such cyber criminals. On the other hand, even if it's about some legal activities those being interested to cope with such findings might gather such evidence in order to follow some trending which can give an outlet to do the entire analytics and statistics of those actions getting in position to make some analytical predictions which can with a very high level of the accuracy suggest what is happening and what could occur in the virtual space, so far.

Further, behind those analytical and statistical investigations there is a strong mathematics being capable to offer a true scientific modeling, which can provide a more predictable research to the law enforcement agencies and the other Police needs. The good analysts are capable to very carefully and with a deep skill process and research a huge dataset giving some reporting as a result of their analyses. Also, they

can document in a mathematical fashion any event in a completely quantitative manner as they cope with the cold logics which can indeed; impact any case or the other actions in a truly rational way. Apparently, it's great dealing with some descriptions, tables, equations and diagrams, but there must be a method to interpret those outcomes as the entire system could cope with those research findings in order to obtain a deep understanding of some policing tasks, so far.

In addition, a similar approach could be applied in following certain events in the cyberspace where the users talk to each other or do some cyber activities such as e-payment, online banking, simple web search or social networking usages. In such a sense, it's obvious many of them even in a legal business would keen to get familiar with the user habits, behavior and interests as once the marketplace tendencies are well-analyzed there can be run certain consumer's campaigns which role is to improve those offerings and attract as many clients as it is possible in order to take a good portion of the marketplace, as well as count on a bigger profit.

At the moment, the user behavior can be observed as a fully lawful concern, but as it is well-known some legal business consumers are everyone being capable to pay for some product or service and as a customer is always right no one will reject the money even coming from a criminal environment as in a business world it's important to make an income, not take that care if the finances are made legally or illegally, so far. From such a point of view, it's clear that something must be done in case of the money laundering through buying some goods, services, retails, estates and much more. At this stage, no lawful business will ask their customer about a background of such money and that's how many will legalize their capital being earned through some crime.

Therefore, the majority of the criminal organizations must pawn some areas over the world and they will deeply go into the legal system trying to in such a case literally pay for their legal status within some communities. Even the modern banking relies on the cyber technologies and any such transactions can be monitored and proved as there are some ways in the ongoing law enforcement to confirm someone's identity just if that person is using some counterfeited details about a certain belonging. In other words, in order to create a bank account or subscribe to some communication plan there will be the entire application form which must be completed and some ID documents must be shown in order to get a permission to use the services of such critical infrastructures. The operator with some telecommunication provider or bank officer with some banking surroundings are supposed to enter data accurately into their online system simply registering a new user to get subscribed to their services which means some footage is left and only through a skillful analysis it's feasible to check out such an account or in another way recommend to such critical assets to put a request on a pending status in order to give some time to the Police to confirm a possible security concern with such an application.

It seems such an approach could serve as a good idea for some crime prevention program which should be well-studied, prepared and implemented among the communities. The counterfeited documents are not necessarily included into the Police register and they might be created with the forgery underworld as those clever offenders can produce something that the modern policing recognizes as a blank ID document. The entire program should be developed very carefully as there can always be some drawbacks with the system which can be overwhelmingly exploited.

In order to avoid such a scenario the law enforcement agencies must assure a comprehensive risk management within a society as in the future those criminal schemes would be completely reduced or at

most rooted off. It's obvious a tomorrow will bring a plenty of the great ideas and suggestions that will truly leverage the Police capacities and give a minimum of the chance to the lawbreakers to even attempt anything unlawful. The current experience regarding such defense community effort indicates that the law enforcement is mainly aware about the possible criminal schemes and those investigators can provide a good portion of the security to their people. The ongoing situation is not yet lawfully resolved as such a task takes time and hard work, but it's getting clear that the future world can count on a much peaceful historical epoch.

The reason why it is expected the coming days will be better than the present ones is today's Police Forces are deeply confident about the global dependability on the cyber technologies as such technical systems can undoubtedly catch any activity within the high-tech space and make it being traceable with those who have a license to pick up such information. In other words, no one is invisible to the system and those being rude to challenge the law must be fully defeated, as well as get strictly punished for their actions. The user behavior analytics is a well-researched fragment of the cyber defense and if there is made some competitive best practice it's reasonable to say that such a field will continue to get improved in order to support the nowadays and next-generation case management efforts, so far.

Collecting Such Left Information

The cyberspace is a segment of the information-communication infrastructure mainly being correlated with the digital technologies that serve in a fast, reliable and accurate findings exchange. In such a fashion, it's obvious there will be a lot of user accounts, as well as direct communications between devices either using peer-to-peer connecting or real-time data transfer. All those activities are such a vulnerable to the hacking attacks as even if there are a plenty of the well-developed and made prevention, monitoring and incident response programs the majority of the incidents in a digital surrounding are not yet mostly covered and investigated.

Combating the cybercrime is a challenge and many defense agencies are aware of such a problem working hard to develop the best practices in fighting that area of the crime. What goes on hand to the authorities is the high-tech asset can memorize anything happening within those networks and in such a sense the majority of those cases can be explained and proved through the entire investigation, so far. The case management outcomes serve to prove someone's guiltiness on the court and in that meaning as that crime area is a product of the emerging time there is yet a heap of the space for learning and improving the skill and expertise contributing in such a manner to the entire law enforcement community.

Putting a cyberspace under exposure requires a great effort as at the present some of the criminal schemes are well-known to the Police Forces, while the others need to be uncovered and literally adjusted to the legal regulations, investigation procedures and the overall case methodology. Just if an incident is reported to the authorities does not mean it will be successfully resolved as some countries in the world simply do not cope with the capacities to combat the high-tech criminalities. In such a sense, it's needed to empower an international collaboration in order to deliver safety and security to the most undeveloped landscapes over the globe.

The reason why some developed economy would support anti-crime actions in any poor community is such a concern occurring there can affect or interfere with the activities of the progressive communities causing asymmetric condition to many at the global scale. In addition, if there are yet critical zones in the world it could be unsafe to send some civilians, business and missions to that region as it could risk a wellbeing of many and threaten some economic interests of the large-scale companies coming to use a local community as a suitable workforce for such a business. Probably through innovations and ingenious approaches the cyber industry will find some ways to prevent or at least reduce the cybercrime within trusted communities simply making their products operate automatically as in such a manner the humans would only deal with the supervision roles.

The automatics and control are a beginning of the modern engineering coming after a very first industrialization happening in the past. With the initial steps in the industrialization across the globe the people have become concerned that machines can take their jobs from them. Indeed, the modern technologies can only make the people's lives being much easier as there are a plenty of the activities and contents the humans could experience and undoubtedly appreciate as the world of a tomorrow will offer much more explorations, expeditions and enjoyable moments to those who belong to the Earth's civilization.

Maybe the entire security will also take advantage over cutting-edge advancements as those endeavors if being applied in a smart way can only make the Police task getting less stressful and much easier to obtain. At this stage of the research effort, it's clear the suggested topic is getting some sort of the reviewing shape as the majority of the cyber defense actors can figure out it was just needed offering some arguments to this discussion which can make it being better explained and analyzed providing everyone with such useful indications and courses regarding such a challenging question as coping with the criminal justice case being tackled mainly relies on the high-tech systems, so far.

Apparently, in order to collect the information being left after someone's activities in the cyberspace it's necessary to apply a digital forensic methodology which is conducted by the forensics investigators which for such a purpose use some specialized tools and software. In such a case, those investigation officers need to carefully examine any incidental situation occurring in the cyberspace as such findings can significantly impact the further actions with the case management, so far. In other words, it's not only about the high-tech criminality cases, but more likely such an approach must be applied in the other areas of the crime as those criminal actors being with the hacking skills or not might take advantage over such a convenient cyber ecosystem.

As mentioned before, there is a strong dependability of everyone in regards with the emerging environment and even if someone is not a hacker that person might be a user of the new technologies. As suggested, anyone today uses the internet, phone communication, banking services and much more and in order to rely on such suitability just the criminals must open up some accounts with those online services. Only the hacker can conduct the entire cybercrime operation and that individual is an advanced user of the cyber capacities. On the other hand, those bad actors dealing with the other crime areas could be just the ordinary consumers of the novel systems as they must cope with some communication and save their finances with some banking organization for a reason those are the ways of organizing the next criminal schemes and remaining in such a business for a while.

The majority of those offenders are not even aware that all their actions could be monitored through the information-communication infrastructure and there are a plenty of the suggestions how to prepare some crime prevention program which can be capable to avoid any criminality occurrence even happens. The criminal masterminds believe and in such a way support their networks to count on the counterfeiting as a method of excluding the authorities awareness about their whereby and the other helpful information. From a today's point of view, it's well-known that confirming someone's identity or recognizing the forged document is not a big deal as there are a lot of the Police techniques which can deeply coping with the ongoing best practices put some case at its final stage leaving some space for a development of some effective crime prevention programs, so far.

