CYBER DEFENSE MAGAZINE

eMAGAZINE

OCTOBER 2022

In This Edition

Cybersecurity For Our Nation's Critical Infrastructure

Micro-Segmentation: Where Does It Fit into Zero Trust?

How To Protect Against The 83 million Cyber Attacks Detected In 2021

...and much more...

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the

Publisher…

We'll be celebrating our 10th Year in business, Young Women in Cybersecurity and our Top InfoSec Innovators, Black Unicorns and Top Global CISO Awards this October at CyberDefenseCon 2022

Dear Friends,

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. These concerns are reflected in the broad spectrum of articles included in this September edition of CDM. As readers can easily see, they cover a broad range of current topics of vital concern.

At the same time, in the broader group of activities of Cyber Defense Media Group, we are currently conducting the Black Unicorns Awards for 2022. This is Cyber Defense Magazine's tenth year of honoring cyber defense innovators with a focus on this specific category of cybersecurity excellence.

Our submission requirements are for high growth and high valuation infosec companies who believe they could be valued at $1B or more within 36 months. The company must be in a high growth revenues stage to be a winner – it's really all about your rapid trajectory through execution and market adoption. This is a very hard category to win and a very coveted award.

October is cyber security awareness month, however to us at CDM, every day is cyber security awareness day. One of the biggest risks to most organizations is a lack of a mature corporate wide cybersecurity culture. More information is found here: https://www.cisa.gov/cybersecurity-awareness-month

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@cyberdefensemediagroup.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 October 2022 Issue

From the Editor-in-Chief

On behalf of Cyber Defense Media Group and our affiliates, we are delighted to bring you this new issue of Cyber Defense Magazine for October 2022. We would like to take this occasion to bring a change in our editorial practices to your attention.

Over the years, CDM has published an editorial calendar on the magazine's website. In the early years, this information served as a guide for authors and their institutions to target issues of the magazine with focus on their areas of expertise and service. More recently, with the growth of valuable articles submitted to us outside the limitations of the editorial calendar, it has become clear that the needs of our authors and readers are not well served by imposing such restrictions. The increasing pace of cybersecurity developments has resulted in the need to publish articles with a sense of urgency, rather than stick to an inflexible calendar.

Accordingly, Cyber Defense Magazine will no longer publish the annual editorial calendar as a strict focus of monthly issues. Instead, we will make it available to potential authors as a guide, or to help them in choosing topics and respond to expected needs in the cybersecurity community.

Any content on any subject and information security which provides insights into best practices, regulatory compliance, understanding the threat and vulnerability landscape and ultimately helping stop breaches is very important to us and our readership.

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 form, 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@cyberdefensemediagroup.com


SPONSORS

CYBER DEFENSE CONFERENCES

THREE EVENTS IN ONE

Orlando, Florida, USA | October 27-28, 2022

One of the most exclusive, fun and educational CISO conferences of the year!

Limited to our selection of the top 100 CISOs in the world, amazing speakers and insider threat mitigation training by a world reknown expert - meets 100 top cyber defense companies in an intimate, high value two day summit

www.cyberdefenseconferences.com

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/

plainID
THE AUTHORIZATION COMPANY

Power of the Policy

Move to an Identity-First Security paradigm.

Download the eBook


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
attila SECURITY
DRAGOS
ENVEIL ENCRYPTED VEIL
INERTIALSENSE
PREVAILION
the cyberwire
refirm labs
BlueRidge.ai
STRIDER
CodeDx
BLACKCLOAK™
SightGain
JOIN THE TRIBE
DATATRIBE.COM

Is your AI Secure?

BOSCH

Widespread AI adoption has profoundly exposed AI/ML models to adversarial attacks. Hackers can subvert AI/ML systems causing financial loss, reputational damage, loss of competitive advantage and intellectual property theft.

> **It's hard to patch or mitigate what you can't find**

Bosch AIShield

Cybersecurity solution for your AI assets

An industry-first, ready-to-deploy and production-optimized solution to secure AI systems against adversarial attacks such as model extraction, model evasion, data poisoning and model inference attacks

www.boschaishield.com

Consulting

Consulting led AI security impact assessment & mitigation plan

Services

Customized enterprise implementation service for AI security

Product

Leverage AIShield API every time a new AI/ML model is deployed or changed

+91 8951989144

AIShield.contact@bosch.com

Bosch Global Software Technologies
alt_future

Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011

Founder & Managing Partner

SEAN DRAKE

U.S.ARMY

"At Stony Lonesome Group, we believe that Freedom Is Not Free and we do not take it for granted. SLG is a pioneer and thought leader in Mission Focused Investing protecting American Exceptionalism and National Security by investing in a vital areas of Cybersecurity, Big Data Analytics, and Artificial Intelligence. "

Sean Drake
Managing Partner
Stony Lonesome Group LLC
203-247-2479
www.stonylonesomegroupllc.com

Database Cyber Security Guard

Don't be the next data breach. Equifax paid $575 million, British Airways $230 million and Marriott $124 million in fines.

Prevents confidential data theft by Hackers, Rogue Insiders, Phishing Emails, 3rd Party Cyber Risks, Dev Ops Exploits and SQL Injection Attacks.

Product Features

- Detects Informix, MariaDB, MySQL, Oracle, SQL Server and Sybase data theft within milliseconds and shuts down Hackers immediately.
- Advanced SQL Behavioral Analysis of the database query activity learns the normal query patterns and detects database data theft.
- View all suspicious database activity and attempted data theft.
- Supports key GDPR compliance requirements. Non-intrusive detection of data theft. Runs on a network tap or proxy server.

Get a FREE COPY now.

www.DontBeBreached.com/Free

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


ARTICLES

Cybersecurity For Our Nation's Critical Infrastructure

How you can do your part to protect mission-critical assets and services

By Kamil Karmali, Global Commercial Manager, Cybersecurity, Rockwell Automation

The Cybersecurity and Infrastructure Security Agency (CISA) describes critical infrastructure as the essential systems and services that are the foundation of American society. They are so vital to our country that if incapacitated or destroyed, there would be disastrous consequences for public health, physical safety or economic security.

Our critical infrastructure includes highways, connecting bridges and tunnels, railways, utilities like water and electricity, food supply, healthcare infrastructure, buildings and related services, according to the Department of Homeland Security (DHS). Our economic survival and daily lives rely on these vital systems.

CISA was created to bolster cybersecurity and reduce critical infrastructure vulnerabilities in the U.S. CISA works with businesses, communities, and governments to enhance the country's defenses in key sectors, making them more resilient to cyber and physical threats.

Spotlight on securing our nation's critical infrastructure

In May 2021, President Biden signed an Executive Order with the goal of improving and modernizing our nation's cybersecurity posture, especially for critical infrastructure.

The White House fact sheet about the executive order states: “Much of our domestic critical infrastructure is owned and operated by the private sector, and those private sector companies make their own determination regarding cybersecurity investments. We encourage private sector companies to follow the Federal government’s lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents.”

A few of the ways the Executive Order will strengthen cybersecurity for our nation’s critical infrastructure include:

- Requiring providers to share breach information that could impact Government networks.
- Establishing a Cybersecurity Safety Review Board to analyze cyber incidents and make concrete recommendations for improvement.
- Creating a standardized playbook for cyber incident response so federal departments can take uniform steps to identify and mitigate a threat. The playbook will also provide the private sector with a template for its response efforts.

Both public and private sector entities are facing alarmingly sophisticated and malicious cyber activity along with a vast increase in less complex attacks like phishing which also can be crippling if not detected.

Steps to critical infrastructure cybersecurity protection

Analysts at ARC Advisory Group recently reviewed requirements for securing critical OT systems. Their subsequent report included the following core recommendations for industrial companies:

- Review OT cybersecurity strategies to confirm that the basics are covered and deliver confidence that your organization can address sophisticated attacks. How frequently are installed base inventories assessed, for example? What detection, mitigation and backup/recovery systems are designed?
- Is cyber awareness training provided to all employees? What physical or product security steps have been implemented at the controller and device levels?
- Confirm that digital transformation efforts include adequate security from the start to reduce risks related to Internet of Things (IoT) devices, cloud services, remote workers, supply chains and third-party systems. Consider third parties to fill gaps in cybersecurity expertise. Cybersecurity talent is in notoriously short supply worldwide. It’s imperative to deploy effective infrastructure security solutions quickly and accurately and consulting firms with this expertise can provide expertise, saving an enormous amount of wasted effort and cost.

Public and private organizations must move urgently to address and close cybersecurity gaps in critical infrastructure industries.

Grant funding to be made available

Congress passed a bipartisan $1 trillion infrastructure bill in November 2021. Part of the infrastructure bill will provide billions of dollars in funding to CISA, the Environmental Protection Agency (EPA) and the Federal Emergency Management Agency (FEMA). All funding will be used for services and grants that help protect the country's critical infrastructure services, including at state and local government levels.

For example, there are provisions to help electric grids and water/wastewater systems strengthen their defenses against ransomware and other cyberattacks. Grants also support needed steps in an approved cybersecurity plan submission, like performing vulnerability assessments, malware analysis, or threat detection.

To be eligible for a grant, a cybersecurity plan must be submitted to the DHS for review, detailing technical capabilities and protocols for detecting and responding to cyberattacks. The plan would be required to meet certain baseline standards. (More information will be provided when published). Rockwell Automation's cybersecurity assessment and planning protocols, based on the NIST framework for effective cybersecurity with categories of Identify, Protect, Detect, Respond and Recover, would be a logical way to begin.

Critical infrastructure cybersecurity: a civic responsibility

Clearly, it's time for both governments and private entities to reduce cybersecurity risk in critical infrastructure operations. The only roadblock is delaying action.

About the Author

Kamil Karmali serves as the Global Commercial Manager for the Rockwell Automation Global Services organization. He has more than 15 years of experience in cross-functional team leadership, sales management, talent development and executive consulting in industrial IoT and manufacturing technology.

Rockwell Automation, Inc. (NYSE: ROK), is a global leader in industrial automation and digital transformation. We connect the imaginations of people with the potential of technology to expand what is humanly possible, making the world more productive and more sustainable. Headquartered in Milwaukee, Wisconsin, Rockwell Automation employs approximately 25,000 problem solvers dedicated to our customers in more than 100 countries. To learn more about how we are bringing the Connected Enterprise to life across industrial enterprises, visit www.rockwellautomation.com.

Micro-Segmentation: Where Does It Fit into Zero Trust?

Micro-Segmentation Is Not Zero Trust Alone Or Vice Versa

By Brian Haugli – CEO, SideChannel

Micro-segmentation is not Zero Trust. It is the technology component to realize a Zero Trust strategy. Do not be misled by vendors that an implementation of a micro-segmentation solution equates to have a Zero Trust environment.

What is Zero Trust?

Besides being the latest buzzword, Zero Trust is a concept, not a technology, to be implemented. It is a strategic initiative to create least privilege across all aspects of an organization. It requires the 3 elements of the triad in any program: people, process, and technology. You generally need an inventory of the users in the environment, the applications in place and the supporting infrastructure. Without that inventory, a move towards Zero Trust will be impossible.

What is Micro-segmentation?

The basic requirement is to expressly allow traffic from a source to a destination and deny all other traffic. Micro-segmentation is created by a technology to logically divide a network or access into separate segments. The ideal goal being to contain accesses to only the areas expected. An example would be ensuring that the HR systems are only accessible by HR professionals with a granted appropriate rights and “need to know”. This technique can be used when separating production from development or user groups from each other in flat networks. How it’s enabled, historically, has been through cumbersome VLANs and firewall rulesets.

Frameworks calling for Micro-segmentation

Any reputable cybersecurity program will be built on a recognized standard. Let's take the NIST Cybersecurity Framework (CSF) v1.1 as the example to highlight where standards and frameworks expect to see micro-segmentation in place. As stated in the introduction, Zero Trust is impossible without an inventory.

NIST CSF calls out the need for inventories in Asset Management (ID.AM) controls; The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. We need to answer the question, "Do we know what we have in our environment that supports our business operations and know their importance?" It's surprising how many companies do not have this identified, let alone documented or managed well.

NIST CSF goes further in how to protect assets once in an inventory with the Identity Management, Authentication and Access Control (PR.AC) control category; Access to assets is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. Now that an inventory is in place, do we use it to control the access needed for users and applications within the infrastructure?

Specifically, within NIST CSF's Protective Technology and Access categories, PR.PT-3 calls for the implementation of incorporating least functionality into the configuration of systems providing only essential capabilities. In addition, PR.AC-5 expects that network integrity is protected via segregation or segmentation. This is where micro-segmentation shines on an all-important set of controls.

From the 2021 published book "Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework".

> *"Many system components can serve multiple functions, but the principle of least functionality, whereby a device serves a single process (for example, a server can be an email server or a web server but not both combined), can help you better manage authorized privileges to the services the device supports. Moreover, offering multiple services over a single device increases risk… Finally, removing unnecessary ports or protocols can help maximize the least functionality status of your devices."*

An implementation of micro-segmentation reduces the attack surface on environments by removing access to port and protocols that shouldn't be available.

Threats that exploit lack of micro-segmentation

It's one thing to build a program based on standards, but we must factor in the threats that are present that the program is built to reduce or stop. Cyber isn't just addressing the defensive needs or accounting for the offensive threats. Ransomware is prevalent in our society today and an all-too-common news story both locally and nationally. When we look at why it's so destructive, it's not the encryption of one system that causes the pain, it is that the impact is across so many systems. This is allowed to happen from flat networks or lack of segmentation between work groups. A properly implemented micro-segmentation technology coupled with a strong managed policy would significantly reduce or even stop ransomware's lateral movement across an environment.

Where do we go from here?

The first question to answer is whether you have a cyber program built to a standard, such as NIST CSF. Then it's onto how your organization meeting is each of the applicable controls. As you define your remediations and mitigations, a micro-segmentation solution should make its way into your plan to address identified gaps in controls. These are your first steps in the march towards Zero Trust.

About the Author

Brian Haugli is the CEO at SideChannel. SideChannel is committed to creating top-tier cybersecurity programs for mid-market companies to help them protect their assets. SideChannel employs what it believes to be skilled and experienced talent to harden these companies' defenses against cybercrime, in its many forms. SideChannel's team of C-suite level information security officers possess a combined experience of over 400 years in the industry. To date, SideChannel has created more than 50 multi-layered cybersecurity programs for its clients. Learn more at sidechannel.com.

Brian has been driving security programs for two decades and brings a true practitioner's approach to the industry. He creates a more realistic way to address information security and data protection issues for organizations. He has led programs for the DoD, Pentagon, Intelligence Community, Fortune 500, and many others. Brian is a renowned speaker and expert on NIST guidance, threat intelligence implementations, and strategic organizational initiatives.

Brian can be reached online at (EMAIL, TWITTER, etc..) and at our company website https://sidechannel.com/

How To Protect Against The 83 million Cyber Attacks Detected In 2021

The 4 Basic Cybersecurity Practices Experts Say Prevent Most Attacks

By CyberLock Defense, Lockton Affinity

It's a familiar message at CyberLock Defense: multi-factor authentication, threat monitoring, response planning and risk mitigation protect against most cyber attacks. But sometimes it helps to hear that message from other top experts in the industry.

Microsoft recently introduced Cyber Signals, a new quarterly cyberthreat intelligence brief that offers an expert perspective into the current cyberthreat landscape. These experts agree that while the risk of cyber-attacks continues to grow and develop, most attacks can be prevented with basic cybersecurity practices. Here's what to know.

Microsoft Detects Millions of Cyber Attacks in 2021

With its software on hundreds of millions of computers, Microsoft has unique insight into the problem of cyber attacks. In 2021, it detected 83 million cyber attacks against commercial and enterprise customers, ranging from phishing emails to malware to brute force attacks.

Microsoft's Cyber Signal Report says that most organizations aren't protected against the identity-focused attacks that plague modern businesses. Digital identifiers such as email addresses and passwords are used everywhere to access apps and services. Yet threat actors use these identifiers to penetrate networks, steal credentials and impersonate employees and consumers online. Microsoft notes that even

nation-state actors, who are increasingly targeting businesses in key sectors, typically use the same simple exploits as ordinary hackers to steal emails addresses and passwords.

Looking at how business customers use Microsoft Azure Active Directory, Microsoft's cloud identity solution, the report found that most did not enable strong authentication. This meant that while some of these cyber incidents targeted protected systems, 78% targeted systems without it, leaving those businesses more vulnerable to the attacks and more likely to suffer a loss or claim.

Microsoft's Recipe for Preventing 98% of Attacks

Microsoft's report offers a simple message to chief information security officers, chief information officers, chief privacy officers and other technology professionals in charge of protecting systems:

- Most attacks are preventable with basic cybersecurity practices.

Echoing CyberLock Defense, Microsoft notes that up to 98% of attacks can be prevented by focusing on a few key cybersecurity areas, including:

1. Multi-Factor Authentication (MFA)

Multi-factor authentication is a security tool that requires something else from you besides your login and password to access your account. That could be a PIN, security question answers, or a temporary security code emailed or texted to you. Some high-security MFA systems even work with badges, key fobs, fingerprints or other biometric data. The idea is to provide two or more levels of security so that only you can access your data.

Microsoft notes that cyber attacks like ransomware thrive on default or compromised credentials. Implementing MFA on all user accounts is recommended, with executive, administrator and other privileged roles being prioritized for earliest implementation. By doing so, Microsoft emphasizes that businesses can minimize the risk of passwords falling into the wrong hands.

For more info on MFA, see our blog on the Importance of Multi-Factor Authentication.

2. Active Threat Monitoring

Active threat monitoring is the practice of periodically checking that systems, accounts and data are all in order. It can take many forms. Your network administrator can:

- Enable automated security features to scan and filter email and web content for viruses and malicious objects.
- Put systems in place to monitor your network for unusual events or user activity.
- Carry out periodic patch and update maintenance to keep devices, systems and applications safe and secure.

- Manage network administrative privileges to protect the network from account users making accidental or intentional alterations.

Microsoft recommends that businesses learn how to identify telltale anomalies in time to act. These often include early logins, file movement, and other behaviors that can introduce viruses, malware and ransomware. Periodic auditing of account privileges is also recommended, with the principle of granting the least privilege necessary to fulfill the required role, and the prompt disabling or removal of any unused administrative privileges.

For more tips on active threat monitoring, see our blog on Ways to Help Prevent Cyber Attacks.

3. Cyber Incident Response Planning

A cyber incident response plan helps guide you on what to do and how to do it when a cyber incident has occurred. As many as 34% of businesses don't have a response plan in place, which increases risk, since confusion over what to do can make a cyber attack worse, increase your liability and leave you unprepared to address the concerns of clients and customers.

Microsoft recommends that businesses have a well-thought-out plan before they need it. While most businesses in the era of cloud sync-and-share maintain backups, these copies are different from the entire IT systems and databases they live inside of. Microsoft recommends conducting recovery exercises to visualize what full restoration will look like so you can fine-tune your response plan.

For more on cyber incident response planning, see our blog on Forming a Cyber Attack Response Plan.

4. Pre- and Post-Incident Risk Mitigation

Reducing the risk posed to your business by a cyber-attack can start now, before one has occurred. Actions such as reading articles like this, training employees on cyber safety, implementing cybersecurity tools such as MFA, monitoring your network for threats and drafting a response plan are all steps any business can take right away. Risk reduction steps are also possible even after you become aware of an incident, and may help lessen its impact. These steps could include working with cyber incident response experts, such as technology consultants, forensics experts, legal defense counsel and public relations.

Microsoft notes that proper risk mitigation often means moving quickly. Businesses need to have systems in place to manage and respond to alerts when they are raised by an employee or an automated monitoring system. A primary focus should be strengthening any weak security configurations that could allow the attack to succeed. With many cyber attacks unfolding slowly over weeks or months, a quick response really can make a difference.

For more on risk mitigation, see our blog on Cyber Specialist Resources for Policy Holders.

How to Further Protect Your Business

Implementing the right cybersecurity practices can prevent most cyber attacks, but there's always a chance a determined hacker could get through. The typical cyber attack can cost businesses as much as $1 million or more, due to data loss, business interruption, loss of income, litigation, regulatory fees and other related costs. To protect your business, it's important to ensure you have the right cyber liability protection.

CyberLock Defense's industry-leading Cyber Liability Insurance coverage is available with broad coverage, flexible limits and no policy sublimits, so you always have access to your full policy limits. CyberLock Defense can help cover the cost of data restoration, business interruption, IT forensics, legal expenses, public relations and more.

Discover more benefits of cyber liability insurance for your business today. Visit CyberLockDefense.com or call us at (844) 868-7144.

About the Author

CyberLock Defense from Lockton Affinity provides industry-leading cyber liability insurance that offers full limits of cybercrime (cyber theft), social engineering, fraudulent funds transfer and more. With more than 35 industry groups eligible, including professional services, health care, retail, financial services and more, this comprehensive coverage helps protect your business against the costs associated with a cyber attack at affordable rates.

Those interested in coverage can visit CyberLockDefense.com or contact CyberLock Defense practice leader Jeff Severino at 913-652-7520 or JSeverino@locktonaffinity.com.

A Professional Organization Designed for Identity Professionals

By Sean Deuby, Director of Services, Semperis

The concept of the identity professional wasn't a known or accepted profession when I first started my career in information technology (IT). We were all sysadmins who also dealt with user IDs and passwords.

Times have changed. In a world of distributed work, cloud software, and a perpetually evolving threat landscape, identity is central to security. Yet for a long time and in spite of this growing importance, no professional organization existed to support identity specialists.

That all changed in 2017, when Ian Glazer, currently Senior Vice President of Identity and Product Management at Salesforce, founded the IDPro® community.

"In 2015, I found myself sitting in the lobby of a hotel where the International Association of Privacy Professionals was hosting their global summit," Glazer recalls. "I remember wondering why identity practitioners didn't have something similar. Where was our international association?"

An Idea Takes Shape

"Part of why I created IDPro involved my own reflection of how I got into identity," Glazer explains. "I didn't learn identity management; I learned a very specific product. Then another one, and another one, and another one until I realized there was more to it than these individual solutions — identity management was a discipline."

And it was a discipline that, at the time, was both costly and time consuming to learn. Instead of having a concentrated body of knowledge, identity practitioners were all forced to follow the same path Glazer had. Everyone agreed this approach was far from ideal, yet no one knew of any alternative.

"It became increasingly clear to me that there was a labor shortage in identity management," says Glazer. "Going to conferences year over year, I also recognized a lot of the same faces but never anyone new. It was like we had this awesome clubhouse but weren't inviting anyone in."

Glazer concluded that identity practitioners needed a professional association to support new entrants and veterans alike. As he circulated the idea, he attracted other stakeholders who felt the same. Through the advice, counsel, and support of multiple people and organizations, the concept of IDPro was born.

A Push for Vendor-Neutral Knowledge

Each year, IDPro releases its *Skills, Programs, & Diversity Survey* to members. A barometer of how identity practitioners feel about the changing landscape of their industry, the survey also examines ongoing trends, developing technologies, and critical skills. Frustration about the lack of vendor-neutral training material represents one of its most consistent findings.

"It's all well and good to learn product X from vendor Y, but that can't be the only way to develop foundational skills," Glazer explains. "One of IDPro's core objectives is the construction of something called a body of knowledge, meant to be a vendor-neutral well to which people can turn when learning the practice of identity management. It's a collection of material curated and written entirely by volunteers from the identity space and available in multiple languages."

This collection is now more necessary than ever. Identity management is a deceptively vast discipline, and one that exists in a state of constant evolution. Keeping pace with changing trends, tactics, and techniques in their industry can overwhelm even veteran identity practitioners, to say nothing of novices to the field.

"One of the questions in our survey asks respondents how long it took them to feel like a proficient practitioner," says Glazer. "Roughly 25% of the respondents every year say they *still* don't feel proficient, while others say it takes between three and 10 years. In my mind, this result reflects that we're part of a growing industry — there are always new topics for a practitioner to learn."

Shaping the Face of the Identity Sector

Alongside its body of knowledge and annual survey, IDPro also provides its members with a sense of community. The association is a place where identity practitioners can interact with one another, including a member-exclusive Slack workspace.

"On any given day, you'll see incredibly technical questions asking for pragmatic guidance on all kinds of identity topics," says Glazer. "It's a wonderful space, a great place to gather information, and an opportunity to give back. It's a community built on industry connections, which creates the fundamental feeling that *you aren't alone,* and that's incredibly powerful to me."

Arguably the most significant undertaking, however, is the recently announced CIDPro, the Certified Identity Professional Certification. First debuted in 2021, CIDPro provides identity practitioners with a way

to validate both their skills and experience. Notably, it represents one of the first foundational certifications for identity management.

"CIDPro is something we're extremely proud of," notes Glazer. "It's part of the promise we made to the identity community, the result of collaboration with some absolutely amazing people."

What the Future Holds

"Coming up on six years, we've done a lot of the things we promised our early members," Glazer muses. "We've created a community, constructed an evolving body of knowledge, and built a certification. The next step is making IDPro a more sustainable, resilient organization in its own right, hiring professional staff to power it 24/7 in lieu of relying solely on volunteers."

From there, it's a simple matter of using that newly resilient organization to keep driving awareness. Glazer and his colleagues also intend to add more certifications over time while continuing to build out the association's body of knowledge. Lastly, Glazer wants to create more opportunities for individuals and groups underrepresented in the profession, such as grants for attending conferences and events.

"There is still a need to create more identity practitioners," Glazer concludes. "IDPro's body of knowledge will never stop growing, and now with CIDPro, identity practitioners can truly show what they know. IDPro has the potential to change the identity market — and provide even more opportunities for my colleagues and I to give back to the industry."

You can learn more about joining IDPro by visiting its website. You can also hear my entire conversation with Ian in the episode *Supporting the Identity Pro Community with Ian Glazer* on the Hybrid Identity Protection (HIP) Podcast.

About the Author

Sean Deuby brings 30 years' experience in enterprise IT and hybrid identity to his role as Director of Services at Semperis. An original architect and technical leader of Intel's Active Directory, Texas Instrument's NT network, and 15-time MVP alumnus, Sean has been involved with Microsoft identity since its inception. Since then, his experience as an identity strategy consultant for many Fortune 500 companies gives him a broad perspective on the challenges of today's identity-centered security. Sean is an industry journalism veteran; as former technical director for Windows IT Pro, he has over 400 published articles on AD, hybrid identity, and Windows Server. Sean can be reached online at seand@semperis.com, @shorinsean and at https://www.semperis.com/.

All-Electronic Eavesdropping: Why Identity Security Must Apply to APIs, Too

By Matt Graves, Vice President Information Security at MajorKey

We've heard plenty about hackers intercepting emails and communications between people to steal information. But what about when the communication isn't between two people, but between two applications?

Application Program Interfaces, or APIs, allow applications and platforms to talk to one another. These powerful tools underline why identity security is foundational in today's world—not just for human users, but non-user identities linked to applications and devices.

One of the more convenient online features that's become more common in the past few years is the ability to log into websites and applications using an account you've already created for another platform. This is an API in action.

Instead of having to create a separate, new user identity and password, users click the "Log in with" button and use any number of existing accounts on other platforms, from Google to Facebook, to access the application. Without actually logging into the network, the API on one site essentially makes a call to Google, Facebook or whatever you're using to log in, and uses that information to authenticate your identity.

APIs are used everywhere, from travel sites that aggregate flight and hotel availability, to retail stores connecting with courier networks about package deliveries. In the business world, they can be used to integrate applications in your environment and increase efficiency.

If a hacker can insert themselves into the connection created by an API and interrupt it, they can access and steal information shared between those applications. This is why API developers undertake

exhaustive testing before deploying. An unsecure API could expose information stored on a database, full of passwords, credit card information and other sensitive materials.

So how can you protect your company against this kind of attack? This is where identity security becomes paramount. Perimeter-based defenses of the past don't protect against someone who gains access to your network, allowing them to move around inside the network and access information they shouldn't. The same goes for APIs.

APIs' non-user accounts should be limited in their access privileges. The same way that human users shouldn't be able to access everything on your network, any APIs you're using should have access limited to only the data they need to perform their essential functions.

Ensuring those kinds of limitations can be time-consuming, which is why a hastily developed API can have a wide range of access, instead of the developer creating a non-user account that can only make certain data requests.

Even well-developed APIs can be vulnerable to attacks such as spoofing, the same false identity strategy used to access data from human user accounts, or man-in-the-middle attacks, where a hacker poses as a server or an element in the API's chain of communication. A sophisticated attack that appears as a valid part of that communication chain can mean a breach can go undetected for a very long time.

So when it comes to your network security, we're essentially talking about APIs as non-user identities. And much like malicious actors stealing credentials and using established identities to access networks, if someone can access an API, they can find backend ways into applications and databases.

This is why your identity security strategy shouldn't only account for user accounts linked to people. You must understand and account for all the non-user accounts that are in your system, like APIs, so that you can monitor their usage and know when those accounts are accessing data *and* what they're accessing.

Then you need to have a governance system in place that includes regular audits of all the accounts used in your system—users and non-users alike—to ensure that your organization is properly tracking every account in your system that can access and retrieve data.

Like Software-as-a-Service and cloud computing, APIs are tremendous tools that can enhance your organization's efficiency and quality. But with these advancements also comes the need to move past the perimeter-based defensive mindset, and shift towards a security based on identity. Only then can your organization deploy APIs and new tools to improve your work with peace of mind, knowing your data is safe.

About the Author

Matt Graves and I am the Vice President of Information Security at MajorKey. An experienced information security and cloud architect, Matt is responsible for IAM solutions development across the MajorKey client community. He advises clients on how to evolve their information security strategies and solutions in ways that align with their business objectives and leads solutions architecture to ensure effective delivery. Prior to his current role, Matt held senior operational positions within Highmetric, helping clients implement service management processes and solutions. An expert with multi-cloud platforms, Matt joined the company from the healthcare insurance industry. You can contact Matt Graves at MGraves@majorkeytech.com. For more information on MajorKey visit www.majorkeytech.com.

As Attackers Grow in Skill, Feds Must Brace Cybersecurity with DevSecOps

Log4J served as a wakeup call for security leaders in the public sector. In order to secure their organizations, these leaders must commit to making fundamental change.

By Willie Hicks, Public Sector Chief Technologist, Dynatrace

It is increasingly clear that IT and Security teams need to remain diligent and collaborate. This commitment to discipline will ensure that in the ongoing fight to secure the nation's digital infrastructure, Log4Shell will remain a watershed moment.

Nine months after the emergence of the Log4Shell vulnerability, the security industry rushed to batten down the hatches and root out the potentially devastating zero-day vulnerability. But the most dangerous enemy we face now is not ransomware gangs, cyber-thieves, or state-sponsored threat actors; the biggest threats are complacency and the tendency to maintain the status quo.

Log4Shell blackened the eye of traditional security solutions. The vulnerability existed undetected for nearly a decade and now potentially affects millions of devices. The discovery forced decision makers in government to act. Consider the many positive changes made since, including the following:

- Increasing adoption of DevSecOps solutions and practices that raise the security level of multi-cloud and hybrid cloud iniatives. For all the many benefits the cloud produces, it has also greatly expanded the potential attack surface, ratcheted up complexity and raised the level of risk.
- More and more security managers recognize the critical importance of adopting real-time observability and automating the many arduous security tasks. They're dedicating themselves to unearthing vulnerabilities before they're introduced into application code. Weaving cybersecurity into the process at the earliest development stages is essential.

- The Federal government is now requiring its agencies to adopt zero trust, a set of security principles based on eliminating implicit trust and mandating continuous verification.

As it stands now, all the momentum is with the good guys. But as those of us who've spent a few years in security know, a high-profile breach often generates a period of increased activity by the security sector. And too often, after the dust settles and things quiet down, people get lulled into a false sense of security. Not this time; there is too much at stake to go back to legacy practices and forfeit the gains.

DevSecOps is the way forward for Federal agencies

No doubt it won't be easy. We face significant challenges.

When it comes to technology, it's common for critics to claim that the feds are always a decade-behind industry. But this is inaccurate. Many federal agencies have begun moving to the cloud. They're trying to become more agile without losing sight of security and taking a DevSecOps approach to development

IT teams from both the private and public sectors have discovered that shifting left with DevSecOps makes development and software applications more secure out of the gate. By default, this shift creates a stronger cybersecurity posture.

