front

Germ Theory & Modern Information Security Threats

Why We are Entering the Age of Mandatory Cyber Hygiene

September 27, 2016

SCCE CEI Session 506 (IT Compliance Track)

Sheraton Grand Chicago

1 digicert

Your Presenters

Joe Grettenberger, CISA, CCEP
Risk and Compliance Manager
Workfront, Inc. -- joegrettenberger@workfront.com

Benjamin Wilson, JD, CISSP
VP Compliance & Vendor Relations
DigiCert, Inc. -- ben.wilson@digicert.com

2 digicert

What Does Hygiene Have to do with Cyber Security?

"...trust in our privacy and security is the oil that takes the friction out of human interaction in all its forms.."

Advancing the Dialogue on Privacy and Security in the Connected World, p.4

The Digital Equilibrium Project

"An ounce of prevention is worth a pound of cure."

Benjamin Franklin

"We have met the enemy and he is us."

Pogo

Walt Kelly

3 digicert

© 2015 Workfront. All rights reserved.

Outline

- How Germ Theory Relates to Information Security
- The Story of Ignaz Semmelweis
- Addressing Risk with Good Hygiene Habits
- Is there an equivalent to a “chlorine solution” for cyber attacks?
- Current Programs to Improve Cyber Hygiene
- Q&A

digicert

Cyber’s Interdisciplinary Vocabulary

- **Military/Combat/Espionage/Counter Terrorism** – TTPs, C&C, reconnaissance, harden, attack surface, exploit, vulnerability, pivot, payload, “kill chain”, (cyber) threat intelligence, back door, exfiltration
- **Law Enforcement/Detective Work/Forensics** – MMO, profiling, organized crime, black market, monitoring, surveillance, investigate, insider threat, root cause / analysis
- **Health Care/Medicine/Germ Theory** – boundary, virus, infection, hygiene, immunize, triage, patch, quarantine, containment, life cycles, eradication, health check-up, duty of care, first responder, preventative controls, survivability (of a zombie apocalypse)

5 digicert

Comparisons to Epidemiology

- Epidemiologists ≈ security researchers
- DNA ≈ computer code
- Host weaknesses (infection vectors) ≈ vulnerabilities
- Micro organisms ≈ computer viruses
- Skin, bones, and cell walls ≈ hardened perimeters
- Vital organs ≈ larger data stores (databases, etc.)
- Vitamins, exercise, sleep ≈ software updates / scans
- Vaccines and white blood cells ≈ antivirus software
- Targeted treatments ≈ end point defenses

6 digicert

© 2015 Workfront. All rights reserved.

Linking Cyber Threats with Germ Theory

- The germ theory of infectious diseases was not accepted until the end of the 19th century. Because of this ignorance, various infectious diseases claimed many thousands of human lives that we now know could have been spared with simple disinfecting or sanitizing precautions.
- Today, "infectious" computer attacks are increasing at an alarming rate. Is our attitude toward the remedy for these attacks repeating the events of 19th century Europe?

digicert

Ignaz Semmelweis

- **1800's** - infants and mothers died in maternity wards from puerperal fever, in some places as high as 35%
- **1847**- Semmelweis, doctor of obstetrics in Vienna reduces mortality rate from 18% to less than 2% when doctors and medical students wash hands with chlorine solution before attending expectant mothers
- **1850** - Semmelweis' recommended procedures do not gain widespread use
- **1865** - Semmelweis dies without recognition or honor
- **1870's** - work of Pasteur, Lister and Koch confirm "germ theory of disease" and Semmelweis vindicated

digicert

What is Due Diligence for Cyber Security?

Obey the laws, And wear the gauze. Protect your jaws from septic paws.

9

digicert

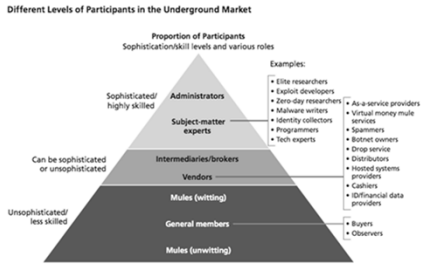
© 2015 Workfront. All rights reserved.

General Healthcare Steps

- **Perform Inventory** - Identity your population that is most vulnerable to disease.
- **Get Health Checkups** - Get a health check-up regularly
- **Educate the Population**
  - **Wash Hands**
- **Patch Open Wounds** - as soon as possible
- **Evaluate Success / Measure Progress**
- **Repeat as Necessary (e.g. periodically & when things change)**

10 digicert

Threat Actors



Source: RAND Corporation

digicert

Consequences of Insecurity

- Hit to reputation, share price, lawsuits, fines, customer credit protection fees, 1000's of hours of cleaning up the mess, hiring better IT staff, new IT solutions, scapegoat gets fired.
- Enforcing sanctions internally, then…
- Off to the races on restoring reputation, share price, good will, sustainability, business continuity, and viability.

digicert

© 2015 Workfront. All rights reserved.