Intelligence is produced via Analyses

In data science, there are a dozen of the techniques for collecting, processing and estimating some dataset being picked up as a sample within some data source. In such a fashion, it's obvious that dataset must come from some technological system as data science is mainly oriented to digital findings. Once a net is thrown in a pool of the data a catch can be quite rich getting on the surface many of so which are more or less known to the data scientists. On the other hand, criminology is a science which also deals with some findings, but mostly about the crime and in such a manner it's significant to conduct some data searches that can bring new content to the Police. Those contents are mainly about some case or the incident indicating how, when and where the offense occurred. In other words, all those coming on the surface can bring some novelties to the investigators and in such a sense it's dealt with the information which will consequently be pushed through the further analysis in order to produce some intelligence being helpful to an intelligence-led investigation, so far.

Apparently, anyone doing an analytics among the case management must possess a strong mathematical skill coping with the strict methodology as the least wanted thing in the case handling is an improvisation. In an essence, for such a task it's needed a great accuracy, precision and objectiveness as in the modern time everyone is equipped with the cutting-edge technology and for such a reason it's necessary to analyze data in a highly skillful way as the outcomes of the analytics would be trusted and the investigators could with a grave level of the confidence coordinate the entire criminal justice case or deal with some kind of the crime prevention program preparations. To clarify, the analytics plays an important role in the ongoing best practice as it can offer the real mathematical precision and accuracy supporting a defense community to better understand the crime itself as the Police officers would be in position to protect their communities from any threat.

The practice suggests those findings being gathered within a cyber infrastructure can serve to uncover some criminal actors or catch some incident happening in both – physical and virtual space. In other words, that's why coping with the user behavior within the grid can provide some valuable findings about some criminal schemes, as well as bad actors habits, plans and actions. If obtained shortly those findings can be applied to avoid the next criminal activities as in such a case the authorities can such a carefully locate the offenders and follow them in a real-time simply putting everything through the evidence collecting procedures which will lead to a removal of such a threat. Less threat to communities means a better quality of the life to the common people and well-organized condition to the majority being captured with such a policing best practice.

Indeed, the majority of the high-tech users strongly cope with the cyberspace leaving there a plenty of the information about their activities within the network. For instance, it's always possible to check out if anyone has used some method of the payment through the banking system as those services are completely online or in other words, belong to the cyberspace. On the other hand, someone can create an email account and offer a lot of the information about such a chosen identity making everything about such a communication channel being visible to the authorities through some tracking techniques, as well as uncovering such time and space coordinates anytime some logging has been done. Such information must be accurate and the defense communities will trust them as they are an outcome of the exact sciences and can offer just a true trustworthiness to the case officers. In a cyber security, there is a strong awareness that any user relying on the current technological advancement in order to take advantage over the online services must leave a footage and in a case of the web-based endeavors those traces are recognized as an IP address within the virtual domain or some signal emitting among some telecommunication assets, so far.

The crime scene is a broadly transferable term which not necessarily covers the incident spot, but more likely the majority of the information about the offenders' motion and planning. In such a sense, it's needed to capture the entire criminals' actions not only being focused on a place of the offense, but more widely observing the case from many different angles trying to figure out the locations where the bad actors might be uncovered leaving some track about their coordinates via activated cyberspace devices. The entire system with the high-tech infrastructure is capable to nowadays detect some footage and once those capacities have finished the identity confirmation gather a true fortune of the helpful findings further concentrating on the case management. In other words, in order to collect and analyze findings from some account or the other cyberspace advancements it's necessary to identify who the person behind those activities is and where such an individual is based.

On the other hand, what the priority with the modern criminology is to very carefully go through all registration forms even belonging to the Police, web accounts, telecommunication assets, banking services and much more and in such a case applying a highly centric analysis attempt to come to certain findings about some persons of the criminal justice case interest to the authorities, so far. Also, if through such an analysis there can be more than obvious any single detail regarding the situational awareness those results can also serve in the crime prevention as any single lawfully resolved case is used in developing some approaches in banning the criminals succeed with the same scheme again. Indeed, the authorities must work hard on patching such vulnerabilities as the risk management techniques would be improved offering a truly dedicated service to the communities. In the practice, it takes time to make a good analytics as there are so many data which must be taken into consideration and correlated with each other as those that are in a lawful business will always seek some information from those who want to use their services and in such a fashion those organizations will require to get provided with some user's details as they must maintain their legal status and if demanded by the law cooperate with the law enforcement in case of any illegal occurrence, so far.

Ways of Coping with Tendencies

The only predictable thing in the future is a change which means a lot of new concepts, theories and practices being capable to accelerate a technological progress and impact the lives of the majority of the

people. It seems even the bad guys can still cause a plenty of the nightmares to both – criminologists and community members as with an invention of the new technologies no one will remain on the rest, but mostly try to find some ways how to take advantage over such created conditions, so far. The law enforcement of a tomorrow must cope with such demands in order to provide an effective response to the upcoming trends and tendencies as the crime itself can get a truly novel dimension making those who must challenge the law find the methods to misuse everything being available on the marketplace as they can stay motivated with the profit believing it can bring them some privileges and opportunities. The current best practice with the Police is a very powerful weapon in combating the ongoing crime, but even after some hard episodes within these days all so will be the past sooner or later and the humankind will need to think hard how to handle the global situation even several decades or centuries ahead as what will be seriously needed is to organize a life on the planet in a completely new way not returning to the past and blindly coping with some previously applied models, but more likely trying to define the new roads to everyone.

Maybe some past models in natural and social sciences are yet a good starting point to many researches for a reason they can get a completely new application if get innovated and reviewed in a fully ingenious fashion, but what the main fact is the next generations of leaders will grow up under a totally different environment than their parents and grandparents and they will not fully understand the life before their birth which means they will probably choose to spend their time on their own mainly being preoccupied with the stuffs, situations and events being actual with their lifetime. Many young individuals believe the world started with them and before they reach a certain level of the maturity they might insist to reject anything from the past believing they can offer a better solution than those before them. For such a reason, it can be from a crucial significance to the law enforcement agencies to deal with the youth as figuring out some needs and interests of such communities might provide such valuable information about the trends and tendencies that will come with an adulthood of those inexperienced persons. Also, those carefully selected young people can very early in their life develop a capacity to serve accepting an authority of the adults and showing a certain degree of the obeying attitude about those who are older than them and can navigate them through their lives and services.

Unfortunately, some experience within developing societies across the globe suggests that the criminal masterminds have also recognized such a pattern and offered the crime as a choice in someone's life separating the youth from some good habits and right attitude not letting them to even get schooled, but most likely believe the crime is a good outlet even much better than some serving to the communities as in such countries the bad actors have shown everything as valueless insisting only crime is a perfect selection to many. In such a time of the crises the majority of the mature and experienced people could not even build up their authority over those generations as the criminal environments have rushed them to taste everything such an early and indeed; those young individuals did not want to share a destiny of their parents, teachers and communities which in those times lived in a misery, but they rather waited to get their wings and leave with their life's choices. The situation worldwide has dramatically changed and there happened a real boom of the concerning societies mostly everywhere as some governments became weaken with certain crises, as well as a good portion of them ignored such situations for being corrupted to tolerate the both – transnational crime and terrorism at the same glance.

Apparently, the new tendencies come with the new people as only the humans are those who can create the majority of the conditions within the global landscape. In other words, some unlawful actors will always

try to work on the perfect crime believing just like that they can take advantage over any situation in the world. The most challenging question for a tomorrow is how to prevent, uncover and respond to the asymmetric threats as those organizations can keep operating within their zoning environments literally trying to threaten the entire communities distantly relying on the online services. Once aware about such a possible scenario the law enforcement agencies can serve hard to develop some sort of the risk management program which could be capable to provide a good response to such a generated threat, so far.

The people of the future will undoubtedly be familiar with the history of the mankind as some brilliant ideas, as well as unresolved problems can be found in the past and be provided with an opportunity in the coming days to get deeply understood by those who lead the entire countries, regions and international community. The change is always a very certain thing for a reason the next generation humans will as during any epoch be busy with their everyday concerns serving hard to contribute to the betterment of many simply offering their commitment to their communities. Also, it is expected with a light of the technological progress and growth there will be more opportunities to everyone as the human civilization must go beyond the frontiers of the ongoing age.

In addition, it appears there are yet a lot of questions from the past which are getting their answers even today or need some dedicated effort to get tackled in the next times. For instance, the digital system findings suggest that even nowadays that scientific stream is not fully researched and there are still endeavors which wait to see the sunrise. Above all, as it's dealt with the exact sciences it's believed that the Earth's civilization will sooner or later be in position to register any single member of the humankind in such a way making such a powerful system that will have a capacity to totally get aware about the habits, behavior and actions of any single individual across the world just via a well-delivered security to all societies, so far.

