Top 10 Big Little Sins about the Infrastructure Security: On Premise & In the Cloud

Paula Januszkiewicz

OWASP Aarhus Chapter Meeting - November

COURE

Top 10 Big Little Sins about the Infrastructure Security:

On Premise & In the Cloud

Paula Januszkiewicz

CQURE: CEO, Cybersecurity Expert, Penetration Tester

CQURE Academy: Trainer

Microsoft MVP on Cloud and Datacenter Management

Microsoft Regional Director

paula@cqure.us

@PaulaCqure @CQUREAcademy

www.cqureacademy.com

CQURE


Featured TechEd 2012 Speakers
More featured speakers →
Wally Mead
John Craddock
Mark Russinovich
Paula Januszkiewicz


Microsoft
CQURE ACADEMY©
We are proud to announce that
Paula Januszkiewicz
was rated as
No 1 Speaker
at Microsoft Ignite!!!
May 4-8, 2015
Chicago, IL


TechEd
Learn

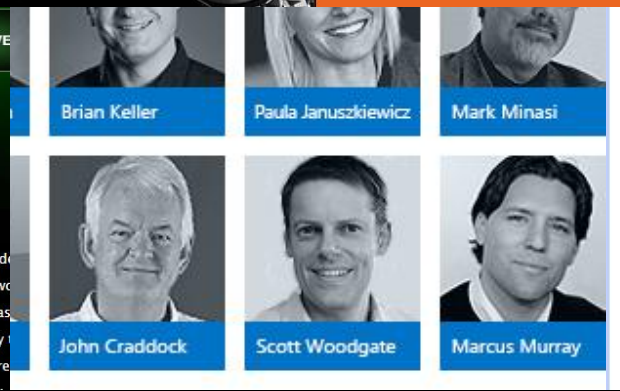

black hat
ASIA 2019
SPEAKER
SPEAKER

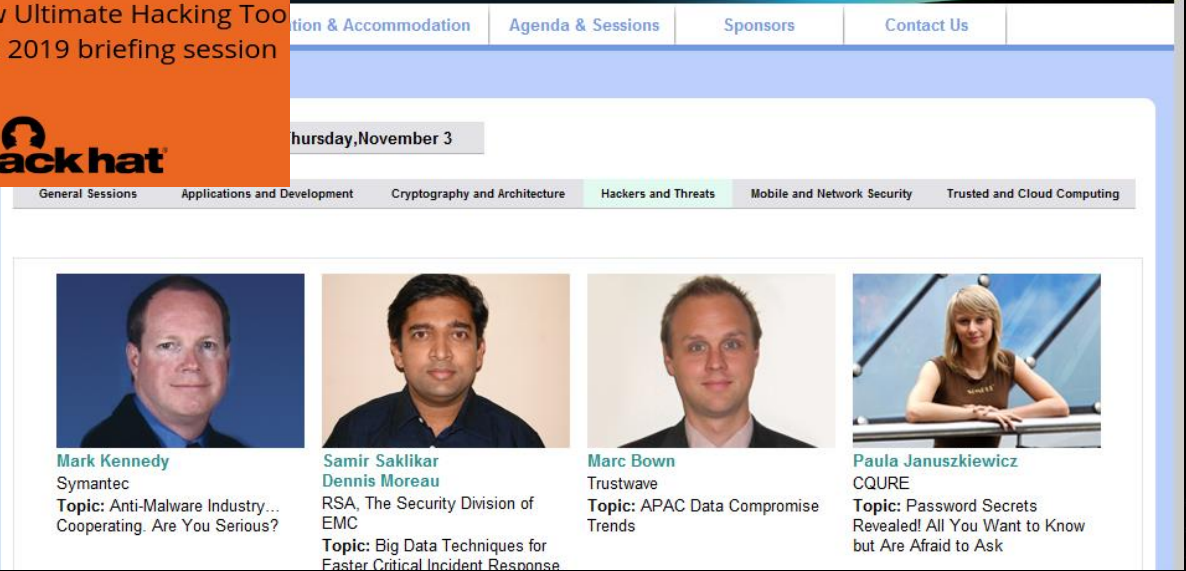

No.1
Speaker
Paula Januszkiewicz
CEO CQURE
She received
a "Best of Briefings" award at her
"CQTools: The New Ultimate Hacking Too
Black Hat Asia 2019 briefing session
black hat


black hat
USA 2017


Where The World
Talks Security
November 2 – 3
China World Hotel
Beijing, China
the adventures of
alice & bob


ATTEND
TRAININGS
BRIEFINGS
ARSENAL
FEATURES
SCHEDULE
SPECIAL EVE
SEE ALL PRESENTERS
SPEAKER
PAULA JANUSZKIEWICZ
CQURE INC.