Threats to Soft Tissue from Outside (and In)

- Unauthorized access privileges (e.g. remote access)
- Weak authentication mechanisms
- Unpatched vulnerabilities
- BYOD / BYOT
- Social Engineering
  - Phishing / Vishing / Spear phishing
  - Pretexting and tailgating
- Obfuscated Malware
  - Encoded payloads
  - Polymorphic viruses
- Port Scanning & Network Intrusion
- Malicious Insiders

digicert

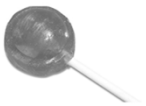
Two Completely Different Types of Attack?

Pictures taken from blog.zestos.co.nz and presurfer.blogspot.com Both images have a Creative Commons license.

digicert

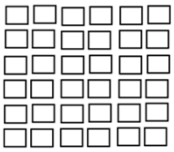
System Security Models

- **Traditional Perimeter**



- **Layered Onion**

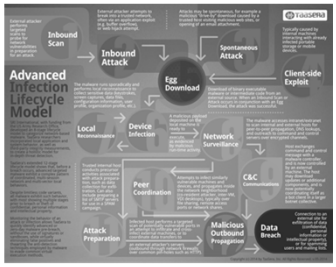
- **Sandboxing**
  - Compartmentalization
  - Containerization of endpoints
  - Micro-virtualization



15 digicert

© 2015 Workfront. All rights reserved.

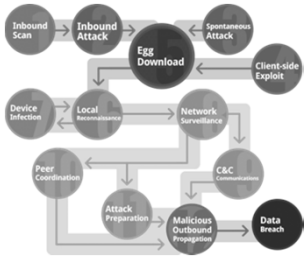
TaaSera's Advanced Infection Lifecycle



16 digicert

© TaaSera 2014 – Used with permission.

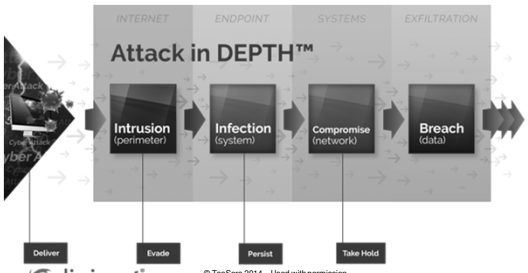
TaaSera's Advanced Infection Lifecycle



17 digicert

© TaaSera 2014 – Used with permission.

TaaSera's "Attack In Depth" Model



18 digicert

© TaaSera 2014 – Used with permission.

© 2015 Workfront. All rights reserved.

Is there a “chlorine solution” for cyber attacks?

Sources: fr.wikipedia.org and imaginelearning.blogspot.com Both have Creative Commons licenses

digicert

IT Security Training Levels - Where are you?

Level of Training	Example Roles	Cyber Hygiene	Cyber Health	Law Enforcement	Military Combat
Level 1	Technical Writer, Project Manager	✓			
Level 2	Customer Support, Receptionist, Receiving Clerk, HR Staff	✓	✓		
Level 3	Programmers, QA staff, Software Test Team Tier 3 Support Staff, CM Staff, Lawyers	✓	✓	✓	
Level 4	System Admins, DBAs, CTO, CISO, Ops Security staff	✓	✓	✓	✓

digicert

The “chlorine solution” for cyber attacks

People: Educate, Communicate, Evangelize

Process: Assess, Audit, Write Good Code, Monitor, Alert, Respond to Incidents, Report / Share

Technology: Configure / Harden, Contain / Segment / Isolate, Scan / Test, Patch / Quarantine

digicert

© 2015 Workfront. All rights reserved.

The "People Solution" for Cyber Attacks

- **Awareness**: Get to know the attack lifecycle & "Top Ten" lists for each applicable area of cyber risk
  - Web apps, mobile, cloud, IoT, social media, etc.
- **Training**: Get your security & privacy professionals trained & certified
- **Practice**: Perform regular exercises (Black Swan scenarios)
  - IR (include social engineering & ransomware), BR, DR, BC, etc.
- **Networking**: Cyber information sharing, ISACs

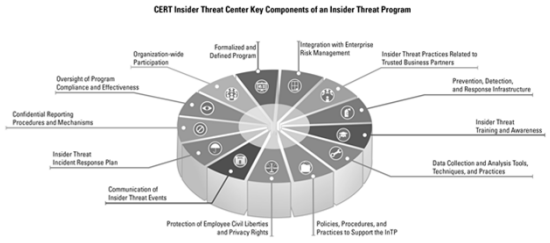
digicert

Dirty Hands and Washing Them

- Making security exceptions without recording them, notifying, or following up on service tickets
- Opening firewall port for testing without closing – ticketing, regular/quarterly firewall audits
- Granting production access to developers
- Backdoors left in by developers for testing
- Commenting out security checks like secure cookies and certificate validation checking, or otherwise ignoring or disabling a security feature (choosing functionality over security)
- Shutting off alerts – like hitting the snooze button

23 digicert

CERT Insider Threat Program Elements

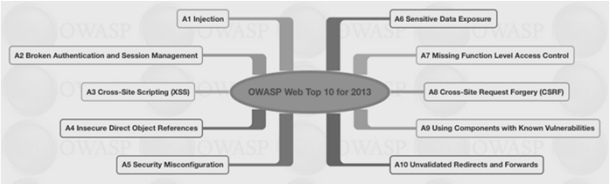


24 digicert

© 2016 Carnegie Mellon University

© 2015 Workfront. All rights reserved.