Investigation Must Deal with Accuracy

As a dependability on the new technologies is increasing it's obvious why anything regarding the information-communication infrastructure can provide a high degree of the accuracy. In such a case, the majority of the criminal incidents can be managed through some investigation giving a chance to those case management teams to collect findings and clues taking advantage over such interconnected actors. If it's about some user behavior recognition it's clear in that fashion some useful actions can be taken in order to make a case and comprehensively explain the entire occurrence being supported with a truly accurate finding, so far. It seems such an approach can significantly improve a quality of the case management, as well as make the entire investigation being less time-consuming and more precise in sense of such produced results. The current best practice in the case management is very impactful and with a greatly followed tendency in the future there will surely be methods to both – tackle and prevent some criminal offenses in the community.

Discussions

In the practice, the investigation dealing with better accuracy can offer a deep understanding of some criminal justice cases, their actors and the entire correlation of everyone with everything as applying such an approach it's feasible to literally smash those threats not leaving an opportunity to anyone even attempts anything similar tomorrow. Apparently, it seems there will yet be a plenty of the space for preparing crime prevention programs in order to reduce a rate of the criminality among the societies.

Conclusion

Finally, it appears it's needed to make a synergy between the different disciplines such as criminology, high-tech security, analytics and technical sciences as some outcomes of the future actions would offer a progress at all levels of the community's life and functioning bringing the certain betterment to anyone being lawful, so far.

References:

[1] Djekic, M. D., 2017. The Internet of Things: Concept, Application and Security. LAP LAMBERT Academic Publishing.

[2] Djekic, M. D., 2021. The Digital Technology Insight. Cyber Security Magazine

[3] Djekic, M. D., 2021. Smart Technological Landscape. Cyber Security Magazine

[4] Djekic, M. D., 2021. Biometrics Cyber Security. Cyber Security Magazine

[5] Djekic, M. D., 2020. Detecting an Insider Threat. Cyber Security Magazine

[6] Djekic, M. D., 2021. Communication Streaming Challenges. Cyber Defense Magazine

[7] Djekic, M. D., 2021. Channelling as a Challenge. Cyber Defense Magazine

[8] Djekic, M. D., 2021. Offense Sharing Activities in Criminal Justice Case. Cyber Defense Magazine

[9] Djekic, M. 2019. The Informant Task. Asia-Pacific Security Magazine

[10] Djekic, M. D., 2020. The Importance of Communication in Investigations. International Security Journal

[11] Djekic, M. D. 2019. The Purpose of Neural Networks in Cryptography, Cyber Defense Magazine

[12] Djekic, M. D. 2020. Artificial Intelligence-driven Situational Awareness, Cyber Defense Magazine

[13] Djekic, M. D. 2019. The Perspectives of the 5th Industrial Revolution, Cyber Defense Magazine

[14] Djekic, M. D. 2019. The Email Security Challenges, Cyber Defense Magazine

[15] Djekic, M. D. 2016. The ESIS Encryption Law, Cyber Defense Magazine

[16] Đekić, M. D., 2021. The Insider's Threats: Operational, Tactical and Strategic Perspective. LAP LAMBERT Academic Publishing.

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, the Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the books "The Internet of Things: Concept, Applications and Security" and "The Insider's Threats: Operational, Tactical and Strategic Perspective" being published in 2017 and 2021 respectively with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert's channel. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU), Censys Press, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

Cyber Defense Magazine– PQC & Biometrics

Why biometric security is crucial in a post-quantum world

By Nils Gerhardt, Chief Technology Officer for Utimaco

Many are saying that passwords have now become obsolete – they can be stolen, 'brute-forced' or guessed, and are too vulnerable to lay the foundations of our digital security as we shift towards a post-quantum future. In fact, given that 70% of people reuse passwords, guessing is very easy. All Cybercriminals need to do is to buy a list of email addresses and, after gaining access to a site's shadowed password file, crosscheck each password against the encrypted passwords. Once matched, the password can be used on the site.

However, new hardware devices are making it possible to avoid using passwords for anything from logging into websites to accessing restricted areas. Combining biometrics with smart design and the latest authentication protocols, they could become part of everyday life for millions of people as we move towards a new age of much stronger security and quantum computing.

The end of the passwords

While foreign espionage groups have been using free USB sticks and phone chargers to install keylogging software on target computers for a while, this technique would only continue to work if passwords remain the most important method of validating users. It can certainly be problematic for online businesses and an even larger problem for businesses and government organisations if they handle sensitive information.

Alphanumeric passwords are not only the standard for logging into websites, but in thousands of other places, including PIN numbers used in bank cards, unlocking phones and in entry keypads. Someone peering over your shoulder could quite easily access your bank account, phone (and with it every other password stored on it) or even your home or office.

Alphanumeric passwords are also far more likely to be compromised by an eavesdropper or 'social engineer' rather than by hacking. Common encryption standards like RSA would take trillions of years to 'brute-force' passwords, so techniques like phishing were used in high-profile penetrations like the 2016 DNC hack. Increasing the complexity of passwords and mandating that each one be unique will only make passwords so complex that most people won't be able to use them.

Two-factor or multi-factor authentication increases the security of password-based systems by adding other factors. However, it is rarely used due to its multileveled complexity. Thus, almost every compromised Microsoft account didn't use multi-factor authentication even when it was available.

The rise of biometric security

Biometric security has been around for as long as alphanumeric passwords and arguably earlier, since recognising somebody by their face has predated writing. Modern biometrics such as fingerprint security, facial recognition and behavioural biometrics have become integrated into everyday life.

Despite it being easier and more secure than alphanumeric passwords, biometric authentication may still rely on information being sent from one place to another (a fingerprint reader sending a user's fingerprint to a cloud server where it will be verified), and although it will be encrypted during transit. If the fingerprint reader or even the cloud server at either end is compromised, for example, then biometric security may still be exploited.

Many of us will already use fingerprint security to unlock our phones, and an increasing number of us will use Near Field Communication (NFC) at least somewhere, whether that is using your phone to pay for a purchase, unlocking a door with a key fob or logging into sensitive systems (the NHS uses NFC cards to log users in to their computer network, for example.) The FIDO security standard allows users to use NFC or USB keys to log in to websites, meaning that only a key holder would be able to log into an account. Of course, an NFC key card can be used by anyone, and there is no way of verifying that the person using a key is its correct user without another form of verification.

Quantum computers being developed could break the cryptography used in passwords in a matter of days or even hours, whereby contemporary computers could not. Therefore, every piece of data would

need to secured by one of the newly developed quantum-resistant algorithms to prevent bad actors from breaking passwords without the need to use phishing or social engineering.

The future of cybersecurity

Although these replacements for passwords may have disadvantages, a card-based biometric system that removes these limitations and allows governments, companies and individuals to verify their identity securely is currently being developed by Pone Biometrics, a Nordic R&D-driven cyber tech company.

With its own operating system and embedded applications, Pone Biometrics aims to develop a fingerprint reader on a card that acts as a microcomputer. Users that log into a website or open a door, can tap their card while pressing their thumb or finger on the reader. The onboard computer checks their print and transmits the encrypted verification to the device securely, meaning that very little is sent between devices.

Since the cards are only active when in use, there is no possibility that they will be 'skimmed' while a user believes that they are inactive and a visual display that shows if it is in use. The internal battery can last 2-3 weeks between charging, and it even has a failsafe system in place that protects users from being forced to use it - they can have a 'failsafe finger' that will wipe the device if used.

These cards could end up being used wherever there is currently the need for authentication – a government employee could use the same device to access sensitive information while at work and use it to open the door to their home and log in to accounts on their home computer.

To ensure biometrics survives, cryptography protecting biometrics from future quantum computers would need to be integrated into any new security systems from the start. After pursuing feasible security for over 25-years, Utimaco has been developing technology to counter quantum computers years, perhaps even decades before they are widely available. By combining next-generation biometric security cards with future-proof quantum resistance we can enter a post-password world.

About the Author

Nils Gerhardt is the Chief Technology Officer for Utimaco, a leading provider of cyber security solutions, and board member of the IoT M2M Council. Before joining Utimaco, Nils worked at Giesecke + Devrient in various executive management roles with regional and global responsibilities in Germany, Canada and the USA. As Chairman of the Board of GlobalPlatform, a global industry organization, Nils brought major companies together to define the standards for secure digital services and devices.

Nils can be reached online at linkedin.com/in/nils-gerhardt-38b6691 and at our company website https://utimaco.com/

About Utimaco

UTIMACO is a global platform provider of trusted Cybersecurity and Compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA). UTIMACO develops on-premises and cloud-based hardware security modules, solutions for key management, data protection and identity management as well as data intelligence solutions for regulated critical infrastructures and Public Warning Systems. UTIMACO is one of the world's leading manufacturers in its key market segments.

500+ employees around the globe create innovative solutions and services to protect data, identities and communication networks with responsibility for global customers and citizens. Customers and partners in many different industries value the reliability and long-term investment security of UTIMACO's high-security products and solutions. Find out more on www.utimaco.com.

