Griffith Law Firm

KANZLEI KOHLMEIER
FACHANWALT · MEDIATOR

Cybersecurity Best Practices for Local Government

IMLA-Conference, 10/16/17, Niagara Falls, Can.

Benjamin E. Griffith
Griffith Law Firm

Sven Kohlmeier
Kohlmeier Law Firm

Griffith & Kohlmeier

Benjamin E. Griffith



Griffith Law Firm

IMLA International Committee

ABA Board of Governors

Sven Kohlmeier



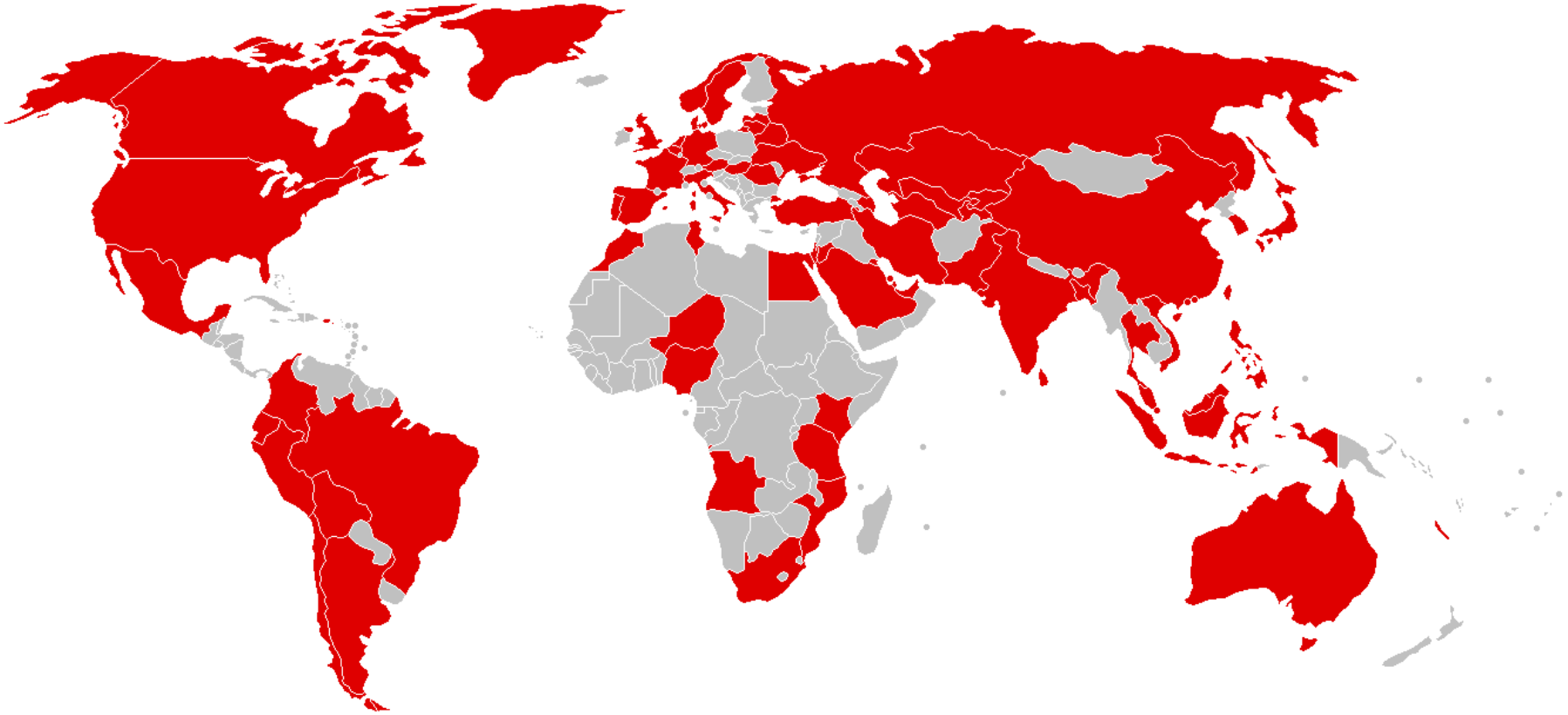
Kohlmeier Law Firm

Attorney at Law, professional lawyer specializing in IT law, Mediator
Member of Berlin House of Representatives

What we are talking about:

- 1. Overview cyber attacks in 2017
- 2. Best Practices
- 3. Conclusion

May 2017: Wannacry



Von User:Roke - File:BlankMap-World-v2.png, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=58863465