The increased momentum behind cloud adoption over the last few years has served as a forcing mechanism for federal agencies to consider DevSecOps. The cloud emerged as a critical lifeline during the pandemic and those agencies who moved to the cloud fared better during the Covid crisis than those who didn't. Among agencies, the pandemic became the single biggest driver of cloud adoption. Because the changes occurred swiftly, this left cloud security teams playing catch-up. Security managers quickly realized that apps and security cannot be distinct. Tight integration is required.

What Log4Shell clearly demonstrated is that not enough organizations know what sorts of vulnerabilities are hidden in the third-party libraries used to build applications and how they could be exploited. Following its discovery, too many organizations turned to traditional tools, such as Software Composition Analysis and Vulnerability Assessment to identify the presence of the vulnerability. Because of how widespread Log4Shell is in their codebase, they then had to manually sift through hundreds or thousands of alerts to eliminate false positives and then manually prioritize. This delayed the remediation timelines by weeks or even months.

Our federal agencies need tools and capabilities that do more than just trigger alerts. They must make the best use of runtime context to identify attacks, implement remediation and countermeasures. Cybersecurity teams need solutions that continuously track down and call out zero-day vulnerabilities and common application attacks, such as SQL injection. It is time to move beyond traditional monitoring and embrace deep observability and intelligent automation.

As agencies embark on their cloud journeys, it is quickly becoming apparent that they will need hybrid and multi-cloud environments to meet their mission requirements. Managing them, at scale, is not humanly possible and agencies will need to consider AI-based approaches to deliver successful mission

outcomes. Security practices should be baked into app development, using real-time observability to help identify attacks and exploits.

In an increasingly complex environment, that is now spilling beyond traditional agency perimeters, IT leaders have to meet performance criteria dictated by the mission. The imperative then is to be able to identify issues and remediate them quickly. According to a Dynatrace survey conducted in October 2021, nearly four of five federal IT managers said they struggle to detect and correct the root causes of systems issues. An equal number said they encounter difficulties when attempting to view and manage complex IT environments.

This is where observability comes in, a capability that represents the next generation of application-performance monitoring (APM). High-quality observability offers full stack visibility and end-to-end, granular situational awareness of all applications and components, including their dependencies and how they affect each other, while adding a layer of automation to address today's varying cloud environments, regardless of scale.

Changing our thinking to bring observability and security to the fore

Not only do we need new observability and automation security tools, but we must also re-examine our beliefs about security and technology.

For a while, people used to fear that AI would replace workers and lead to mass unemployment. The federal sector is known for being especially cautious in its introduction of technology that has the potential to disrupt existing workflows. But AI has been around awhile now and we're not seeing mass layoffs of civil servants. On the contrary, AI in many fields has led to job growth. AI has liberated IT staff from staring at dashboards and fighting fires all day. AI has enabled them to perform high-value tasks at a greater scale — coding important applications or conducting research and analysis — the jobs they were hired to do.

The mission of government and constituent demands require us to stay abreast of new technologies and embrace new paradigms at increasing speed and to do more with less resources. If we're asking more from our IT staff, then we must supply them with the right tools and solutions to help them become more effective.

Most importantly, we must shed the belief that legacy security practices and perimeter defenses are enough. We need to focus on evolving paradigms and solutions that can help us overcome new challenges as we shed our dependencies on outdated tools.

About the Author

Willie Hicks, Public Sector Chief Technologist for Dynatrace, Willie has spent over a decade orchestrating solutions for some of the most complex network environments, from cloud, to cloud native applications and microservices. He understands tracking and making sense of systems and data has grown beyond human ability. Working across engineering, product management to ensure continued growth and speed innovation, he has implemented Artificial Intelligence and automation solutions over hundreds of environments to tame and secure their data.

Willie also enjoys woodworking, playing old-time banjo and fiddle, and, most importantly, spending time with his wife and two children. Willie has an MS in Electrical Engineering from the University of Alabama, Birmingham.

Willie can be reached online at (LinkedIn) and at our company website https://www.dynatrace.com/

Automatization of Cyber Defense

By Milica D. Djekic, Independent Researcher

Protecting cyberspace is a challenge several decades back. At this stage, there are some solutions being available on the marketplace, but those endeavors yet need human resources to manage them. Some experts predict that artificial intelligence could overcome such a concern, while the others suggest that it's necessary to deeply overuse digital technologies as binary algebra is a branch of mathematics which can offer more outlets.

At this moment, there is not clearly defined tendency or at least their set which could indicate what direction should be taken. Cyberspace is a critical infrastructure with asymmetric connotation which can once attacked cause disastrous consequences to lives and businesses. Also, those impacts can go that far away to threaten safety and security of many. Modern SOCs cope with outstanding analytics, but they still need workforce to terminate unwanted connection to monitored network.

Some research in an area of binary systems suggest that there could be logic circuits and programming code which could reject access of untrusted signal. In addition, those findings return us in a time of the 3rd industrial revolution putting some cream of defense on a top of such a cake. Ongoing trend in technology can be recognized as a cyber-physical systems age and main imperative in that case could be to provide better security to everyone.

There are a plenty of great ideas within R&D sector and the future is quite promising about what can come going deep into that branch of science and technology. In other words, all being done manually nowadays will be obtained automatically applying a minimum of human effort. Even in

such a fashion it's obvious there is no an absolute security as human factor always can turn into insider's threat as some of sensitive information can leak out through those means.

Some perspectives say that humans will yet remain masters of machines, but their role will mainly be about observing and following those activities. Progress is something inevitable which will happen in times that come and purpose of humankind is to cope with such a new epoch, so far.

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.

Understanding Health Data Privacy in The Digital Age

Recent news regarding the lack of digital privacy protections has prompted major concern about the potential misuse of consumer health data

By Brian Foy, Chief Product Officer at Q-Centrix

Over the past decade, the proliferation of health apps has made everything from fitness-tracking to calorie-counting more convenient for the everyday consumer. However, recent news regarding the lack of digital privacy protections has prompted major concern about the potential misuse of consumer health data. For example, the recent overturn of Roe v. Wade left some users unsure if the data collected by period-tracking apps could be used against them by law enforcement or other federal agencies. While worries over how third parties use data are more than warranted in this context, it is imperative to distinguish this from the use of health care data within hospitals and health care systems. Consumers should remain vigilant about the information their mobile devices and wearables collect about them while also understanding the protections in place that secure the data utilized by hospitals and health systems.

In hospitals and health systems, health care data comprises information providers collect from a variety of sources This could include a patient's diagnosis, test results, medications, and treatment plans, among others. This data is often used and shared to determine a targeted approach to a patient's particular care within and across networks and is protected under the Health Insurance Portability and Accountability Act (HIPAA). Under HIPAA, the privacy of protected health information is protected by limits and conditions on the disclosures that may be made without an individual's authorization. HIPAA also gives individuals rights over their protected health information and regulates identifying data such as names combined with health information. As a result, the patient and their data are prioritized within hospitals and health care systems. Without HIPAA, there would be little incentive for safeguarding data—and little chance of repercussions if there were a failure to do so.

These protections differ drastically from those afforded to data produced by mobile apps. HIPAA only protects data shared by health care providers, health plans, health care clearinghouses, and their business associates. Consumer health apps, because they are not classified as an official entity recognized under HIPAA, do not have the same obligations to secure and protect the privacy of the data they collect. Therefore, apps that fail to properly protect health data are not subject to the harsh consequences health care providers face. In fact, one study found that 88% of mobile health apps sold in the GooglePlay store are designed to harvest user information, despite many users' assumptions that these apps protected the privacy of their sensitive health data. Furthermore, the study indicated that 23% of user data transmissions took place on insecure communication protocols, and less than half of data transmissions complied with the app's privacy policies.

In all, health care data contains sensitive information that can be easily exploited and misused if not properly secured. Until mobile apps are held accountable for the wealth of information they store, consumers must better inform themselves on the current state of their data and privacy and take action accordingly.

About the Author

Brian Foy, Chief Product Officer at Q-Centrix- He joined Q-Centrix in 2014 to lead product development, by 2017 he led both the product and engineering teams. As Chief Product Officer, Foy led the development and launch of the only enterprise clinical data management software on the market. The eCDMTM software enables healthcare systems to capture, submit and analyze clinical data from varying service lines throughout the hospital as an enterprise.

Prior to joining Q-Centrix, Foy has spent most of his career with strategic accountability for software applications in the health information technology (HIT) space. At TransUnion Healthcare and later, at Altegra Health, Foy led a Healthcare Analytics application through an acquisition while overseeing the addition of key quality reporting and care management features. At Blue Cross Blue Shield of Illinois (HCSC), Foy oversaw the implementation of a care and condition management reporting system, which fulfilled a key gap in that company's care management product offering. Foy has an M.A. in Health Services Administration from Xavier University in Cincinnati, Ohio, and a B.A. in Economics from Ohio University in Athens, Ohio.

Brian can be reached online at brian@q-centrix.com and at our company website https://www.q-centrix.com/

Combating Cyber Threats

Why Building a Comprehensive Cybersecurity Strategy Includes Ad Fraud

By Adam French, Regional Vice President (EMEA), TrafficGuard

Ad fraud is one of the most overlooked aspects of cybersecurity and, in terms of proactivity, is getting left behind. It's often due to a lack of understanding or visibility into what is considered an external challenge or not a real threat to an organisation. However, losses to ad fraud are bigger and more far-reaching than most executives assume. As an overall market, Statista reported the 2021 cost of digital ad fraud worldwide at $65 billion, approximately half of what is spent on digital advertising in the United States annually.

Advertising fraud is ad engagements, such as clicks or app installs that are generated with malicious intent. Due to the intelligence of the technology and methods fraudsters use, combined with a general lack of awareness around the problem, it's an attractive industry for criminals looking to make money.

Ad Fraud in Numbers

Marketers in both B2B and B2C organisations face pressure to maximise budget and give themselves a competitive edge. Engagements from ad fraud have no genuine interest in the ads interact with and result in no advertising ROI which is bad news when margins are tight.

As well as the direct impact on businesses' budgets, the indirect impact on ROI causes just as much damage. Without any clear or accurate visibility, large volumes of invalid traffic can cause marketers to direct spend to traffic sources that appear lucrative but are in fact producing non-opportunities.

There are reputational consequences to consider too. Back in 2020, T-Mobile was thrust into the spotlight as entrants of its weekly 'T-Mobile Tuesdays' questioned the large portion of winners in one location. The culprit was exposed as fraudulent bots, maliciously created and distributed to take advantage of the monetary rewards offered. Legit customers had a much smaller chance of actually winning, and the telecommunications company was directly paying out to sophisticated criminals. Not ideal.

Even with such a wide range of ramifications, it's not a priority for organisations, despite the significant impact on customer experience, wasted budget and lead generation.

Ad Fraud Techniques

There's a wide variety of ad fraud being perpetrated within your marketing campaigns, both by seasoned professionals, competitors and the networks that host your adverts. Because of the lack of awareness and protection, I see a similar story across the businesses we work with, and some common issues organisations can't get away from:

Click Farms - Groups of people organised to click ads, purchased by competitors or other parties wanting to sabotage your campaigns.

App Install Farms - Banks of physical devices that click on ads, download apps to devices and then open them to trigger install events.

Crowdsourcing and Incentivised Ads - Publisher-generated invalid clicks to inflate the advertising engagement of their site and increase their ad revenue.

Domain spoofing - Bad actors monetise the traffic from low-quality sites by manipulating the domains and making it appear to come from high-quality sources.

Ad Stacking - Occurs when a fraudster layers or stacks multiple ads on top of one another so that only the top ad is visible to the user. When the user clicks the ad, they unknowingly click all the ads underneath the intended ad.

If these known types of fraud are repeatedly impacting your advertising, unknown types of fraud that are being developed and committed by sophisticated criminals can have an even greater impact.

Cybersecurity isn't caught up to ad fraud yet. Part of this is down to a common thought process: isn't this a problem the marketing team should be dealing with? In reality, CISOs and the C-Suite should be taking notice of how ad fraud is impacting their organisation and the repercussions to the business' bottom line. Across many organisations, it's a problem that's overlooked but could be a massive competitive advantage if security teams understand and address it.

The Role of Artificial Intelligence

For CISOs, the need for more sophisticated methods of protection as fraudsters evolve their techniques is clear. Proactive, preventative strategies and solutions are required so that cyber threats can be stopped before they impact data, operations or budget.

The same sentiment is true in stopping ad fraud. Machine learning is a type of artificial intelligence (AI) that adopts an 'always-learning' approach instead of being rules-based.

One of the most beneficial parts of machine learning is that not only can it analyse traffic and determine validity in real-time, but because of the sophistication of the algorithm, it can block known and unknown types of fraud. This means it doesn't need to wait weeks or months until more is known about the method of fraud, and once you have already paid out for the fraudulent traffic.

Organisations require intelligent, real-time cyber defences, but ad fraud continues to be a blind spot. For CISOs that want to give their business the best chance of staying ahead of fraud, they need to adopt a proactive approach.

Looking to the Future

Organisations have solutions and strategies for almost every cyber threat except advertising. It's a problem across every geography and organisation type – ad fraud has no limits. It shouldn't be accepted as a constitute of an organisation's marketing strategy, it can and should be prevented to drive ROI.

For CISOs looking to best protect their organisation, it's time to be proactive and create a strategy that incorporates protective and preventative measures, so budgets can be put to good use in real-time, instead of manually requesting refunds.

By understanding ad fraud, gaining insight and visibility into how it's impacting your organisation and building a business case to tackle it, advertisers and cybersecurity teams alike can work together to prevent their organisation from losing out to the lesser-known cyber threat.

About the Author

Adam French is the Regional Vice President (EMEA) of TrafficGuard, an international ad fraud detection and protection software provider. He has over 20 years of experience working for multiple blue chip brands including Microsoft, Nokia and Telefonica commercialising their data for utilisation across digital advertising channels. Adam can be reached online on LinkedIn and at our company website https://www.trafficguard.ai/.

Cyber Defense Matters in the Smart Home

By Steve Hanna, Distinguished Engineer, Infineon Technologies

Will we finally realize the "smart home" vision in 2022?

In 1966, five years before the invention of the microprocessor chip, a Westinghouse engineer created the Electronic Computing Home Operator (ECHO IV). An 800-pound computer was the brains of the first true home automation device. In addition to controlling temperature and appliances, it stored items such as shopping lists, recipes and other family notes for later retrieval.

With its grand opening on March 28, 1980, the House of the Future, in what today is Ahwatukee, Arizona, was promoted as "the first microprocessor-controlled house." The Frank Lloyd Wright-inspired architecture used computers as appliances to provide comfort, convenience, and more.

Addressing environmental concerns with a system of solar panels, the computer could select between three different modes of air conditioning based on efficiency, use heat sensors that would automatically adjust windows and shades, and even centrally control the home security system. Signals were transmitted throughout the house with radio waves. Several buttons in the house were programmed with different functions depending on the time of day. For example, turning on the kitchen coffee maker in the master bedroom from a light switch. One of the computers, could even speak to and take commands from people.

Four years later in 1984, the term “smart” was finally attached to an advanced home, with the National Association of Home Builders (NAHB) Smart House project. The two-room, 30-member cooperative effort integrated power and telecommunications functions into a single, computer-controlled operation.

While smart was applied after this time to numerous products to improve the home, it wasn’t until the widespread availability of the internet that smart home started to have serious consideration. The main difference from early demonstrations, including technology advancements that occurred over time until the modern era, was rejecting a fully completed smart home as the goal – and acknowledging a piece meal implementation.

Getting Smarter and More Secure

Unlike early concepts, the smart home in the 21st Century is typically built over time by the homeowner. While architects and engineers can work together to ensure that many existing technologies come together in an initial implementation, the intent is to add more capabilities as technologies advance. Interoperability has been one of the major complaints of those connecting a variety of smart home products.

Today, many of the features of the smart home can be monitored, activated, and even controlled remotely through internet connectivity. This means that attackers and thieves can access the features of the smart home as well and wreak havoc. In fact, many consumers (71% according to incontrol) acknowledged fear of their personal information being stolen while using smart home products.

In 2021, after several years in development, the Matter standard was announced by the Connectivity Standards Alliance (CSA). This standards activity involved diligent efforts by technical experts from hundreds of companies from across the smart home industry and around the world. Matter aims to address the primary smart home challenges including interoperability, ease of use, security, and privacy.

Interoperability & Ease of Use

The Matter standard runs on top of IPv6, so it works with many widely deployed communications network protocols like Wi-Fi and Thread. Legacy networks and devices can be supported by bridges that translate legacy protocols. This should permit Matter to work with many of the networks and devices that consumers already have in their home.

The set of Matter devices supported in the 1.0 release is a broad range of simple devices across the home: lighting, electrical, blinds, shades, HVAC controls, TVs, access control, safety, and security. These initial products cover the most common widely used devices in existing Zigbee or home security systems. However, some of the most common connected consumer devices including IP cameras, connected doorbells or appliances are not yet covered. While this is unlikely to slow Matter adoption, it is important to add these devices in the future to have a more seamless consumer experience.

Interoperability of these varied products should be increased because CSA provides an open source implementation of Matter and requires all Matter products to pass certification tests using a common test harness that all companies can use to pre-test their products.

The interoperability enabled by Matter should permit users to choose their favorite device or cloud to control their home. To give them even more flexibility on this count, Matter supports a feature called multi-admin. With this feature, users can connect a device to multiple clouds at once.

Ease of use will also be improved by the standard commissioning process that Matter defines for bringing a device into the smart home. Setup problems should be a past problem.

Matter goes far beyond the underlying network protocols, defining standard protocols for secured and reliable unicast and multicast communications, standard interaction models, and even the data models (nouns and verbs) needed to define how a particular device type should operate. Thus, a light switch from one company will know how to control a light bulb from another company using the standard.

Security & Privacy

In a smart home, security is essential to prevent attackers from initiating denial of service (DoS) attacks like Mirai and others. Consumers are aware of the potential for these unauthorized access attacks and realize that smart home devices have had security problems in the past. These concerns are a significant impediment to widespread consumer adoption.

To address security concerns, Matter includes several protection features. The first step is knowing that a real device, from a qualified supplier and not a fake, is being connected to the network. Since consumers often use wireless networks in the smart home, protection from eavesdropping is also required. Protection from manipulation of data over the air or on the device itself is another threat. Access control prevents unauthorized access to security cameras and other sensitive devices. Finally, firmware updates are essential to keep systems well-secured so these need to be securely installed while avoiding illegal updates with malware.

Security measures in Matter to protect against these threats include:

- Device attestation
- Mutual authentication of all parties
- Secured communication among devices using secured protocols
- Secured storage, especially of private keys
- Secured firmware updates
- Device integrity to prevent and detect compromise

Matter takes every step possible within its scope to protect the privacy of consumers' data, including these measures:

- Secured data communications
- Data minimization
- Data sharing only for a defined purpose

Hardware-based security is especially important for Matter. Instead of using passwords, Matter uses cryptographic keys preferably stored in hardware security to provide a more secure approach keeping the key out of unauthorized hands. Since the cryptographic keys used by Matter are large random numbers and the algorithms are well-tested, it is nearly impossible to break the encryption.

Conclusion

With the development of the Matter specification by the Connectivity Standards Alliance and 100s of key suppliers, the smart home is poised to provide unprecedented connectivity and security and overcome the concerns of existing and new smart home product buyers. So, the answer to the question posed at the beginning is yes – the smart home has truly arrived.

About the Author

Steve Hanna is a Distinguished Engineer at Infineon Technologies. On a global basis, he is responsible for IoT security strategy and technology.

As a security expert, Steve is a leader in many standards groups.

- Within the Matter Work Group in the Connectivity Standards Alliance, he is the Lead of the Threat Model Tiger Team, the Lead of the Device Attestation Tiger Team, the Vice Lead of the Cryptographic Primitives Tiger Team, and the Secretary of the Secure Channel Tiger Team.
- Within the Trusted Computing Group, he co-chairs the IoT Work Group, and Industrial Work Group.
- Within the Internet Engineering Task Force (IETF), he is a member of the Security Area Directorate.
- Within the International Society of Automation, he is co-chair of the Industrial IoT Security Work Group.

Mr. Hanna has a deep background in information security, especially in software and systems. He is an inventor or co-inventor on 48 issued patents, the author of innumerable standards and white papers, and a regular speaker at industry events. He holds a Bachelor's degree in Computer Science from Harvard University.

Steve can be reached online on LinkedIn at: @SteveHanna and at our company website http://www.mycompany.com/

Cyber Insurance Is the Biggest Problem in Cyber Security and The Most Hopeful Solution

By J. Foster Davis, COO/CRO & Co-Founder, BreachBits

When I talk with businesses that are beginning to take cyber security seriously, I often give this advice: "Before we evaluate your security stack, first get a cyber insurance policy and make sure it doesn't exclude ransomware."

My words are often met with a brief moment of confusion and the inevitable question about making cyber defense the priority. When I share stories from my years of leading red teams and ethical hackers within the U.S. military, my point becomes clear. Where there is a will, there is a way. A dedicated attacker will always find a way to breach. So, for many, it makes sense to protect against a catastrophic loss first and then work to improve the margins.

Cyber insurance presents one of the biggest headaches in today's security landscape, but it also provides the most hopeful solution to delivering secure outcomes across the cyber ecosystem. That's not because of the insurance itself and not because the risk of covered perils can be transferred. It is because of the side effects. From my perspective as a cyber security professional, the second and third-order results of wide adoption of cyber insurance has a micro effect that results in a macro impact across industries.

These beneficial side effects are the result of a quantification of risk. When a single company adopts cyber insurance, that company is forced to quantify the potential damage of adverse events – even if this is only done in a rough estimation. As the potential risk-holder, the insurance company validates that estimate, grounds it in reality and delivers the benefit of precedent.

And what's even better is that the risk quantification is done in a universal metric – money. There can be no mistaking the magnitude of risk in these terms. It requires no technical expertise to understand and translate across the company's departments and functions.

Even if the company is merely going through the motions of managing transferable risk, it grows in its understanding of cyber risk at the same time. At that point decisions to invest in manpower, security tools, design decisions and other capital investments can be balanced against the quantified risk and alternative options.

We can realize even more benefits once the adoption of cyber insurance becomes more widespread. As quantification methods advance, observing dozens and then hundreds of thousands of policyholders yields insight to patterns of risk that are difficult or even impossible to observe in a single company. We begin to learn and gain valuable perspectives from that scale of insight.

The insurance provider is incentivized to identify these patterns in order to improve loss ratios. Policyholders benefit from gaining insight on where they could be at risk and are incentivized to reduce the cost of the policy by controlling exposures. Company customers benefit from better security policies that actually deliver more secure outcomes. Everyone wins.

But cyber insurance is a huge headache right now. If you are looking for coverage now, you see doubling premiums, lowered limits and growing exclusions – such as ransomware. If you are a provider, you are struggling to quantify the risk in a standardized way and at scale in a manner that policyholders want to consume. Hint, another survey isn't what we want.

For the moment, these headaches are symptoms of creative destruction in the insurance market. Providers scramble, technology advances and security profiles change rapidly while hackers continue to get better at attacking. Some providers are trying new approaches, others are doubling down on old practices, and they are all watching each other to see who will gain traction and by what method.

One of the problems facing providers is trying to find scalability and standardization without sacrificing the diligence necessary to control loss ratios. With so many policies, providers are pressured to simplify the application phase to conduct basic qualification and to then somehow assess each applicant – and thousands of others – in a way that is fair and standardized. To assess a small number of policies in a standardized and diligent way is achievable, but the problem is scale. An alternative is of course to scale by sacrificing diligence, which leads us right back to where we are now.

This creative destruction begets innovation. And when technology enables an advancement in the state of the art, scalability, standardization and diligence can all be simultaneously improved without compromise.

We saw this firsthand when we conducted an in-depth study on cyber risk across 98 upstream, midstream, downstream and supply chain companies in the U.S. oil and gas sector. We assessed

BreachRisk for those companies the way an innovative insurance provider would. We discovered the micro circumstances of each individual company along with the macro trends within the sector, subsectors and at other pattern points. Our method of assessing each company from the hacker's perspective with pre-attack planning provided standardization and diligence. Automation and A.I. provided scale.

When rigorous diligence can be done at scale and security can be quantified, security is enhanced and optimized. Each company can make informed risk decisions in terms they understand – money. There are some risks that companies will choose to not address. They will be held accountable by their premiums, limits and exclusions. Other perceived risks will be proven on a macro level to not be risky at all.

The argument of "but you should do the right thing and have the best security" doesn't work, doesn't make business sense to companies (who think in terms of risk) and doesn't deliver secure micro or macro outcomes. In other words, companies are not afraid of the dark and mysterious attacker that they can't see – and why should they be? How could they be? They need an adversary that speaks a language they understand – the language of money.

So what about regulatory fines or government fines? These bring a host of other problems, the primary of which is that such fines are not rooted in reality. They are not rooted in the reality of risk, loss ratios, competition, innovation and a dynamic enemy (cyber attackers) that are always advancing and are notorious for finding loopholes. These rules grow stale, get out of touch and result in rejection – or worse – companies comply with arbitrary, unbalanced fines and are relieved of their individual responsibility and culpability when things go awry.

Regulatory fines are a convenient approach to governments and in some cases might seem good for individual companies seeking to abdicate their culpability. But business is tough, and companies only exist and thrive when they can optimize rates and consequences by balancing risk. A regulations-based approach does not maintain balance. This lack of balance leads to misaligned incentives, allows for loopholes and compels companies to make decisions that are therefore not aligned with secure outcomes – and then consumers lose.

And so the best hope is an adversary that speaks the language of money that is rooted in reality. An adversary that must balance the books and be incentivized to continuously optimize while balancing risk exposure – and that healthy adversary is cyber insurance.

The cyber insurance market will escape its present quagmire as it achieves and matures the ability to conduct quantified, rigorous, standardized diligence at scale. That's when companies will reap the benefits of optimized coverage. All incentives will align to deliver secure outcomes, and everyone will win… everyone except, that is, for cyber attackers.

About the Author

J. Foster Davis, C|CISO, is an EC-Council Certified Chief Information Security Officer and Co-Founder of BreachBits, a cyber risk rating and monitoring company that evaluates and tests organizations from a hacker's perspective to empower them to anticipate attacks. He served for 15 years in the U.S. military where he built and led the U.S. Navy's premier cyber resiliency exercise and co-authored the Secretary of the Navy's Cybersecurity Readiness Review. He also specializes in cyber risk management and goal-oriented unsupervised Complex Adaptive Systems. Foster can be reached online at foster@breachbits.com and through the BreachBits website: https://www.breachbits.com/

Cyber-attacks a Most Common Threat in Recent Times

By Udayan Lahiri, Research Analyst at Strategic Market Research

Cyber security safeguards internet-connected devices like hardware, software, and data against various online threats. Cyber security ensures that the public can rely on government services and organisations. Businesses require cyber security to protect their data, intellectual property, and financial assets. Cybersecurity has risen to the top of the priority list for businesses around the world in recent years. Privacy legislation such as Europe's General Data Protection Regulation and the upcoming California Consumer Privacy Act will play a larger role in CIOs' data handling and privacy decision-making.

The global cyber security market in 2021 was $216.10 billion, and by 2030 it will reach $478.68 billion at a CAGR of 9.5% during the forecast period 2021-2030.

According to June 2021 statistics, the total number of ransomware attack attempts (78.4 million) was higher than in the four quarters of 2020. The first half of 2021 saw 304.7 million attempts, more than all ransomware in 2020. The second half was even worse, reaching around 318.6 million. For example, a thorough survey reveals that Iran has the highest percentage of malware-infected mobile devices at 52.68 %.

Beyond legislation, the potential vulnerabilities created by involved parties will be a prominent subject of discussion at the water cooler and in board meetings. CIOs will need to do more investments in employee education to stem the tide of internal data theft, or the present system will persist. Whether intentional or unintentional, data exposure by company stakeholders has cost organizations badly in 2019, and limiting this threat must be a top priority for all.

Types of cyber attacks

- One of the most common types of privacy risks to websites and web applications is ransomware attacks.
- Another major threat to web application security is the supply chain attack.
- Businesses are experiencing an increase in cloud-based web attacks as cloud adoption grows. Various types of cloud-based attacks are SQL Injections attach, cross-site scripting attacks, botnets, spyware, and others.
- Unsuspecting victims are scammed into clicking malicious website links or downloading attachments that harm their system in phishing attacks.

Strategies to stay ahead of cyberattacks:

The restriction will have an impact on both internal threat management and platform security, making it the most critical matter for security professionals in the coming year. The "safe harbor" provisions included in new legislation, such as the CCPA's safe harbor for data encryption, will almost certainly receive a lot of attention. Organizations can and should work hard to adapt to safe harbor clauses with varying degrees of success.

Strategies to stay ahead of cyber threats:

- Many businesses will try to front-load their data protection investments, paying more upfront to avoid high costs later on. It is a smart strategy, but it needs to be well thought out and executed. Spending on security measures only for regulatory compliance should wait until your organization understands what the law demands. Companies should prioritize spending to avoid having a significant negative impact on cash flow for the year and ensure that the solutions being applied comply with the safe harbor clauses as written now that they are aware of these potential "get out of jail free" clauses in new legislation.
- Perhaps now more than ever, speed and response times are important. Recognizing incidents before they rise into full-fledged crises will be important for any organization that collects and stores customer or employee data. Cyberattacks are unavoidable, but long-term harm is not. Companies can manage threats and avoid fines, severe revenue losses, and public relations nightmares if they can detect data egress in near real-time.
- Internal threat mitigation should be a top priority for every business, and it all starts with knowing who has access to what data. Employees in smaller businesses frequently have access to valuable information they do not need to carry out their day-to-day responsibilities. Most employees want the company to succeed, but good intentions do not qualify them as security experts. Create a system that allows granting appropriate permissions to spend more time dealing with external threats.

The strategies listed above are all parts of an overall security posture that will put you in the best position to achieve success in an increasingly dangerous digital environment.

There is a need for access to legal counsel and compliance experts to help navigate new and upcoming regulatory standards, as well as a finance department that can direct y investments in such a way that unnecessary spending is minimized while compliance and security are not jeopardized. IT team must be versatile and agile enough to detect threats as they appear and knowledgeable enough to respond appropriately when data does leave your system. Perhaps most importantly, a workforce is required that prioritizes security at all times.

By making cybersecurity a core responsibility of every employee, from the CEO to the newest intern, a network that is more adaptable and resistant to constantly evolving cyber threats can be built.

About the Author

Udayan Lahiri is a Research Analyst at Strategic Market Research, where he handles custom, and consulting research for topics related to Information technology. His expertise lies in cyber security, metaverse, robotics and health IT etc. Udayan Lahiri can be reached online at udayan@startegicmarketresearch.com and our company website at https://www.strategicmarketresearch.com/

DDoS Attacks in the First Half of 2022

Despite a Preliminary Decline in Attack Numbers, the Threat Situation is Increasing

By Marc Wilczek, COO, Link11

Digitalisation, networking, automation, and globalization are seen by many experts as a blessing for the state and the economy. On the one hand, these aspects facilitate communication and cooperation between people. On the other hand, however, they also represent risk factors. Since the world is technically interconnected, cybercriminals are given the opportunity to attack IT infrastructures at digital entry points. As a result, cyberattacks cause considerable damage to companies, state institutions, and authorities and can even paralyze them. The latest data from Link11's DDoS Report shows the extent to which the threat situation is manifesting itself in the digital space today.

The threat of DDOS attacks

Anyone dealing with the topic of DDoS attacks must first realize how many professionals globally use the internet to communicate, buy or conduct business. This year's survey by the consultancy Horváth also shows how relevant the defense against cyberattacks remains. According to the study, securing digital resilience is the second most crucial management task according to internationally present decision-makers.

With regard to the latest developments in the DDoS threat landscape, the Link11 Security Operations Center (LSOC) has noted that the number of DDoS attacks temporarily decreased by 80% in the first half

of 2022 compared to the same period last year. However, DDoS attacks proved to be faster as well as more dangerous and unpredictable than ever before. The reason for this is the so-called DNA of the attacks, which is changing decisively. The cybercriminals no longer attack impulsively but instead act in a more targeted manner and precisely select the targets for DDoS attacks. Overall, the attacks have been shorter, more intense, and more sophisticated.

Various reasons could have accounted for the falling DDoS figures. First, the shutdown of the world's largest darknet platform, "Hydra Market," in April 2022 caused a possible decline in the numbers. Until German law enforcement authorities successfully unplugged the platform, Hydra served as a hotspot for cybercriminals and was considered a popular destination for DDoS-as-a-service providers. Additionally, waves of extortion attempts linked to mass DDoS attacks have declined to date. This form of attack previously contributed to the disproportionate growth in attacks, especially in 2020 and 2021.