Virtual Security and why it matters so much to SMEs

By Jack Viljoen, Head of Marketing, Prodinity

In recent years, there has been an exponential rise in the number of cyber criminals targeting small to medium-sized businesses (SMEs) – many of whom are extremely vulnerable to cyber crime due to inadequate security infrastructure and cyber awareness training.

In this Q&A, Jack Viljoen, Head of Marketing at data-driven insights specialist, Prodinity, discusses some of the issues facing SMEs and why advanced cyber penetration (PEN) testing is vital to stress-test and strengthen their security capabilities.

Why is Cyber Security so important?

Firstly, I'd like to start by mentioning that I really don't like the term Cyber Security. It's vague, futuristic and doesn't really mean anything to someone who isn't in the industry. I much prefer the term "Virtual Security".

What exactly is "Virtual Security" and why is it something we need to worry about? If you are a small-medium sized business owner or executive, there is a good chance that you do not think it applies to you.

Why are SMEs targets for cyber criminals?

Why would hackers be interested in breaking into your organisation, when there are multi-billion dollar companies or governments to hack? It's certainly a valid question. We always hear about it when a huge organisation is broken into but rarely when it happens to small businesses.

The truth is it does happen - and far more often than you might think. In fact, there were over 400,000 reports of fraud and cyber crime in the UK last year alone (Source: NFIB Fraud and Cyber Crime Dashboard) and in 2021, UK businesses lost more than £736 million to hackers (Source: Cyber Crime Cost UK £2.5bn in 2021 (Holistic.iT)).

Hackers will often target smaller businesses because there is less sophistication in their security systems, and they are easier targets. In fact, some statistics say that SMEs are three times more likely to be the victims of cyber crime than large businesses.

What is PEN testing / ethical hacking, and why is it important?

Through a targeted attack simulation, a penetration (PEN) test can take your business safely through real-world attack scenarios, allowing you to find and fix vulnerabilities before attackers can exploit them. You then receive a complete accredited report, which can be submitted to cyber insurers.

With cyber crime on the rise, cyber insurance claims have also seen an unprecedented increase, but many companies are finding that their current insurance packages simply aren't covering them. They have had claims refused on account of neglecting basic virtual security, and with so much uncertainty, obtaining comprehensive cyber insurance is becoming more and more difficult.

So, what can you do to make sure that you are protected? Start by viewing virtual security the same way as you view physical security. Cyber criminals will often look for openings in systems like burglars walking down a street, knocking on all the doors until they find one that has been left unlocked. You wouldn't dream of leaving your doors and windows unlocked so why do the equivalent virtually.

Red teaming – testing defences where the physical world meets the data world. Why does this matter?

Red teaming is like a PEN test in the sense that it is a simulated attack on your system. Where it differs, however, is that with a PEN test, the goal is to identify all the vulnerabilities and provide targeted solutions.

Red teaming really allows you to view a cyber attack from a hacker's perspective. The team will do everything and anything to breach an organisation's security, including but not limited to targeting hardware, systems, software and even employees. This is vital as 95% of cyber security breaches are still caused by human error which means testing your employees' responses to attack simulations is still the most effective way to prevent serious data breaches.

Red teaming can even include breaching the organisation's physical security, and really puts security protocol to the test. This can often bring to light vulnerabilities you may never have thought of.

What does continuous improvement look like from a cyber defence perspective?

It isn't all doom and gloom though. Statistics show that an annual "Virtual Security" review is the most effective solution to prevent data breaches. This could include a PEN test, as well as red teaming and a cyber security seminar to keep employees informed about new threats and up-to-date cyber security information.

Cyber criminals and virtual crime are constantly evolving. Instances of cyber crime have been steadily rising over the last decade and will continue to do so - and as our technology becomes more sophisticated, so do the hackers and cyber criminals.

It's important to continually update your Virtual Security and ensure that you are always protected.

About The Author

Jack Viljoen is an experienced sales and marketing specialist who has had considerable success executing strategic marketing initiatives and effective key account management in both domestic and international markets. He started his career in the telecommunications and further education sectors and he now brings this expertise to Prodinity's new cyber security solutions, helping clients secure their assets and protect their most valuable data.

Jack can be reached online at jviljoen@prodinity.com, LinkedIn and Prodinity website.

Why "Point-In-Time" Solutions Are Losing The Battle Against Sophisticated Fraud

By Alisdair Faulkner, CEO at Darwinium

Cybersecurity and fraud teams have been locked in a technology arms race with their adversaries for years. Once again, they are on the back foot. Over two-thirds (68%) of businesses face the challenge of fraudsters adapting faster than their current tooling according to our latest research. The stats speak for themselves. US consumers reporting losing nearly $6bn to scammers in 2021 alone, a 70% increase on the previous year. The real cost to businesses will be many times higher.

It's time for change. Legacy fraud and risk solutions rely on incomplete, siloed intelligence extracted from "point-in-time" interactions. They're inflexible, unwieldy, slow to deploy and update, and add needless customer friction—which can end up costing businesses more than potential fraud losses. Organizations need a better way: risk-based journey orchestration that works seamlessly across the entire customer journey for better-informed decision making.

Deep fakes and adversarial AI: an armory of innovation

There's no doubt the offensive team holds much of the advantage today. Fraudsters are leveraging the latest tools and techniques to emulate devices and mimic user behavior, disrupt risk models through

adversarial AI, and automate attacks by testing millions of stolen identities in seconds. They use stolen and synthetic data to open new credit accounts, hijack existing accounts for payment and personal info. They deploy highly convincing techniques like social engineering to trick users into handing over data and money, and use stolen card details to make fraudulent payments.

According to one estimate, new account fraud (NAF) in the US surged 109% between 2020 and 2021, account takeover (ATO) increased 90% and credit card scams rose 69%. Another predicts that payment card fraud losses alone will exceed $343bn globally between 2023 and 2027.

The problem with point-in-time: the risk of digital snapshots

The challenge for fraud teams faced with this onslaught is that they're mainly working with first- or second-generation tools which exacerbate existing operational silos between security and fraud divisions. In short, attacks span the entire user journey, from browsing and new account creation to logins, payments and more. Yet security and fraud teams lack full visibility and context. Security analysts might have insight across all traffic, but without the full context of customer behavior further downstream. And fraud teams have full business context but only make risk assessments based on single, point-in-time digital interactions. Put simply, attacks happen across the journey so why is prevention technology currently point in time?

For fraud and risk specialists, this disjointed approach plays right to their opponents' strengths. Fraudsters masquerade as real customers in ever more complex attacks across a business's digital touchpoints, safe in the knowledge that risk decision engines will not be able to join the dots between user information silos to flag suspicious behavior. Even worse, these legacy systems require significant integration effort and a high level of front and back-end development resource. And they often create extra customer friction, leading to cart abandonment and churn.

Why understanding risk is a continuous journey

Rather than adopting this point-in-time approach, fraud teams need a way to continuously scrutinize the digital journey of their customers from before they even land on a site to the second they leave it.

How would this work in practice? The smartest move would be to install these risk-based orchestration capabilities at the content delivery network (CDN) layer, residing on the network edge. This way businesses could risk assess all digital traffic from the perimeter edge, rather than via individual API calls on certain pages of their website. This delivers several advantages around latency, security and privacy. Data is processed within existing infrastructure; reducing risk and better protecting customer experience.

Making sense of complex data

Once a continuous view of a customer journey has been established, how can businesses best aggregate this complex and extensive data to make effective and quick risk decisions? One of the challenges of

current fraud solutions is that their risk assessments rely on the aggregation of multiple rules based on digital identity data and user behavior across multiple individual interactions. For some organizations, these rules can run into the hundreds and thousands, which means making a risk decision is both complex and lengthy. Alongside this, there is an industry movement towards simplicity in systems due to lengthy, adhoc and often complicated decisioning processes which can fail during times of employee churn and talent shortages.

Businesses need a simple way of aggregating complex data over time so that they can compare an existing action, or user journey, against previous patterns, but without overcomplicating this with multiple, extensive lists of rules.

Creating ways of aggregating data across devices, locations, behaviors and user journey behavior would allow risk assessments to be made based on patterns, or signatures, rather than binary rules.

This is particularly powerful across user journey behaviors. For example, businesses could track similar journey signatures for something like Account Takeover, linking particular credential testing and bot attacks with downstream attacks on a user accounts, or fraudulent credit card payments.

Trusted behavior patterns can essentially be “cohort-modelled” to reduce the number of legitimate customers that are stepped up, even if they’re new to a business and the system hasn’t had time to baseline them. Further, any anomalies can be spotted at multiple stages of a digital interaction and interventions made in real time, on a per-user basis. It all makes for a more seamless customer experience while keeping fraud losses and chargebacks to a minimum.