May 2017: Wannacry

- 230.000 computers in 150 countries were infected
- Encryption of computer data
- demanded ransom in bitcoins
- UK hospital National health service gone down
- Spain Telefonica infected
- US FedEx Logistic infected
- China PetroChina (Oil), 20.000 Petrol Stations no cashless payment
- Romain Forein Ministry

May 2017: Attack on Nuclear Facilities



May 2017: Attack on Nuclear Facilities

- hackers have been penetrating computer networks of companies that operate nuclear power stations and other energy facilities
- also target Wolf Creek Nuclear Operating Corporation, Kansas
- whether the cyberattacks were an attempt at espionage — such as stealing industrial secrets — or part of a plan to cause destruction
- hackers not control facility-systems

May 2017: Data of 143 Million US citizens were stolen



Equifax Inc.
@Equifax

Folgen

(2/2) We apologize to our consumers and business customers for the concern and frustration this causes. Learn more: equifaxsecurity2017.com.

00:20 - 8. Sep. 2017

1.802 508 295

May 2017: Data of 143 Million US citizens were stolen

- attack on US finance company Equifax
- data of up to 143 Million citizens were stolen – credit card number, social security number
- stock of Equifax lost more than 5% after published that information
- in 2013 Equifax were already hacked
- Equifax himself sell products against cyper- and data-theft

Juni 2017: News reports Russion cyber hacks on 39 U.S. Electoral Systems



The U.S. voting system, a loosely regulated, locally managed patchwork of more than 3,000 jurisdictions overseen by the states, employs more than two dozen types of machinery from 15 manufacturers. Elections officials across the nation say they take great care to secure their machines from tampering. (AP Photo/Mary Altaffer)

June 2017: News reports Russian cyber hacks on 39 U.S. Electoral Systems

- attack on electoral systems wider than previously known
- Illinois: investigators found evidence that cyber intruders tried to delete or alter voter data
- US investigators: Russian hackers hit systems in total of 39 states
- Russian officials denied any role in cyber attacks connected to the US election
- Internet Research Agency: targeted Facebook ads exploiting BLM, LGBT & Immigration issues

June 2016: data of 198 million US voters published



The personal details were available to anyone who had the right web address

Saul Gravy/Getty

June 2016: data of 198 million US voters published

- online for almost two weeks
- accidentally left unsecured on a web server
- easy to download the unencrypted dataset without entering a password
- address data could be interesting for criminals

July 2017: Attack on Reedere Maersk



REUTERS/Phil Noble/File Photo

July 2017: Attack on Reedere Maersk

- Biggest shipping giant in the world (danish)
- hited by a major cyber attack
- restored its major applications
- Took 1 week to fully functional 1500 applications

July 2017: 500 Million login data leaked

- Found in the darknet by Federal Criminal Police Office
- Login data with password and Email



July 2017: Hackers steal $7 millions in digital currency

- a link for depositing digital currency on the CoinDash website was not legitimate
- CoinDash website was hacked and a malicious address replaced
- Moe than 2,000 investors sent ETH to the malicious address
- Amount of 37,000 ETH was stolen
- CoinDash managed to secure $6.4 million
- (ETH = digital currency)



July 2017: Hacker „31337“ hacked the US security firm Mandiant

- in 2016 Mandiant was the security-company to secure the computer of the clinton-campaign
- hacker group had access to the LinkedIn-profil, Microsoft-account and find-my-own-device of a security manager

July 2017: Hacker found out how to hack Nissan Leaf

- Hacker found out that Nissan on board electronics could be hacked using a chip



- here: every car needs special hack
- But: be prepared that networked cars could be hacked

Sept 2017: federal election in Germany – attacks and desinformation campaign



Bundeskanzlerin Angela Merkel und der damalige EU-Parlamentspräsident Martin Schulz im Gespräch. (picture-alliance / Belga / Christophe Licoppe)

http://www.deutschlandfunk.de/bundestagswahl-2017-ist-angela-merkel-doch-besiegbar.1784.de.html?dram:article_id=378607

Sept 2017: federal election in Germany – attacks and desinformation campaign

- 2015 and 2016 the German Parliament's IT infrastructure and some political parties were the targets of several cyber attacks
- no documents or emails were published on wiki-networks during the election weeks (in distinguish to the US-election (clinton campaign leaks)

Sept 2017: federal election in Germany – attacks and desinformation campaign

- shortly before the election on 09-24 the „Chaos Computer Club“ published that the software to transfer the election results from local polling place could be hacked because of several security problems
- The head of the federal election commission announced to update the software before election day