Characteristics of today's DDoS attacks

Bandwidth also played an essential role in DDoS attacks in 2022. The average maximum attack bandwidth increased from 266 Gbps in 2021 to 325 Gbps in the first half of 2022. The most significant bandwidth detected by LSOC was 574 Gbps in 2022. During this period, the volume of data packets transmitted also increased from approximately 277,000 to 1.5 million per second.

The key figures regarding maximum traffic value or critical payload are also crucial for today's DDoS attacks. The decisive factor here is how much time passes after the transmission of the first bytes until the maximum traffic value, i.e. the critical payload, is reached. For example, while the time until the peak in 2021 was 184 seconds, it was only 55 seconds in the first half of 2022. The consequence of such "turbo attacks" is that they can paralyze a network before the defense measures can even take effect.

When developing efficient protection solutions against DDoS attacks, it is necessary to bear in mind the correlation between the duration and intensity of DDoS attacks, which is currently changing significantly. Today's attacks are shorter and, at the same time, much more intense. With growing concentration, higher targeting accuracy, and greater sophistication in the execution of such attacks, more precision and speed are needed in identifying and defending against the attacks. Time will therefore play an increasingly important role in dealing with DDoS attacks in the future.

Industries affected by DDoS attacks

Companies are by far no longer the only target of DDoS attacks. Cybercriminals, such as the pro-Russian hacker organization Killnet, are increasingly attacking state institutions or authorities. Cybercriminals have declared a digital war on Western European states such as Germany, Norway, and Italy. In February, for instance, there were attacks on Ukrainian authorities, such as the Ministry of Defence. At the same time, the websites of Russian government institutions and the Russian stock exchange were also shut down - presumably due to a digital counter-attack (DDoS) caused by the international hacker collective Anonymous.

In April 2022, the online portal of the Hesse police was the victim of a hacker attack. Later that month, the websites of the email service provider Posteo, the Eurovision Song Contest, and the Port of London followed suit. In addition, Norway and Finland have been victims of DDoS attacks throughout 2022. In the economic sphere, cybercriminals primarily attack companies with systemically critical infrastructure.

Efficient IT security solutions fend off DDoS attacks

Overall, it can be postulated that every industry must expect to be confronted with DDoS attacks. More than ever, DDoS attacks are striking the structures of victims with greater intensity and speed. Digital resilience is thus becoming a critical practice for IT decision-makers.

About the Author

Marc Wilczek is the COO of Link11, which is a leading IT security provider in the field of protecting web services and digital infrastructures against cyber-attacks. With its North American headquarters in Vancouver, the company offers fully automated, cloud-based anti-DDoS protection with the fastest Time to Mitigate (TTM) available on the market. Link11 utilizes AI and machine learning to ensure that its TTM accurately recognizes malicious traffic as fast as possible.

Wilczek has more than two decades of leadership and management experience. At Link11, he is responsible for strategic business development, growth initiatives as well as marketing and sales. In addition to management functions within the Deutsche Telekom Group, he was previously Senior Vice President Asia-Pacific/Latin America/Middle East and Africa at the eHealth group CompuGroup Medical and headed the Asian business at the IT security expert Utimaco Safeware (now Sophos), among others. He has a Master of Science in Management from The London Business School and was awarded the Sloan Fellowship.

Marc Wilczek can be reached online at (https://twitter.com/MarcWilczek) and at our company website https://www.link11.com/de/

Exposing and Preventing Security Flaws in Wireless Systems using SDRs

By Brendon McHugh, Field Application Engineer & Technical Writer, Per Vices

Introduction

The use of wireless systems is rapidly expanding and putting more pressure on the finite radio-frequency (RF) spectrum. There are solutions to this pressure that are being employed in various essential systems that require top-notch security. It is vital to ensure that the internet-of-things (IoT) infrastructure can resist attacks over wireless networks, as the growing number of attacks on IoT devices have exposed various vulnerabilities and security flaws.

This article discusses the capabilities of software defined radio (SDR) and its suitability for exposing vulnerabilities and security issues in critical wireless systems, such as industrial internet-of-things (IIoT) infrastructures. SDR platforms are suitable for various security-related applications, including spoofing wireless communication channels, testing wireless security schemes, and optimizing the security of wireless systems.

What is an SDR?

An SDR is a flexible transceiver system that contains a radio frontend (RFE) and a digital backend. This device offers a variety of onboard digital signal processing (DSP) capabilities and an interface to a host system or other external equipment for data storage or additional processing. The RFE performs transmit (Tx) and receive (Rx) functions and can operate over a wide range of frequencies. The highest

performance SDR systems offer an instantaneous bandwidth of 3 GHz and multiple independent analog-to-digital converters (ADCs) and digital-to-analog converters (DACs) channels. Figure 1 shows the key components of a generic SDR system.

The digital backend of a high-performance SDR platform contains a field programmable gate array (FPGA). These FPGA chipsets have various onboard digital signal processing (DSP) capabilities, such as upconverting, downconverting, filtering, data packetization over Ethernet links, modulation, and demodulation. The highest bandwidth SDR systems offer high data throughputs of up to 4 x 100 Gbps, which can transfer vast amounts of data to host systems and storage solutions.

SDR systems have performance characteristics that make them ideal for various wireless security applications. These include high flexibility, low and deterministic latency, multiple-input multiple-output (MIMO) channels, wide bandwidth, and DSP resources. Furthermore, SDR platforms are compatible with many open source toolkits, including GNU Radio and GNU Octave. In addition, custom software for SDR platforms can be developed using programming languages such as Python and C++.

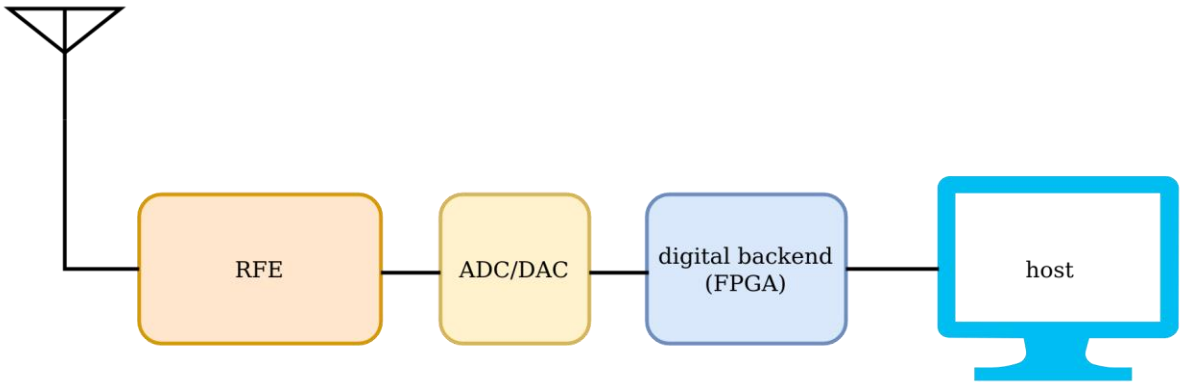


Figure 1: Components of a typical SDR system

SDRs for wireless network security applications

The capabilities of SDR platforms are valuable for various security testing applications for wireless networks. Firstly, SDR platforms can connect to various systems, such as antennas and amplifiers. Secondly, these devices can be used as transmitters since they generate many pulses and waveforms. Moreover, the GNU Radio toolkit allows an SDR system to serve as a channel emulator, spectrum analyzer, and power meter. In addition, SDRs can perform multiple network tests, including jamming, spoofing, penetration testing and eavesdropping tests.

SDR platforms have a wide tuning range and can support a broad array of wireless and wired technologies. The onboard DSP capabilities of SDR platforms allow the implementation of frequency hopping and other techniques that can help to enhance security between wired and wireless communication technologies. The FPGAs used in SDRs are suitable for implementing network layer and application layer solutions. Furthermore, the reconfigurability of SDRs allows the implementation of new and upgraded wireless protocols and DSP algorithms on existing hardware.

New and emerging network models, such as mesh networks, require encryption and security features to be implemented on the devices. FPGAs allow such features to be implemented and updated without the need to modify the hardware.

Wireless networks and IoT/IIoT vulnerabilities

Wireless networks are required to have security features that ensure integrity, availability, confidentiality, and access control of network operations. To start with, confidentiality requirements help to ensure that data cannot be accessed by unauthorized parties. Integrity features enable detection of intentional or unintentional changes to data as it travels through a network. Network availability features ensure that the network is available to users when they need it. Lastly, access control features restrict the network and its resources to only users who are authorized. Figure 2 shows a 4-layer IoT network architecture.

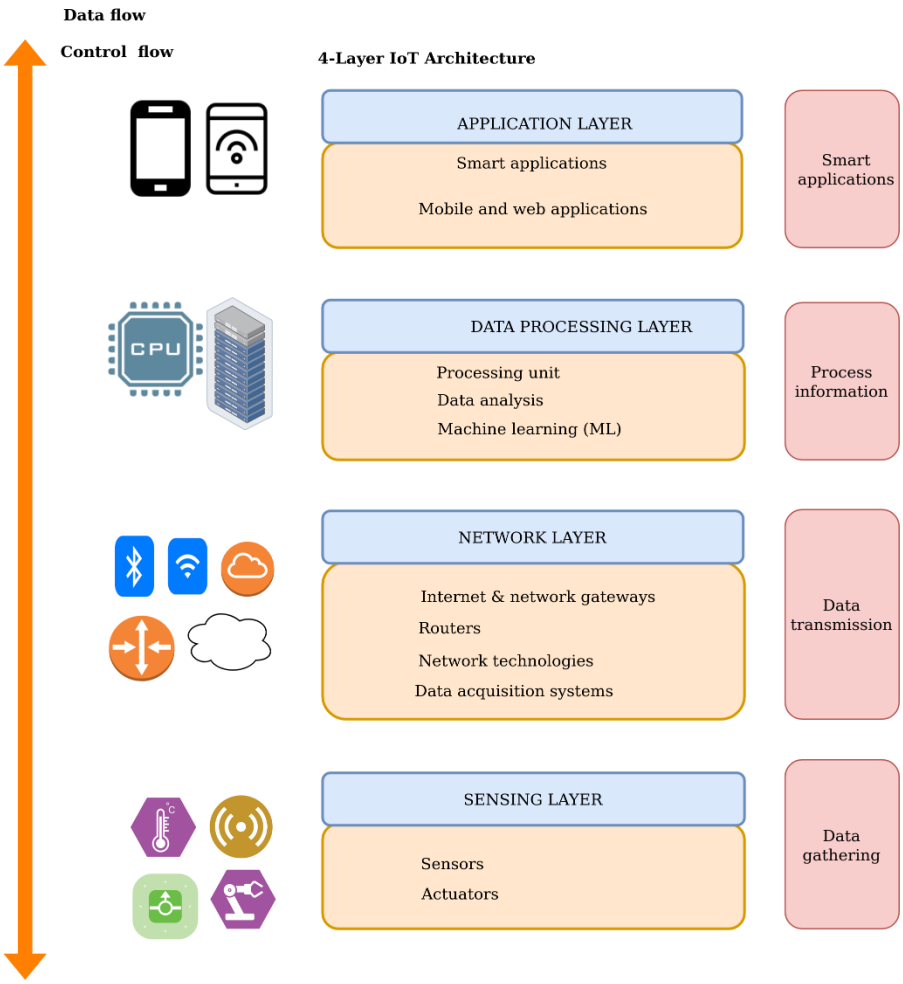


Figure 2: A 4-layer IoT network architecture

Wireless, IoT, and IIoT networks are susceptible to a variety of security flaws and vulnerabilities. Some of the most common wireless network security vulnerabilities include rogue cell towers, rogue WiFi networks, eavesdropping devices, unapproved cellular devices, and unapproved IoT transmitters.

Rogue cell towers utilize IMSI catchers or stingrays to enable unauthorized users to listen to calls and read SMSs. Rogue WiFi hotspots are commonly used by attackers to launch man-in-the-middle attacks, which can be used by attackers to steal users' credentials and illegally monitor network traffic.

Eavesdropping and other types of surveillance devices are usually hidden in meeting rooms to record voices of the targets. Most of these devices are voice-activated and utilize various network technologies including FM and GSM to transmit captured voices. Similarly, wireless cameras and cellular devices can be used to breach security in restricted areas. Furthermore, wireless peripherals such as wireless keyboards and mouses that lack data encryption can be exploited in keystroke injection attacks.

Home automation systems with unsecured configurations can be exploited by attackers in a variety of ways. Similarly, unapproved IoT emitters such as wireless sensors and thermostats utilizing Zigbee, LoRA and other wireless protocols can be used to compromise the network security of a building. Furthermore, attackers can jam vulnerable security alarm systems such as motion detectors and door sensors using SDR-based solutions.

IIoT attacks can be broadly classified into application data, transport routing attacks, and perception physical attacks. Some of the most common application data attacks include deal-of-service (DoS) attacks, jailbreak, and malicious code injection.

Transport routing attacks take different forms including data transit attacks and DoS attacks. Hackers use a variety of perception physical attacks to compromise IIoT systems, including routing attacks, data transit attacks, spoofing, and DoS attacks.

SDRs for assessing IoT/IIoT security

The diversity of protocols and standards used in IoT and IIoT networks makes authentication a challenging task. Authentication in such network infrastructures demands complex security schemes.

SDR platforms offer capabilities required to execute different hacking strategies on IoT systems. The stages involved in such a process include capturing/recording, demodulation, decoding, and information exploitation.

Signal decoding entails utilizing algorithms to decrypt the demodulated data on the SDR platform or host system. The information exploitation stage may take different forms, such as extracting sensitive information, corrupting transmitted data, and gaining control of a device.

Various testing techniques are used to enhance the security of wireless and IoT systems. To start with, fuzz testing or fuzzing is a common method for performing liability verification in software solutions. This automated testing method entails providing software with random or unexpected input data and monitoring the output to identify flaws such as memory leaks, bugs, and crashes.

Penetration testing or pen testing involves performing a mock cyberattack on a computer or IoT system to identify exploitable vulnerabilities. The results from these simulated tests are used to configure applications to enhance the overall security of a system.

An SDR platform can be used to implement flexible fuzzing solutions suitable for exposing potential liabilities in the physical and media access control (MAC) layers of wireless network systems. SDR-based fuzzers are ideal for testing many flaws, including memory leaks, crashes, and failing built-in assertions. Furthermore, these solutions support a variety of interfaces, engines, protocols, and test cases. In addition, SDR-based fuzzers are suitable for exposing vulnerabilities associated with different protocol stack layers.

SDR systems are ideal for implementing WiFi protocol fuzzing test solutions such as Owfuzz. This framework allows fuzz testing of WiFi frames and interactive testing of various WiFi protocols. Furthermore, SDRs can be used for implementing solutions for assessing the security of new and emerging IoT protocols.

Various SDR-based tools for performing penetration testing and analysis have been developed and tested. To begin with, scapy-radio is an SDR-based solution for performing wireless monitoring and injection. This wireless security assessment solution is based on scapy framework and was used to study the security performance of Z-wave protocol-based devices. Tests with this SDR-based solution showed it was highly effective in performing penetration tests.

In a different study, researchers used an SDR platform to implement a solution for testing the security flaws of products that use Bluetooth Low Energy and Zigbee. The implemented penetration testing solution was capable of assessing the security of the two protocols.

Summary

Wireless and IoT systems have many security flaws that attackers can exploit. SDR platforms have unique capabilities that make them ideal for implementing tools for testing the security of wireless and IoT systems. These capabilities include MIMO channels, DSP resources, reconfigurable FPGAs, a wide tuning range and a high bandwidth. These capabilities make SDR platforms ideal for implementing various solutions for testing the security of wireless systems, including penetration testers and fuzz testers.

About the Author

Brendon McHugh is the Field Application Engineer and Technical Writer at Per Vices Corporation. Per Vices has extensive experience in developing, building, and integrating software-defined radios for iOT and network security applications. Brendon is responsible for assisting current and prospective clients in configuring the right SDR solutions for their unique needs, and possesses a degree in Theoretical and Mathematical Physics from the University of Toronto. Brendon can be reached online at solutions@pervices.com and at our company website https://www.pervices.com/

Exposure Management as The Practical Arm of Digital Risk Management

By Patricia de Hemricourt, PMW, Cymulate

In the last few years, the cyber landscape has evolved rapidly on multiple fronts. The large-scale adoption of agile development methods led to constant changes in organizations' digital environments and sweeping inclusion of open-source code snippets in CI/CD pipelines, the massive trend to move partial or entire infrastructures to the cloud, the unplanned wholesale move to work-from-home resulting from COVID 19, the ever-expanding number and types of connected devices, all are elements that changed the digital landscape beyond recognition.

At the same time, the profile of the typical cyber attacker evolves from hooded loners relying on intensively honed skills to entire criminal organizations and increasingly aggressive nation-states. The darknet now hosts full-blown cyberattack-as-a-service marketplaces offering a rich and varied choice of off-the-shelf offensive tools, some of which are of high complexity. This removed the erstwhile barrier of entry that limited the number of potential attackers to people with advanced programming skills and fed the growth of cyber-criminal organizations' ranks.

Faced with these fundamental changes and the resulting ballooning number of vulnerabilities, the cybersecurity space had to evolve and adapt to the new reality on the ground. One of the cardinal shifts of focus required is pivoting the security focus from passively detecting and mitigating vulnerabilities to evaluating the risks, in terms of potential operational damage and direct and collateral costs, for the different components of a digital infrastructure.

Actively including cybersecurity in the company's GRC framework requires establishing a high-level business layer – digital risk management -, as well as a practical layer – exposure management.

Shifting to Digital Risk Management

As, regardless of their sectors, organizations increasingly rely on a digital infrastructure progressively permeating all aspects of operability, executives need to be actively involved in the digital risk management process.

Cymulate 2022 Data Breaches Survey Report shows that organizations where leadership and cybersecurity teams met 15 times a year experienced no breaches, compared to at least six breaches for those meeting less than nine times per year. Digging deeper into the data showed that the frequency of discussions around risk reduction for leadership and cybersecurity teams is a key factor in lowering the probability of breaches, which tallies with the positive correlation between executives' awareness of the cyberattacks and the health of their security posture.

Gone are the days when the CISO could be blindly tasked with keeping the infrastructure secured.

With limited resources, the CISO or designated IT manager needs to know which assets are most crucial in terms of potential business interruption, legal damages from fines to compensation, reputational damage, loss of intellectual property, loss of business, cyber insurance premium hike, cost of ransom or cyber investigation, or other risks. That information is crucial to enable defining on which assets preemptive mitigation efforts need to be focused on first.

The frequency of discussions around risk reduction for leadership and cybersecurity teams is a key factor in lowering the probability of breaches, which tallies with the positive correlation between executives' awareness of the cyberattacks and the health of their security posture.

Once the risks are mapped to the assets, the CISO or designated IT manager can begin to manage the infrastructure exposure.

Implementing Exposure Management

The idea underlying switching from a vulnerability management approach to an exposure management one is to eliminate wasted time, efforts, and resources patching vulnerabilities with a high CVSS score but a low exploitability in the organization's context due to several factors ranging from the lack of available exploits for specific vulnerabilities to the effectiveness of compensation controls in the organization's infrastructure.

The first step to effectively managing exposure is to map all external and internal assets. For optimal results, this should be performed before risk management meetings with executives as it enables mapping assets' business value to the corresponding digital infrastructure components.

To evaluate the exposure resulting from individual components and the connections between them, the most efficient approach is to emulate cyber attackers and run a comprehensive array of emulated attacks with inactive payloads. This adversarial validation approach provides an in-context evaluation of breach feasibility and potential propagation depth of successful breaches.

Mapping outcomes such as gaps in security enforcement or emulated attack routes to the assets' value established with executives during risk management meetings informs the CISO or designated IT manager as to how to prioritize their remediation efforts to achieve maximal impact with the available resources.

Exposure Management Technologies

Until recently, penetration testing was the only avenue to run adversarial validation of an organization's security posture. Penetration testing remains an indispensable tool for evaluating the security posture health, but it suffers from major flaws in today's fast-paced world.

Aside from the high fees they command, penetration tests require an organization to prepare extensively and might disrupt operations even if preparations are thorough. Due to these limitations, penetration tests can only be performed infrequently. Even if the penetration test report is timely provided, the evaluation and security flaw identification it contains is only valid for that point in time, and its rapid obsolescence means its value is very limited in time.

This led to the emergence of new technologies such as:

- **Breach and Attack Simulation (BAS):** Focused on the validation and optimization of security controls, BAS is a service recreating and emulating real-world attacks and launching production-safe attack campaigns against your environment to test defensive tool stack vectors ranging from email gateways, web gateways, Web Application Firewalls, (WAF), endpoint security (EDR), and resilience to emerging threats, data exfiltration and other actions on objectives. BAS is typically agent-based, which means it does not evaluate breach feasibility. Some BAS vendors include end-to-end attack scenarios containing attack path mapping elements. BAS limitations are that, though it can independently test any attack technique on any segment of the attack kill chain, it lacks end-to-end attack route context.
- **External Attack Surface Management (EASM):** EASM emulates the recon stage of a cyber-attack by scouring the Internet to uncover exposed assets. Unmonitored exposed assets are a choice entry point for cyber attackers.
- **Red Team Automation:** Focused on evaluating breach feasibility, Red Team Automation technologies emulate attacks from recon to actions on objective. As opposed to BAS, it lacks the capability to comprehensively assess specific attack kill chain segments.
- **Attack-Based Vulnerability Management (ABVM):** Using the information collected with the technologies above, vulnerability prioritization technology such as ABVM lists the security gaps by order of criticality in context, decreasing the criticality of vulnerabilities compensated for by security controls and streamlining the patching process for maximum impact.

Extended Security Posture Management (XSPM) platforms combine some or all these technologies, providing a unified interface to manage the data collected.

Testament to the rising significance of exposure management, Gartner recently published a Continuous Threat Exposure Management (CTEM) program delineating the recommended approach to increase cyber resilience through threat exposure management.

The shift from vulnerability to exposure management is mirrored in regulatory bodies by a shift from cybersecurity to cyber resilience, a topic that will be covered in a subsequent article, but both trends are powered by the same need to respond to the rapid and wide-ranging evolution of cyberspace.

About the Author

Patricia de Hemricourt, PMW at Cymulate. In her role, Patricia is responsible for articulating the company's product functionalities, capabilities, and use cases. Patricia is a veteran technology writer with over 25 years of experience and is passionate about cyber technology. Patricia can be reached on LinkedIn https://www.linkedin.com/in/patriciadehemricourt/ and at our company website http://cymulate.com/platform/ Cymulate comprehensive continuous security validation technologies unified in a single platform optimizes exposure management by mapping attack path, validating security controls' efficacy and streamlining vulnerability prioritization.

How MFA and EDR Can Help Bolster Your Cybersecurity and Minimize Risk

Understand Cybersecurity Evolution to Understand Tactics of Bad Actors.

By David Corlette, Vice-President of Product Management, VIPRE Security Group

Cybercrimes are growing at an exponential rate. So much so that Cyber Defense Magazine predicts cybercrime costs will increase by more than 10% per year over the next five years, reaching into the many trillions of dollars in losses and related expenses.

While the volume of cybercrimes continues to climb, business owners are faced with the task of trying to stay one step ahead of bad actors – and their relentless attempts to circumvent their company's defenses.

Threats and threat protection have always been a rat race, with attacker technology evolving and defensive technology adapting in response. Add this cat-and-mouse game to the complexities of protecting today's hybrid workforce and it's clear that managing cybersecurity should top every company's to-do list.

To fully appreciate how fast bad actors have evolved their tactics, you need to first understand the cyberattack evolution.

Bad actors are constantly evolving their game

Not so long ago, malware threats were basically single files that were sent out to a lot of people with the hope that a percentage would lack the cyber smarts and fall prey to an attack. Once an antivirus (AV) team or vendor got hold of a copy of the malware threat, they could easily craft a “signature” to detect and block the potential threat.

Then bad actors started to make their malware variants evasive, obfuscated, and polymorphic. Still, AV vendors and teams could analyze known malware to develop specific signatures for detection.

Next came the advent of even more obfuscation, file-less malware, and the like. AV vendors and teams then deployed machine learning (ML) models to monitor running process behavior to detect malware threats. In this era, the ML model was tasked with doing the detection, using millions of pre-known malware samples – all of this driven by the AV vendor or team.

Most recently, threats have evolved to depend less on actual malware binaries, using living-off-the-land techniques, remote exploits, and other methods previously seen solely in custom Advanced Persistent Threats – but now automated and deplaned to target smaller and smaller businesses. Since portions of these attacks don’t use malware files, more advanced correlated endpoint activity detection is needed to discover potential attacks using these techniques.

However, while the sophistication and obfuscation techniques of attackers have improved, detection has gotten “fuzzier” as we’ve moved away from signature-based detection to more rule-based or ML-based detection. This means that “false positives” are also more prevalent, as any such rule-based system comes with the risk of misidentification.

With the constant – and ever-increasing – threat of potential cyberattacks, many companies are applying for cyber insurance, which generally covers a business’s liability for a data breach involving sensitive customer information, such as social security numbers, credit card numbers, account numbers, driver's license numbers, or health records.

In the past, cyber insurance submissions were simple and it was easy to obtain bindable quotes from multiple vendors, but times have changed. Now organizations applying for cyber insurance have to show they are implementing a long list of cybersecurity technologies and practices including multifactor authentication (MFA) and endpoint detection and response (EDR) to acquire coverage.

Multifactor Authentication (MFA)

MFA is a security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction. Multifactor authentication combines two or more independent credentials: what the user knows, such as a password; what the user has, such as a security token; and what the user is, by using biometric verification methods.

The goal of MFA is to create a layered defense that makes it more difficult for an unauthorized person to access a target, such as a physical location, computing device, network, or database. If one factor is compromised or broken, the attacker still has at least one or more barriers to breach before successfully breaking into the target.

MFA should be used to protect remote access, email access, and administrative access. This helps prevent intruder's access to deploy ransomware, steal sensitive information, or erase valuable data. Just how effective is MFA? According to Microsoft, MFA provides an added layer of security that can block up to 99.9% of attacks stemming from compromised accounts.

Endpoint Detection & Response (EDR)

Endpoint detection and response (EDR), also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.

EDR is designed for endpoints, not networks, and these endpoints can become entry points for cyber attackers. EDR uses endpoint data collection which is software installed into machines. This tracks and gathers data which is then reported to the EDR vendor for review. Once data is collected, the technology and algorithms track what is "normal" behavior for a user. If suspicious activity is found, an alert is generated. EDR also has the capability to automatically block malicious activity to temporarily isolate an infected endpoint from the rest of the network to not allow malware to spread.

Protecting your business, your employees, and your customers is your responsibility

While no single IT security process, patch, or software is s a silver bullet for preventing 100% of cyberattacks, by implementing both MFA and EDR you will significantly minimize the threat of a breach. Additional ways to minimize risk include employee training, increased awareness, and routine software patching and updates.

Small and mid-size business owners are most susceptible to attack. In fact, 60% of small businesses fold within six months of a cyberattack. By working with a trusted partner to help implement MFA and EDR technology, monitoring your business, staying vigilant, and training your employees on cybersecurity, you can help protect your employees, your customers, and your business from potential threats.

About the Author

David Corlette is the Vice President of Product Management at VIPRE Security Group. He works with customers and partners to design and build best-of-breed IT security solutions. He has broad experience in advanced threat, SIEM, networking, cloud services, security standardization, open source, agile development, and technology policy. David can be reached online at https://www.linkedin.com/in/davidcorlette/ and at our company website https://vipre.com/

Identifying Assets to Prioritize a Better Cyber Defense

By Joel Fulton, Co-Founder and CEO of Lucidum

While many organizations feel safe with their cybersecurity strategies through in-house or third-party IT infrastructure, various scanning or agent software, or other means to protect enterprise essentials, there are numerous risks lurking beneath the shadows. Ransomware, insider threats, malware and other cybersecurity threats have become increasingly intelligent and have no trouble surpassing and compromising an enterprise through ever-evolving factors.

Complex, distributed, and federated modern architectures exceed the capabilities of even modern defensive strategies. Despite security perimeters, compromises continue to occur where threat actors discover attack vectors, such as invisible components to the organization's attack surface, resulting in zero-day exploits. Facing our current cybersecurity climate head-on by performing a comprehensive asset inventory is necessary to mitigate these risks while protecting an enterprise.

Bloated Cyber Infrastructures

Enterprise architectures are often held together through microservices, SaaS vendors, and personal technologies from employees. The increased footprint expands an enterprise's most sensitive network. Its ecosystem is constantly changing, therefore many cybersecurity frameworks that are thorough enough for one system can ignore others entirely. A more comprehensive method is necessary that goes beyond archaic, outdated services that can no longer keep up with a more progressive technological environment. Every new connection opens the door to a new vulnerability.

Failing at Detection

Using the latest in microservices and multi-platform applications are often the starting point for cybersecurity, but unfortunately, they come up short in more complex and federated enterprise architectures. The process of detection, isolation, and response is the modern proactive security focus, but the detection point has become increasingly more difficult.

As many security compromises lie outside the intended security perimeter, attack vectors find their way through hidden backdoors and result in zero-day exploits. More attacks are the effect of invisible components from the attack surface of an enterprise, the sum of all technologies that enter, exit, and touch upon the entire infrastructure itself.

Addressing Ineffective Strategies

Enterprises have a variety of procedures and techniques at the ready to combat possible cyber threats. While the following are popular options, they too have blind spots:

- Inexperienced IT: A human being can only do so much. While the most astute IT personnel can assess problems of interest from contextual red flags and interactions, an untimely miss is bound to happen. Additionally, if the in-house or third-party IT team is not receiving continued education, their expertise will soon be out of date.
- Software Agents: Although performing constant monitoring and tech correspondence, they only work if every system in the ecosystem is known. They work accordingly when detecting devices that are in known use with corporate governance or security policies but fall short in that they must be installed purposefully on every user device and service within the network. As soon as an employee brings a new device into the network, possibly granting API permissions or failing to follow security protocols, it creates an easily accessible pathway for bad actors.
- Scans: While scans are successful at sending out a pingable response for discovered abnormalities, it leaves too much to the imagination. The surface-level strategy is apt to miss targets, all while slowing down the network. If it manages to catch a bad actor, it does not provide enough information to take necessary action.

As points of detection are continuing to fall beyond the grasp of these cybersecurity methods, a practice of performing a broader asset inventory is necessary.

Utilizing Machine Learning Power

An answer to the outmoded deficiencies is found in machine learning. Using the latest in artificial intelligence, machine learning has the capabilities of using contextualized data and metadata to course through trillions of interactions per minute in an ecosystem. The process allows an enterprise to uncover and acknowledge every asset for every device, file, user, or any other relevant piece of the puzzle connected through the network.

Without interfering with an ecosystem's daily processes, machine learning is in constant-detection mode, investigating every bit of information uncovered for a full analysis. All assets are cross-referenced to historical data points, revealing conflicting or redundant information, and accurately triangulating its position, as well as assessing their potential risk.

Additionally, machine learning has the capability of detecting and defining assets without relying on the use and installation of a software agent on every device, capturing what traditional programs could easily miss. It provides powerful analytics that can be integrated into all ecosystem platforms. Data extracted through detection cycles is minimal, only storing relevant information when needed – all while keeping a minimized footprint and staying malleable to risk and compliance policies.

Safeguarding for the Future

Using machine learning advances the goals of dated and flawed technology to reach the next chapter of cybersecurity. Capturing and accurately identifying assets provides essential context for an ecosystem to catch problems before they arise. By prioritizing asset inventory businesses can address network vulnerabilities and ultimately create the right defense against any threats lurking beneath the surface.

About the Author

Joel Fulton is the Co-Founder of Lucidum, the cyber-asset visibility and discovery solution. He is also the Co-Founder of Silicon Valley CISO Investments, a leading group of Chief Information Security Officers that operate as an angel investor syndicate.

Previously the Chief Information Security Officer for Splunk, Dr. Fulton has also led security and risk teams at Symantec, Google, Starbucks, Boeing, several financial institutions and led a security and regulatory compliance consulting firm for ten years.