Eliminating the siloes that fraudsters exploit

By understanding the context of the entire user journey and harnessing aggregated digital “signatures” to simplify risk decisions, organizations can start to join together every step of a user’s digital journey, removing the siloes that fraudsters play in and better separating good and bad intent.

And as part of this approach, real time intervention is key. Businesses want to block high-risk behavior before it impacts either their customers or their bottom line. They can’t afford to wait for the next release cycle or resource availability. Seeing high-risk behavior and either stopping a transaction dead, or sending it for further review, reduces both risk and the opportunity for fraudsters to pivot to a new vulnerability. In this way, they can enhance the user experience by making sure their best customers are recognized and rewarded with digital experiences they deserve.

About the Author

Alisdair Faulkner is the CEO and Co-Founder of Darwinium, a pioneering customer protection platform that holistically assesses every digital interaction to identify bad behavior, in real time. The Darwinium team has a combined experience of over 200 years managing fraud and risk for some of the world's largest banks, ecommerce platforms and fintech providers.

Prior to building Darwinium, Alisdair co-founded, built and scaled ThreatMetrix, the world's leading Digital Identity company which he sold in 2018 for $830 million. Alisdair created the Digital Identity category, grew recurring revenues from $0-100M USD, resulting in a billion-dollar acquisition by a FTSE 100 company.

Before ThreatMetrix, Alisdair was a founder and head of products and business development for NetPriva, a leading network performance software provider, acquired by Expand Networks now Riverbed.

He is now a noted industry expert in issues relating to online fraud, cybercrime, identity theft, information security and networking technology.

Alisdair can be reached via the company website at https://www.darwinium.com/.

Why Finding The Right Load Balancing Solution Is Crucial For Hybrid Cloud

By Jason Dover, VP of Product Strategy at Progress

In today's competitive landscape, every business seeks to find ways to carve advantages that give them a small edge over their counterparts. The large number of new digital and web 2.0 entrants into just about every industry is one of the key drivers that's made this more important than ever. Out of this operating environment have emerged the concepts of digital transformation and business agility, where enterprises seek to use IT as a revenue generator and differentiator as opposed to simply being a necessary utility. This environment has proven to be the perfect incubation ecosystem for cloud adoption.

Drivers for Hybrid Cloud

While many approaches and patterns for cloud usage exist, the most common is hybrid cloud. By definition, a hybrid cloud includes at least one private cloud ecosystem along with one or more public cloud environments that are managed using unified models, tooling and playbooks. The primary benefits of this model are agility and the ability to provide the best platform for given applications and services while minimizing swivel chair management.

Despite these benefits, not every workload should be deployed in a public cloud. On the other hand, other services and applications are much more efficient when coupled with the just-in-time deployment options and horizontal scale options that a public cloud natively facilitates. In order to be efficient, the additional

complexity of a hybrid environment must be tied together with common management, unified policies and a consistent security model.

Load Balancing in a Cloudy World

In cloud operating environments, whether on-premises or hosted, the principles around load balancing have changed significantly. While the core of load balancing is still fundamentally centered on providing intelligent traffic distribution across endpoints, data centers or clouds, there are new considerations that must be taken into account.

In the past, the common approach was to consolidate as many applications as possible onto a centralized multi-tenant set of physical appliances. With the advancements made in x86 architecture and efficiency, virtualized load balancers have become more popular given they are now able to deliver significantly more performance. The idea of creating smaller blast radii that allow for more frequent changes with micro-impact footprints has driven the adoption of per-app or per-service load balancers that are only responsible for proxying a very small part of the environment.

With this approach, modifications and updates that have unintended impacts have a minimal impact on the overall environment. Similarly, when this architecture is used to facilitate segmentation and support the limiting of lateral movement, successful breaches from threat actors only impact a small amount of the ecosystem.

Cloud-native application architecture is another key driver for enterprise strategy around load balancing. When building new apps with cloud-native architecture principles as the cornerstone, it's very likely that these workloads will be deployed alongside traditional infrastructure. Load balancers with the right capabilities can help to bridge gaps in this scenario, for example, by enabling the scaling dynamism that exists within a containerized environment to be reflected in the physical network automatically.

The need for this is reflected by the increase in customer RFPs that call out the need for load balancers under consideration to have the ability to understand the context and schema of Kubernetes container management environments.

Blueprint for a Sustainable Strategy

Principles are key in IT because they allow operators to be flexible and respond in a way that's not possible with a fixed set of static rules. Good principles drive good decision-making in agile and dynamic environments.

Given the complexity of modern IT, the demands on the office of the CIO and the operational challenges facing I&O teams, it is vital to have a set of foundational principles to drive the strategy around the selection and use of the critical component of load balancing.

Here are a few principles to consider:

1: Identify Application Business Goals

Load balancing selection must be based on the outcomes of the applications, services and workloads being serviced. Despite the general trend towards virtualizing network functions such as load balancing, if a specific application or environment requires compliance with higher-level versions of standards such as FIPS 140-2 or a very high level of TLS transactions, a hardware solution may be the ideal option.

On the other hand, a highly scalable and modernized enterprise deployment that is looking for high levels of isolation combined with the ability to prevent independent tenants from impacting their neighbor's performance may prefer a virtual deployment of a fabric of micro-per service instances. The main point is that instead of letting your incumbent vendor drive the development of your RFP, it's important to first evaluate key outcomes and objectives.

2: Consider How What You Implement Will Impact Security Posture

With the increase of cyber threats, it's become more popular for organizations to consider how they can apply existing components within their environments to improve their security posture. One of the most under-utilized components is the load balancer. As the point of ingress for all client application requests and egress for all service responses, the load balancer occupies a privileged position. When optimally implemented with the right product capabilities, this position can be leveraged to help address security requirements.

As an example, certain key PCI DSS compliance requirements can be addressed with the implementation of a web application firewall (WAF). Most security-minded load balancer vendors have implemented WAF functionality as a core load balancing function. By design, a load balancer serves as a rudimentary firewall by preventing access to proxied services other than what's explicitly defined to be allowed. When combined with embedded authentication and authorization services that can be integrated with third-party identify providers, a properly equipped load balancer can serve as a key supporting pillar of a zero trust strategy for application access.

Additionally, as a common consolidation point for certificate management, a load balancer can further be used as an enforcement point for the prevention of the use of insecure ciphers that provide potential conduits for threat actors. The ability to identify the characteristics of incoming requests can also be used to control access policies to applications and services for internal traffic versus external traffic and to bolster a defense-in-depth strategy.

3: Ensure Licensing and Consumption Flexibility

Today's approach to IT requires that flexibility and future-proofing are integral to all implemented solutions. This is a critical buying criterion to support the typical office of the CIO's objective for achieving greater agility. One way that this emerges in the context of load balancing is around licensing and consumption. Historically, the primary licensing of load-balancing solutions was based on purchasing perpetual licenses on a per-instance basis combined with an annual or multi-year maintenance contract.

When the environment scaled and capacity limits were breached, a “rip-and-replace” approach was required to scale the environment vertically with higher-performant instances.

While this is often still sufficient, there are many cases where flexible approaches, such as buying access to capacity pools or having scale-out/scale-in mechanisms directly tied to actual usage, are desirable as well. When assessing a provider, ensure that these options exist and that there is a way to transition between models based on the changes in your business’s requirements. This will ensure that you will be able to achieve maximum agility.

What load balancing looks like now is the result of a progressive evolution over the past couple of decades. It’s likely to change even more significantly over the next few years thanks to a convergence of cloud and digital transformation trends combined with foundational changes to how modern applications are built. The underlying principles that made these solutions such a critical part of current application infrastructure, however, still remain applications and services that need to be highly available, performant and secure, and certain functions need to remain best handled outside of the application itself.

This means that when considering what solutions to implement, enterprises should consider how the options they review will support those needs in the environment they expect to have over the next several years. Given the likelihood of having a hybrid cloud model, businesses should significantly factor in the characteristics associated with a heterogeneous cloud ecosystem. In doing so, they can ensure an optimal application experience enabled by a well-configured and adaptable load balancer and can evolve their infrastructure wherever their cloud infrastructure strategy takes them.

About the Author

Jason Dover, Vice President of Product Strategy at Progress, and have over a decade of technology leadership experience working across enterprise organizations. At NYSE Euronext and Deutsche Bank, I provided consultative services for directory and messaging integration projects including the integration of key systems between Liffe, AEMS, AMEX and Euronext with the New York Stock Exchange. At Kemp Technologies, I held various roles across sales, marketing and product management. I am currently President of Product Strategy, responsible for overall application experience (AX) product portfolio direction, product marketing, support of corporate development activities, strategic partner engagement and Horizon 2 initiatives.