Brian Keller
Paula Januszkiewicz
Mark Minasi
John Craddock
Scott Woodgate
Marcus Murray


Tuesday,November 3
General Sessions
Applications and Development
Cryptography and Architecture
Hackers and Threats
Mobile and Network Security
Trusted and Cloud Computing
Mark Kennedy
Symantec
Topic: Anti-Malware Industry... Cooperating. Are You Serious?
Samir Saklikar
Dennis Moreau
RSA, The Security Division of EMC
Topic: Big Data Techniques for
Marc Bown
Trustwave
Topic: APAC Data Compromise Trends
Paula Januszkiewicz
CQURE
Topic: Password Secrets Revealed! All You Want to Know but Are Afraid to Ask

What does CQURE do?

1. Consulting Services:

- Extensive IT Security Audits and Penetration Tests of all kinds,
- Configuration Audit and Architecture,
- Design Social Engineering Tests,
- Advanced Troubleshooting and Debugging,
- Emergency Response Services

2. R&D & CQLabs Tools & Hacks Publications

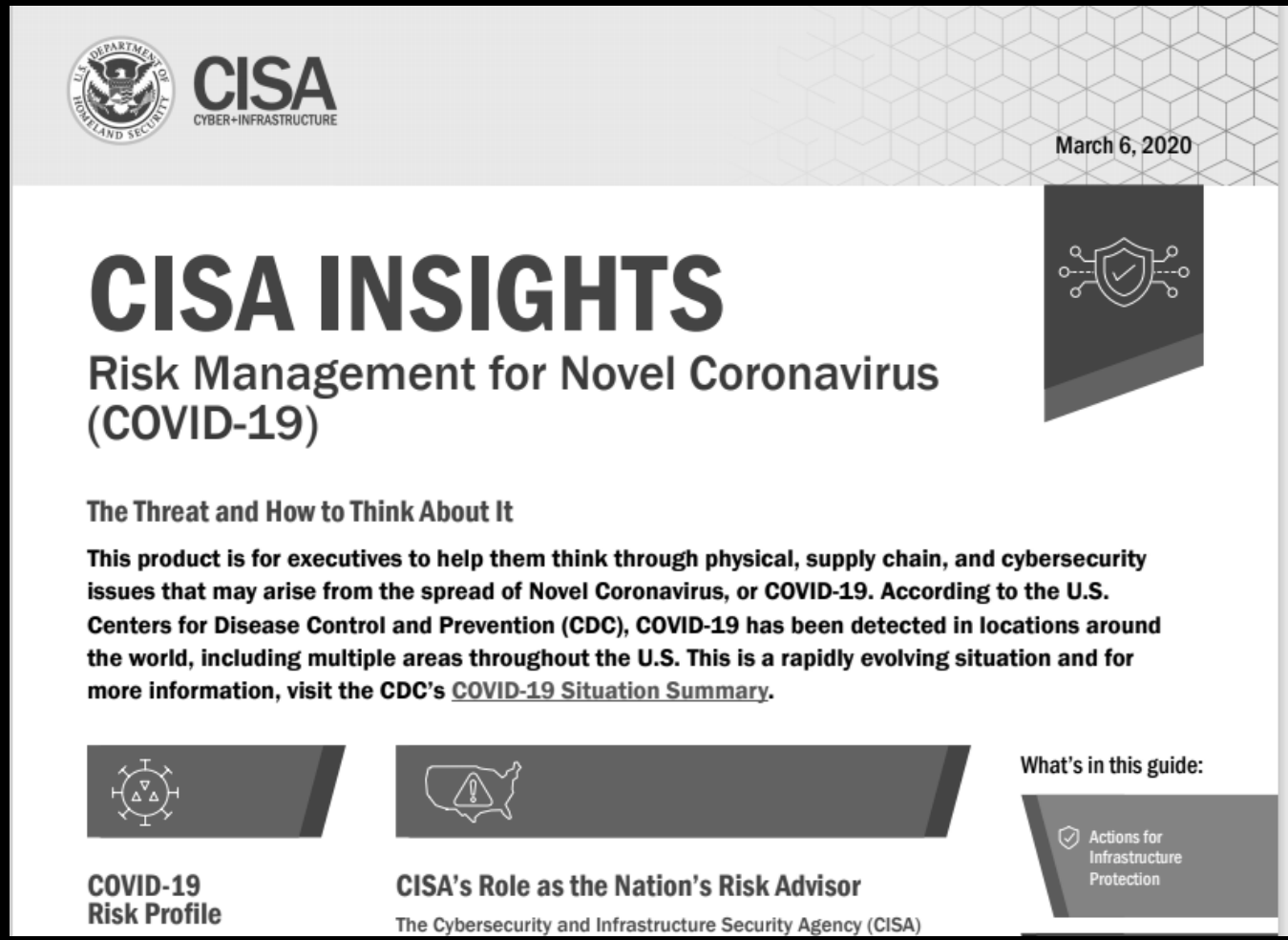
3. Trainings & Seminars:

- Offline (mainly in New York or via our partners worldwide),
- Online


Adrianna
Doris
Kama
Artur
Liza
Paula
Mike
Krystian
Mariusz
Dominika
Adrian
Łukasz
Antoni
Ken
Janusz
Kacper
Ernest
Michal
Ola
Aga
Ula
Grzegorz
Adrian
Milosz
Michael
Matus
Kamil
Piotr
Tomasz
RSA CONFERENCE
HACKER FEST
Microsoft tech·days
Hacker Halted
TecHFuse
Microsoft Technology Summit
black hat
TechEd Microsoft
nordic infrastructure conference
cyberday
Microsoft Ignite
UTmessan.
SC MAGAZINE
COURE

The Impact of Cybercrime

Cybersecurity and Infrastructure Security Agency (CISA) encourages organizations to adopt a heightened state of cybersecurity.



CISA
CYBER+INFRASTRUCTURE

March 6, 2020

CISA INSIGHTS

Risk Management for Novel Coronavirus (COVID-19)

The Threat and How to Think About It

This product is for executives to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19. According to the U.S. Centers for Disease Control and Prevention (CDC), COVID-19 has been detected in locations around the world, including multiple areas throughout the U.S. This is a rapidly evolving situation and for more information, visit the CDC's COVID-19 Situation Summary.

What's in this guide:

- Actions for Infrastructure Protection

COVID-19 Risk Profile

CISA's Role as the Nation's Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA)

Australia's federal government plans to invest A$1.35 billion in cybersecurity over the next decade.

Deloitte–NASCIO Cybersecurity Study

The US federal government's demand for vendor-based information security products and services is expected to increase from US$11.9 billion in FY2019 to US$15.4 billion in FY2024, growing at a compound annual growth rate of 5.3%.

Deloitte–NASCIO Cybersecurity Study

Impactful Hacking Stats for 2020

70%

of breaches were caused by outsiders

17%

of breaches involved some form of malware

22%

of breaches featured phishing or social engineering

86%

of breaches were financially motivated

Source: Verizon's 2020 Data Breach Investigations Report (DBIR)

Since COVID-19, the US FBI reported a 300% increase in reported cybercrimes

"THERE ARE TWO KINDS OF BIG COMPANIES, THOSE WHO'VE BEEN HACKED, AND THOSE WHO DON'T KNOW THEY'VE BEEN HACKED."