In 2017, Security Magazine named Dr. Fulton one of the Most Influential People in Security. He is a frequent speaker at external conferences and customer events on Insider Threat, AI/Machine Learning & Cyber Security, pragmatic risk management, and global security management. He holds a bachelor's degree in business administration from Excelsior College, a master's of science in information security from Capella University, and a doctoral degree in information assurance and security from Capella University. Joel can be reached online at @drjoelfulton on Twitter and at our company website https://lucidum.io/.

Implementing a Data Bodyguard

By Navindra Yadav, CEO and Co-Founder, Theom

Modern security solutions – be they application, endpoint, IoT-focused, etc. – have evolved. Security has been shifted both left and right. However, data breaches continue to increase. The reason is very simple: almost all security solutions focus on protecting and monitoring the infrastructure or the device, but not the data.

Think about the first family of the U.S. They have an entire security team focused on protecting them, no matter where they go. Organizations need a similar approach to keeping data safe – think of it as a "data bodyguard" or protection that moves with your data. Data is any organization's most important asset, and yet time and time again, legacy solutions are failing to protect it.

What cybersecurity gets wrong

Data breaches continue to take place all the time, despite far more awareness than ever before and a proliferation of cybersecurity solutions. In fact, according to IBM's 2022 Cost of a Data Breach report, 83% of organizations studied have had more than one data breach. And these breaches are getting more expensive, reaching an average cost of $4.35 million in 2022, up 2.6% from the prior year.

The biggest challenge stems from how data is being protected in most organizations. It's the most important asset for almost any organization, and yet security solutions are traditionally failing to really focus on it. There is no shortage of cloud security, endpoint security, application security solutions and the like – but these still don't solve the major challenge of protecting your data as it moves or gets copied, because they are oblivious of what they are supposed to be protecting. In these cases, the protection or controls you have in place don't necessarily follow that data. That's why breaches happen.

What's needed is a way to protect your data as it moves from location to location – in a way that's affordable and operationally easy to use, without causing more stress on organizations already grappling with limited budgets and the ongoing cybersecurity skills gap. In addition, enterprises need an anti-fragile

zero trust solution focused on data. A working zero trust system has zero implicit trust, and it puts data in the center and then builds protection outward.

Security that moves with your data

Breaches keep happening because we're not watching the data. Instead, we're focusing on applications, endpoints and so on. Most people know they have a problem when it comes to protecting their data, and part of the issue stems from not knowing how to prioritize the data. To protect it, you need a better way to understand the value of that data, and most companies don't have an internal crawler that indexes their own data.

And it's not just about the data – it's also about who is trying to access the data. For instance, in a financial services organization, imagine that certain sensitive financial data can only be accessed by financial analysts inside the U.S. You need the right controls and rules in place that govern who can access what data, when and from where. This is tedious and time-consuming work for humans; automation is a better solution.

An anti-fragile, data-centric approach

A best practice is to implement what's known as an anti-fragile, data-centric zero trust system:

1. Establish "data intelligence": Know the data you are trying to protect. If you do not know what you are trying to protect, you will never successfully protect it. This includes visibility of cloud data stores, data lakes, your data warehouses – where your data is stored and data-in-transit points (message Queues/APIs), etc.

Establishing data intelligence entails these steps:

- Create a protection surface. An effective protection surface (or minimal attack surface) can only be built by putting data at the core and defending outward from it.
- Use an automated tool to discover the data, catalog it, establish the criticality and business value of it, and map the data flows. This requires continuous data discovery, data classification (standard taxonomy and custom taxonomy), and data flow/lineage mapping.
- Using the above two steps as input apply the principle of least privilege of access all the way to data tables and granular data store constructs. Automating this step and marrying it with the policy guardrails is critical to create an anti-fragile system.
- Deploy an automated tool to discover and baseline who (electronic or human) accesses what data.

2. Asset and alert prioritization: Automatically establish the priority of risks based on business criticality of data. You need an automated way to essentially put a financial or business value on your data to help prioritize it. How important is each piece of your data? And who is accessing it? What are their roles? Automatic data centric prioritization means you don't have a run away security budget in terms of hiring more people and buying unnecessary tools.

3. Coarse business policy guard rails for security and compliance: Coarse policies are key to anti-fragile zero trust systems. Set up very simple to express and coarse business policy guardrails to get continuous data assurance and data compliance. You can start to put in the right controls and then prioritize the risks to the various stores of data. These rules should be oblivious of the data store or data in motion constructs. Enforce the rules through a SIEM/SOAR where data is stored, or over which APIs data is moved.

4. Workflow integration and harmonization: Enforcement of the data assurance, compliance and protection guardrails must be done using a SIEM/SOAR integration.This step ensures you have investment protection and also do not have to re-train the cyber security staff. Automating the prior steps eliminates the need to train cyber security staff on data technologies.

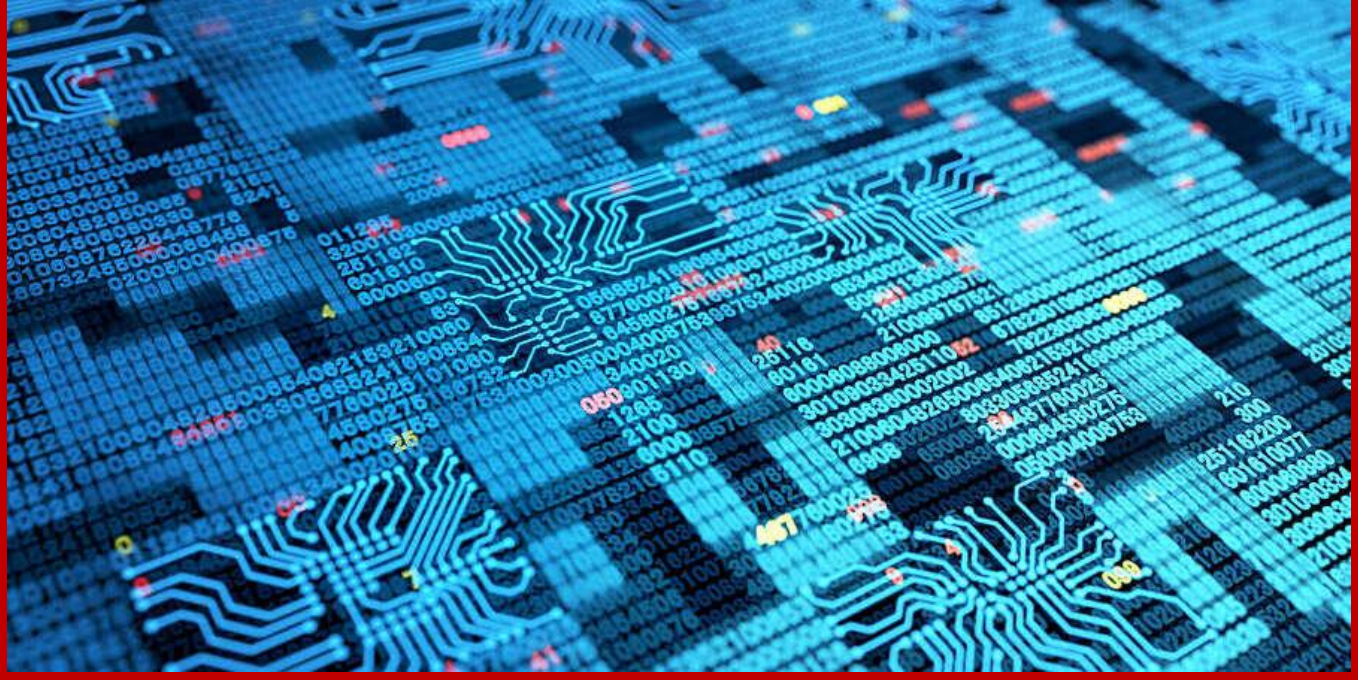
5. Monitoring: This enables continuous system improvement for a data-centric, anti-fragile zero trust system. It provides a historical timeline view-based tracking of data access and relationships between different security attributes of data. Monitoring helps with high-quality incident reviews and also forms a solid foundation to drive a feedback loop.

Defending the core

Building defenses outward around a core of data is a common-sense approach to data security. Cyber attackers are going to get in, but you can take steps to ensure they can't access your valuable data. This is the benefit of implementing a data-centric, anti-fragile zero trust system. Use the approach outlined above to deliver a zero trust approach to data protection.

About the Author

Navindra Yadav is the Co-Founder and Chief Executive Officer of Theom. As CEO, Navindra is focused on ensuring every Theom customer successfully secures and protects their data easily and within budget. Navindra is intimately familiar with the challenge, he has lived the life of a CISO/CIO, besides being the CEO, he was responsible for all security and data assurance operations for Tetration for 7 years. Before Theom, he founded Tetration Analytics and was a Cisco Fellow (highest technical level @ Cisco). Tetration is the flagship CWPP, CSPM product of Cisco. Before Tetration, Navindra was a founding engineer and a Distinguished Engineer at Insieme (also acquired by Cisco), where he built the ACI switch fabrics which is Cisco's DC/Cloud offering. Before Insieme, he worked on cyber security, and network compilers for Google Infrastructure (AI/Game theory/programmable networks). A long stint at Cisco where he built the extremely successful Cisco Catalyst 2k, Catalyst 3k, and Catalyst 4k line of switches. He has also worked for Lockheed Martin and Bell Labs (Lucent). He has 193+ patents to his name.



In a Worsening Cybersecurity Climate, AI can be a Cyber Security Team's Best Friend

By Peter Barker, CPO, ForgeRock

The cybersecurity landscape is evolving

The pandemic has driven a rapid increase of, and reliance on, tools that enable consumers and remote workforces to access digital services. Remote employees were given access to critical systems via mobile authentication, schools opened their networks for students to make use of via home WiFi for virtual learning, and banks performed crucial identity checks without any in-person requirement. These digital shifts allowed us to stay productive and connected at a time of huge disruption. However, the more reliant we are on digital channels, the more the cyber attack surface expands, exposing new chinks in the armor of even the best security systems.

Today's cyber threat landscape is evolving at an alarming rate. According to ForgeRock's latest research, breaches involving passwords skyrocketed by 450% between 2020 and 2021. Given growing malicious activity with a bigger digital footprint, it is clear that cybersecurity teams should escalate their defenses proportionately. But with the current talent shortage leaving 3.5 million cybersecurity positions unfilled in 2021, the obvious question arises: how can strained security teams do more with less to meet growing threats?

AI is a force multiplier

One answer is to make effective use of AI. AI has the potential to mitigate much of the strain currently felt by under-resourced cyber teams thanks to its ability to strengthen existing cybersecurity teams and systems by automatically identifying and counteracting threat actors based on machine learning algorithms. Abnormal activity can be swiftly flagged to IT teams based on an understanding of individual user behavior, curbing the threat of bots and suspicious IPs.

What's more, AI can process a far greater volume of data than humans are capable of, freeing cybersecurity professionals from laborious identification tasks and allowing them to take a more strategic view of operations. Decision making is made easier because AI can provide teams with a greater level of data to back up findings with impressive accuracy and speed. Put simply, AI is a force multiplier for IT teams, allowing them to function at optimum capabilities at low cost and fast integration.

The AI market is primed to grow exponentially by $19 billion between 2021 and 2025.

Avoiding the pitfalls

As businesses look to incorporate AI into their tech security stack they must be aware of the dangers posed by those that might over-sell AI or "AI-wash" less sophisticated products. Companies must make sure they invest in products that use true AI as a core part of its functionality, and not through vague connections or useless 'add-on' automation. Much like "cloud-washing" and "green-washing" before it, AI-washing is a real problem and companies must ensure they take the time to properly examine any AI-powered security solutions to make sure they are not simply trying to harness the power of the latest buzzword.

Another potential pitfall when implementing AI within your security stack is "data poisoning," a form of attack specifically designed to penetrate weak AI systems. In these instances, hackers plague weak AI systems with erroneous data, tricking machine learning algorithms into mis-categorizing abnormal behavior as normal. If effective, this tactic can open the door to malicious actors. Fortunately, these attacks are easily guarded against, by sourcing machine learning training data from verified sources, and hiring experienced data scientists who can oversee an end-to-end ModelOps process to monitor the internal processes of AI modeling.

Despite security teams' best endeavors, the increase in malicious activity is outpacing most human defense efforts. AI is therefore an invaluable counter-force that will effectively protect businesses from the rapidly evolving threat landscape while also helping to mitigate the rising cost and scarcity of talent. At a time when defending networks, endpoints, and data is more challenging than ever, AI can add enormous value by taking on some heavy lifting and keeping security teams focused on the bigger picture by providing accurate, real-time alerts, and quick-moving defense procedures. Whatever your sector or industry, every company should be developing its strategy for effective use of AI security in the years ahead.

About the Author

Peter Barker is a Chief Product Officer at ForgeRock, driving the company's global product vision, design and development, and leading product management and all of engineering. Peter joined ForgeRock from Oracle, where he served as senior vice president and general manager of the Identity Management and Security business. Based in Austin, Texas, Peter previously held executive-level positions at Good Technology, Motorola, FedEx and other companies.

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customers including the BBC, HSBC, Vodafone, and Toyota, orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. Headquartered in San Francisco, ForgeRock has more than 600 employees around the world – including a team of more than 140 in Bristol in the UK.

Peter can be reached at our company website https://www.forgerock.com/

Island Hopping: The Rising Strategy Among Cyber Adversaries

By Tom Ammirati, Chief Revenue Officer, PlainID

In the face of non-stop cyberattacks, litigation, and federal penalties, enterprise companies are upping their game when it comes to new security measures to fortify their environments. Small businesses, unfortunately, are not always quite that fortunate.

Most small businesses lack the budgets, resources, and expertise to protect themselves against cybercriminals. Not many startups or family-owned companies can afford a compliance officer or cybersecurity expert. They might have budgets to backup and recover their data and operations However, solid defenses that stop the penetrations are seldom in place.

According to a recent cyberattack prevention survey, only half of small businesses are prepared to prevent a cyberattack, even though the threat of one is a top concern. Cybercriminals are abusing these two disparities to target a new vulnerability with an intrusion method called “island hopping.”

This approach allows them to bypass corporate security infrastructures by piggybacking on interactions with vendors or suppliers. Accessing communications, for example, that might include invoices or other forms of data, is just a hop, skip and jump away from their ultimate destination, sensitive data and employee/customer credentials.

Cybercriminals use island hopping to target third-party companies to gain access to a treasure trove of data with a national retailer, large healthcare provider, or critical infrastructure. They know the chances are great that vendors, third-party service providers, and partners may have weaker security hygiene, training, and infrastructure.

History Behind the Name

Island hopping got its name from the World War II practice of targeting islands to orchestrate an attack on the mainland. Think of the Japanese attack on Pearl Harbor and Midway Island. You might expect an attack on your network from more well-known threat sources like state governments or cyber groups. Instead, it comes from vendors and suppliers you trust.

Attackers are taking advantage of human error for third-party companies to access the larger network. Nearly 90% of financial institutions are concerned about their shared service providers' cybersecurity. Other industries, including healthcare, manufacturing, and infrastructure providers, are all at risk as long as they receive services from outside sources.

Adversaries are already finding great success through Island Hopping

Island hopping can subvert your supply chain and open you up to phishing and ransomware attacks. A recent example includes Toyota Motor Corp., which was forced to suspend its factory operations at 14 plants in Japan after a supplier of plastic parts and electronic components was hacked last February. As a result, the company's output was cut by nearly 13,000 cars.

On a smaller scale, island hopping might occur if you frequently order food for your employees from the same website. Island hoppers can leverage that information to hack the restaurant's website and use it as a watering hole to gain data that can be leveraged to target your company.

How Zero Trust Plays a Major Role in Cybersecurity Posture

To prevent such devastating damage to your network, security measures like Zero Trust must be combined with a clear single panel view of your data and the knowledge of who is authorized to access and authenticate it.

No singular cyber solution can prevent an island-hopping cyberattack, but authentication can prevent further organizational damage. To protect your networks against island hopping, you must understand that your security perimeter extends beyond your company. This perimeter includes looking at the security posture of your suppliers.

You could require an audit of their policies and procedures, or you could even share your experience and resources to help them protect themselves from attacks. It could be argued that this investment in time and resources is far more manageable and affordable than an attack on your networks, or having to find a new supplier in these days of compromised supply chains.

Educate Yourself and Your Teams

With many organizations so tightly intertwined, it's important to look at the larger vulnerability landscape. Train your suppliers and your employees who interact with them, on how to safeguard against attacks. Teach them about the vulnerabilities and techniques that are commonly used by cybercriminals.

Then, arm that unified front with solutions that implement authorization and authentication over a single panel to view your company's network, and the overall landscape of transactions and communications coming in and out of your company.

About the Author

Tom Ammirati is a technology executive with 25+ years experience in the enterprise software industry encompassing the cybersecurity, digital identity, ERP, HCM and storage software / hardware sectors.

Tom has held executive positions at both early stage, hyper-growth firms as well as established public enterprises. His leadership assignments have been distinguished by building high performance and customer-centric sales, partner, customer success and marketing organizations that have disrupted key technology markets and achieved category leadership. This includes ADP, Veritas, Symantec, Success Factors, Cipher Cloud, ForgeRock and Onfido.

He has had the privilege in serving some of the world's largest and most disruptive organizations across multiple public and private sectors.

Latest Cyber Threats Facing Small Businesses and How to Minimize Them

By Wendy Taccetta, SVP, Small and Medium Business for Verizon Business.

We all know, support and love small businesses. The neighborhood pizzeria with the tasty crust, the pub with the best growler selection, and the hair salon that can squeeze you in on a Friday afternoon all have a place in our hearts. These small businesses work hard to deliver excellent products and customer service — just like their bigger counterparts. They also face the same cyber threats — including ransomware — yet they often do not have the company resources to tackle these growing threats. They may know pizza ingredients, but data encryption is not their speciality and it shouldn't be.

Small organizations are just as enticing to criminals as large ones, and, in certain ways, maybe even more so. Threat actors have a "we'll take anything we can get" philosophy when it comes to cybercrime. And they will do it by exploiting vulnerabilities.

Day-to-day cyber threats to small and medium-sized businesses (SMBs), along with employee actions can cause significant damage to a business and its customers. Exposing a customer's sensitive information, such as a credit card number for example, can have immediate and long-lasting repercussions that can last well beyond a negative Yelp review. In fact, the financial loss and reputational damage can be catastrophic and security incidents can and have put SMBs out of business.

What are the latest cyber threat trends impacting SMBs? According to a recent Mobile Security Index report from Verizon, it turns out mobile devices may be the new threat in this new remote and hybrid world. In fact, more than 45% of SMB respondents suffered a severe-mobile-related compromise in the past 12 months, which involved data loss, downtime and other repercussions. Managing both risk and compliance is a lot to handle–especially for small and medium-sized businesses. Their biggest challenge? More than 54% indicated it was about having the right technology and tools to support and protect them against the human element and bad actors.

Futureproofing

It's true, the human element continues to drive data breaches. Whether it is the use of stolen credentials (also on the rise), phishing, or simply an error, people continue to play a large part in incidents and breaches alike. This could be clicking a bad link and launching malware, responding to a phishing email, or a configuration error. In fact, the dominant misconfiguration trend is misconfigured cloud storage. While there is no such thing as a 'sure thing,' there is one thing that's for sure–and that's ensuring you are arming your staff with the tech, tools and knowledge they need so that both their and your data are protected. These include developing a "bring your own device" BYOD policy, implementing a mobile device manager solution to help remotely secure, manage and support personally-owned devices, and educate team members on the dangers of malware, which was present in almost 70% of breaches and ransomware, which 75% begin as email phishing campaigns.

Rampant Rampaging Ransomware

Ransomware is a type of malicious software that encrypts your data so that you cannot view or utilize it, and once the ransomware is triggered, the threat actor demands a (frequently large) payment to unencrypt it. While insidious, ransomware alone is simply a model of monetization of a compromised organization's access that has become quite popular. Ransomware operators have no need to look for data of specific value, such as credit cards or banking information. They only need to interrupt the organizations' critical functions by encrypting their data.

How it works is simple: attackers use stolen credentials and phishing techniques to exploit vulnerabilities to compromise an organization's network. Think of this as locking the data, with the intention of selling it back to the victim for a profit. In fact, nearly 80% of incidents affecting small businesses are ransomware attacks.

Three out of four security incidents point to outside the victim's organization. Most data thieves are professional criminals deliberately trying to steal information that they can turn into cash. Highly targeted attacks use fake invoicing or attempts to exploit a specific published vulnerability in software.

How SMBs Can Address Security Issues without Requiring a Major Overhaul

It is crucial that even very small businesses take precautions to avoid becoming a target. Fortunately, it does not take a major overhaul to improve cybersecurity at an organization. Small preventative fixes can go a long way. Consider these eight smart practices:

1. Use strong passwords, and practice good password management
2. Update commercial software regularly
3. Educate employees about the importance of handling customer data
4. Deploy simple employee training and practice day-to-day security awareness, such as how to spot a fake email or phishing attempt, what "not to click," etc.

5. Limit employee access to confidential company data that may live on hard drives, servers, and the cloud
6. Back up data regularly. Look into offline backups

Install encryption software, especially if you manage personal information that includes credit cards, bank accounts, and social security numbers. This is essential. If hackers steal encrypted data, it will be useless for them since they will not have the keys to decrypt and decipher the data

Look into working with a cybersecurity expert, such as a managed service provider (MSP), who can offer customized solutions to best suit your security needs and address your company's blind spots. The reality is security does need to be built into the infrastructure, such as secure coding, lifecycle management, etc.

By protecting both your data and your customers' data (personal information and financials), you can help protect your business reputation, save money — and to put it starkly, help keep your business open. No matter how you slice it, good security practices are good for business. And this means keeping your favorite pizzeria, pub, and hair salon thriving.

About the Author

Wendy Taccetta is SVP, Small and Medium Business for Verizon Business. My team and I are focused on creating the best end-to-end wireless experience for small business owners who trust their business to Verizon.

Wendy can be reached online at LinkedIn here: https://www.linkedin.com/in/wendytaccetta/ and at our company website https://www.verizon.com/business/solutions/small-business/

Looking Beyond Centralized Security to Meet Today's Data Protection Requirements

By Daniel H. Gallancy Co-Founder & CEO, Atakama

We cannot pretend that the pandemic was the only factor forcing enterprises to embrace a more distributed workforce and infrastructure. The demand for flexibility was increasing far before the events of early 2020. The pandemic was merely an accelerant of a pre-existing trend. In its wake, we have incontrovertible evidence that centralized security truly is obsolete, unable to keep pace with the rising tide of advanced threats targeting sensitive data.

Fortunately, advances in data protection strategies – fuelled by multifactor encryption – provide a powerful alternative to the archaic practices that govern today's complex network environments.

With centralized identity and its downstream access controls, hackers inherently have the upper hand. The welcome mat is automatically rolled out as soon as a bad actor gains valid credentials, regardless of the nature of the exploit through which the credentials were gained. The adversary is granted access to all systems, databases, and files – just like any authenticated user.

At least the data is encrypted, right? Wrong. Conventional encryption solutions rely on centralized keys, bound to the very same user credentials the attacker has stolen or spoofed. As such, traditional encryption is merely a feel-good checkbox, providing no true protection against even the most basic of attacks.

Once credentials are breached and the encryption keys are compromised, data becomes a pawn in the hacker's game, whether that is to exfiltrate it for their use as a nation-state-sponsored organization or to use it in a ransomware sting that could cost millions of dollars. The same goes for malicious insiders.

Once they have a central set of keys, they can quietly extract, destroy, or augment data. A modern-day approach to eliminating data exfiltration starts with multifactor encryption.

Multifactor encryption

A decentralized approach to cryptographic key management protects organizations from data exfiltration, even when identity and rules-based access controls fail. Multifactor encryption allows for the highest levels of data security without sacrificing business performance and productivity. The concept is simple, but the approach completely changes the way data is protected.

With multifactor encryption, data at rest is encrypted using AES-256. A unique key is generated for each object and then automatically fragmented and distributed across physical devices - a mobile device, laptop, tablet, or key shard server, eliminating central points of attack and central points of failure.

Decryption occurs seamlessly: a user clicks on a file and then approves a notification prompt on a mobile device, or through a secure, automated workflow facilitated by a key shard server. In the context of the user of a mobile device, the notification is a request for the device to provide the relevant key shard to reconstitute the encryption key, which is subsequently used to decrypt the file. Consequently, users can access the file with ease and without disruption.

Multifactor encryption also enables the analysis of encryption status and usage of data for compliance, business reporting requirements, and operational decision-making. User activity is logged and can be aggregated at the administrator level to gain a better understanding of individual users and overall usage trends of encrypted data. Administrators can also create customized alerts and notifications with detailed user file interaction logging that can be fed into existing SIEMs and SOCs.

No need for credentials

Credentials-based approaches are a serious weakness. In this year's IBM Ponemon Cost of a Data Breach Report, the use of stolen or compromised credentials was again the most common cause of a data breach, at an average cost of $4.5 million per incident. These statistics drive home the point: conventional encryption and key management provide attackers with the keys to all parts of an organization's cyber citadel, enabling them to do as they please. After all, the attackers are simply using the credentials as any legitimate users would, with identical permissions including the ability to decrypt files at will.

The use of multifactor encryption and distributed key management enables an enterprise to eliminate reliance on identity as the root of data security, and the unshackling from identity occurs without any additional password burden. Organizations that embrace this paradigm achieve not only better security regarding their data but also send an important signal to a potential attacker, "don't waste your time trying to burglarize us, you're better off breaking into the next house." That signal serves to convince attackers that security is hardened overall, not just within the realm of protecting data but also within other aspects

of security. Conversely, organizations that continue to rely on encryption tied to IAM send the exact opposite message and are likely to suffer unpleasant consequences.

Eliminate complexity, enable productivity

The flaws in conventional key management extend beyond security. Encryption key management becomes time-consuming, especially where organizations have multi-cloud or hybrid cloud architecture. In the Ponemon encryption trends report, 59% of respondents said encryption key management has become “very painful”. Hardly surprising when businesses are stuck with centralized key management systems that need constant supervision and updating, and which makes for an administrative nightmare, for IT admins and end-users alike.

This is not how businesses become truly cloud-enabled and agile. Decentralized multifactor encryption, by contrast, is designed with simplicity and user productivity in mind as well as rock-solid security, eliminating the conventional trade-off between data security and data accessibility.

Satisfy compliance mandates

Consider for example, how the Automated Clearing House Network, which processes billions of payments each year, has upgraded data security requirements in line with this year’s changes to National Clearing House Association rules to include multifactor encryption. These rules govern electronic payments between almost every bank and credit union in the U.S. The rules require account numbers to be unreadable when stored electronically by large non-financial institution originators and third-party service providers and senders. In effect, they challenge the continued use of passwords and user credentials for security authentication. By using multifactor encryption, they remove the threat of file exfiltration through password compromise and remove the central key server as a single point of failure. This is a great example of how multifactor encryption works at scale with complex file types and interactions that demand the highest levels of security.

A relatedly powerful combination is the use of multifactor encryption with the use of data discovery and classification tools. The combination enables organizations to stay ahead of shifts in the modern threat landscape by automatically encrypting files according to the policy defined by data classification tools. Businesses can easily choose which critical assets should be prioritized and encrypted before a cloud migration project, for example.

Ensure Flexibility

Among the many advantages of distributed key management and multifactor encryption is its flexibility. Organizations have the freedom to choose various thresholds of security based on the context within which the data resides. For example, access to the most sensitive data can be subject to the requirements

of a quorum of participants for decryption (i.e., five possible participants of which at least three are required).

Administrators also gain the benefit of visibility, the ability to see in real-time precisely who is accessing data. This is an invaluable resource, providing a detailed view into how files are used in a company, who by, and at what times. This is a major counter to insider threats and gives organizations insight into how they should develop their security policy, not to mention the data insights required for operational and compliance reporting.

Development and evolution affect cyber security and encryption just as much as any other area of enterprise technology. Conventional centralized encryption is no longer suited to the frequency and sophistication of threats or to the way modern businesses have grown their attack surfaces through remote working and explosive expansion of the cloud. The use of distributed key management and multifactor encryption keeps data secure and bolsters zero trust initiatives while dovetailing perfectly with normal workflows. It achieves the right balance between data security and accessibility, boosting productivity without putting an organization at risk of a serious data breach or compliance failure.

About the Author

Danniel Gallancy – CEO & Co-Founder, Atakama. Learning to program in C at age 10, Daniel admits to being security obsessed. He has been CEO at Atakama since 2018. Prior to founding the company, he was CEO of SolidX Management LLC, at the intersection between Bitcoin and traditional financial services.

He previously spent ten years in the asset management industry where his areas of focus included semiconductor capital equipment, IT hardware, software and telecommunications. An investment professional at Beaconlight Capital and, before that, at Alson Capital Management, his responsibilities ranged from corporate diligence, to financial analysis and investment decision-making.

In the course of his career he has provided bitcoin and blockchain-related advisory services for private corporations, investment management firms, post-trade processing companies, central counterparties, and US State and Federal regulators. He has also consulted on crypto for the Boston Consulting Group, the Depository Trust & Clearing Corporation, the Monetary Authority of Singapore and many others.

Daniel's early entrepreneurialism and ability with technology enabled him to build a secure, laser-based, point-to-point ethernet bridge at age 22, before wirelesss ethernet was widely available. He holds a BA in physics and BSE in electrical engineering from the University of Pennsylvania and an MBA from Columbia Business School.

https://www.atakama.com/

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

More Than Half of Organizations Hit with Cyberattack in The Cloud

Detection Rates Down Significantly as Attacks Become More Sophisticated

By Dirk Schrader, Resident CISO (EMEA) and VP of Security Research, Netwrix

In a recent report Netwrix found that 53% of organizations suffered a cloud cyberattack in the last 12 months, and detection rates were down, compared to 2020, while ransomware has become harder to uncover.

The Netwrix Cloud Data Security Report revealed the average detection time for most types of attacks has increased since 2020. The most significant slowdown was for supply chain compromise: In 2020, 76% of those surveyed spotted attacks within minutes or hours. This year, just 47% identified supply chain compromise in the same timeframe. The survey found that ransomware has also became harder to uncover. In 2020, 86% of organizations needed only minutes or hours to detect ransomware. This rate dropped to 74% in 2022.

More Attacks Lead to Expense

Not only are attacks increasing in number, but also in cost. If in 2020 51% of attacks had an impact on business, in 2022 this rate grew up to 68%. This means that almost two in three security incidents led to an expense of some kind.

The report found that in 2022, for 49% of respondents the attacks led to unplanned spending to fix security gaps, up from 28% in 2020. The share of those who faced compliance fines more than doubled (from 11% to 25%), as did the number who saw their company valuation drop (from 7% to 17%).

The most common attacks on the cloud consistently came from phishing. Phishing was the leading cause of attacks in 2020 at 40%, increasing to 73% in 2022. Moreover, 63% of respondents said they experienced a phishing attack multiple times this past year.

Most of the security challenges have remained the same compared to 2020. Respondents continued to express their concerns about the lack of IT staff, lack of expertise in cloud environments, and budgetary restrictions. In these circumstances IT teams should clearly understand how areas of responsibility are split between their organization and the cloud provider as well as pay special attention to their organizations' cybersecurity bucket to avoid security gaps.

Cloud Risk is Internal and External

The threats to cloud-stored sensitive data are both external and internal. When IT professionals were asked what they thought was the biggest risk to cloud security, 55% of respondents said hackers topped the list, while 39% expressed concern over their own employees.

As cyber criminals become more skilled in finding and navigating security gaps, implementation of a layered security defense across all three primary attack surfaces – data, identities, and infrastructure – must be prioritized. One way to solve this problem is to build a security architecture with a select, smaller group of trusted vendors that develop, offer, and support an extensive portfolio of solutions. Such an approach helps avoid security gaps caused by overlapping or conflicting functionality of point solutions from different vendors operating in the same IT environment.