Jason can be reached online at (jason.dover@progress.com, https://twitter.com/jaysdover) and at our company website https://www.progress.com/

Why Low-Code AI Is Needed Now More Than Ever

By Solomon Ray, Director of Innovation, Strategy, and Special Projects at Iterate.ai

As a business leader and executive, a “low-code strategy” may not be on the top of your mind, but it presents a valuable opportunity to transform your organization digitally. At Iterate, we take an even more bullish view on low-code adoption; it will become table stakes for every digitally agile organization in the near future. The trends have been shifting. Gartner notes “By 2025, 70% of new applications developed by organizations will use low-code or no-code technologies, up from less than 25% in 2020. The rise of low-code application platforms (LCAPs) is driving the increase of citizen development, and notably the function of business technologists who report outside of IT departments and create technology or analytics capabilities for internal or external business use.” John Selvadurai, Ph.D., VP of R&D at Iterate, has seen the immediate impact of implementing a low-code strategy. He emphasizes, "Maintaining enterprise applications long-term is a very costly operation. These enterprises can reduce that maintenance overhead significantly by having an organizational level low-code strategy."

The relevance of low-code application platforms is not limited to software developers or IT teams. It is certainly befitting of a top-down *business* strategy. Low-code adoption is a catalyst for increased

organizational agility, faster go-to-market product cycles, better cost-effectiveness, and greater talent and resource management. To further elaborate:

- **Agility:** The speed of technology evolution dictates organizations to be more agile. Yesterday's tech stack may already be outdated today. The elegance of low-code is its modularity. Independent components create a plug and play environment within an application flow. Therefore, an organization can make small changes rapidly, literally iterating to the market.
- **GTM**: Low-code componentizes blocks of code, allowing their reusability, which improves development times compared to traditional coding methods. Rapid assembly of pre-built components into flows, nodes, and templates simplify software development. Consider the current traditional model, where teams of developers, even in remote locations, have to manage complex sprints to enable integrations between frontend and backend applications, legacy systems, and data silos. Many low-code platforms claim a 10x faster app development. At Iterate, we have measured up to 17x with our platform.
- **Cost-effectiveness**: Code reusability, shorter development cycles, and simplifying workloads all cumulatively reduce software development costs. Furthermore, over the long run, these savings make a significant impact to your budgets in building, upgrading, and integrating new applications.
- **Talent and Resource Management**: If we consider a macro picture, there are roughly 25 million software developers in the world. In contrast, the global talent for AI engineers is at 300,000 (in 2017) according to Tencent. An organization with limited resources would be hard challenged to compete for AI talent, yet at the same time, it would be foolhardy to ignore the importance of AI application development, given that enterprise AI technology is growing at over a 20% CAGR. Low-code brings accessibility to AI development. Using the same methods of componentizing blocks of codes, pre-built AI/ML models can quickly be customized and deployed for commercial applications. Iterate's platform, Interplay, has 43 of them. From a micro point of view, low-code upskills your existing developer team. For example, a web engineer can easily use a low-code platform, with existing AI components, to build AI-powered chatbots/voicebots, product recommenders, knowledge graphs, computer vision applications, and much more. With Interplay, it is possible to build and deploy these applications at a production level, with the scalability and security requirements met. Similarly, non-developers can embrace a low-code environment to drag and drop blocks and make enterprise applications, not necessarily just AI ones. These can be frontend web forms, mobile apps, HR/finance databases, etc. Upskilling with low-code in effect maximizes the productivity of not only your developer teams, but also your entire organization.

The preceding arguments are explicit reasons to apply a top-down low-code strategy. Additionally, there is an implicit but powerful advantage to strongly investing in low-code for your enterprise AI development. There is a "dirty secret" about relying on external vendors to develop AI applications provided by vendors, whether via SaaS or license models. The intellectual property that comes from developing your use cases - the AI/ML models and algorithms - is not necessarily yours. Oftentimes, your proprietary data that is needed to build out your AI use cases are training your vendors' models, which is their IP. Considering the effort required to gather, manage, and process data, not being able to own any of the final assets is a considerably missed opportunity.

Before you assume that owning your AI/ML IP necessitates recruiting a team of data scientists and AI engineers, low-code offers a very practical solution. While pre-built AI/ML models and open source libraries can be easily integrated into the environment, these resources can be customized (by your existing developer team as previously established) into your own proprietary IP. Training these models with your own data, you can create your own "derived" AI, which you can tailor to your own unique business cases. Brian Sathianathan, CTO and Co-founder of Iterate.ai, affirms, "***AI development follows the 80/20 rule; 20% of the AI methods can address 80% of your AI solutions in the market. Derived AI is more than sufficient for most organizations to capture those 20% of methods, and leaders should treat it as a competitive advantage.***" Keeping your own AI model development in-house ensures your complete stewardship of your valuable data and its privacy, as well as the flexibility to use those models and their algorithms for any other use cases. Again, adopting low-code within your organization affords innumerable benefits for your business strategy.

The general philosophy around digital innovation is to resist inertia, be agile, and adapt to change. As such, digitally forward leaders and their organizations should always have a sense of urgency about technology. When thinking about innovation, **today is the day to start. Tomorrow is too late**. Low-code is no exception; the opportunities you embrace with its strategy will pay off the sooner you start.

About the Author

Solomon Ray has extensive experience in management consulting, startups, and technology. He has worked at companies such as Samsung, Applied Materials, and Xerox PARC, advised seed-stage startups, and consulted large enterprises. He holds a BS in Electrical Engineering from UCLA and an MBA from the Johnson School of Management at Cornell University.

Why Power Matters in Cyber Protection

Defending power management equipment in an era of more connectivity

By James Martin, Global Connectivity Product Manager, Eaton

It's well understood that as digital evolution continues opening doors for greater connectivity of devices, enterprises must ensure that new potential entry points are protected from potential cyber attackers. Businesses that strike this balance stand to capitalize on IoT while reaping the benefits from advancing solutions like predictive analytics to help streamline operations and make more proactive, data-driven decisions.

Power devices are becoming a bigger priority for cyber defense as enterprises bring them into their expanding network infrastructure. Earlier this year, the Cybersecurity and Infrastructure Security Agency and the Department of Energy issued a warning concerning network-connected uninterruptible power supply (UPS) devices, urging organizations to take steps now to stave off potential attacks.

Enterprises should evaluate their current cybersecurity game plans now and incorporate power management, considering the steps that follow.

Assess current readiness

Protecting power devices can not only boost enterprises' cyber defenses, but also strengthen trust with their customers. Gartner predicts that by 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements. Having a well-rounded cybersecurity approach that includes power management can serve as example to customers or partners that an enterprise takes network threats seriously across the board.

Global safety standards offer a strong benchmark for IT teams to work from when deploying power devices and solutions. Underwriters Laboratories (UL) and the International Electrotechnical Commission (IEC) provide important guidelines for the implementation of appropriate cybersecurity safeguards in network-connected devices, including those in the power management space. Deploying UPSs with network management cards that carry UL 2900-1 and ISA/IEC 62443-4-2 certifications can give teams peace-of-mind that their devices were developed with cybersecurity in mind.

Employ best practices

In addition to leveraging power management solutions with baked-in cybersecurity capabilities, enterprises should use best practices with power management technologies that apply across an interconnected network. Examples include using firewall and industrial security solutions as well as encrypting information; conducting routine security assessments; regularly updating antivirus software and antispyware; using advanced email filtering; establishing powerful password policies and end point protection; and offering employees cybersecurity awareness training.

Enterprises should also look to execute remote firmware updates to keep current with the latest features. Selecting power devices that require cryptographic signatures for all firmware updates can help IT teams avoid cybersecurity risks. Additionally, looking for vendors that offer 24/7 monitoring across converged IT/operational technology (OT) environments will add an extra layer of protection and visibility for critical infrastructure.

Although primarily developed to monitor and manage power devices – as well as gracefully shut down critical loads during outages – power management software can also be used to provide an inexpensive, highly viable air gap solution. This measure helps keep secure networks physically isolated from unsecured ones including the Internet. Organizations such as Grandeur Housing use this method to safeguard against ransomware attacks while enhancing overall cybersecurity.

Embrace the evolution

By leveraging power management software, enterprises can stay on top of emerging cybersecurity threats like the Ripple20 vulnerabilities, which surfaced during the early days of the pandemic and put many internet-connected devices in jeopardy. Power management software allows IT teams to keep up with the latest patches and secure their power management components from Ripple20 and other new threats that develop.

Enterprises may also find it useful to partner with technology and solutions providers that demonstrate an ongoing commitment in protecting against cybersecurity risks as the proliferation of smart, connected devices link together more elements of IT operations. A key advantage that comes with this

type of collaboration is the ability to continuously monitor distributed networks and make necessary updates quickly as new threats are identified.

Some enterprises could be tempted to overlook physical security when it comes to protecting power devices and other IT equipment. However, this should be given careful consideration since attackers can use physical infrastructure to target critical data. Measures such as putting smart security locks on IT racks can be helpful to ensure only authorized personnel have access to these components.