Sept 2017: federal election in Germany – attacks and desinformation campaign

- desinformation campaign from other countries ?
  not happened or not yet known

- Social Media bots? IT-expert: 7,4% of election social media traffic were from robots
  interesting fact: the strong right party AFD had 30% of the social media traffic with real users (more than they got in election votes)

Best Practices - Checklist

- 1. risk analysis
- 2. backups
- 3. staff training
- 4. vulnerability scanning and patching
- 5. updating and patching product servers
- 6. application whitelisting
- 7. incident response

Best Practises - Checklist

- 8. business continuity
- 9. restriction administration privileges
- 10. network segmentation and segregation into security zones
- 11. input validation
- 12. file reputation
- 13. unterstand and unsing firewalls
- 14. penetration testing

Best Practice: staff training

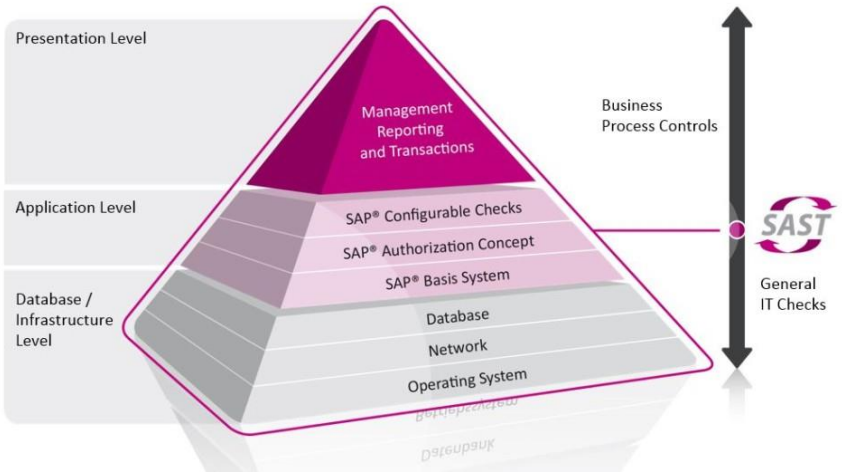


- Cybersecurity Awareness Training

Cybersecurity Awareness Programs



End-User Education



- Security Audits, Penetration Tests and Monitoring
- Security Information and Event Management (SIEM) Tools
- Continuity of Operations Plans

Questions for Local Government Leaders to Consider

1. Questions the human resources department on whether it can help support a security awareness-training program.

2. Give support for new hardware, software, or services.

Questions for Local Government Leaders to Consider

3. Perform assessments, within the limits of funding, at the executive management level regarding the amount of risk the local government is willing to mitigate or simply accept.

4. Make the backup and recovery plan a good as the government can afford, since a cyber attacker with the time and desire will gain access one way or another.

Basic Cybersecurity Best Practices

1. Effective password management policies, using best practices for password management

2. Least privilege user access (LUA).3. Harden client devices by deploying multilayered firewall protections

3. Conduct regular penetration tests and vulnerability scans of infrastructure.

Basic Cybersecurity Best Practices

4. Mobile device management program, requiring authentication to unlock a device, locking out a device after five failed attempts, using encrypted data communications/storage, and enabling the remote wiping of devices if a mobile device is lost or stolen.

5. Continuous monitoring in real-time the security of the organization's infrastructure.

Basic Cybersecurity Best Practices

6. Deploy web application firewalls to detect/prevent common web attacks.

7. Permit only authorized wireless devices to connect to the network.

8. Implement Always On Secure Socket Layer (AOSSL) for all servers requiring log in authentication and data collection.

Basic Cybersecurity Best Practices

9. Review server certificates for vulnerabilities and risks of domains being hijacked.

10. Develop, test, and continually refine a data breach response plan.

Best Practice – Overseas view:

- State of Berlin (Germany) use their own IT department for all local authorities
- All authorities of Berlin supposed to have one IT security officer
- Computer Emergency Response Teams (CERT) collects and processes IT security incidents
- Using Encrypted communication

State and Local Government Cyber-exercises



- Many valuable state and local government cyber-exercises have taken place across the United States, demonstrating successful public-private partnerships and substantive sharing of information and cyber technology.

Conclusion



Cybersecurity Best Practices for Local Government

Thanks for your attention

Griffith Law Firm
2086 Old Taylor Road,
Suite 1023
Oxford, MS 38655
Phone: (662) 238-7727

www.glawms.com

Kohlmeier Law Firm
Friedrichstrasse 61
10117 Berlin
Germany
Phone: (+49) 30 2260 5000

www.kanzlei-kohlmeier.de