-JAMES COMEY, FORMER FBI DIRECTOR

200+

Median number of days attackers are present on a victims network before detection

80

Days after detection to full recovery

$3 Trillion

Impact of lost productivity and growth

$3.9 Million

Average cost of a data breach (15% YoY increase)

Remote work by the numbers

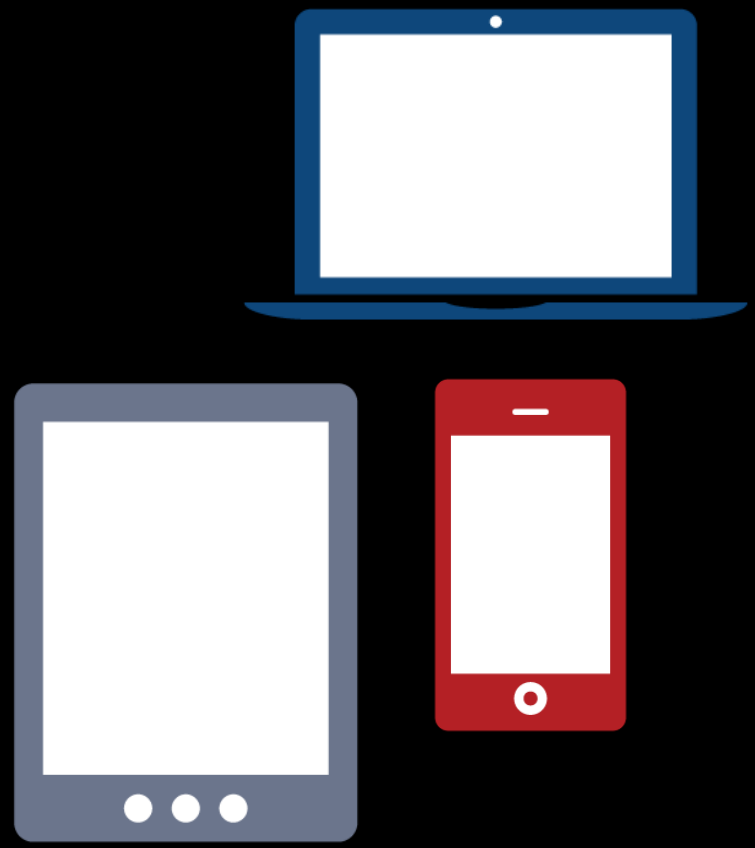
PEOPLE WILL USE THEIR PERSONAL MOBILE DEVICES ON THE JOB, REGARDLESS OF WHETHER THEIR ORGANIZATION HAS A FORMAL 'BYOD' POLICY

Use a personal electronic device for work-related functions **81%**

Connect to a company via a free or public wi-fi connection **31%**

Who use a personal electronic device for work-related functions say their company has not implemented a BYOD policy **66%**

Who use a personal device for work let someone else use it **46%**



SOURCE: ESET, Harris Interactive

Top 10 Biggest Threats When Working From Home

#1 Disabling firewall

- Key learning points:
  - Windows Firewall is often misconfigured
  - Firewall is a great segmentation tool
  - You can allow only certain processes to communicate with the Internet or locally
  - No need-to-know processes to block them, you can operate on the services list

DEMO: Initial Access Privilege Escalation

#2 Overly simple passwords and security questions

- Key learning points:
  - Passwords are almost always re-used
  - There is almost always (ekhm… always) some variant of the company name with some number (year, month etc.)
  - It's highly reasonable to check for obvious passwords and continuously deliver security awareness campaigns

DEMO: Untrusted Networks

#3 No network segmentation

- Key learning points:
  - Network segmentation can be a blessing or a curse
  - Greater control over who has access to what
  - Allows rules to be set to limit traffic
  - Allows exposure to security incidents to be reduced
  - Performance: allows Broadcast Domains to be reduced so that broadcasts do not spread on the entire network

DEMO: VPN Pivoting

#4 Lack of Server Message Block Signing (or alternative)

- Key learning points:
  - Set Service Principal Names (SPN) for services to avoid NT LAN Manager (NTLM):
  - Reconsider using Kerberos authentication all over
  - https://technet.microsoft.com/en-us/library/jj865668.aspx
  - Require SPN target name validation
  - Microsoft network server: Server SPN target name validation level
  - Reconsider turning on SMB Signing
  - Reconsider port filtering
  - Reconsider code execution prevention but do not forget that this attack leverages administrative accounts

DEMO: SMB Relay

#5 Allowing unusual code execution (1/2)

- Key learning points:
  - Common file formats containing malware are:
  - .exe (Executables, GUI, CUI, and all variants like SCR, CPL etc.)
  - .dll (Dynamic Link Libraries)
  - .vbs (Script files like JS, JSE, VBS, VBE, PS1, PS2, CHM, BAT, COM, CMD etc.)
  - .docm, .xlsm etc. (Office Macro files)
  - .other (LNK, PDF, PIF, etc.)