Secure for the future

Enterprises will need to get used to the concept of weighing cybersecurity capabilities for their power management equipment, as this will only grow in importance as IT infrastructure becomes more interconnected. Every network access point needs to be safeguarded from potential cyber threats. By securing power devices as part of a full network defense, enterprises and their IT teams can have peace of mind knowing that they aren't enhancing connectivity at the expense of cybersecurity.

About the Author

James Martin is the global connectivity product manager at Eaton. He has promoted Eaton's software and connectivity solutions for the past 10 years and built trusted technical adviser relationships with channel partners, field sales, and sales operations. James can be reached online at (jamesmartin@eaton.com) and at our company website https://www.eaton.com/us/en-us.html?percolateContentId=post%3A1

Why Ransomware Costs Need to be Prioritized in Your 2023 Budget

By Anurag Lal, CEO and President of NetSfere

No one expects a hostage takeover, ever. Businesses never think a ransomware attack could happen to them, and yet it very well can at any moment. These attacks have been steadily increasing over the last few years, with a 16% increase from 2018 to 2022. In fact, 2022 saw over 70% of businesses experience a ransomware attack.

As enterprise leaders look ahead to Q1 and 2023 financial planning, IT officers and cybersecurity staff need to press the importance of allocating ransomware costs into the annual budget. A study by ThoughtLab saw cybersecurity budgets grow 51%, from .53% to .80% in 2020 to 2021. This is likely due to the risk increase associated with remote work environments and the vulnerability that comes with them.

One of the biggest ransomware attacks in recent days is the May 2021 Colonial Pipeline Company fiasco. Colonial Pipeline holds almost half of the East Coast's fuel and after a major hack takeover, Colonial Pipeline is said to have paid nearly $5 million in ransom to the DarkSide ransomware hackers to get a decryption key.

Even with the potential to face mountainous fines such as these, ThoughtLab's report shows 40% of chief information security officers (CISO) say their organizations are unprepared for a rapidly changing threat landscape. Another study said there is a 20% chance of paying more than $5 million and a 5% chance that the impact would be greater than $50 million.

Further research shows that the enterprises most at risk for these attacks, aside from personal home computers, are healthcare services or other providers. This is because they carry the most attractive, sought-after data and information for hackers.

When considering the new year's budget, CISOs can suggest allocating expenses for updated software protection services, full encryption and zero-trust security policies, and ask to set aside extra funds as a safety net in the event of a ransomware attack. Even investing in ransomware insurance is an option. How much a company is willing to spend on ransomware protection and mitigation is likely to be a hefty conversation with the Board.

Most hackers request ransom payments to be paid through cryptocurrency services, with 98% of 2019 ransomware payments were paid through Bitcoin. The thieves request this kind of payment because cryptocurrency offers anonymity and ease for them.

How greatly a ransomware attack impacts a business comes down to how prepared that business is for an attack. Investing in the right protections at the beginning of the year can turn an attack from an emergency to an inconvenience. Ultimately, finding room for proactive solutions against ransomware attacks can potentially save a company millions of dollars in the long run. By safeguarding the company's confidential and valuable information, CISOs are lessening the chance for hackers to get in and building trust across the board.

About the Author

Anurag Lal is the President & CEO of Infinite Convergence Solutions and NetSfere. With more than 25 years of leadership and operating experience in technology, mobile, SaaS, cloud and telecom services, Anurag leads a talented team of innovators who are transforming everyday messaging technology into secure, highly scalable communication platforms that can be leveraged across a variety of markets and segments. Appointed by the Obama administration, Anurag also previously served as a Director of the U.S. National Broadband Task Force (part of the Federal Communications Commission). A frequent contributor on wireless connectivity, broadband and related security issues, Anurag has received various industry accolades, including recognition by the Wireless Broadband Industry Alliance in the U.K. for exceptional individual contributions to the wireless broadband industry.

Anurag Lal can be reached on LinkedIn at https://www.linkedin.com/in/anuragl For more information about NetSfere, please visit https://www.netsfere.com/.


EVENTS

AVAR 25 INTERNATIONAL CONFERENCE

AVAR 2022

CYBERSECURITY COUNTER PUNCH

1ST - 2ND DECEMBER 2022 | SINGAPORE

AVAR INTRODUCES

CISO Connect

Gather insight on the challenges and opportunities faced by CISOs through Panel Discussions:

1. Challenges in Organizational & Industrial Cybersecurity
2. Cybersecurity Trends for 2023 & Beyond
3. Is the CISO the Next New Board Member?

CISO Awards

- Best CISO Startup
- Best CISO Midsize Organization
- Best CISO Enterprise

Join Us
at the only platform that brings together Security Researchers and CISOs!

https://aavar.org/cybersecurity-conference/

Gold Sponsor

ESET

Silver Sponsors

CYBER THREAT ALLIANCE

AV comparatives

AhnLab

T-Shirt Sponsor

SE Labs

Lanyard Sponsor

K7 SECURITY

Media Sponsor

AV-TEST The Independent IT-Security Institute

Supporting Sponsor

AppEsteem

Media Partner

CYBER DEFENSE MAGAZINE

/avar-asia/ /avar_asia /aavar.org

e-CYberHealth 2022

Diagnostics - Hospitals - Pharmaceuticals

Nicosia - Cyprus

12 December 2022

The Conference aims to raise awareness on medical data security and to analyze secure new ways of using modern information & communication technologies (ICT) to meet eHealth requirements.

More details at **www.e-cyberhealth.eu**

UNDER the AUSPICES

MINISTRY of HEALTH
REPUBLIC OF CYPRUS

MAIN SUPPORTER

REPUBLIC OF CYPRUS
National eHealth Authority

SENIOR SPONSORS

20 YEARS ODYSSEY cybersecurity

MEDIGATE by Claroty

SUPPORTERS

DEPUTY MINISTRY RESEARCH, INNOVATION & DIGITAL POLICY
REPUBLIC OF CYPRUS

COMMISSIONER OF COMMUNICATIONS
Digital Security Authority

CYPRUS COMPUTER SOCIETY

CYPRUS CYBER SECURITY CHALLENGE

CAIPP

CYPRUS ORGANISATION FOR STANDARDISATION

SPONSOR

GUARDBYTE

Media Partner

CYBER DEFENSE MAGAZINE

Organizer

ZOMIDEA design & services ltd
T: +357 22 515561
E: zomidea@cytanet.com.cy
W: www.zomidea.com

ZOMIDEA design & services

Organized by

CRAFTING DIALOGUE

2ND ME EDITION

DIGITAL TALENT ECOSYSTEM DIALOGUE

#DTECOSYSTEM

Organization of Future | Digital Talent & Skill Gap
Digital Experience | Future Workplace

2 - 3 FEBRUARY, 2023 | DUBAI, UAE

KEY FEATURED DISCUSSIONS

- Evolving role of CIO & CHRO in digital talent ecosystem
- Facilitating digital transformation with the right technology, talent & culture
- Aligning CX & EX for Organizational Success
- Data driven workplace & employee experience in the digital era
- Evaluating future of work for tech teams & long-term implications of a distributed work environment

KNOW MORE

Contact Info:

MILAN ROY

info@crafting-dialogue.com

ESTEEMED SPEAKERS

YAHYAH PANDOR
Chief Information & Digital Officer
Fine Hygienic Holding, UAE

SHUMON A ZAMAN
Chief Information and Digital Officer
Ali & Sons Holding LLC, UAE

HEIKE VERMOND
Chief People Officer
Kitopi, UAE

FRANCIS ARUL
Chief Information Officer
Alshaya Group, UAE

KELLY LUKER
Chief People Officer
Tabby, UAE

DGI

Geospatial Intelligence for National Security

DELIVERING GEOSPATIAL INTELLIGENCE FOR INTERNATIONAL SECURITY

SAVE 5% OFF ticket price using our code DGI5CDM

27 FEB-03 MARCH 2023

THE QUEEN ELIZABETH II CENTRE, LONDON

Visit:
dgi.wbresearch.com
Or simply scan the QR Code

600+
Geospatial Intelligence Professionals to Network With

100+
Geospatial Intelligence Experts Sharing Their Practical Insights

30+
Nations Represented from Around the World

15+
Hours of Invaluable Networking Time

3 DAYS
of Insightful Content

DIGITAL REVOLUTION SUMMIT

8th - 9th MARCH 2023

THE EMPIRE BRUNEI

Leaders In *Powering A Digital - Age,* Interconnected World

30+ SPONSORS & **EXHIBITORS**

30+ **SPEAKERS** & PANELISTS

TECHNICAL **WORKSHOPS**

REAL-TIME **DATA CENTER**

INTERNATIONAL **CONFERENCE**

UNLIMITED ACCESS TO MEET THE **DECISION MAKERS**

UNLIMITED NETWORKING

PRIOR NOTIFICATION OF **ATTENDEES**

EVENT OVERVIEW

Brunei is currently undergoing a **major transformation** in the **Information** and Communications Technology (ICT) sector. The **Digital Economy Masterplan 2025 vision** is to become a **smart nation through digital transformation.** Hence in an **effort to support** the **government's vision** of a **smart nation Brunei,** we at TraiCon will be hosting The **"Digital Revolution Series"** scheduled on **March 2023** in Bandar Seri **Begawan, Brunei. Digital Revolution Series** is connecting the global **digital transformation** experts and **technology providers** with the CIO, CTO, CDO, CISO and Head of **IT under** one roof. This event is an international platform where **government authority,** policy makers, industry leaders & **solution providers** to gather and discuss the challenges, **technologies and initiatives** that are driving **digital transformation** in the **region.**

For More Opportunities

Eng. Prasanna | Tel: +91 77085 23918 | **Email:** prasanna@traiconevents.com

JOIN EUROPE'S BIGGEST EVENT
ON INTELLIGENT TRANSPORT SYSTEMS AND SERVICES

22-24 May 2023

CALL FOR CONTRIBUTIONS IS OPEN!