Unclouding on the Rise

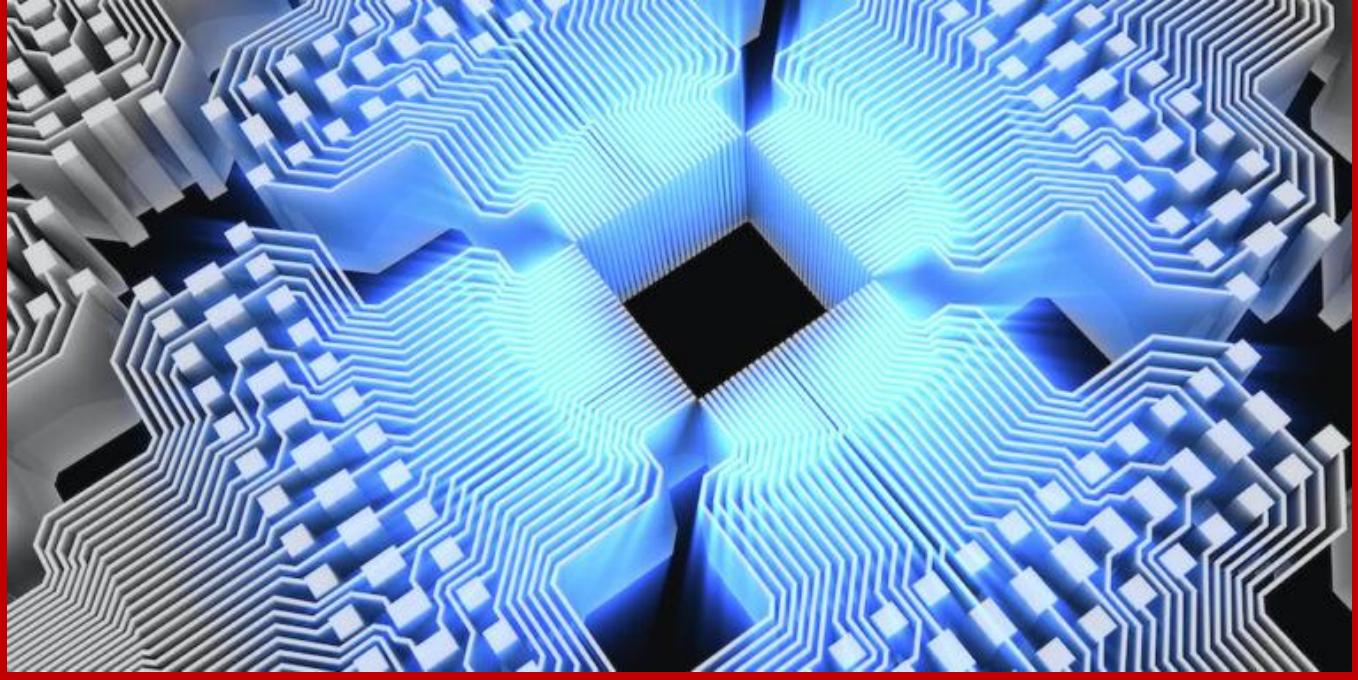
Another way to reduce the risk of overexposure from the cloud is to "uncloud" the sensitive data and move it back in on-premises environments. In 2019, 48% of respondents had either unclouded or were planning to uncloud their data; this increased to 62% in 2020. By 2022, this figure became even higher and reached 66%.

Nevertheless, 80% of organizations store sensitive data in the cloud and plan to proceed with cloud adoption by raising the share of workloads moved to the cloud from current 41% to 54% by the end of 2023. It means that IT teams must learn how to use the cloud effectively and securely while training their colleagues. It is time to pay closer attention to security measures that improve the ability to identify, protect against, detect, and respond to threats, to reduce both the likelihood and impact of a breach.

About the Author

Dirk Schrader is resident CISO (EMEA) and VP of Security Research at Netwrix. A 25-year veteran in IT security with certifications as CISSP (ISC²) and CISM (ISACA), he works to advance cyber resilience as a modern approach to tackling cyber threats. Dirk has worked on cybersecurity projects around the globe, starting in technical and support roles at the beginning of his career and then moving into sales, marketing and product management positions at both large multinational corporations and small startups. He has published numerous articles about the need to address change and vulnerability management to achieve cyber resilience.

Dirk can be reached online at dirk.schrader@netwrix.com, on Twitter @DirkSchrader_ and at the Netwrix website at www.netwrix.com.



NIST Fires the Starting Gun for The Long March to Quantum Safety

By Kevin Bocek, VP of Security and Threat Intelligence, Venafi

Quantum computing is a technology so nascent that even future-gazers find it hard to predict what era-defining innovation it might unleash. However, what everyone is pretty settled on is that it will eventually spell the end as we know it for asymmetric (public-key) cryptography which underpins the system of machine identities that enables our online world to exist. As such, the race is on to achieve "quantum safety" by finding algorithms resistant to cracking by quantum computers. And NIST recently fired the starting gun, by announcing the first four contenders.

While change is not imminent, smart CISOs will want to start planning now. And they should assume that the transition between pre- and post-quantum worlds will be characterized by hybrid use of both new and old machine identities.

The quantum conundrum for cryptographers

Today's computers process and store information in a binary numerical system – that is, zeros and ones. Quantum computers use qubits: quantum particles which don't behave according to the traditional rules of physics. That effectively means they can be a zero and a one at the same time, which theoretically will significantly reduce the time required to process data and solve mathematical problems.

This gets to the heart of the challenge for cryptographers. Current public-key encryption systems rely on mathematical problems which computers find extremely difficult to solve given their processing power. Quantum computers, on the other hand, have the potential to solve these problems in the blink of an eye, which means they'll be able to break the current standards of encryption with ease.

A transfusion for the internet will take time

Why does it matter if this system of encryption is upended? Since RSA produced the first crypto-system in 1977, public key cryptography has been the primary mechanism for establishing trust and authentication online, by underpinning the digital certificates and cryptographic keys that give machines identity. These machine identities have grown to be the primary method for securing everything from our online communications to financial transactions, sensitive customer data to national security secrets. They enable all machines – from servers and applications to Kubernetes clusters and micro-services – to communicate securely. They run through our digital world like blood running through the veins in a body. So, replacing them with quantum-resistant versions will be like giving the whole of the internet a transfusion.

Yet despite talks of a "crypto-apocalypse" when quantum computers finally start to come online and crack the current systems of cryptography, the reality is likely to be far less dramatic. There will not be a single catastrophic doomsday event when all the world's secrets are exposed and the global economy as we know it ceases to function. Instead, we're likely to see a slow and steady journey to quantum safety driven by the needs of leadership teams and markets. It's taken almost 40 years from the inception of the original RSA crypto-system to get to the point we're at now, so the journey to quantum resistance is likely to take decades rather than days, weeks, or years.

Setting the standard

The US government's National Institute of Standards and Technology (NIST) is leading the way here in its efforts to develop a post-quantum cryptographic standard for organizations to rally around. It's already been a long journey which began back in 2016 when NIST called on the world's leading minds in cryptography to devise new ways to resist an attack from quantum computers. In July, an important milestone was reached after it announced the first group of four quantum-resistant algorithms. Four more will be announced in due course.

Why so many? Because NIST recognizes that cryptography is deployed in many different use cases, therefore an effective standard needs to support varied approaches. It must also mitigate the risk of one or more algorithm turning out to be vulnerable to quantum cracking after all. In this way, NIST selected the CRYSTALS-Kyber algorithm for "general encryption" – highlighting its relatively small encryption keys and speed of operation. And for digital signatures – such as those currently used within TLS machine identities – it selected the CRYSTALS-Dilithium, FALCON and SPHINCS+ algorithms. CRYSTALS-Dilithium is recommended as the primary algorithm, with FALCON useful for applications which need smaller signatures. SPHINCS+ is said to be larger and slower than both of these, but it's based on a different math approach and may therefore be a useful backup option.

Most importantly, with things accelerating from a standards perspective, organizations now have a clearer path towards planning their own post-quantum future.

The journey starts now

There will be a temptation to continue doing nothing. After all, this kind of planning will take considerable effort – we're talking here about a transformation akin to changing the way you drive or the current in an electric socket. But while the current machine identity system is working just fine, this won't always be the case.

Now that early-stage standards exist, it makes sense to start planning laboratory condition testing. Choose a single application and understand the performance impact of the new algorithms, how to deal with larger machine identities, and how to operate dual pre- and post-quantum modes. The latter point is important, because – much like the move to electric vehicles starting with hybrid cars – for decades the world is likely to transition to quantum safety via a hybrid approach. That will mean running old machine identities alongside the new as we transition from today's standards to tomorrow's. Having a control plane to automate the management of these machine identities will be crucial to this hybrid model, as it will enable visibility over what machine identities are being used within what context and how they are performing.

It's difficult to predict exactly how long this transition period will take. But it's certainly a timescale that will mean many currently in the industry will not see the end of it. Yet like climate change, it's not something we can put off for another generation to deal with. So, select an application to test and factor that into next year's budget. Having the first quantum-resistant app up and running should be considered a five-year plan. The roadmap may change over the coming decades. But it's time to take those first steps.

About the Author

Kevin Bocek, VP of security strategy and threat intelligence, Venafi. Kevin Bocek is responsible for security strategy and threat intelligence at Venafi. He brings more than 16 years of experience in IT security with leading security and privacy leaders including RSA Security, Thales, PGP Corporation, IronKey, CipherCloud, nCipher, and Xcert. Kevin has successfully deployed authentication and encryption solutions for the world's most demanding financial institutions, telcos, and government agencies. Kevin can be reached online at @kevinbocek on Twitter and LinkedIn https://www.linkedin.com/in/kevinbocek/ and at our company website https://www.venafi.com/

Password Resets Need to Become Extinct

By Thomas (TJ) Jermoluk CEO and Co-Founder of Beyond Identity

In the aftermath of almost every data breach, the most common advice we see from security experts and regulatory professionals is to “make your passwords stronger”. Fundamentally, this is flawed advice as passwords alone are innately insecure and should not be relied upon. Instead, the most effective advice would be to eliminate passwords altogether and implement a more cohesive authentication solution to safeguard the access to your critical business assets.

Data breaches through password leaks are far too common in the current digital landscape. In fact, more than 80% of all data breaches are a direct result of password leaks. Whether it's through phishing, social engineering, exploiting weak credentials or using third-party tools, adversaries use compromised passwords as the first entry point for most cyberattacks.

Because of their fundamental vulnerability, passwords are likely to remain a common attack vector. Whenever potential threats are identified or a breach takes place, most companies seek a quick resolution through password resets and the implementation of traditional multi-factor authentication (MFA). Take leading game developer Ubisoft for example. The company recently experienced a security breach, and its response was to initiate a company-wide password reset. Unfortunately, password resets further extend the security loophole, rather than adding a proactive layer to the security infrastructure.

It is a common misconception that longer passwords with various special characters and numbers are harder to crack. The reality is that advanced malware and phishing kits don’t care how good your password is. Threat actors also steal passwords by cracking poorly encrypted databases or buying stolen passwords from underground cyber markets. These tactics don’t even target user passwords, rather they target the medium that’s storing the passwords, or trick the user into giving up the passwords themselves.

Furthermore, passwords only act as a single layer gateway between users and critical system components. As soon as that layer is compromised, all valuable assets within the network are exposed

to an attacker. That's why password-based solutions will always be a vulnerable factor in identity and access management.

The problem with traditional MFA

When businesses realise the potential risk of depending solely on passwords, they immediately focus on multi-factor authentication. However, the traditional MFA systems used by most organisations are highly vulnerable to threat actors. Legacy MFA is based on push notifications, one-time codes, texts, and magic links, all of which are compromisable factors - whether by social engineering or by malicious software.

SIM swaps, man-in-the-middle, and other malicious social engineering tactics have evolved to exploit these methods. So, the only feasible solution is to implement invisible and unphishable MFA solutions based on a Zero Trust framework.

The core principle of Zero Trust, which is "never trust, always verify", needs to be incorporated strictly into the authentication policy of organisations. Next-gen phishing-resistant solutions can eliminate passwords and interceptable factors altogether, allowing organisations to validate user identities with complete accuracy.

Legacy multi-factor authentication systems do not align with the Zero Trust protocol. They still rely on a certain degree of trust that the password is correct, and it's being accessed by the true user. None of the standard MFA factors can 100% assure that the person logging in is the true user as they can be intercepted by a third party.

Traditional authentication processes also kill a considerable amount of time, as users are bogged down with validation tasks. Considering the number of times a user accesses different systems and the number of total users on a network, the accumulated time spent on traditional MFA functions can significantly impact the overall user productivity.

Achieving true Zero Trust through invisible and phishing-resistant MFA

To eliminate password-based threats, organisations need fundamentally strong authentication methods that are not vulnerable to any interception. The new generation of passwordless invisible MFA solutions bind user identity to their authorised devices using cryptography. The access activity of devices is also analysed on a continuous basis to detect potential risk signals before they lead to critical attacks. Device security is a fundamental part of phishing-resistant MFA solutions, as authorised devices have to meet the security policy requirement every time a user requests access. Thus, the risk of password-based attacks and interceptable factors are completely eliminated. As no factor of this authentication process is visible to the user, it is, in effect, 'invisible' multi-factor authentication.

Using such solutions also increases access efficiency and reduces user friction. Removing passwords or traditional authentication factors means that users no longer have to rely on push notifications, one-time

codes, or third-party authenticators. For users, it also eliminates the common scenario of forgetting passwords and having to access help desk resources for password resets.

Invisible MFA solutions allow all the authentication and validation processes to happen on the system back-end, thus safeguarding system access from any third-party interceptions. It truly underpins the Zero Trust value and removes a massive threat vector, securing the critical SaaS resources, data repositories, and other critical assets of a corporate network.

About the Author

Thomas (TJ) Jermoluk CEO and Co-Founder of Beyond Identity

He has served as President and COO of Silicon Graphics, Inc., Founding Chairman and CEO of @Home Network, General Partner at Kleiner Perkins, CEO of Hyperion Development Group, and founded nine companies, including Beyond Identity, HiCMOS, AOptix, and SmartPipes. TJ attended Virginia Tech.

TJ can be reached online on LinkedIn and at our company website Beyond Identity | Go Passwordless and Beyond

Qakbot: An Analysis of The Threats Posed by Modern Trojans

By Brett Raybould, EMEA Solutions Architect, Menlo Security

Financial firms continue to bear the brunt of cybercrime.

According to IBM's X-Force Threat Intelligence Index 2022, almost a quarter (22.4%) of all cyberattacks are directed at finance and insurance organizations, the tech giant's Cost of a Data Breach Report 2021 also revealing that the average cost of a single data breach suffered by financial organizations is as much as $5.72 million.

These statistics are telling, yet in many ways somewhat unsurprising. With almost nine in every 10 cyberattacks being financially motivated, it makes sense that threat actors would focus their attention where the money is.

It is for this reason that many techniques have been tailored towards targeting financial institutions, Qakbot being a prime example.

Otherwise known as QBot or Pinkslipbot, Qakbot is a renowned banking Trojan that has existed for over a decade. Having originally been identified in the wild in 2007, it continues to plague financial institutions even today, having continually evolved through continued maintenance and development efforts.

Qakbot serves several purposes. While it is primarily used to steal banking credentials, it has also been deployed to spy on financial operations and install ransomware within compromised organizations.

How Trojans are hotting up

A key reason why the Qakbot Trojan is such a problem today is that there are several different strains of the Trojan, with each leveraging different Highly Evasive Adaptive Threat (HEAT) techniques.

Threat actors continue to expand their understanding of those technologies typically seen in traditional security stacks – their weaknesses, and vulnerabilities that can be exploited. As a result, we have seen several tactics such as data obfuscation, HTML smuggling, and JavaScript obfuscation emerge, capable of avoiding detection from common tools.

This is the very essence of HEAT: by leveraging innovative attack methods, cybercriminals can bypass traditional security mechanisms.

This is exactly what we have seen in the case of Qakbot. Indeed, the delivery vehicle of the Trojan via email has involved both an email attachment and URL, with the former generally involving a document that downloads the Qakbot payload.

In our analysis at Menlo Labs, we identified four different HEAT techniques used in Qakbot campaigns:

1. Email lures

Here the threat actors compromised a benign domain, using it to host a malicious payload before sending emails (including URL directing them to the malicious ZIP file) to their select targets. To evade detection from traditional security defenses, Qakbot used password-protected ZIP files. Inside the ZIP file is a link file with the ability to easily provide PowerShell commands or JS to execute. If opened, the link file downloads the JS file, and the JS file in turn downloads the Qakbot payload.

2. Excel 4.0 macros

We also saw Excel 4.0 macros being used to add commands into spreadsheet cells and send email attachments to the attackers' intended targets. Upon opening the malicious XLS documents, victims are asked to enable the macro to execute the Excel 4.0 macros. These commands present in the XLS file download, and then execute the payload from C2.

3. CVE-2022-30190

The CVE-2022-30190 vulnerability, otherwise known as Follina, is also being leveraged as a HEAT method to deliver Qakbot. When executed, a malicious document containing the key exploit calls out to an external HTML file to execute PowerShell code. In our analysis, when we open the document, it tries to download the HTML file, which further downloads the Qakbot payload.

4. HTML smuggling

We also saw the use of a specially crafted HTML attachment or web page in building malware locally behind traditional firewalls. In this attack sequence, the victim would begin by opening a HTML email attachment which would then construct a malicious payload by decoding the Base64 format. A fraudulent Adobe image and password-protected ZIP file would then be displayed and, upon extracting the ZIP file with the password, an ISO file "Report Jul 14 71645.iso" is dropped in the victim's machine. Resultantly, the ISO file that contains the Qakbot payload can reach the endpoint device.

The importance of prevention in security strategies

Critically, Qakbot represents just a handful of examples of HEAT threats being used against organizations in the wild.

Given the rising usage of this new breed of attacks in undermining legacy security technologies, never has it been more important for organizations to update their security stacks and combat the increasingly sophisticated efforts of threat actors.

So, how do you effectively protect against HEAT techniques, used by the Qakbot malware, or otherwise?

All too often, security strategies remain rooted in the notion of solely detecting and remediating threats. Yet this is no longer adequate. Today, organizations must also embrace the vitally important preventative piece of the security puzzle.

Thankfully, there are solutions which provide easy to implement yet comprehensive support in protecting against the myriad of threats, with isolation technology being a prime example.

Take the Excel 4.0 Macros as an example. With isolation, all attachments received from outside the organization – including potentially malicious XLS files– are converted to a safe version that can be viewed by the user while inspection engines determine whether they are harmful.

Here, the technology ensures that the malicious aspects of the file never have an opportunity to reach the endpoint, and therefore can't execute.

The same goes for password-protected ZIP Files. All documents and archives downloaded from the internet are again contained, away from the user's endpoint device. Even if a download is password protected, users will be prompted to enter a password whereafter the file is inspected.

Despite the fact Trojans have been around for years, they continue to be deployed against organizations today, and it's clear they are not going away. For this reason, it is vital that entities proactively protect themselves, embracing solutions that focus on prevention alongside detection and remediation tactics.

About the Author

Brett Raybould, EMEA Solutions Architect, Menlo Security. Brett is passionate about security and providing solutions to organisations looking to protect their most critical assets. Having worked for over 15 years for various tier 1 vendors who specialise in detection of inbound threats across web and email as well as data loss prevention, Brett joined Menlo Security in 2016 and discovered how isolation provides a new approach to actually solving the problems that detection-based systems continue to struggle with.

Relentless Cyber Attacks Leave European Healthcare Institutions with Little Breathing Space

By Michael H. Zaman, CEO of SecTeer

Still reeling from the Covid-19 pandemic, the European healthcare industry is attempting to fence off a growing spate of cyberattacks. The repercussions of a successful breach reverberate beyond the financial domain, with patients being unfortunate victims of relentless cybercriminal acts.

With no signs of abating, European healthcare's cyber resilience is under tight scrutiny, particularly on its preparedness to mitigate future attacks and safeguard the interest of patients, medical professionals, and key stakeholders.

Revisiting past cyber-attacks that cripple European healthcare systems

In recent years, too many cyber incidents have rained down on European medical facilities. Belgium healthcare company, Vivalia, suffered a massive ransomware attack in May 2022. Bad actors threatened to expose 400GB of data in a move that caused severe disruption to 7 hospitals.

A year earlier, another Belgium hospital, CHwapi, was struck in an almost similar attack. While the bad actors did not demand ransom, the attack rendered 37% of the hospital's servers inoperable and disrupted scheduled procedures.

Ireland's Department of Health and Health Service Executive (HSE) was not spared from malicious attacks either. The department's network was compromised by the 'Conti' ransomware in 2021. Meanwhile, 81% of hospitals in the UK were reportedly affected by ransomware attacks in 2020.

Devastating impacts of cyberattacks on medical infrastructure and patients

We know that cyberattacks on commercial infrastructure can be devastating. A successful lockdown of facility-dependent servers will result in severe financial losses. Hospitals have no option but to postpone MRI, X-ray, surgery, and other medical procedures.

Besides monetary loss, a crippling cyber attack can also increase health risks. With automated healthcare systems out of operation, medical staff face difficulty manually coordinating patients' movements and treatment. For example, a ransomware attack led to a case of mortality in 2019 by disrupting critical medical equipment.

During a breach, perpetrators might retrieve patients' data from hospitals' private cloud and trade them on illegal marketplaces. Such incidences tarnish the healthcare institution's reputation, and patients might question its integrity and capability to prioritize their health and privacy.

Why are Healthcare Institutions vulnerable?

The healthcare industry has undergone a rapid digital transformation in the past decade. Like their peers in other industries, hospitals migrate medical systems to the cloud to improve operational efficiency, cost, and convenience. Simultaneously, the move exposes the web-connected system to new digital challenges.

Migrating healthcare workloads to the cloud requires a different security approach. Data stored in the cloud is subjected to the vendor's security policy. However, hospitals have an equal responsibility to encrypt, secure, and regulate access to the data.

Meanwhile, the emergence of medical IoT devices also contributes to the security risks for healthcare systems. These devices are usually more vulnerable and become the target of exploitation by bad actors. Some of these devices have insufficient space to run a full-fledged anti-malware software, which calls for a different intrusion detection approach.

Cloud computing allows medical staff to easily access medical data stored on distributed servers on tablets, computers, and other remotely-connected devices. This increases the attack surface, which requires sufficient endpoint protection such as automated patch management.

Lack of security awareness amongst medical professionals and an understaffed IT team also partially contributed to successful attacks. For example, most malware attacks capitalize on social engineering by tricking the staff into downloading malicious attachments.

How healthcare providers can strengthen security posture

Healthcare providers must now take decisive action to effectively mitigate and respond to possible attacks in the future. Doing so requires an organization-wide approach that involves several strategic steps.

1. Create security awareness amongst medical staff and professionals, particularly those overwhelmed by the rapid digitization. Train them to adopt good security habits to prevent falling victims to social engineering maneuvers.
2. Conduct a thorough risk assessment for existing infrastructure. Categorize critical assets, identify potential vulnerabilities and assess measures to deter or mitigate impacts.
3. Isolate critical assets such as robotic surgery arms and patient support systems from the public network. Enforce a zero-trust policy to prevent bad actors from gaining unauthorized access to sensitive data, IoT devices, or other critical systems.
4. Use automated cyber security technologies to aid IT staff in strengthening defense posture. It helps to ease the learning curve when deploying advanced countermeasures against cyber criminals.

Bad actors might have early wins, but it's time to turn the tide in favor of European healthcare providers. At SecTeer, we help organizations secure their digital assets against unauthorized access with automated security patch management solutions.

About the Author

Michael Zaman is the Co-Founder and CEO of Secteer, an established cybersecurity scale-up that helps secure enterprises with automated patch management solutions. Michael's career in the cybersecurity industry spans over 20 years, during which he served as the founder and VP of Secunia, now owned by Flexera.

Michael can be reached online at e-mail: mz@secteer.com, Twitter: @mikaelzaman) and at our company website https://secteer.com/

Social Engineering Can Make Your Employees a Cloud Security Threat

By Zac Amos, Features Editor, ReHack

Cloud security is about more than just having the right technical defenses. Threats like hacking and malware deserve the attention they get, but it's important not to overlook the human side of things. Thanks to social engineering, a company's own employees can become some of its biggest vulnerabilities.

People with insider access can cause a lot of damage, and they don't have to be malicious to do so. Even well-meaning, otherwise reliable employees can become a security risk through social engineering. Here's a closer look at these attacks and how to prevent them.

What Is Social Engineering?

Unlike other types of cybercrime, social engineering focuses on people, not systems. Some experts claim human error is the No. 1 security threat to a business, and social engineering aims to take advantage of that.

Social engineering targets insiders to get them to make mistakes that expose valuable data or give attackers insider access. Sometimes, that involves targeting high-level executives or people in departments with the most network privileges. In other cases, any employee will do, so hackers look to those who may be more susceptible to their scams.

These attacks can take many forms, but they all revolve around taking advantage of people. Hackers don't need advanced technical skills to get around company defenses if they can convince someone to give away what they need.

Social Engineering Examples

Social engineering attacks come in many different packages. Here are a few of the most common types that businesses may encounter.

Phishing

Phishing is the most common and recognizable form of social engineering. These attacks involve messages, most often emails, that impersonate a trusted source to trick users into clicking a malicious link or giving away sensitive information. They're also remarkably effective, with 57% of global organizations suffering a successful phishing attack in 2020.

Baiting

As the name implies, baiting involves luring users into a trap by offering something they want. These could be links promising a giveaway, scam messages saying they have won a contest, or anything else that entices people or piques their curiosity. These traps will then either ask for personal information or provide a link that installs malware.

Pretexting

Pretexting makes users feel obligated to comply with requests from hackers posing as an authority. These are often long-term attacks where criminals impersonate officials like police officers or tax authorities and slowly gain people's trust. That way, it doesn't feel out of place or suspicious when they ask for sensitive information like financial data or Social Security numbers.

Scareware

Scareware ironically tricks users into installing malware on their devices by giving them fake security alerts. These often take the form of pop-ups warning they've detected malware on the device, only to install it when users click them. These threats can be effective since more Americans are concerned about cybercrime than any other type.

Why Is Social Engineering Such a Threat?

Social engineering is one of the most pressing cybersecurity risks businesses face. It plays a role in 98% of cyberattacks today, often serving as the first step to larger, more disruptive attacks like ransomware.

Cybercriminals like social engineering because it lets them bypass even the most high-tech defenses. It only takes one mistake to grant an attacker access to sensitive information or company networks. These attacks don't rely on technical prowess, so they're a relatively easy way for cybercriminals to cause substantial damage.

Social engineering attacks have also grown increasingly common. These threats rose 270% in 2021 as remote work and ongoing COVID-related disruptions made people more susceptible. People become more likely to click things that promise information when confusion and fear rise.

How to Protect Against Social Engineering

Several actions can help prevent successful social engineering attacks. The most important step is to train all employees, raising awareness about these threats and teaching them to spot them.

Phishing emails often contain unique characteristics that give them away as scams. Urgent calls to action, unknown senders, spelling errors, unusual-looking links or domain names, and inconsistent email addresses should raise alarms. As a rule of thumb, users should never click on any unsolicited links and verify everything before taking action.

Setting up multifactor authentication (MFA) is another important step. MFA can stop 99.9% of attacks, according to some experts, and they protect against social engineering by reducing credential-related risks. Even if an attacker gains a username and password through social engineering, it won't be enough to access an account with MFA.

Restricting access privileges won't stop social engineering attacks, but it will mitigate their impact. Each user should only have access to the files and systems they need for their job. Minimizing insider access in this way means that even if an attacker breaches an account, they won't be able to get into the whole system.

Secure Human Vulnerabilities in Your Cloud Environment

Technical defenses are crucial for cloud security, but human vulnerabilities can render them useless. All businesses should follow these steps to prevent user error-related breaches in light of the rising risks of social engineering. Employees may be a company's most significant risk, but proper training and fail-safes can mitigate these vulnerabilities.

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.

Spate Of Network Outages Illustrates the Need for Secure Network Modernization

Enterprises and service providers need agile, programmable, reliable networks

By Shekar Ayyar, CEO, Arrcus

As networks get larger and more complex, outages are on the rise.

Just consider all the outages that occurred in July alone.

A country-wide network outage rocked Canada. The Rogers disruption lasted more than 15 hours and knocked out 911 emergency hotline services, bank ATMs and transport.

KDDI in Japan had a massive outage that disconnected over 30 million people for more than three days. The company will spend an estimated ¥7.3 billion to compensate those subscribers.

To add to this, Zoom was down recently, Twitter and Hurricane Electric also suffered brief but major disruptions. And AT&T, Arelion and Cogent each grappled with network outages that impacted their customers, partners and multiple downstream providers across the planet.

These outages are the latest examples of why network operators need a different approach to networking. One that is resilient, secure and offers better visibility and remediation capabilities across their complex networks. This can be achieved by moving to software-defined transport networking that addresses both routing and switching.

Everything runs on the network – so network modernization for security is critical

These outages are concerning because people and organizations rely on network operators to ensure their applications and services run smoothly. So, when people find that a website is down, they're unable to make a call or find that their videoconferencing doesn't work – or when their application is running too slow – it has a massive impact both on businesses and the entire economy.

Estimates on the cost of downtime vary. But no matter how you slice it, downtime is costly. The cost of cloud downtime for an average business is $5,600 per minute, according to Gartner and GlobalDots. Parametrix Insurance says that downtime costs can be as a high as $9,000 per minute. ITIC research indicates that the hourly cost of server downtime now exceeds $300,000 for 91% of enterprises and that for 44% of mid-sized and large enterprises a single hour of downtime can potentially cost their businesses over $1 million. Outages cost network operators dearly, too, in terms of customer service, fines, loss of reputation and SLA service credits.

That's why network operators must modernize their networks to address today's applications, which are increasingly plentiful, bandwidth-hungry and latency sensitive. Modernization is critical because legacy networks don't support today's demands in a programmable way.

It is important to ensure that networks are programmable, and also have the following capabilities built in for multi-layered security:

- sFlow – for the ability to identify flow and apply ACL based on flow count
- SSH – for secure access for CLI
- Transport layer security to secure communications
- Routing security using Resource Public Key Infrastructure (RPKI)
- IPsec encryption for securing cloud-bound traffic

A unified, intelligent approach enables network simplicity, visibility and rapid remediation

Network operators need to think about the network architecture as a fabric – that brings together routing and switching and addresses multicloud environments – and upgrade their infrastructure to be programmable and edge-ready so that developers and end users don't have to worry about whether the network can support performance and latency requirements.

Adopting a single, software-based solution that supports both routing and switching eliminates much of the complexity of today's networks. With a unified fabric, network operators can write policies once and run them everywhere – across all of their applications; in their aggregation, edge and core networks; and on any or all of the public cloud services they may be using.

Network operators that evolve from centralized architectures and adopt distributed architectures also can increase efficiency and lower latency by enabling endpoints like point-of-sale systems, mobile phones and smart city gear to make decisions on the network edge.

Open, software-based networks are also highly programmable and scalable, making network operators more agile, thus more competitive. They also make network operators more resilient to supply chain issues by enabling them to use the hardware and components of their choice.

While network operators are transitioning to next-generation architectures, they should be implementing modern solutions that have an intelligence layer on top that allows for analytics and automation. This will provide network operators with the visibility they need to know what's happening on their networks and enable networks to self-correct as fast as possible.

It's also critical to consider that the world is becoming dependent on cloud architectures. And, increasingly, companies rely on multicloud environments. Enterprises and network operators can get best results from multicloud networking by partnering with software solution providers that offer full-stack networking capabilities with a strong foundation in security – default encryption is critical for all data. Look also for providers that offer day-zero deployment; modern orchestration with good automation frameworks for day-one operations; and support for deep integration with OpenConfig/YANG models, configuration playbooks and troubleshooting tools for day-two and beyond management.

We live in a world in which applications and connected devices are everywhere. When networks fail to perform as needed – or just plain fail – it creates unnecessary costs, inefficiency, loss of reputation and stress. But when enterprises and network operators modernize their networks, those networks can be more secure, reliable, performant and cost efficient. And network operators can better monetize those networks with new revenue-generating services.

About the Author

Shekar Ayyar is the CEO and Chairman of Arrcus, a San Jose, CA based infrastructure technology company focused on edge networking solutions for Service Providers and Enterprise Customers.

Until April 2021, Ayyar was with VMware for nearly 14 years, serving most recently as executive vice president and general manager of VMware's Telco and Edge Cloud business unit. He helped create the business unit to equip communications service providers as well as enterprises with integrated platforms for 5G, edge, telco cloud and IoT use cases.

Under his leadership, VMware expanded its core strength in virtualization to become one of the industry's leading providers of telco cloud and NFV infrastructure solutions - enabling CSPs to rapidly develop and deliver new monetizable 5G services, significantly reduce CAPEX and OPEX costs and enhance customer experiences.

Prior to July 2019, Ayyar led VMware's strategy and corporate development efforts for nearly 10 years and also helped incubate the telco Network Functions Virtualization (NFV) focus area. Under his leadership, the company executed on dozens of acquisitions including significant platform additions such as Nicira, AirWatch, VeloCloud and Heptio, as well as a portfolio of strategic investments in technology startups.