Top 10 Web Application Vulnerabilities



From www.owasp.org under the Creative Commons 3.0 License at https://creativecommons.org/licenses/by-sa/3.0/

digicert

SANS Top Twenty – CIS Critical Controls

Now called the "Center for Internet Security's Critical Security Controls for Effective Cyber Defense"

- Adopted by the California Attorney General as the legal definition of "reasonable security"
  - https://oag.ca.gov/breachreport2016
- Covers: inventory, configuration, access controls, training, patching, blocking, monitoring and testing

26 digicert

CIS & GHSAC Cyber Hygiene Campaign

- **Count**: Know what's connected to and running on your network
- **Configure**: Implement key security settings to help protect your systems
- **Control**: Limit and manage those who have admin privileges for security settings
- **Patch**: Regularly update all apps, software, and operating systems
- **Repeat**: Regularly revisit the Top Priorities to form a solid foundation of cybersecurity

27 digicert

© 2015 Workfront. All rights reserved.

ASD's Top 4 (plus 1 by James Lewis)

80-20 Rule - These top 4 eliminate 85% of intrusions

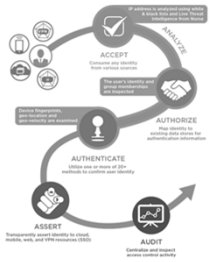
- Mitigation 1: application whitelisting
- Mitigation 2: patch applications
- Mitigation 3: patch the operating system
- Mitigation 4: minimize administrative privileges
- Mitigation 5: continually monitor for risk

http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

28 digicert

The 3 A's (and then some)



29 digicert

© 2016 SecureAuth – Used with permission.

Strong / Multi-factor Authentication

- Use passwords only for systems that cannot support multi-factor authentication
- Multi-factor – something you know, have, and are
- One-Time Passwords (RSA, Yubikey, homegrown or open source generators)
- Public key cryptography – smartcards/cryptotokens
- Biometrics - Fingerprint readers, etc.

30 digicert

© 2015 Workfront. All rights reserved.

Recommendations

31

Tips and Takeaways

- Encrypt the data on whatever can sprout legs, e.g. removable media
- Deploy strong auth including dynamic/adaptive & multi-factor
- Use only complex, one-time-passwords (OTPs) without storing them
- Encrypt or never store administrator credentials
- Have a Security & Privacy Standing Meeting at the Board Level
- Collaborate with external resources (FBI, industry groups)
- Collaborate internally across departments
- Develop trust relationships with CEO, CFO, GC, ERM, CISO

More Tips and Takeaways

- Enforce Independent Reporting of CISO & CIO
  - They don't own their respective areas of risk, the board does.
  - They have a conflict of focus. Let the board relieve the conflict. That's their job.
- Manage service provider relationship risk
  - Send service provider surveys, verify service providers do background checks, security training, encryption, strong auth, perform your own security evaluation, provision for audit when requested in the service provider contract
- Document, Document, Document (for transparency, etc.)
- Give your privacy and security personnel a voice
- Move PII & sensitive data to secure file systems
- Train workforce members to report security incidents timely

© 2015 Workfront. All rights reserved.

What Technologies Can Help?

With Cyber Hygiene
- Encryption & strong/adaptive authentication
- Detection tools that go beyond signature-based models
- Identity & Access Management
- Integrated solutions
- Continuous Auditing and Monitoring Tools
- Tools that can help Incident Response Teams

With performing SRAs
- Continuous Auditing and Monitoring Tools
- SRA software

digicert

Additional References

https://securityintelligence.com/malware-patient-zeros-how-threat-intelligence-and-herd-immunity-can-help-prevent-the-spread-of-infections/

http://slideplayer.com/slide/10066778/

http://www.nature.com/articles/srep05659

http://er.educause.edu/articles/2015/4/cybersecurity-in-higher-ed-searching-for-a-better-model

http://www.econinfosec.org/archive/weis2012/papers/Kelley_WEIS2012.pdf

35 digicert

Joe Grettenberger, CISA, CCEP
Workfront, Inc. -- joegrettenberger@workfront.com

Benjamin Wilson, JD, CISSP
DigiCert, Inc. -- ben.wilson@digicert.com

digicert

© 2015 Workfront. All rights reserved.