EUROPEAN CONGRESS
LISBON, PORTUGAL
22-24 MAY 2023
ITS: The Game Changer.

WHAT TO EXPECT

800 delegates

120 Exhibitors

2500 Attendees

100 Programme Sessions

50+ countries represented

Government, state and city representatives

Private sector representatives from multiple industries

A UNIQUE EXPERIENCE TO:

- Network with 3200+ smart mobility stakeholders
- Discover the latest mobility solutions and services
- Share experiences through lessons learnt
- Monitor progress and measure results
- Exhibit and experience innovative technologies
- Benefit from first-hand experience through demonstrations

ORGANISED BY ERTICO ITS EUROPE

HOSTED BY LISBOA CÂMARA MUNICIPAL · ITS PORTUGAL

SUPPORTED BY Turismo de Lisboa · TURISMO DE PORTUGAL

www.itseuropeancongress.com/call-for-contributions/

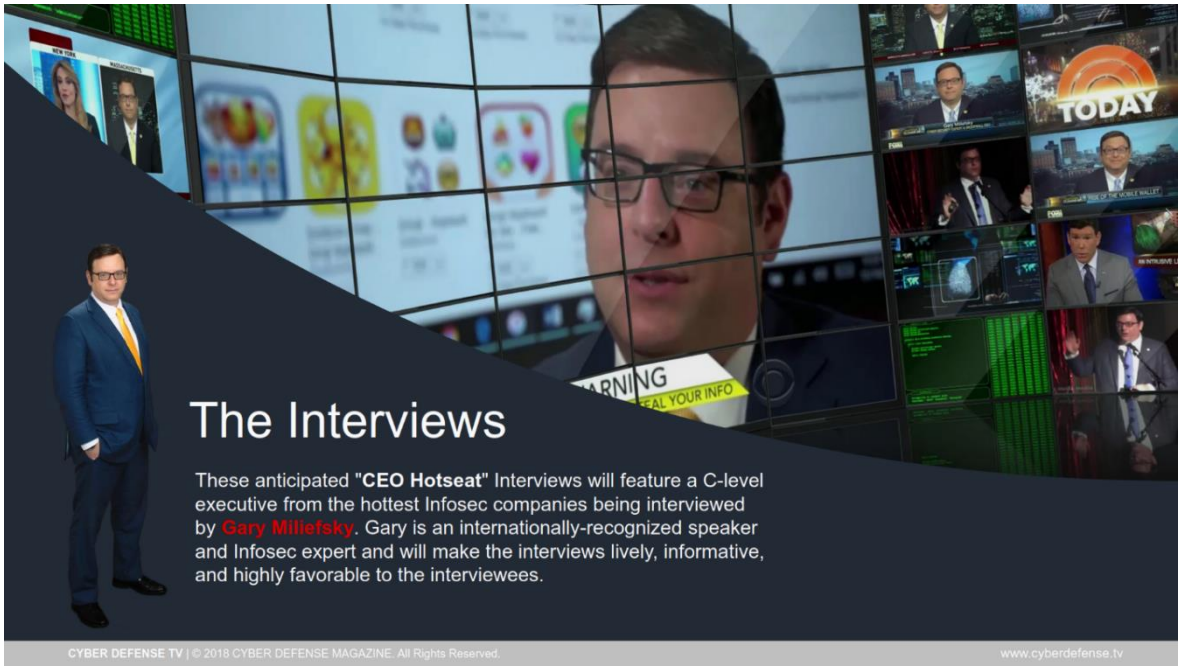
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

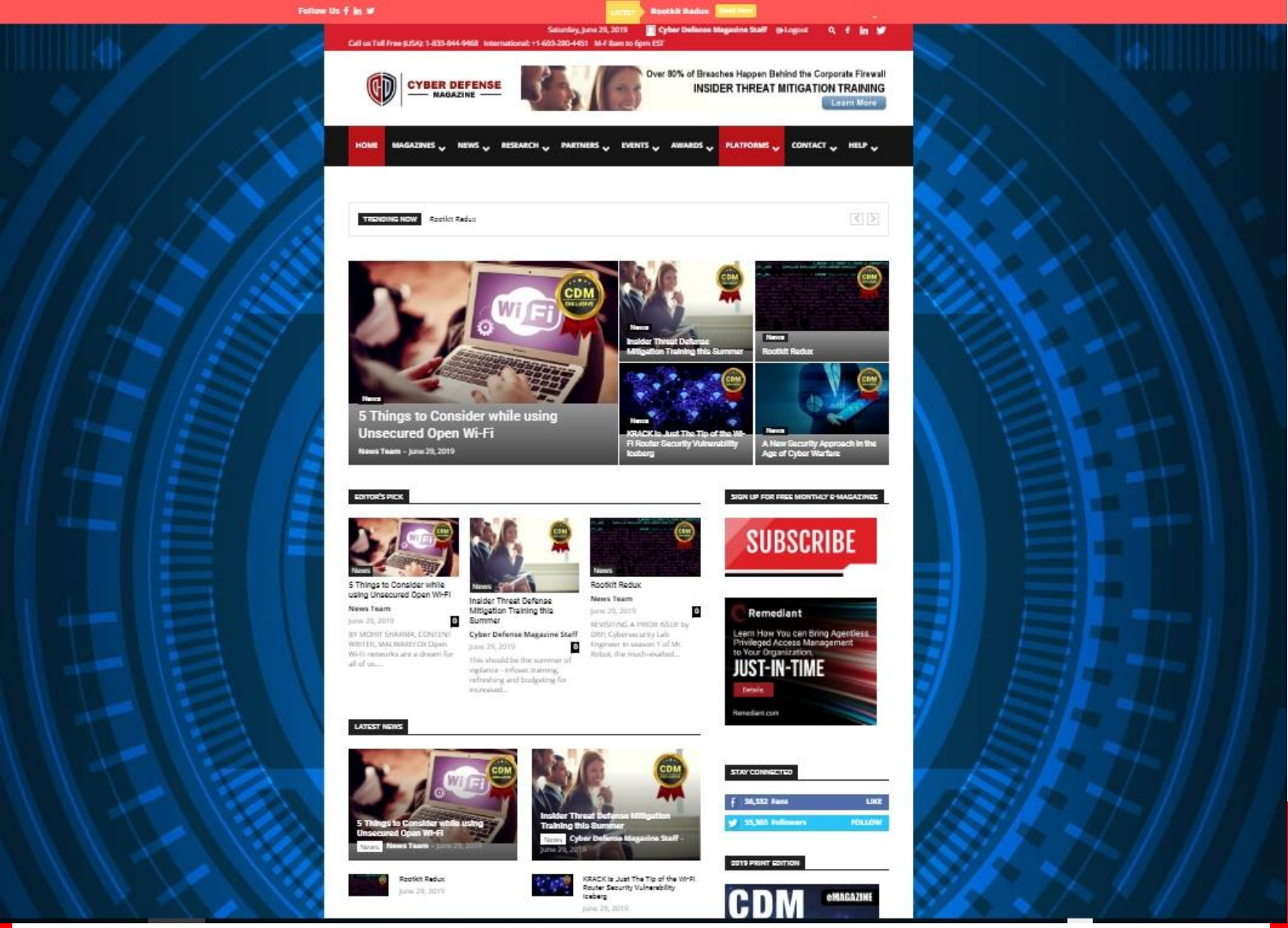
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 12/02/2022



Books by our Publisher: https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)

10 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites and our new B2C consumer magazine CyberSecurityMagazine.com. *Millions of monthly readers and new platforms coming…starting with www.cyberdefenseconferences.com this month…*

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefensemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert

ALWAYS FREE
NO STRINGS ATTACHED

Preventing Tomorrow's Malware

Today.

www.cythereal.com

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

*** with help from writers and friends all over the Globe.**