Ayyar has more than 25 years of senior leadership experience in enterprise software, communications and semiconductors. Prior to joining VMware, Ayyar held senior executive roles at BindView, Instantis and Lucent, spanning product management, marketing, and business development, and was also a consultant with McKinsey & Co. Ayyar earned his Ph.D. in electrical engineering from the Johns Hopkins University and his MBA from the Wharton School, where he graduated as a Palmer Scholar. He earned his bachelor's degree in electrical engineering from the Indian Institute of Technology, Mumbai.

Ayyar is also CEO of AdMY Technology Group, Inc., a SPAC focused on leveraging the convergence of Communications and Cloud Computing, catalyzed by 5G and Edge Computing. He is a Venture Partner at NTTVC, an independent venture capital firm formed in collaboration with NTT to back founders across the technology spectrum, and a member of the Board of Directors of Altair (Nasdaq: ALTR), and on the California board for Room to Read. Ayyar has advised on the Boards of a number of other companies and organizations including Puppet, the US India Business Council, and the VMware Foundation.

The 8 Most Common Social Media Scams Brands Need to Be Aware Of

By Nikhil Panwar, Security Researcher at Bolster

Almost 60% of the global population is using a social media platform. Because social media is a core component to how the world interacts with one another and how businesses advertise and engage with customers, these platforms have become ideal hunting grounds for scammers.

The platforms are popular among scammers in part largely due to the fact that the scams are challenging to identify. According to the FTC, social media scams made up 26% of the total fraud losses reported in 2021. It is in the best interest of a business to help prevent fraudulent activity as the scammers impersonating them negatively impact their brand. However, with over 20 platforms to manage and counting, it's an uphill battle for IT security teams to learn each interface and conduct manual monitoring. There are some common, go-to social media tactics that companies should be on the lookout for:

1. **Lottery and gift card scams.** These scams are the most common as many people are eager to earn money quickly and effortlessly. Typically, this looks like a scammer sending out unsolicited messages on a platform stating they are handing out gift cards or entry into a lottery to win a big prize. Naturally the links that are being shared direct the users to a malicious web page that is branded to appear as though it is a business-sponsored site. On this malicious page, the users are prompted to fill out their personal information and share the link with their network to receive their reward. For lottery scams, users are often notified that they were selected as the winner and to collect their prize. They are then tricked into paying for "transaction fees" - which can be thousands of dollars for bigger so-called prizes.

2. **Quizzes and other information mining tactics.** One of the most coveted assets cybercriminals want is data. To get this data, one tactic deployed is attracting users with compelling quizzes with

clickbait titles. The quizzes may be free but are a trap to mine valuable data and sell it on the dark web.

3. **Social media phishing.** Scammers have developed a host of tactics to lure people in. Often this looks like text messages with interesting information but in order to access that information, you have to enter your personal details. Once completed, your information is stolen and used for other cybercrimes. A large amount of scams fall under this phishing umbrella such as the gossip scam, healthcare scam, photo scam, account deleted scam, and the infamous Nigerian prince scam.

4. **Executive impersonations**. With millions of people utilizing social media platforms and the accessibility of personal information, it can be frighteningly easy to impersonate a well-known public figure. Recently, Twitter accounts have impersonated Elon Musk and Jeff Bezo and shared tweets asking for investments into various crypto accounts. If users see a verified account built with the correct information of the well-known figure, they are easily tricked into believing it is real. While believing the scam is legitimate, users have ended up transferring large sums of money into scammers' accounts.

5. **Account hacking.** Why impersonate when you can just steal an account? With millions of social media credentials having been (and actively being) exposed in data breaches, criminals will use compromised credentials to change the passwords to accounts and lock out the actual account holder. Now in possession of a legitimate account, criminals are better equipped to scam that user's network of connections.

6. **Crypto investment scams.** With the increase in crypto values, this type of scam has become increasingly common. Criminals position themselves as investment professionals and trick users into transferring funds to their accounts with the promise of immense investment return. In 2021, 37% of social media fraud loss was reported to be aligned with investment fraud.

7. **Hidden or shortened URLs.** Shortened URLs are often clicked without much concern for where it may lead. Visibility is blocked to the full URL which usually directs an unsuspecting user to a malicious website. These websites are run by scammers that save information or download malware onto the users' device.

8. **Counterfeit/pirated goods.** According to the FTC, online shopping scams make up 45% of money lost to social media scams. Consumers are often naive to these scams where they are tricked into buying fake goods through social ads but never receiving what they paid for. This is particularly dangerous for brands as potential customers may not know they were scammed and blame the brand for not receiving the items they paid for.

While those of us in the security industry may scoff at some of these scam tactics because we are more aware of tactics malicious actors take - these scams are common because they are effective. Many of the sites that scammers set up are expertly branded to seem legitimate which negatively impacts the brands they are impersonating.

With the never-ending stream of scams and fraud, it's near impossible for IT security teams to monitor for social media scams manually. Businesses who are intent on protecting their potential online customers as well as their brand reputation need to turn to AI-powered automation to help build out workflows, scan posts, images, and advertisements all while detecting illicit activity continuously. Many vendors throw the AI buzzword around needlessly but in this particular use case of fraud monitoring, AI is truly needed to protect brands and customers from the growing social media scams.

About the Author

Nikhil Panwar is a Security Researcher at Bolster, focused on Continuous Integration and Continuous Delivery (CI/CD), Cyber Threat Intelligence (CTI), Cyber Threat Hunting (CTH), OSINT, and Python (Programming Language). Prior to Bolster, for two years Nikhil was a freelance writer working on automated content generation systems, telegram bots, and complex data scrapers. Nikhil has a Bachelors in Technology for Computer Science and Engineering from Uttarakhand Technical University. Nikhil can be reached via LinkedIn and at our company website https://bolster.ai/.

The Balance of Power: One Disturbance Could Ignite the First Cyber World War

The Russian invasion of Ukraine has led to the awful re-emergence of war on the European continent. This time round however, we've witnessed a significant development: the ongoing conflict has a cyber facet at its very core. And one wrong move could have cataclysmic repercussions.

The fate of the wider tensions between nations is in the hands of a few key players. Global powers – namely the United States, China and Russia – have had access to each other's national critical grids for years. However, there has been an agreement between these states that prevents them from going beyond the realms of what they already have access to – an unspoken balance of power. As the developments in Ukraine continue, we're seeing a strain on this agreement, and therefore a threat to this Détente of the modern day.

By Guy Golan, CEO, Performanta

A building pressure

Cyber-attacks on critical infrastructure are nothing new to the cyber community. However, this is the first time in history where a mutual understanding between powers could spill out into a fully-fledged cyber world war. The cyber element is an incoming aspect of modern warfare, and this is something that is only going to play more of a significant role in years and decades to come.

We are just one major act of aggression away from triggering a devastating series of events. An attack on one party's critical infrastructure will cause further retaliation and greater damage. But equally, an attempt to remove the others' control and take back their systems could force the hands of parties involved. Relieving one pressure could result in a larger pressure elsewhere. Maintaining the 'balance of power is therefore of fundamental importance to avoid global devastation.

It is important to note that Russia, in effect, have less to lose. Critical infrastructure in Russia is less advanced as many rural areas still depend on wells. In this sense, Russia is in a stronger position to disrupt this equilibrium as its impact on the western nations would be far more severe than that on itself. However, it must not be presumed this is an inevitable step for Russia to take. The main cause of this precarious position is down to external factors, including the role the IT Army plays.

A heroic act in a troubling climate

Made up of over 300,000 independent cyber experts, the IT Army has played, and will continue to play, a major role in how this situation escalates or de-escalates between Russia and the West. This new variable, lacking any real accountability, has the potential to completely usurp the balance of power between these states. Successful attacks from the IT Army on Russian resources will most likely put strain on the relationship between Russia and the west – there is no political advantage for Russia to hit back at the IT Army due to their nomadic foundations.

The IT Army is admirably supporting Ukraine but, in doing so, a new pressure point has been added. Whilst independent from any global power or alliance, if its activities are viewed as the opposite, then there is a risk of an aggressive response from Russia as the balance of power comes under threat of disruption. One foot over the line could be enough to tip the balance, and the escalation would be immediate.

A valuable stalemate

All sides of the balance of power know that crossing the line could result in physical catastrophe that would endanger millions of lives, such as long-term damage to critical infrastructure or even nuclear fallout. However, neither side wants this to happen, so the stalemate continues, and the risk of this situation changing is low. But for the first time, this balance has come under genuine threat.

Where cybersecurity was previously kept in the shadows, a discreet use of aggression between governments, organisations, and countries, has now broken through the surface and into the public domain. The emergence of the IT Army and the pressure point this has created has caused havoc to this balance of power between nation states. The shift has, and will continue to, change the way that cyber is viewed and utilised moving forwards, for all of us – especially in times of war.

About the Author

Guy Golan is the CEO of global cybersecurity firm Performanta. He has worked in various director roles in the cybersecurity industry for the past 17 years. He started in the Intelligence Brigade for the Israeli Defence Force and now runs a firm made up of over 150 security professionals in four countries spanning three continents. Guy can be reached online at https://www.linkedin.com/in/guygopurple/ and at our company website https://www.performanta.com/

The Best Offense Is a Good Defense: How A Graph-Fueled "Defense-In-Depth" Cybersecurity Approach Can Strengthen Your Organization's Security Posture

By Harry Powell, Head of Industry Solutions, TigerGraph

"GM Customer Accounts Hacked"

"Hacker Steals Database of Hundreds of Verizon Employees"

"Ransomware Attack Hits New Jersey County"

Another day, another breach, hack, or ransomware attack.

In fact, the average cost of a data breach today is $4.24 million — and rising. More anxiety-provoking is the fact that it can take between 290 and 315 days for an organization to identify and contain a breach, according to recent research from the Ponemon Institute and IBM. Yes, cybersecurity has always been a moving target. When you factor in an ongoing global pandemic and the war in Eastern Europe, it's not surprising that President Joe Biden has urged U.S. companies to "harden [their] cyber defenses immediately." The approach used varies by company but complete visibility is critical.

Defense-in-Depth: A Multi-Layered Approach

While it is nearly impossible to prevent all cyberattacks, organizations can indeed harden their defenses to detect potential breaches earlier, act more quickly, and minimize damage. In today's attack laden era, it is not about prevention of an attack, but the focus must be on early detection. How can organizations stay one step ahead of everything from phishing emails and ransomware rings to distributed denial-of-service (DDoS) attacks and synthetic identity fraud? Smart companies have embraced "defense-in-depth," (DiD) a cybersecurity strategy originally deployed by the NSA that involves a series of systems, mechanisms, and controls layered together to protect your company's network, computer systems, and the data contained within these resources. This strategy is a replication of the military strategy used as far back as the 3rd and 4th centuries by the Roman Army. Today, the implementation of DiD is being deployed by smarter companies using graph analytics to power their multi-layered, defense-in-depth cybersecurity ecosystem with extended visualization and real-time analysis with in-depth machine learning and AI.

Why graph? When a bad actor enters a network, they are looking for bread crumbs or metadata stored on devices that lead to the more interesting and potentially sensitive information (think data systems, financial systems, HR systems or email servers). In a way, attackers are "thinking in graphs," scouring for bits of data they can follow to locate critical data deep within your organization's infrastructure. The goal is to identify these threats earlier in the Mitre Att&ck kill chain, or cyberattack lifecycle. We can apply graph analytics to detect anomalies and suspicious patterns of activity as well as unusual lateral movement of data and abnormal user interactions with systems or its respective data.

Graph-based Cyber Attack Defense: A Centralized View of Your Security Landscape

Today's organizations are swimming in massive amounts of data spread among multiple data sources — and that doesn't even factor in multi-cloud systems or interconnected data structures and architectures such as services and microservices. When you add in things like IOT systems, IP-based cameras or door locks, HVAC systems, and remote devices that have exploded due to the global pandemic, graph's deep link analytics, multi-dimensional entity and pattern matching, centrality identification, as well as hub and community detection can help companies take preventative, defensive, and corrective action against potential threats and threat actors.

When combined with your security stack, graph database technology boosts your level of visibility into user patterns, data mining, lateral movement of users and data, privileged user permissions escalation, malware attacks, payload disbursement and deployment, ransomware data encryption, and more. With the flexibility and in-depth strength of graph algorithms, the use of an existing IOC embedded into these easy-to-create algorithms allows for extended search and analytics across all of your data from all of your systems in one place at one time. A real-time graph model of your network allows you to set up monitoring and defenses at certain points, making early identification of active cyberthreats possible. Graph can detect if one service receives a larger number of different requests from the same IP than usual. Graph can also identify if a user who happens to be moving data with newly escalated permissions happens to be on vacation. It can also uncover the number of hops between a specific user and a

blacklisted IP, system, application or account, highlighting the potential for fraud, money laundering, a potential breach or other malicious activity.

Cybersecurity Defense-in-Depth + Graph Analytics: A Double-fisted Punch

The combination of a defense-in-depth cybersecurity strategy and graph analytics provides multiple and duplicative defenses for your organization. Defense-in-depth layers in the necessary controls to protect the technical, administrative, and physical aspects of your business network. Meanwhile, graph allows you to use the connected data from your security stack, IOT systems, administrative systems and more to correlate activity across multiple environments and systems ensuring you can proactively respond to threats as they are identified. Together, especially with the implementation of ML and AI, the use of these tools together can anticipate cyberattacks and disrupt them when they happen versus before your organization becomes a statistic. A combined, multi-layered approach incorporates the following:

- Administrative Controls: Defense-in-depth encompasses the administrative aspects of your business, including policies and procedures directed at the organization's employees as well as the labeling of sensitive information as "confidential." The use of PAM (Privileged Access Management) solutions, along with graph analytics, controls who gets into what systems and flags any anomalous privilege escalations for user accounts.

- Technical Controls: This refers to the hardware you put in place to protect network systems and resources. Software such as an NDR (Network Detection and Response) system and network firewall appliances, IDS/IPS (Intrusion Detection and Prevention System) or an antivirus program work hand in hand with the hardware controls. Deploying an EPP and EDR (Endpoint Protection and Endpoint Detection and Response system) to control unwanted activities on your endpoint devices is also part of the technical controls. The connected data analytics as well as algorithms used to automate threat hunting, threat analysis, and attack vector tracing and analysis will bolster the security team's efforts while providing the needed level of automation.

- Physical Controls: These defense-in-depth measures prevent physical access to your IT systems. These should include security guards, locked doors, and alarm systems, cameras, biometric systems, and more. The log data from each of these systems will be added to the other security data collected to complete the picture of your environment and enable complete visibility.

- Access Measures: Access to any data will require access codes, or measures such as biometrics, timed access pins, encryption key pairs, and/or controlled authentication. The use of identity and access management (IAM) and multi-factor authentication ensures proper validation of users and the systems they use to access sensitive systems or information. Graph database technology ensures you can connect events and alerts with the data from all of your security stack tools, administrative systems and log systems to best react to threats as they arise.

- Additional defense mechanisms and measures: Perimeter Defenses such as intrusion detection systems, firewalls, proxy servers, and data encryption; Monitoring Prevention, which includes auditing network activity, logging, sandboxing, vulnerability scanners, penetration testing, attestations, and security awareness training; Workstation Defense Mechanisms, which include anti-spam and antivirus software including where possible client side data encryption; and Data Protection Mechanisms, which involve hashing, data-at-rest encryption, secure data transmission with current day technologies such as TLS, and encrypted backup systems. You can monitor logs, SIEM data, XDR, NDR, EDR, EPP, IOT and administrative data sources as well as other system data in a single graph database to ensure you are protecting your data through proactive defense-in-depth strategies.

Cyberattacks are a constant, ever-evolving threat to businesses. Bad actors are always looking for the chink in an organization's armor, a weak link, or a security gap to exploit. A defense-in-depth cybersecurity strategy coupled with least privileged model and graph analytics ensure your organization has multiple lines of defense to safeguard your network systems, users and data. Breaches, hacks, and cyberattacks will always be a part of the technology landscape. A multi-layered cybersecurity model gives your organization a proactive, preemptive edge — an edge that may keep your organization from being in the headlines for the wrong reason.

About the Author

Harry Powell is Head of Industry Solutions of TigerGraph, provider of a leading graph analytics platform. In this position, he leads a team comprosed of both industry subject-matter experts and senior analytics professionals focused on key business drivers impacting forward-thinking companies as they operate in a digital and connected world.

A graph technology veteran, with over 10 years industry experience, he spent the past four years running the data and analytics business at Jaguar Land Rover where the team contributed $800 million profit over four years. At JLR he was an early adopter of TigerGraph, using a graph database to solve supply chain, manufacturing and purchasing challenges at the height of the Covid shutdown and the semiconductor shortage.

Prior to that he was the Director of Advanced Analytics at Barclays. His team at Barclays built a number of graph applications and released world-class data science innovations to production, including the first Apache Spark application in the European financial services industry.

The Top Four Issues Companies Should Focus on During Cybersecurity Awareness Month

How companies can show employees they have a critical role to play in cybersecurity

By Matt Lindley, CISO, NINJIO

October is Cybersecurity Awareness Month, an ideal time to remind all employees that they have an indispensable role to play in preventing cyberattacks. Despite the fact that the vast majority of breaches involve a human element (82 percent, according to Verizon's most recent Data Breach Investigations Report), many employees believe cybersecurity falls outside their purview. This dangerous misconception is due to a lack of cybersecurity awareness, which is why companies should take the opportunity to educate employees.

With that goal in mind, here are the top four subjects companies should focus on to demonstrate just how destructive cyberattacks can be – and how effective well-trained employees are at thwarting them.

1. **Business email compromise (BEC)**. According to the most recent FBI IC3 Internet Crime Report, BEC is by far the most financially destructive type of cyberattack. BEC refers to cybercriminals who break into a victim's email account and use this access to deceive and manipulate employees, company leaders, or partners. For example, a cyber criminal could hack into a CEO's account and demand an immediate wire payment from the accounting department, which would then be routed into a fraudulent account. Cyber criminals also exploit employees' trust that messages are coming from a legitimate source by convincing them to click on links or attachments that install malware on their devices, and this is often a ploy to gain wider access to their networks.

   What companies and employees can do: There are many ways to spot and stop BEC attacks. First, employees should always confirm wire transfers or deliveries of sensitive information in multiple ways – through phone calls, in-person discussions, and so on. Second, they should be wary of urgency – if a superior is asking for a large amount of money to be sent within the next few minutes or for immediate privileged access to be granted, proceed with the utmost caution. And third, employees can examine messages for inconsistencies and other red flags, such as different email headers, links that don't go where they should, unfamiliar language, or strange attachments.

2. **Phishing**. The FBI reports that there are more victims of phishing each year than any other type of cyberattack. Of all the social engineering breaches tracked in Verizon's 2022 DBIR, phishing was the top action variety. Beyond the fact that phishing is one of the most common methods used to scam individual consumers, it's also a highly effective entry point for hackers who want to infiltrate a company. Hackers can use a single compromised device to access an entire network.

   What companies and employees can do: While phishing remains the tactic of choice for many cybercriminals, there are many ways employees can repel phishing attacks. They should beware of what information they're providing on social media, as hackers often leverage that information to break into professional accounts. Employees should pay close attention to email addresses, domain names, and attachments, as well as message content: are words misspelled? Does something seem out of the ordinary? Do you know the sender? Are there more reliable ways of contacting that person? Companies can run phishing tests to determine whether their employees know what warning signs to watch out for. Finally, employees need to be aware of the unique threats posed by remote work. According to a Deloitte survey, 42 percent of employees say they've never received security awareness training on how to work safely from home, and this is putting many companies at unnecessary risk.

3. **Credential security**. Account credentials should always be viewed as keys to your entire organization. According to the most recent DBIR, stolen credentials are right behind phishing in BEC incidents – and in many cases, cybercriminals use phishing to acquire credentials that they later use for other attacks. In many sectors, credentials are one of the top types of data breached, and they're often part of multi-stage attacks (as they allow hackers to access secure systems and initiate new social engineering attacks from the inside). However, credential hygiene is abysmal – a survey conducted by Google and Harris Poll found that just 35 percent of respondents use a different password for all their accounts, while 13 percent use the same password everywhere. Less than a quarter use a password manager.

   What companies and employees can do: The first step toward improving your credential security is ensuring that employees have the right resources to protect their accounts. A password manager is a simple and intuitive way to prevent the most common credential-based account intrusions. Instead of asking employees to create and track complex passwords for all their accounts, companies can require them to use password managers on all work devices (a policy that will also help IT teams identify unauthorized devices). Now that we've entered the era of remote work, companies should also make sure employees are using a VPN when they're on public WiFi, which will prevent cybercriminals from using keystroke loggers to steal their credentials. Finally, employees should understand that sharing privileged account access information is strictly prohibited.

4. **Ransomware and proactive cybersecurity awareness**. Several of the largest cyberattacks in history were ransomware attacks: from SolarWinds to NotPetya to Colonial Pipeline. However, employees are still woefully unprepared for ransomware attacks – according to a 2021 survey, 29 percent of employees didn't even know what ransomware was before their company fell victim to it. The survey also demonstrated the fact that social engineering is a major element of a significant proportion of ransomware attacks: 42 percent were caused by phishing emails, 23 percent were caused by malicious websites, and 21 percent resulted from compromised passwords.

What companies and employees can do: Despite all the evidence that untrained employees pose a major ransomware risk, 90 percent of companies provided employees with more cybersecurity training after they were attacked. This is a powerful reminder that proactive cybersecurity awareness is critical for companies to avoid the often-devastating financial and reputational costs of a successful ransomware attack. A proactive cybersecurity awareness platform should seize employees' attention – and account for how busy adults learn – with relevant and engaging content based on real-world cyberattacks (such as the ones mentioned above). They should also offer concrete strategies for preventing these attacks. Your platform should reinforce what employees learn with assessments, consistent messaging, and the encouragement of healthy habits – all of which will help companies build a culture of cyber awareness.

There are many other cybersecurity issues that companies have to prioritize, but the basic principles are the same: provide engaging and relevant cyber awareness content, earn employee buy-in at every level, and reinforce what employees learn. Cybercriminals will always try to exploit gaps in your employees' knowledge, so it's your responsibility to fill those gaps and change employee behavior.

About the Author

Matt Lindley is the COO and CISO of NINJIO, and he has more than a decade and a half of experience in the cybersecurity space. Prior to NINJIO, Matt was the CEO of REIN Cybersecurity, LLC., the senior technology manager and director of security services at Cal Net Technology Group, and the virtual CIO at Convergence Networks. He has held many other leadership positions in the industry, and he's an authority on IT, security, and a range of other issues. Matt can be reached at mlindley@ninjio.com.

Three Steps of PSD2 Security

As we reach three years since the inception of regulated open banking in Europe, it is a good time to look back at the security issues which have emerged in open banking ecosystems and what steps are necessary to mitigate these risks.

By Brendan Jones, Chief Commercial Officer, Konsentus

The final deadline for compliance with the revised Payment Services Directive (PSD2) passed on 14th September 2019. PSD2 mandated financial institutions to share their customers' data with third-party providers (TPPs), thereby enabling open banking by allowing TPPs to offer customers innovative products and services. Since 2019, the open banking ecosystem has transformed dramatically – with a huge influx of new fintechs and millions of open banking transactions a month.

As the ecosystem has matured, the risk of unauthorised or fraudulent transactions has grown with it. Many security measures which were put in place at the time have not been able to scale and leave financial institutions exposed. If an unauthorised TPP manages to access a customer's account, it can result in grave financial and reputational damage for the financial institution and potential PSD2 or GDPR non-compliance fines.

Part of the issue stems from the fact that financial institutions are sometimes unclear about the difference between the three sides of PSD2 security: identification, authentication, and authorisation.

Identification

The first step in securing an open banking transaction is to establish who the third party is. According to PSD2, this is the purpose of eIDAS certificates, which are used by third parties as identity credentials when interacting with financial institutions.

A third party can apply for an eIDAS certificate with a Qualified Trust Service Provider (QTSP). QTSPs are regulated entities subject to PSD2 and issue two types of eIDAS certificates to TPPs:

Qualified Website Authentication Certificate (QWAC), which enables a secure channel to be established between the two parties

Qualified Electronic Seal Certificate (QSealC), which provides legally assured evidence of transaction data, including data integrity and proof of origin

The use of eIDAS certificates is crucial to ensure independent, government assured trust in the identity of the third party. However, PSD2 explicitly states that the certificates should be used solely "for the purpose of identification" (Article 34). Confirming that a transaction is authenticated and authorised involves two additional steps.

Authentication

The second step makes sure that the TPP is authenticated. For this, QWACs are used to establish a secure communications channel using Transport Layer Security (TLS). As part of the Mutual authenticated TLS (MTLS) protocol, the TPP signs part of the communications data, passing between the two parties, with its private key. The financial institution can check the signature confirming that it matches the public key certificate. This confirms that the TPP holds the corresponding private key and therefore serves as proof of the TPP's authentication.

The authentication step can also involve a QSealC to ensure the data integrity and proof of origin of the transaction, using digital seals and signatures to ensure the TPP is authenticated. The confidentiality of the data is provided by the encrypted TLS session.

Authorisation

Although QWACs and QSealCs provide secure identity and authentication mechanisms required by PSD2, they do not provide the regulatory check needed to ensure that the TPP is authorised. A financial institution must know in real-time that the TPP is:

Still regulated by its National Competent Authority

Still approved to perform the service requested (account information or payment initiation)

Still approved for services in the country of the request

Still authorised by the PSU to carry out the transaction

eIDAS certificates, though crucial to identify a TPP, cannot be used to validate the authorisation status of the TPP at the time the transaction is taking place. eIDAS certificates are issued with a lifespan of one

to two years and so cannot be relied upon to provide authorisation status, as the information can quickly become outdated when a TPP is acquired, goes out of business, changes roles or loses permissions. In addition, eIDAS certificates contain no information on passporting and so it is not clear whether the TPP is authorised to operate in another country.

Security Solution to PSD2 Open Banking

TPP changes are increasing as the market matures and open banking transactions are now in excess of millions a day. As a result, financial institutions require a mechanism which can carry out the identification, authentication, and authorisation security steps in real-time.

After confirming the identity and authenticity of the TPP with a thorough eIDAS certificate check, Konsentus instantly verifies that the TPP is authorised by checking relevant institutions among 70+ trust service providers and 31 NCAs (which have over 115 registers with regulatory information).

This ensures that a financial institution only ever approves a transaction with a third party that is authorised for the appropriate service in that country at the time of the account access request. Konsentus Verify protects customer data from any unauthorised or fraudulent use, upholding the reputation of financial institutions and shielding them from compliance fines and the costs of managing disputes.

About the Author

Brendan Jones is the Chief Commercial Officer of Konsentus. Brendan has enjoyed a leadership career spanning banking and financial technology companies. Brendan has held director roles in the banking industry including MBNA and Bank of America. He has also held senior roles within the payments industry for companies such as Datacard and Giesecke & Devrient UK. Brendan set-up Konsentus, a RegTech company, with his two co-founders, to provide critical identity and regulatory checking services for financial institutions so that they can comply with the European Payment Services Directive 2 (PSD2) and open banking.

Brendan Jones can be reached online at becci@openbankingexcellence.org and at https://www.konsentus.com/

Understanding Hashing Algorithms in Details

Understand the Concept of Hashing & Hashing Algorithm

By Anna Shipman, Cyber Security Consultant, SignMyCode

A single person has multiple accounts today. There are different or same passwords for these accounts, and we also share data or conduct transactions on some accounts. While everything we do online is vulnerable, and hashing is one of the ways to authenticate data transfer and ensure data integrity.

Put simply, hashing is one of the ways to authenticate and verify the security of a file, data, or password. Confused? Don't be we will explain everything here.

Hash function, algorithms, or hashing is a mathematical process. While hashing plays a key role in public key cryptography, it helps secure passwords, helps verify data integrity, and facilitates a process for authentication.

While there are other methods of ensuring public key cryptography, and hashing is a popular method used in a wide range of transactions. How hashing secures passwords and helps verify the integrity of a file is what we will understand in this article, along with knowing the best hashing algorithms used today.

What is Hashing?

Hashing or hash function is the process in which the plain text is converted into a cipher text of fixed length. The plain text length can vary, but the output of cipher text is fixed according to the hashing algorithm used. Plus, the output hash value or cipher text is unique, which is crucial in implementing this function.

In a general sense, we take hashing as a form of encryption, which is not true. Because hashing does not imply encryption. Although the purpose of encryption and hashing is similar, to ensure secure communications. But we cannot decrypt a hash function, whereas an encrypted text can be decrypted.

Hashing helps when you want to send data to another person over the web and want to make sure that no one can change the contents. This is one of the use cases of hashing. So, to send the data without allowing any edits, you have to use a hash function and generate a hash value. As this value is unique and specific to the content you have sent, and any changes in the value when the person receives it means the contents are changed.

What are Hashing Algorithms?

Hashing algorithms are the programs or structures we use to create hash values. It's a mathematical algorithm used for mapping data structures or characters of any size to generate a fixed-length hash value.

From time to time, we have come across different forms of hash algorithms, and consequently, the position of the best hash algorithm was given to different algorithms.

Any hash algorithm is designed to be a one-way function. We can only create a hash value to facilitate encryption. The generated value cannot be reverse engineered to find the original plain text. This is one of the strongest security aspects of a hashing algorithm.

Hashing is a one-way function. This means that it's not possible to reverse engineer a hash function with the current computing value and resources. The one-way function denotes the computing power, time, and cost required to hack the hash value with a brute force attack.

Consequently, breaking the hash value of SHA-512 will take 3.17*10^64 years. This means that it is impossible to crack the hash.

Hashing algorithms generate different results depending on the function. A 16-bit function's output will be smaller than the output of a 32-bit function. Consequently, as the bit size increases, the resultant hash value also increases, and it gets more difficult to crack.

Hashing algorithms work with data blocks converted from the input value. These data blocks also have a fixed value. For instance, the SHA1 hashing algorithm takes data in 512-bit size. Any more than this, it will create another data block.

So, for the data sized 1024-bit, it will take input data in two blocks. The data blocks may vary, but the hash value generated by the hashing algorithm will be one only.

However, due to the wide expanse and presence of data everywhere, hashing algorithms are built to use padding for generating a common hash value. In Padding, the entire plain text is divided into fixed data-sized blocks. And the same hash function applies to every data block.

Supposing there are 9 data blocks, and we want to generate a single hash value for all. The hashing function will first generate the hash value for the first block, and this output will be fed to the hash algorithm along with the second data block.

Continuing like this, we will get a common hash value of the combined data. And this will also retain the core principle of hashing that when even a single character is changed, the entire output also changes.

What are the Ideal Properties of a Strong Hash Function?

From time to time, we have built different hash functions and algorithms, where the latest function is an improved version of its predecessor. So, the need to generate or create new hash algorithms will continue until we have the best hashing algorithm. But to identify the best, it must have some properties meant to improve the outcome.

- Deterministic: No matter the size of the input data, the best hash function must always give you the output of the same length. In other words, if you are hashing a single sentence or creating a hash value for an entire book, the hash value must be the same. This makes identifying and working with the hashing functions easier and streamlines the work.

  Otherwise, imagine getting a different length of the hash value as you change the input. This would simply beat the purpose of using a hash function. If you could compare the contents of an entire book, why use hashing?

- Quick: The time required by a hash function to generate the output is also considered a good property. However, it is not ideal to consider the quickness of generating the hash value as the best property. Because quick might not always be the best here. The speed is subjective, as, with website connection encryption, quick hashing is required, but when it comes to storing passwords, a relatively slower operation is better.

- Avalanche Effect: The Avalanche effect is the key contributor in determining the best hash algorithm. It means that even a minor change in the hashing algorithm will result in a massive change in the hash value.

  For instance, if the has value of “avalanche effect” is c085fbf70ff97c7abc4d8fa925b355ff8f37aad8b9de5b78a26094e3d84c8f30
  The hash value when we change the plain text to “avalanche affect” is cf9962304011975dcbeb8be1c09cfe989320095d0440be9d85e8a38276553591
  This change in the hash value is called the avalanche effect.

- One-Way Function: Any hash function that can be reverse engineered to identify the original text is ineffective. One-way function means that the algorithm cannot be hacked to reveal the input message.