#5 Allowing unusual code execution (2/2)

- If SafeDllSearchMode is enabled, the search order is as follows:
  - The directory from which the application loaded
  - The system directory
  - The 16-bit system directory
  - The Windows directory
  - The current directory
  - The directories that are listed in the PATH environment variable

DEMO: Evilginx

#6 No whitelisting on board

- Key learning points:
  - Code execution prevention implementation is a must
  - PowerShell is an ultimate hacking tool, possible solutions: block it for users, use Just Enough Administration etc.
  - Verify where users have write access to: accesschk.exe –w .\users c:\windows
  - AppLocker can run in the audit mode
  - AppLocker is great but not with the default configuration

#7 Old protocols or their default settings

- Key learning points:
  - SNMPv3 addresses: user-based system for access control, a means to properly authenticate users, and a method for encrypting SNMP traffic between agent and host
  - SQL issues – TDS provides by default lack of encryption
  - ODBC Driver – check if it has a secure networking layer built into it

#8 Trusting solutions without knowing how to break them

- Key learning points:
  - The best operators won't use a component until they know how it breaks.
  - Almost each solution has some 'backdoor weakness'
  - Some antivirus solutions can be stopped by SDDL modification for their services
  - Configuration can be monitored by Desired State Configuration (DSC)
  - DSC if not configured properly will not be able to spot internal service configuration changes
  - Example: How do I get to the password management portal?

#9 Misusing service accounts + privileged accounts

- Key learning points:
  - gMSA can also be used for the attack
  - Service accounts' passwords are in the registry, available online and offline
  - A privileged user is someone who has administrative access to critical systems
  - Privileged users have sometimes more access than we think (see: SeBackupRead privilege or SeDebugPrivilege)
  - Privileged users have possibility to read SYSTEM and SECURITY hives from the registry

DEMO:
CQSecretsDumper

#10 Falling for hipster tools

- Key learning points:
  - Worldwide spending on information security is expected to reach $90 billion in 2017, an increase of 7.6 percent over 2016, and to top $113 billion by 2020, according to advisory firm Gartner
  - With increasing budget the risk of possessing hipster tools increases too – do we know where these tools come from and what are their security practices?
  - Lots of solutions where not created according to the good security practices (backup software running as Domain Admin etc.)
  - Each app running in the user's context has access to secrets

The 11 key cyber security questions (1/2)

- Do we treat cyber security as a business or IT responsibility?
- Do our security goals align with business priorities?
- Have we identified and protected our most valuable processes and information?
- Does our business culture support a secure cyber environment?
- Do we have the basics right? (For example, access rights, software patching, vulnerability management and data leakage prevention.)

The 11 key cyber security questions (2/2)

- Do we focus on security compliance or security capability?
- Are we certain our third-party partners are securing our most valuable information?
- Do we regularly evaluate the effectiveness of our security?
- Are we vigilant and do we monitor our systems and can we prevent breaches?
- Do we have an organized plan for responding to a security breach?
- Are we adequately resourced and insured?

Summary: Best Practices

- Continuous vulnerability discovery
- Configuration reviews
- Context-Aware Analysis
- Put on the Hacker's Shoes
- How can we know what to prevent if we do not know what is the threat?
- Prevention is the key to success
- Remediation and Tracking
- Prioritization

DOWNLOAD THE TOOLS

https://resources.cqureacademy.com/tools/

Username: student

Password: CQUREAcademy#123!

Visit our BLOG and discover more about cybersecurity solutions & tools:

https://cqureacademy.com/blog

Thank you!

COURE

Top 10 Big Little Sins about the Infrastructure Security:

On Premise & In the Cloud

Paula Januszkiewicz

CQURE: CEO, Cybersecurity Expert, Penetration Tester

CQURE Academy: Trainer

Microsoft MVP on Cloud and Datacenter Management

Microsoft Regional Director

paula@cqure.us

@PaulaCqure @CQUREAcademy

www.cqureacademy.com

CQURE