- Collision Resistance: Collision between two hash values is existent with the older versions of the hash algorithms, like MD4 and MD5. These hash functions have produced identical hash values for two different inputs. And this is called collision. Any hash function that produces one hash value for two unique inputs should not be used. So, we want to use a hash function that does not generate similar outputs.

The risk here is that anyone can generate the same hash value for a malicious file and pass it as a verified and secure data matching the integrity of a genuine file.

Hence it is imperative to use the hash function that can pass these ideal properties tests. Any hash value missing any one of these properties is not safe and should not be used.

Conclusion

Hashing algorithms are required to process the plain text and convert it into hash value. The manner and length of the hash value generated depends on which hash algorithm you are using.

About the Author

Anna Shipman is the Cyber Security Consultant at SignMyCode. She has been involved in the information security industry for more than a decade. In her free time, we find her helping small and medium businesses strengthen their information security infrastructure. Anna can be reached online at https://twitter.com/AnnakShipman and at our company website https://signmycode.com/

VPN Use in Russia: The Rise in Popularity of The Virtual Private Network and How Putin Is Trying To Stop It

By Callum Tennent, Site Editor at Top10VPN.

In 2020, VPNs were used by just under a quarter of Russian internet users. Fast forward to this year and the cybersecurity tool has exploded in popularity following the country's invasion of Ukraine and increased censorship in the country. But measures taken by Putin's regime may be slowing VPN adoption and this raises concerns for those who are relying on a VPN to access reliable information.

Since Russia's invasion of Ukraine back in February, Putin has ramped up Russia's propaganda machine in an attempt to control the country's war narrative. As well as pushing pro-Russian angles, authorities have been blocking thousands of apps and websites showing pro-Ukraine sentiment. Notable blocks include Instagram, Facebook, BBC News, the Russian news site Meduza and Amnesty International.

With popular social media and global news sites unavailable, some Russians have turned to censorship circumvention tools to communicate with friends abroad and access information. Of these tools, VPNs have fast become one of the most popular. We recorded a peak in VPN demand of 2,692% above the pre-invasion average following the Instagram block in March.

But while demand for VPNs has increased, so has authorities attempts to stop their use.

Even before Russia's attack on Ukraine, the Roskomnadzor (responsible for overseeing all media and telecommunications in the country) had banned 15 popular VPN services including ExpressVPN, NordVPN and IPVanish. Most of these VPNs were banned in 2019, the same year authorities passed a controversial cybersecurity bill that laid the groundwork for Russia to isolate the country's internet from the rest of the world.

Recently, the war on Ukraine has led the Roskomnadzor to take even more steps to try and prevent people from using VPNs.

Back in May of this year, the blocking of popular VPN protocols IPsec and IKEv2 began to be tested in Krasnodar and parts of Western Siberia. Different VPNs use different protocols to run and the disruption of a specific protocol can stop a VPN from working. While most consumer VPNs rely on the OpenVPN protocol, the blocking of IPsec and IKEv2 is not insignificant and would cause disruption if rolled out permanently across Russia. This is because IKEv2 is very popular with mobile VPN users and the blocking of IPsec could impact businesses that rely on VPNs for remote access capabilities.

The Roskomnadzor also confirmed in June that they were actively blocking some VPN services completely due to their help in bypassing the blocking of illegal content. Several popular VPNs, including ProtonVPN and NordVPN, became unavailable overnight. Moreover, the digital rights NGO Roskomsvoboda confirmed in early August that seven VPN services are being prepared to be blocked in Russia.

The blocking of these popular apps is especially concerning because it means that people looking to download a VPN will have less reliable options to choose from. They could end up downloading an obscure VPN app with shady data handling practices. These apps are risky at the best of times, but even more so when used in an undemocratic country that actively punishes those going against the government.

As well as technical blocking of specific VPNs and VPN protocols, Russian authorities have launched an anti-VPN press campaign claiming that VPNs drain batteries and steal data. While this could be the case for some lesser known services, a reliable VPN should only increase your privacy. Given the relatively low uptake of VPNs in Russia before the invasion of Ukraine, it's likely that at least some Russians will be put off by this misinformation campaign due to low technical literacy.

With all of these measures being undertaken to prevent Russians from using VPNs, it's worth considering the likelihood of their success. While there's no doubt that the technical blocks have already caused disruption to VPN use, Russia's track history indicates that widespread blocks may fail.

Back in 2018, the messaging app Telegram was banned in Russia and authorities started trying to block it. Two years later and the app still remained widely available, a fact which ultimately led to Telegram's ban being lifted.

Alongside Russia's own technical inefficiencies, some VPN companies are making it easier for Russians to access their products. For instance, Mullvad has worked with Doxa to hand out free VPNs to those most in need via Telegram. The US government has also started funding VPN companies to support their recent surge in Russian users.

But while Russia's attempts to prevent widespread VPN adoption may fail, any disruption that authorities cause will have a grave impact on people's ability to access information and communicate with those outside the country. In fact, Putin's clampdown on VPNs in Russia only serves to highlight their importance.

While there are other means of getting around government censorship, such as Tor and mirroring sites like Samizdat Online, VPNs provide a relatively straightforward way of accessing blocked content while simultaneously increasing the privacy of a connection. In this way, they can be seen as a key weapon in the war against misinformation and defending our digital rights. We must continue to fight for their recognition as such and pushback against attempts by oppressive governments to unfairly restrict and ban their use.

About the Author

Callum Tennent is the Site Editor at VPN review website Top10VPN.com. A member of the International Association of Privacy Professionals and former consumer technology journalist, he specializes in VPN technology, information security, and online privacy. Callum can be reached via Twitter at @TennentCallum and email at callumtennent@top10vpn.com.

When Software Needs a Patch, Try Micropatching

Most organizations take 60 days to fix a software vulnerability. A patch management solution can help close that security gap.

By Michael Crystal, Technical Program Manager, Draper

Government, banks, airlines, the military—nearly every major sector is dealing with old IT that makes resolving issues difficult and fixing vulnerabilities expensive.

These older systems are often used in unanticipated ways for which they were not designed, which can uncover bugs and vulnerabilities that need to be corrected for safe, secure and effective continued use. Consider what happens when a legacy system is only able to handle two-digit years (the Y2K bug), or in the future when 9 digits are inadequate for an SSN or 10 digits are not enough to encode a telephone number.

The problem is particularly acute in legacy software. Most experts acknowledge that the original source code for many legacy software programs is lost, fractured or incomplete. Other problems arise when you find out the original people who wrote the code are retired, or the technologies on which your software is based (COBOL, for example) are beyond the knowledge of your IT resources.

So, what happens to your legacy software if the code isn't available? What if a vendor no longer supports your software? What do you do then?

Patching gets a new look

Computer engineers are addressing this challenge by developing a capability for rapidly patching legacy software in its original binary form. With the new capability, IT teams will be able to analyze, modify and fix legacy binaries, and produce assured targeted micropatches for known security flaws.

The new capability is designed to address several challenges. Fixing security vulnerabilities in legacy software, for instance, requires patching at the binary level. Manual binary editing, however, is slow and error prone. Additional challenges arise when patched and recompiled binary code changes an IT system's performance.

Current methods for software patching are also complicated, and the recertification process is largely manual and relies on human evaluators combing through piles of documentation, or assurance evidence, to determine whether the software meets certain certification criteria.

These limitations and challenges can result in mission-critical software going unpatched for weeks to months, increasing the opportunity for attackers and the risk of the software becoming noncompliant. EdgeScan found that the average organization's mean time to remediate a vulnerability once it's identified—known as the security update gap—is 60 days. That gives an attacker 60 days to find and exploit systems hosting that vulnerability.

For these reasons and many others, it's crucial to have a patch management solution to ensure critical aspects of an IT system stay up to date.

Fixing, without the guesswork

Micropatches are available primarily from third-party providers, rather than original software vendors. A growing number of providers are also entering the business of legacy systems' security maintenance and patching unsupported systems.

One micropatching toolkit, described briefly here, was developed by Draper and Carnegie Mellon University (CMU) and funded under DARPA's Assured Micropatching program. The patching software and method, called VIBES, which stands for Verified, Incremental Binary Editing with Synthesis, is built on top of the CMU Binary Analysis Platform.

The toolkit uses program synthesis and constraint programming techniques to compile a source-level patch and insert it into a preexisting binary program. The toolkit uses formal verification to prove that only the intended change is made and provides evidence of correct behavior for subsequent recertification or accreditation processes.

The new capability changes the fewest possible bytes to achieve its objective, which minimizes potential side effects, and enables proofs that the patches will preserve the original baseline functionality of the system and not introduce unintended behaviors. With these proofs, the time to test, recertify and deploy the patched system can be reduced from months to days.

VIBES was released as an open-source software in February. CMU's open-sourced software, which serves as the foundation for VIBES, was originally released in 2015.

Resources for cyber defense professionals

Concern that software products are (in)secure has been around for more than three decades, but until relatively recently was given little attention by the vendor community. More recently, an industry consortium was formed by some of the larger software companies to define best practices for building secure software.

Government agencies can be another helpful resource for cyber defense professionals. White papers, best practices and weekly malware alerts are available at the Cybersecurity and Infrastructure Security Agency's website. Another resource is the Department of Homeland Security.

IT and security teams need to implement a plan and process for regularly reviewing their technology stack and sunsetting applications that no longer serve a business function. They also need to explore options for code patching—from off the shelf and downloadable apps to in-the-code micropatching.

Micropatching is all about enabling software operators and maintainers to quickly and accurately patch legacy binaries in the deployed software systems upon which their enterprises depend. With micropatching, you should be able to test, package, stage and deploy patches automatically, saving time and money over limited, manual processes.

About the Author

Michael Crystal is a Technical Program Manager at Draper with 35+ years' experience managing a broad spectrum of U.S. Government, Cyber, Human Language Technology, Machine Learning, and Artificial Intelligence R&D programs from program ideation through engineering, to test & evaluation. He has served as Principal Investigator (PI) or Program Manager (PM) on multiple, multi-year, multi-site DoD, R&D efforts. Michael can be reached at mcrystal@draper.com.

Why is Multi-Factor Authentication (MFA) No Longer Enough?

And why you should find out about FIDO2 right now…

By Tomasz Kowalski, CEO and Co-Founder, Secfense

According to Verizon's 2022 Data Breach Investigations Report, nearly 50% of data security breaches involve the use of stolen credentials. Financial institutions are often their number one target. Banks use various cybersecurity technologies, one of them is multi-factor authentication (MFA), which until recently was one of the most recommended tools to protect identity online. Today, however, MFA is no longer enough. Or we should say any MFA is no longer enough. There is an open authentication standard, a new sheriff in town and its name is FIDO2. What distinguishes FIDO2 compared to other MFA methods is that it is the only authentication method that is fully resistant to phishing and the theft of logins and passwords.

Banks and financial institutions very often become the target of attacks. According to a report by The State of Authentication, 80% of them experienced at least one data breach in the last 12 months, and phishing was the most widespread threat, accounting for 36% of all attacks. One of the reasons for the escalating incidents is insufficient protection of users' identities.

A global problem

Until a few years ago, MFA, was considered one of the most effective methods of protecting users online. Today, however, sophisticated intruders have found ways to effectively trespass it.

2FA or MFA is not a new thing. But still there are tons of companies that do not use MFA to protect their apps. Why? Because of the high level of complexity and diversity of IT environments in organizations. That complexity leads to difficult or even impossible implementations of effective MFA methods.

For this reason, in many large organizations, most systems and applications are either not protected with MFA or if protected, it's usually done with some outdated methods such as SMS or TOTP codes. And these methods no longer protect against modern phishing attacks.

Old MFA methods

According to a study by HYPR Report: State of Authentication in the Finance Industry 2022, 32% of bank employees from the US (200 people), UK (100 people), France (100 people) and Germany (100 people) still use traditional MFA methods such as SMS and one-time passwords, 43% rely on password managers and 22% rely solely on usernames and passwords.

But how does the FIDO2 actually protect against phishing? It uses cryptography, sometimes in the form of physical U2F keys (Universal 2nd Factor), but more recently in the form of physical devices that we always have with us, such as laptops with a built-in camera equipped with Windows Hello or smartphones with a fingerprint reader. These biometric readers are used to confirm your identity online - apart from, or sometimes even instead of the password.

Security comes late

The opinion of IT security specialists is also confirmed by people working in the financial institutions audited by HYPR. As many as 99% of respondents admitted that the authentication methods used in their organizations require modernization. However, it is currently not possible, because it is prevented by problems with IT systems (75%), including management complexity (33%) and integration difficulties (27%).

The biggest problem is still the implementation. MFA implementation is difficult, burdensome and costly. Moreover, if a bank has hundreds of applications in its IT infrastructure - which is the case in most large organizations - mass implementation on all applications is practically impossible. Effect? One of the best authentication methods, the FIDO2 authentication standard - although designed in April 2018 - after more than four years is still just an addition instead of being the universal way of securing our identity online.

Is FIDO2 free of charge?

The FIDO2 method has revolutionized authentication security. It is an open standard, thanks to which every service on the Internet can be secured today with a free, fully resistant to phishing and credential theft method.

How to solve implementation complexity?

We knew that the only way to make FIDO2 fully accessible was to create a technology that would eliminate implementation burden. The User Access Security Broker (UASB) introduces FIDO2 authentication (and in fact any other MFA method as well) without any interference with protected applications. FIDO2 can be implemented in a no-code way, without hiring a single software developer.

UASB has been designed in such a way that in the conditions of 'zero' knowledge about the applications and the IT environment it is still able to add MFA on top of an application without changing its code.

Wolf is full and the sheep are whole

There are many cybersecurity solutions on the market that protect against various attack vectors. Currently, however, FIDO2 based authentication is considered the most convenient and effective. According to the HYPR survey results, most respondents believe that passwordless authentication (based on FIDO2) is the method of the future. As many as 89% of them claim that it significantly increases not only the security but also comfort and satisfaction of users.

And aren't these factors the most important to us all?

About the Author

Tomasz Kowalski is a CEO and Co-Founder of Secfense. He has nearly 20 years of experience in the sale of IT technology. He was involved in hundreds of hardware and software implementations in large and medium-sized companies from the finance telecommunication, industry and military sectors. Tomasz can be reached online at (tomek@secfense.com, Tomasz Kowalski | LinkedIn) and at our company website https://secfense.com/

Why Purpose Is Needed to Drive Profits

By Jonathan Shroyer, Chief CX Innovation Officer, Arise Virtual Solutions

For many industries and businesses, profits have driven their purpose. The bottom line has centered around one simple goal: how to make more money.

However, as a society, consumers are now demanding more from companies. No longer do our consumer demands center solely around receiving excellent products or services for reasonable prices, but now consumers are seeking ethical and responsible business practices. Consumer demand is changing, and it would be practical and wise for companies to not just follow suit, but stand out as leaders in the new age of consumer demand.

This remarkable change in consumer trends is forcing executives and business leaders to shift the way they think and operate. Rather than thinking about profit as the end all be all, companies now must consider how to secure customers and profits while simultaneously following ethical business practices. Additionally, they must be operating with a purpose that transcends numbers and dollar signs.

So how can companies and leaders shift the way they think about their business?

Ask questions

While this seems simple, business executives can benefit from asking some basic questions. These are a few questions that business leaders and executives must ask themselves and be willing to answer honestly, if they want purpose to drive profit and encourage lasting business success in today's world.

Is my company doing something to improve the well-being of my employees?

Is my company doing something philanthropic?

Does my company improve the lives of others in some way?

What are some goals I can accomplish this month for myself? What are some goals I can accomplish this month for my team's success?

How can I better perform as a team leader?

What can I do to make my team more successful?

These questions can be the first step to shifting a company's business objectives from one that is solely focused on profits, to one that is focused on purpose-driven profits. In order to understand why purpose is becoming fundamental to driving profits, we have to look at changing consumer viewpoints.

Understanding the consumer

For years, companies have strived to understand their consumer in order to maximize profits, but now, what a company needs to know has evolved. In previous decades, consumers have wanted great products and services at great prices. Companies thus focused on how to make as much profit as possible while still appealing to consumers with affordable prices and quality goods and services.

Now, however, in the wake of climate change, the COVID-19 pandemic and other societal current events, consumer demand has shifted. People are looking for more purpose-driven companies, companies that are seeking to do good for the sake of doing good as a way of making positive change in the world. There is a growing sentiment that companies are the ones with the power to make change fastest, and consumers are now putting their money where their values are.

This is due, in part, to the development of social media, which has given consumers more power to understand the businesses they are purchasing from, and to also find new companies that back the core values they support. Social media holds businesses accountable by making information more widely available to the public, including both company praise and blame. What was before hidden from the public eye no longer is. If companies fail to conduct business ethically, modern consumers now have easy access to alternative businesses and companies that do provide that level of ethical standards they want.

No longer is it sufficient for business to focus solely on business. Consumers want to know that business employees are being treated fairly, that the environment is being considered at every stage of business development and that businesses are addressing social issues in some way. This has resulted in a new era of business that means companies need to do a deeper dive into their own values and ensure they

match with what their customer base is now demanding of them. Businesses and business executives today must have a deeper purpose that drives their business, and thus their profits.

Finding profits and purpose

Businesses can still succeed financially while simultaneously considering their purpose. Here are a few ways businesses can maximize their profits while maintaining ethical, purpose-driven business practices.

1. Utilize remote work opportunities

Offering remote positions allows businesses to prioritize their employees' work-life balance while reducing the need to pay rent on physical office space, particularly in cities with high rent. It can also empower companies to hire talent in less expensive cities, while being able to find extraordinary talent from anywhere. Additionally, the less cars are commuting on the roads, the more sustainable it is from an environmental standpoint, which shows your customers that you are taking the environment into account.

2. Listen to your employees

This seems simple, but it is probably the most impactful thing you can do as a business owner or executive. Your employees have ideas, concerns and solutions that make your business better. When you create an environment that prioritizes your employees and their voices, it will propel your business and make it purpose-driven. Consumers have a growing need to know that companies are treating their employees well, and with the rise of social media and other online platforms, people will know when you don't treat your staff well.

3. Allow consumer voices to be heard

Your employees are incredibly important. So are your customers. They see a unique side of the business and are likely to have insight that you need to perform better as a company. Actively listen to your customers and your competitor's customers to see what they want and how to be better. This can be analyzed using consumer surveys, looking at the social media comments on your company's page as well as your competitors' social media pages.

4. Write, publish and follow an ethical code of conduct

People want to make sure their data is secure and kept safe from malicious actors. They also want increased transparency from companies, they want employees to be treated well and they want environmental sustainability from businesses. Writing, publishing and following an ethical code of conduct

not only holds your business accountable in the public's eye, but it also allows business executives and their teams to see their purpose and goals outside of profit.

Conclusion

Purpose is needed to drive your company's profits in today's world, and this will only get more important the more time that passes. Consumers are demanding more from businesses and see them as modern day change makers. Consumers want to buy products and services from companies that prioritize their employees and the environment, value their consumers and their security and privacy, and from companies actively working to make the world a better place.

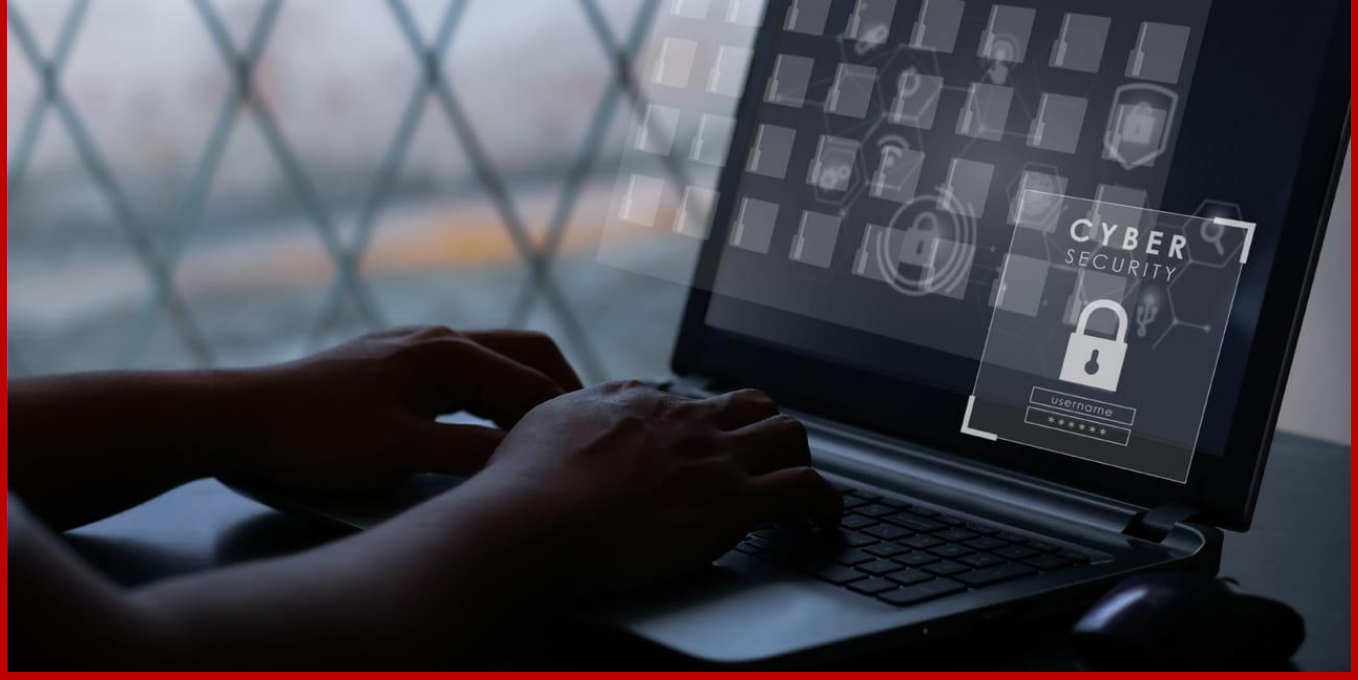
Companies who value and prioritize purpose will see profits naturally. Business leaders can realize their purpose by asking themselves questions, asking their teams questions, seeking to understand the consumer and by discovering ways to maximize their purpose and see real, sustainable business results.

About the Author

Jonathan Shroyer is Chief CX Innovation Officer at Arise Virtual Solutions. There, he leads the gaming and consulting verticals and runs the CX Lab in San Francisco. Shroyer has two decades of experience building companies and leaders up. CIO Journal, a publication of The Wall Street Journal, named Shroyer among its "Top CX Professionals of 2022.

Jonathan can be reached online at https://www.linkedin.com/in/jerryleisure/ and on https://twitter.com/ChiefCXOfficer

and at our company website https://www.arise.com/



Why Using Universal Default Passwords in Consumer Iot Products Is a Bad Idea

And why this can be a huge cybersecurity risk

By Maxime Hernandez, IoT Cybersecurity Expert & Lead Process Engineer, TÜV SÜD

In today's digital age, consumers are increasingly recognising the convenience and benefits afforded by Internet of Things (IoT) products. These connected devices offer a wide array of smart features that make everyday life easier and better. Looking to the future, the global consumer IoT market is forecast to reach $204.8 billion by 2027, rising at a market growth of 15.9% CAGR from 2021 to 2027.

But as their popularity grows, there is an increasing need to better secure these connected devices from potential cyber threats. Recent developments such as the launch of the ETSI EN 303 645 cybersecurity standard for consumer IoT devices is a step in the right direction.

In this article, we look at the first section of the ETSI EN 303 645 cybersecurity standard, which is 'No universal default passwords', and examine why having default passwords is a bad idea for consumer IoT products.

How consumer IoT devices grant access to users – and why weak passwords are vulnerabilities

The first line of defence to protect consumer IoT devices is through authentication, the process or action of verifying the identity of a user or process.

Factors of authentication

To grant access to a device, identification (such as a username) is used, and authentication is needed so users can prove their identity. Authentication can be based on:

- Something you know (such as a password)
- Something you have (such as a smart card)
- Something you are (such as a fingerprint or other biometric feature)

The danger lies in using weak passwords, highlighting the necessity of using no universal default passwords. Every device has attack surfaces, which include all the software and hardware interfaces an unauthorised user can exploit to gain access or to retrieve data from the device.

A typical vulnerability is posed by the usage of a weak password. Characteristics of weak passwords include the following:

- Easily brute-forced: Having a low (<6) number of characters, predictable sequence (123456), and/or being found in a dictionary (administrator)
- Susceptible to social engineering: Your name is Peter and your password is Peter01
- Unchangeable: Can be retrieved by looking at the software's source code

To mitigate weak passwords, one common recommendation is to fulfil the following criteria for a password:

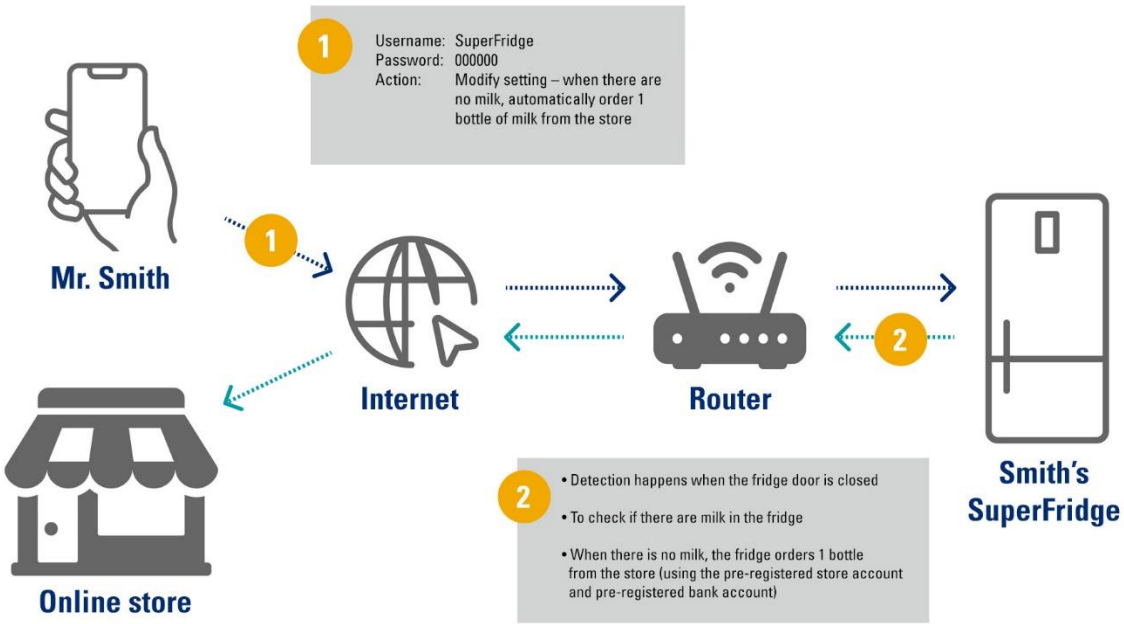
- It must be at least seven (8) characters in length
- It must include characters from at least three (3) of the following character classes:
    - digits.
    - lowercase letters.
    - uppercase letters.
    - special characters

A universal default password is used when the same password is used on all devices of a model when they are in operational state.

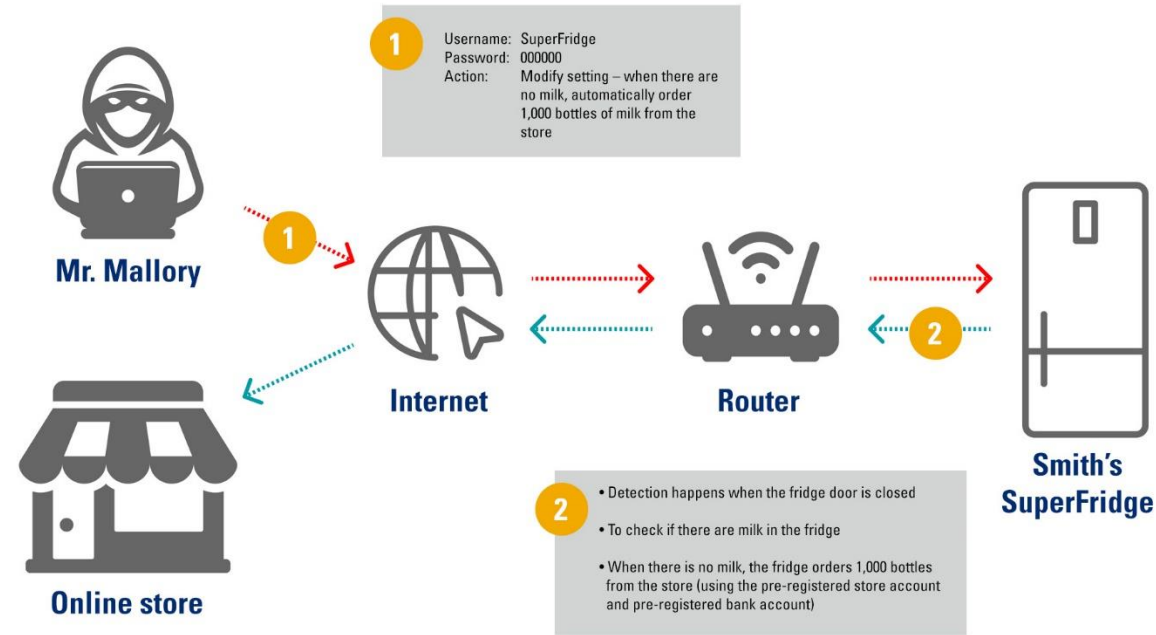
Exploiting default password vulnerabilities: Theory

Manufacturers using a universal default password for a device create a vulnerability which can be exploited by hackers. Let's illustrate that with the following scenario.

Mr. Smith buys a smart refrigerator called SuperFridge which, when connected, can be accessed through an APP (through the Internet) with a default username "SuperFridge" and default password "000000". Mr. Smith is not tech savvy and finds his new smart fridge convenient because he has configured the settings of the smart fridge via the APP so that when he runs out of milk, the smart fridge automatically orders a bottle of milk from the local food store.



Mr. Mallory, meanwhile, is a malicious hacker. He buys the same fridge model to study its flaws and quickly finds out that the device is using a default username and password which means he can connect to any of these smart fridges and send malicious messages:



Another way is through 'brute force'. This type of attack involves 'guessing' credentials (usually username and passwords - but it can also be a token if they are of short length) to gain unauthorised access to a system.

Password generated method

When a password is used by default on a device, it should be unique for each device and its generation method should not be easily guessed.

Using the example of Mr. Smith and the SuperFridge, creating a password this way: “SuperFridge” + factory batch number = SuperFridge462” would be too easy to guess. A generation mechanism should produce a password that appears random like “f2wd34hsd2aead89”.

Authentication and cryptography

When users send their username and password over a network, they need to ensure that even if a malicious hacker is “listening” to the communication on the network the data they are sending cannot be read.

To avoid sending cleartext credentials, the user will send its credentials over a secure communication channel. A common method is to use TLS 1.2 (or 1.3) which provides data encryption.

Password anti-brute force mechanism

A brute force attack involves ‘guessing’ credentials (usually the username and/or password) to gain unauthorized access to a system.

The image below shows an attacker using the tool Hydra to brute force some credential by trying different passwords:

```
[ATTEMPT] target 192.168.23.2 – login “SuperFridge” – pass “margot” – 80 of 100
[ATTEMPT] target 192.168.23.2 – login “SuperFridge” – pass “123456789” – 81 of 100
[ATTEMPT] target 192.168.23.2 – login “SuperFridge” – pass “test” – 82 of 100
[ATTEMPT] target 192.168.23.2 – login “SuperFridge” – pass “444444” – 83 of 100
[ATTEMPT] target 192.168.23.2 – login “SuperFridge” – pass “super” – 84 of 100
[ATTEMPT] target 192.168.23.2 – login “SuperFridge” – pass “admin” – 85 of 100
[80][http-get-form] host: 192.168.23.2     login: SuperFridge     password: 000000
1 of 1 target successfully completed, 1 valid password found
```

In the image above, the password was guessed with only 85 attempts, but the hacker can send millions of requests to try to guess credentials.

To avoid these millions of attempts, devices can prevent brute forcing attacks with:

- Account lockouts after failed attempts
- Use CAPTCHA

- Limit logins to a specified IP address or range
- Employ 2-Factor Authentication (2FA)
- Use unique login URLs

Exploiting Default Password Vulnerability – in the wild

The Mirai botnet made the headlines of newspapers in 2016 by creating an Internet outage in the US West Coast with a distributed denial of service. It was a botnet of millions of IoT devices which an attacker had control over.

To get control of all these IoT devices, infected devices were scanning the Internet to find other devices. If a targeted device responded to the probe, the malware would try to log into them by brute forcing authentication using a list of 60 default passwords (such as: 1111, 6666, password, admin, guest) and usernames (mainly root, admin).

To grasp how widespread default passwords are, one can take a look at publicly available repositories of default passwords, for example: https://many-passwords.github.io/

What is the ETSI EN 303 645 standard?

To address cybersecurity concerns in consumer IoT devices, the ETSI EN 303 645 cybersecurity standard was launched to provide a comprehensive set of provisions for device manufacturers – and the industry at large – to strengthen cybersecurity for these devices. The standard also serves as a basis for certification of IoT products.

Containing 13 sections, it is a globally applicable cybersecurity norm for consumer IoT devices covering security needs of equipment, communication and personal data protection. The first section on the list covers the use - or rather misuse - of weak passwords.

What can be done about weak or universal default passwords?

The first section stated in the ETSI EN 303 645 cybersecurity standard is that no universal default passwords shall be used. According to this standard, the following shall apply for consumer IoT product passwords:

- Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.
- Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.
- Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.

- Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.
- When the device is not a constrained device, it shall have a mechanism available which makes brute force attacks on authentication mechanisms via network interfaces impracticable.

From a reading of the provisions, we can see that it rules out using passwords that can be easily guessed or hacked by brute force, while also calling for ways to allow users to change authentication passwords.

About TÜV SÜD and ETSI EN 303 645 testing

Consumers are increasingly paying attention to cybersecurity for their consumer IoT devices. Device manufacturers can provide great confidence and reassurance to consumers when making purchases by certifying their products under the ETSI EN 303 645 standard.

One way to do so for manufacturers is by working with organisations such as TÜV SÜD for their ETSI EN 303 645 testing and certification.

TÜV SÜD experts are very familiar with the cyber fraud and data privacy regulations in specific markets and have a deep understanding of the cyber threat field, working with customers around the world to fully unlock the potential of the digital future.

Cybersecurity and data protection are one of our core capabilities. From product design, manufacturing to operations, we provide you with professional support at every step to reduce the cybersecurity and data privacy disclosure risks.

Learn more about our ETSI EN 303 645 testing and certification services here: https://www.tuvsud.com/en/industries/consumer-products-and-retail/consumer-iot-cybersecurity/etsi-en-303-645-testing

About the Author

Maxime Hernandez, IoT Cybersecurity Expert & Lead Process Engineer, TÜV SÜD. Maxime is a mechatronics engineer. He started his career in software development for the transportation industry in Europe. He is currently based in China, bringing solutions to European vendors and Asian manufacturers for consumer products.

Maxime can be reached online at Maxime.Hernandez@tuvsud.com and at our company website https://www.tuvsud.com/

What Role Can AI Play in Threat Detection and Violence Prevention?

By Brian Sathianathan, Chief Technology Officer at Iterate.ai

The frightening rise in mass shooting incidents—now sadly occurring at a rate of more than two per day in 2022—demands thoughtful and effective changes. Certainly, new public policies and broad societal transformation are needed to address this troubling issue at its roots. But the most realistic expectation is that those shifts will be slow, and these terrible incidents will continue to occur.

Artificial intelligence may represent one of the most immediately applicable paths for reducing the risks of physical harm during potential violent incidents. Numerous technology companies are now developing powerful applications with threat response capabilities for stores, malls, schools, public gatherings, places of business, and other at-risk locations.

These security applications can utilize an organization's existing security cameras positioned on the outside of buildings, in parking lots, or at other high-traffic locations, and combine that visibility with AI-based image recognition and machine learning algorithms. The resulting solutions provide fully automated identification of individuals carrying firearms or other weapons, or even those demonstrating aggression or suspicious behaviors recognized as precursors to violence.

For example, consider a scenario in which a person drives into a parking lot, steps out of their vehicle, and approaches a store with guns and knives concealed under their clothing. Security cameras positioned in the parking lot offer a view of this individual, but even experienced human security personnel viewing the footage may not be able to recognize the hidden weapons. However, the AI application is able to identify distinctive patterns that the human eye cannot, understand the danger, and proactively implement preset safety protocols. Store personnel receive alerts, immediately lock down the store and contact the police, and take further measures to protect the safety of shoppers. The predictive physical threat detection and prevention in this scenario have the potential to stop violent incidents before they begin.

The AI technology behind this real-time threat recognition capability isn't some long-off prospect in the research phase, it's available and scaling today. Startups and other providers in this AI threat detection and prevention space are seeing quick growth—and an equally fast rise in attention from venture capital firms along with increased M&A activity. Providers are now focused on training their AIs to respond to all of the threats that may occur at the types of locations they'll be used to secure and protect.

In practice, this means performing AI object detection training and making algorithms study security footage to recognize threats in context. These algorithms must be ready to deliver instant and accurate decisions across countless scenarios where a human couldn't, from identifying multiple armed subjects at once to spotting dangerous individuals within crowded environments.

Stores and places of business have an obligation to protect customers and employees at their locations. Public sector entities such as schools and organizations operating public gatherings are equally eager to implement more effective protections and achieve greater peace of mind. While security camera systems and AI technology have largely been invisible to the average person in such settings (with AI powering customer recommendations and backend capabilities behind the scenes), these new safety solutions will likely have a highly visible role in communicating the commitments to safety they represent.

Brands and public leaders can publicize and demonstrate the safety they're able to provide by adding AI-based applications to their security protocols. Retail store brands, for example, know that customers are deterred from visiting locations where they aren't absolutely assured of their safety. AI-powered threat prevention technology helps earn that customer comfort and confidence.

AI threat prevention will continue to advance, and I expect it to play a large role in the multi-faceted change we need to ensure security outside of the home. Today, applications offer the relatively easy entry of utilizing existing security camera systems. Tomorrow, organizations will likely upgrade to wireless and IP-based cameras able to interface directly with AI systems, and add thermal imaging and further hardware-based advantages to increase effectiveness. There's a long way to go, to be sure, but AI will be a big part of the answer.

About the Author

Brian Sathianathan is the Chief Technology Officer at Iterate.ai, where he leads the development of the company's low-code platform, Interplay. Previously, Sathianathan worked at Apple on various emerging technology projects that included the Mac operating system and the first iPhone.


EVENTS

CYBER DEFENSE CONFERENCES

THREE EVENTS IN ONE

Orlando, Florida, USA | October 27-28, 2022

One of the most exclusive, fun and educational CISO conferences of the year!

Limited to our selection of the top 100 CISOs in the world, amazing speakers and insider threat mitigation training by a world reknown expert - meets 100 top cyber defense companies in an intimate, high value two day summit

www.cyberdefenseconferences.com

CYSEC SAUDI

04 OCTOBER 2022

DAMMAM, SAUDI ARABIA

JOIN US IN-PERSON

SECURING KINGDOM'S CRITICAL INFRASTRUCTURE IN THE NEWLY CONNECTED WORLD

SPONSORS

PLATINUM SPONSOR

SITE
الشركة السعودية لتقنية المعلومات
Saudi Information Technology Company

GOLD SPONSOR

iTalent

ORGANIZED BY

MAK

ENERGIA MIDDLE EAST

saudi.cysecglobal.com

NORDIC CYBER SUMMIT

4th - 5th October 2022

Copenhagen, Denmark

Join Free With Code: CDM-VIP

Join Us at the Nordic Cyber Summit Summit on 4th - 5th October!

The 4th annual **Nordic Cyber Summit** brings together **120+ IT security leaders** from across the **Retail, FMCG, Banking & Finance, Automotive, Utilities, Food & Beverage industries** for 2-days of insight building and expert knowledge exchange on **4th - 5th October.** Join us in **Copenhagen, Denmark** to hone your skills in areas including:

- *Staying Ahead of an Evolving Threat landscape*
- *Working with Third Parties*
- *Revamping Your Cyber Security Approach*
- *Migrating to the Cloud*
- *Ransomware: Reducing Risk and Incident Response*
- *The Human Factor in Cyber Security*
- *And, more!*

CPD CERTIFIED
The CPD Certification Service

Speakers include CISOs, VPs, Heads of IT Security at: **Carlsberg, Danske Bank, Velliv, Total, Nomeco, Orkla** and more...

Jarkko Rautula
CSO
TOMTOM

Duong Anders Le
CISO
JYSKE BANK

Moon Carlbring
CISO
Region Västmanland

Predrag Gaiki
Deputy CISO/DPO
QLIRO

Stale Risem-Johansen
CISO
SpareBank 1

Anne Hännikäinen
CISO
IKEA

Geir Arild Engh-Hellesvik
CISO
VY

Tobias Ander
Deputy CISO, Security Expert
ÖREBRO

Ingegerd Wirehed
Head of Hotels IT Security
LUNDS UNIVERSITET

Mikael Nyman
Head of IT Security
Länsförsäkringar

This is a one-of-a-kind opportunity for cyber security leaders across the Nordic region to come together and safeguard their assets. View the agenda & **secure your place for FREE** using the discount code: **CDM-VIP** at: **nordic.cyberseries.io/register/** T&Cs apply.

CYBER SECURITY & CLOUD CONGRESS

NORTH AMERICA

5-6 October 2022
Santa Clara
Convention Center

We're Back!
Join Us Live & In-Person

The Cyber Security & Cloud Expo will host two days of top-level content and thought leadership discussions around Cyber Security & Cloud, and the impact they are having on industries including government, energy, financial services, healthcare and more.

8 Conference Tracks

250+ Speakers

150+ Exhibitors

6 Co-Located Events

6,000+ Attendees

Speakers include:

Kavitha Venkataswamy
Senior Manager - Product Security
Capital One

Michael Fulton
Adjunct Faculty
The Ohio State University

Elizabeth Cartier
Director - Information Security
Headspace Inc.

Register now for free tickets!

> www.**cybersecuritycloudexpo**.com/northamerica
> enquiries@techexevent.com

GITEX GLOBAL

NEW GLOBAL DEV SLAM

عالم الذكاء الاصطناعي EVERYTHING

NORTH STAR DUBAI
INSPIRED BY GITEX GLOBAL

Fintech SURGE. فينتك سيرج

FUTURE BLOCKCHAIN SUMMIT
قمة مستقبل البلوك تشين

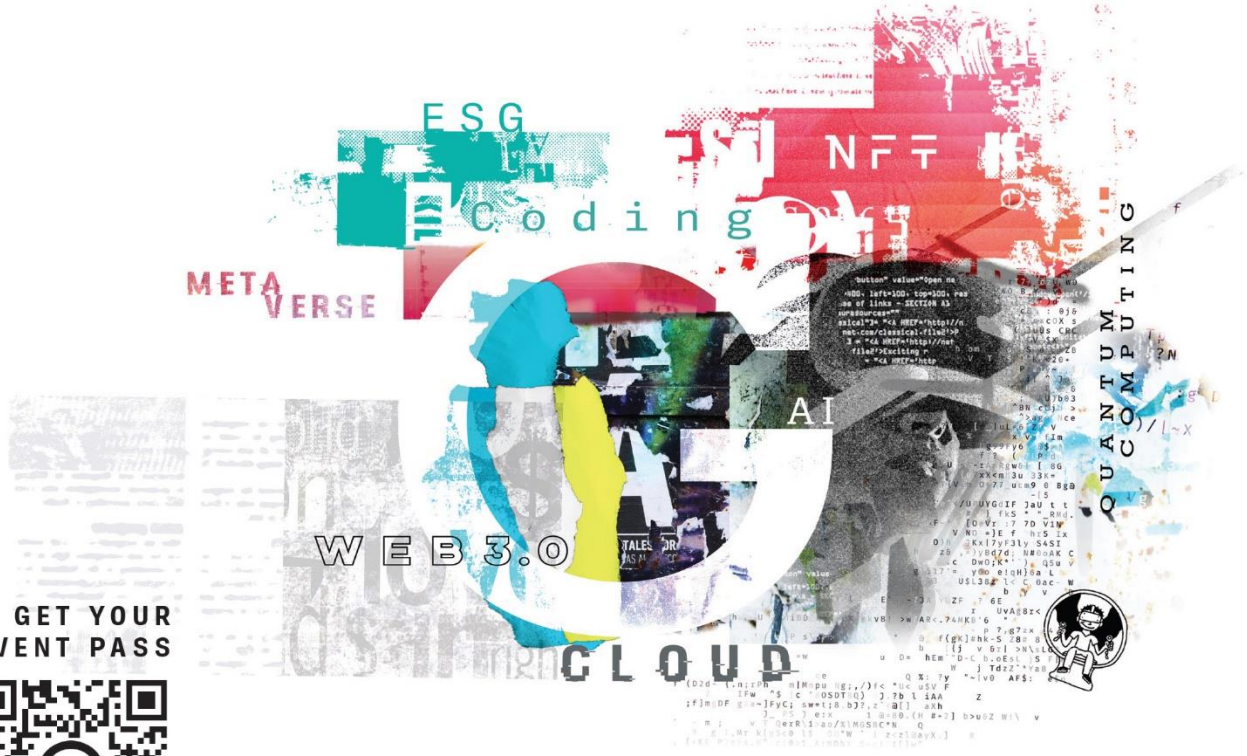
NEW XVERSE

ماركتنغ مينيا Marketing Mania

10-14 OCT 2022 DUBAI WORLD TRADE CENTRE

SHOW TIMINGS: 10 Oct - 11am to 5pm | 11 - 14 Oct - 10am to 5pm

THE WORLD'S LARGEST & MOST INFLUENTIAL TECH + STARTUP EVENT



GET YOUR EVENT PASS

Believe the hype, it's here.

ENTER THE NEXT DIGITAL UNIVERSE

DIAMOND SPONSOR

HUAWEI

TECHNOLOGY & DIGITAL PARTNER

TECH & DIGITAL
A NEOM COMPANY

PLATINUM & LANYARD SPONSOR

TII Technology Innovation Institute

GOLD SPONSOR

ERICSSON

GOLD SPONSOR

e&

SILVER SPONSOR

ManageEngine
a division of Zoho Corp.

INNOVATION PARTNER

@ DUBAI INTERNET CITY

CONNEXIONS LOUNGE SPONSOR

TECH dem NATION PAKISTAN

MAJLIS LOUNGE SPONSOR

midis GROUP

ATTENDEES BADGE SPONSOR

VINFAST

GLOBAL DEV SLAM

10-13 OCT 2022
DUBAI WORLD TRADE CENTRE

X GITEX GLOBAL

Supported by
مقر المبرمجين
coders(hq)

Featuring the inaugural
python powered
PYCONMEA

POWERING CODING INGENUITY

THE WORLD'S LARGEST MEET UP FOR THE DEVELOPER & CODING COMMUNITY

TECH PIONEERS ON STAGE

Travis Oliphant
Creator of NumbPy & Co-Founder
ANACONDA. USA

Sebastian Ramirez Montano
Creator
FastAPI Germany

Ketan Umare
Co-Creator of Flyte, Co-Founder & CEO
UNION USA

Pablo Galindo Salgado
Physicist & Software Engineer - R&D Python Infrastructurea
Bloomberg UK

DON'T MISS OUT, GET YOUR DELEGATE PASS

For delegate group booking, call Fahad Khalife at:
+971 4 308 6805 | globaldevslammarketing@dwtc.com

GLOBALDEVSLAM.COM
#GLOBALDEVSLAM

Founding Partners: Microsoft | ORACLE | Red Hat

Gold Sponsor: TECH & DIGITAL A NEOM COMPANY

Silver Sponsor: OVERCOM SOFTWARE DESIGN

BENELUX CYBER SUMMIT

11th - 12th October 2022

Amsterdam, Netherlands

Join Free With Code: CDM-VIP

Join Us at the Benelux Cyber Summit Summit on 11th - 12th October!

The 3rd annual **Benelux Cyber Summit** brings together **100+ IT security leaders** from across the **Retail, FMCG, Banking & Finance, Automotive, Utilities, Food & Beverage industries** for 2-days of insight building and expert knowledge exchange on **11th - 12th October**. Join us in **Amsterdam, Netherlands** to hone your skills in areas including:

- *Balancing the business's push for digitalisation with cyber security needs*
- *Devising modern supply chain security strategies*
- *Strategies to enhance the responsiveness to attacks and their mitigation*
- *Managing risk in an evolving threat environment*
- *Updating security to work cross-functionally in order to secure the supply chain*
- *How to monitor data security in the cloud and address compliance management challenges*
- *And, more!*

CPD CERTIFIED
The CPD Certification Service

Speakers include CISOs, VPs, Heads of IT Security at: **Amazon, RTL, Philips, PayPal, Volvo Financial Services** and more...

Jacques Federspiel
CISO
HÔPITAUX ROBERT SCHUMAN

Victoria van Roosmalen
CISO & DPO
COOSTO

Haissam Hariz
Deputy CISO
NIBC

Stanislav Sobolevsky
CISO
OMP.

Steffen Minkmar
Sr Head, IT Security Unit
European Investment Bank

Rick Veenstra
Sr Advisor IT Risk & Security
isala

Andre Adelsbach
VP, Group Information and Cyber Security
SES

Stella Dineva
IT Security Architect
ucb

Filip Nowak
Global Head of Cyber Defence
FERRERO

Fred Jekel
Executive Director Cyber Security
VAN LANSCHOT KEMPEN

This is a one-of-a-kind opportunity for cyber security leaders across Benelux to come together and safeguard their assets. View the agenda & **secure your place for FREE** using the discount code: **CDM-VIP** at: **benelux.cyberseries.io/register/** T&Cs apply.

Industrial Transformation ASIA-PACIFIC

Asia-Pacific's Leading Trade Event for Industry 4.0

18-20 October 2022
Singapore EXPO

www.industrial-transformation.com

We help companies in Asia-Pacific to **START, SCALE** and **SUSTAIN** their business transformation journey

CONNECT WITH US • CONNECT WITH ASIA-PACIFIC

Register now to attend in-person at **Singapore EXPO**

INDUSTRY 4.0 FOR BUSINESS SUSTAINABILITY

Themed 'Industry 4.0 for Business Sustainability', the 5th edition of the Industrial Transformation ASIA-PACIFIC - a HANNOVER MESSE event (ITAP) happening on 18-20 October 2022 will deep dive into trends and developments in three key dimensions i.e. Digitalisation, Talent & Workforce Development, and Environmental Sustainability, which influences the magnitude of sustainable business development for advanced manufacturing and its related sectors locally, regionally and globally.

An Event Of

constellar

International Partner

Deutsche Messe

a HANNOVER MESSE event

Industrial Transformation ASIA-PACIFIC

EURONAVAL

THE WORLD NAVAL DEFENCE EXHIBITION

28th edition

18 21 OCTOBER 2022

PARIS LE BOURGET

euronaval.fr

GOVWARE

ASIA'S PREMIER CYBERSECURITY EVENT RETURNS!

Join **10,000 government and private sector participants from APAC and beyon**d at GovWare 2022 this October in Singapore.

Put your finger on the pulse of Asia's cybersecurity landscape and global issues from **over 70 expert-led keynotes and track sessions**. Explore cutting-edge technologies at the leading pure-play cybersecurity exhibition, showcasing **300+ exhibitors and partners**.

Members of Cyber Defense Magazine **enjoy S$200 off GovWare Conference Pass**! Use **promo code GWxCDM** when you register. Limited to the first 200 registrations using this promo code. Register now at **www.govware.sg**.

REGISTER NOW

GOVWARE 2022

CONFERENCE AND EXHIBITION
18-20 OCTOBER 2022
SANDS EXPO AND CONVENTION CENTRE, SINGAPORE

A PART OF SINGAPORE INTERNATIONAL CYBER WEEK 2022

الشرطة المجتمعية
Community Police

20 October 2022 | Madinat Jumeriah Hotel, Dubai, UAE

Hosted by: شرطة دبي DUBAI POLICE **INVITES YOU TO PARTICIPATE**

Community policing plays a crucial role in ensuring security and maintaining a stable environment for economic growth and prosperity. Through strong partnerships and collaboration with community key persons and active groups, Dubai police forces can gather valuable insights and proactively prevent imminent threats that can affect individuals and businesses.

WHO WILL ATTEND

- CEO's
- Managing Directors
- General Managers
- Security Directors & Managers
- Project Managers
- Engineering & Operations Managers
- IT & Cyber Security Managers
- University Deans & School Principles
- Security Consultants

ORGANIZATIONS

Residential community
(Facility management companies, residentials compounds, towers, villas, apartments, etc.)

Commercial community
(Free zones, ports, airports, etc.)

Home-owner associations and communities

Academia community
(Schools, universities, institutes, etc.)

Entertainment and leisure community
(Malls, theme parks, public parks, hotels, gyms, etc.)

INTERESTED IN FINDING OUT MORE ABOUT HOW YOU CAN PARTICIPATE?

Email us directly at **partnerships@gmevent.ae** or call **+971 52 969 7209** and a member of the team will be happy to help.

visit: communitypoliceconference.com

SCAN THE QR CODE TO LEARN MORE

CYSEC UAE

SUPPORTED BY

هيئة أبوظبي الرقمية
ABU DHABI DIGITAL AUTHORITY

OFFICIAL GOVERNMENT SUPPORTING PARTNER

شرطة أبوظبي
ABU DHABI POLICE

1 - 2 NOVEMBER 2022

JOIN US IN-PERSON, ABU DHABI, UAE

Accelerating UAE's Digital Transformation with Next-Gen Cyber Resilience

Asma Al Yassi
Cyber Security Governance
Confidential

Dr. Lt. Col. Hamad Khalifa Al Nuaimi
Head of Telecommunications Division, Information Technology Center
Abu Dhabi Police General Head Quarter

Dr. Ebrahim Al Alkeem
Digital Transformation
Cyber Security
Artificial Intelligence
Expert Director
Government of Abu Dhabi (UAE)

Eng. Ahmed Sherif
Senior IT Support Engineer & Cloud Solutions Expert
Abu Dhabi Digital Authority – UAE

Mohammed Darwish Azad
Chief Information Security Officer
Emirates NBD

Bader Husni Zyoud
Senior Information Security Risk Management Specialist & Incidents Manager
Central Finance Department, Government Entity

Hala ElGhawi
Sr. Information & Cyber Security Risk Manager
Standard Chartered Bank

Jeevan Badigari
CISO
DAMAC Properties

Ellis Wang
Board Of The Executive & Advisory Team
The Private Office of Sheikh Saeed bin Ahmed Al Maktoum

Omar Osman
Information Security Officer
Malaffi (Abu Dhabi Health Information Exchange)

Taha Hussain
Specialist Information Security
DEWA (Dubai Electricity & Water Authority)

Shafiullah Ismail
Vice President & Head - Cyber Security and Risk
Mubadala Capital

Malak Trabelsi Loeb
Director of Corporate Global Affairs
Cyber Security Global Alliance

Munther Bin Amr
Director of ICT
Abu Dhabi Quality and Conformity Council

Khawla Al Badi
Head of Innovation and Technology
Etihad Airways

OFFICIAL MEDIA PARTNER

Industry Events

MEDIA PARTNERS

SECURITY MIDDLE EAST — THE MAGAZINE FOR SECURITY AND SAFETY PROFESSIONALS

CYBER DEFENSE MAGAZINE — WHERE INFOSEC KNOWLEDGE IS POWER

GlobalRisk Community

OXFORD BUSINESS GROUP

INTERNATIONAL BUSINESS MAGAZINE

JUMPSTART

TECH OUTLOOK CIO

ICOHOLDER

ORGANIZED BY

MAK

uae.cysecglobal.com

DIGITAL TRANSFORMATION KUWAIT

ACHIEVING 2035 VISION THROUGH DIGITAL TRANSFORMATION

02 – 03 NOVEMBER 2022

JUMEIRAH MESSILAH BEACH HOTEL & SPA - KUWAIT

IN COLLABORATION WITH:

Central Agency for Information Technology

With digital transformation as a key pillar for Kuwait Vision 2035, the country is focusing on adopting smart and digital technologies to innovate its services, drive the economy, and improve quality of life, while increasing operational efficiency and performance of key sectors. This goal has pushed for greater investment in Kuwait's ICT market which is expected to reach 10B USD by 2024 (Global Data).

EVENT IN NUMBERS

250+ ATTENDEES

150+ SENIOR DECISION MAKERS

25+ SPEAKERS

20+ MEDIA PARTNERS

30+ SPONSORS & EXHIBITORS

INTERESTED IN FINDING OUT MORE ABOUT HOW YOU CAN PARTICIPATE?

Email us directly at **partnerships@gmevent.ae** or call **+971 52 969 7209** and a member of the team will be happy to help.

WWW.DIGITALTRANSFORMATIONKUWAIT.COM

ORGANIZED BY:

GM EVENTS

SCAN THE QR CODE TO LEARN MORE

6th Edition

CONNECTED BANKING

West Africa

formerly (Africa DIGITAL BANKING SUMMIT - Innovation and Excellence Awards)

November 15th - 16th, 2022

Join Us In Person

Accra, Ghana

Conceptualized and Organized by ICSA

For More Info Log into:

www.connected-banking.com

AVAR 2022

25th International Conference

CYBERSECURITY COUNTER PUNCH

1ST- 2ND DECEMBER 2022 | SINGAPORE

AVAR 2022 HIGHLIGHTS

45+ Presentations	60+ Speakers	3 Panel Discussions
CISO Connect	CISO Awards	200+ Delegates

Insight From

Avast | Cisco | Check Point | Cybereason | Deep Instinct | Dragos | ESET
Fortinet | Intego | K7 Computing | Microsoft | NortonLifeLock | SANDS Lab
SentinelOne | Sophos | Trend Micro | Trustwave

Register for AVAR 2022 at
https://aavar.org/cybersecurity-conference/

AVAR 2022 is Supported By

LEVELLING UP UK CYBER SECURITY

We believe there is a knowledge gap between the expertise of the cyber community and UK business leaders.

We want to close that gap.

Contribute to the programme by visiting www.ukcyberweek.co.uk/call-for-papers.

OUR PARTNERS

IASME CONSORTIUM

Chartered Institute of Information Security

CREST

UK CYBERWEEK

3 ›› 4 NOVEMBER 2022

Business Design Centre | London

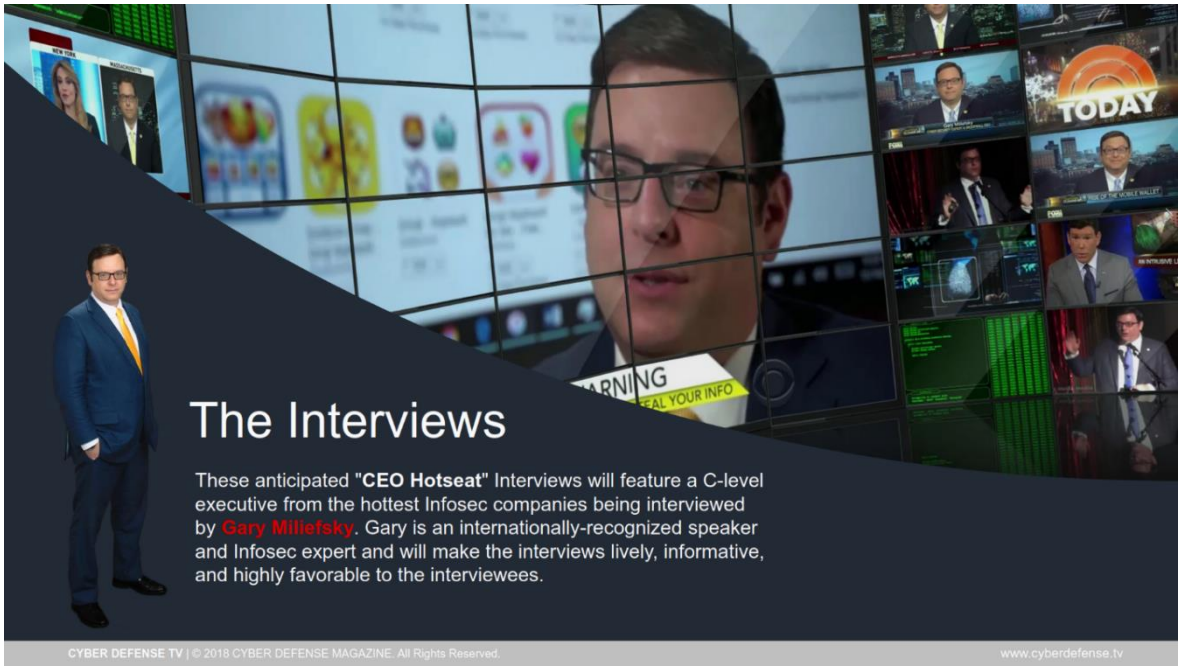
CYBER DEFENSE TV

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.

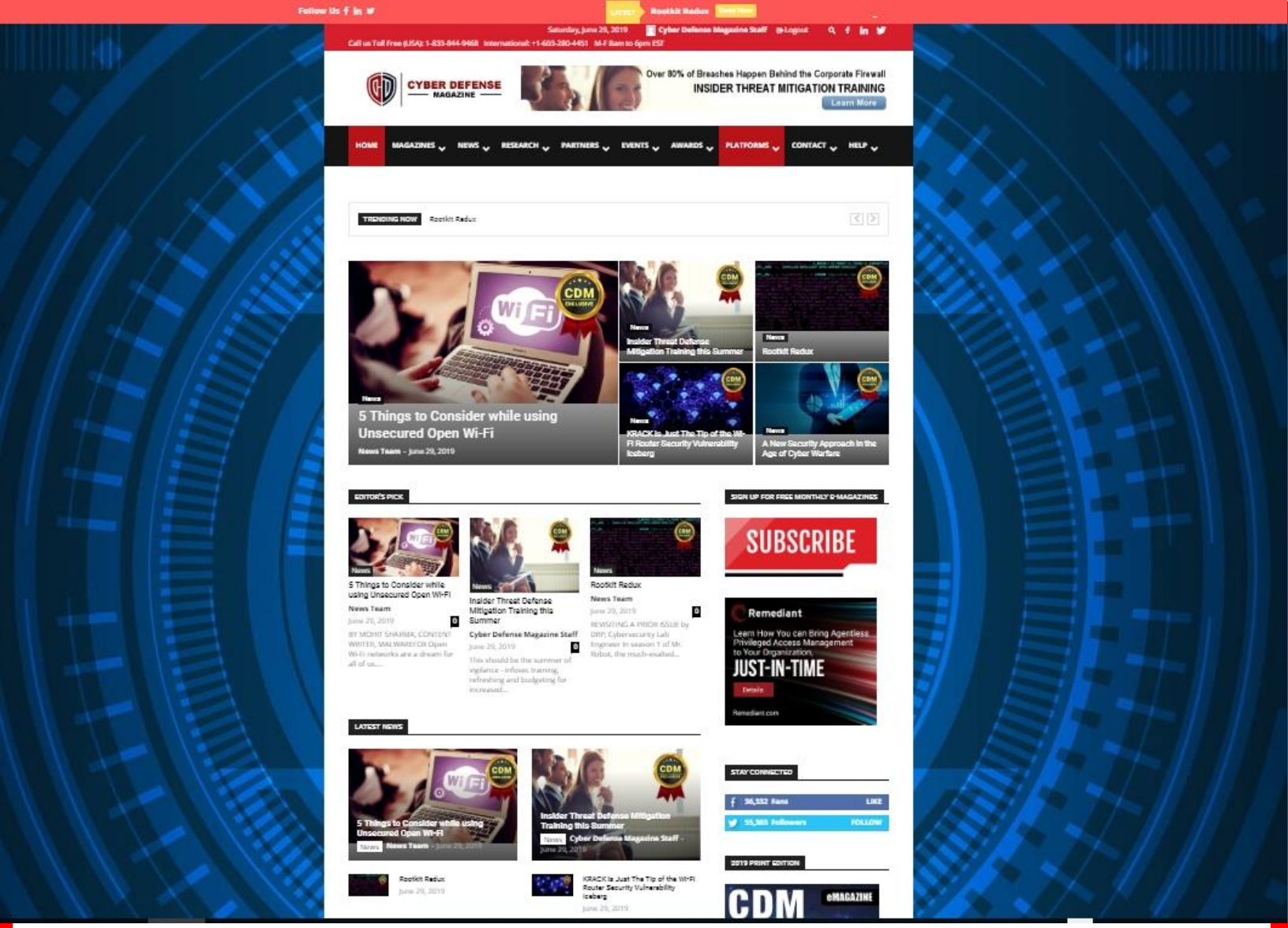
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 10/03/2022



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...*

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.**