Griffith Law Firm

KANZLEI KOHLMEIER
FACHANWALT · MEDIATOR

Cybersecurity Best Practices for Local Government

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

Best – Practice – Checklist

for your work, for your government,
for your office, for you

Handout by (*):

Benjamin E. Griffith
Griffith Law Firm

Sven Kohlmeier
Kohlmeier Law Firm

(*) for more information about the speaker see last page

Best – Practice – Checklist

- ✔ check here what you already did

⬇

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

Best – Practice – Step-by-step

✔ 1. Risk analysis

The first step in this grass-roots approach of the cyber security fight is the recognition of the importance of cyber-security by local leaders to include mayors and town councils, chambers of commerce, school boards and civic groups. Such leadership has the ability to raise awareness of cyber-security among their respective constituencies.
Asking yourself some questions and give an honest answer: Do you feel well prepared against cyber attacks on your personal or office device? Are you well trained to identify unsecure emails, programs or computer devices? Who in your company or government is the “Chief Information Security Officer“?

Risk analysis is the description of the complete process to identify, evaluate and score the risk and last but not least fix the risk. The steps for a risk analysis are

- risk identification
- risk analysis
- risk evaluation

Depending on the size of the office, importance for the local or state people, importance for city or national security pp the level of fixing the risk could be different: software update, new acquisition of it infrastructure, moving in a new building.

If you need help with your risk analysis use a specialist or specialized company. Or ask similar local authorities about their risk analysis. In some states or countries it could be required by law or in house/company-rules to made and written down a risk analysis.

Best – Practice – Step-by-step

✔ 2. Backups

Secure your data by making backups in the time your data are not stolen, lost, hacked or changed by a criminal. Or lets take a typical example: your cup of coffee tip over the device, unwillingly or willingly (happened!) you destroy your device by kicking it by foot. Or an employee become ill and you need his/her data to work on a project.

Make the backup and recovery plan as good as the government can afford, since a cyber attacker with the time and desire will gain access one way or another. With a backup and recovery plan you will have the main guideline for your data backup. Make sure that the backup device is secure located or secure treasured. The backup media should be located on a different place than the original data (e.g. in case of fire, burglary). If you are using a cloud solution to backup your data read the terms and conditions carefully. Some cloud solution scan the data for commercial purposes or will give the data to third parties (government, investigation). Some terms and conditions also contain provisions concerning the place of jurisdiction, which is often where the cloud provider is based. If you are working with sensitive data you have to encrypt the backup data.

In the fist step it doesn't count how often you backup your data (every hour, every day, every two days). It really counts that you backup your data and having a professional backup plan.

Ask your IT-department or IT-service for a backup plan. Specialized IT-company, data protection officer will support you for a perfect backup plan.

Best – Practice – Step-by-step

✔ 3. Staff training

Training, training, training!! Implement an employee cyber security training program. Realize that it is not a matter of whether, but when, a cyber-attack or security breach will occur; be prepared through training. Cyber Hackers usually hit the easiest targets first, much like thieves operating in a neighborhood during the holidays. A common breach can occur after a user clicks on a link in a spam or phishing email, and whether such an attack is financially motivated, or an attempt to cause mayhem in the city, or an act of revenge by a terminated city employee, it must be confronted and effectively mitigated. Conclusion: Training, training, training.

Use conferences like IMLA for you training and expertise update. Questions the human resources department on whether it can help support a security awareness-training program. Or ask us for training you, your local authorities, your staff.

✔ 4. Vulnerability scanning and patching

Conduct regular penetration tests and vulnerability scans of infrastructure. The increased vulnerability that comes with this increased technology raises security concerns about Advanced Persistent Threat (APT), which are targeted attacks executed by a hacker or group of hackers, perhaps using malware, in which the attackers are motivated not by financial gain so much as by political gain or "hacktivism." The Smart London Initiative is the focal point of an analysis cited above, Poul Nielsen, Smart City Security and Cyber Attacks, Feb. 25, 2016, http://www.informationsecuritybuzz.com/articles/smart-city-security-and-cyber-attacks/, in which a troubling scenario is outlined for a city of over 8.5 million people in which a critical service is attacked and many operations dependent on that service malfunction or shut down.

The cause of vulnerability is diverse: the concept or configuration of an IT-product (software, hardware), how many people using the product, which person has which user rights.

This points to the need for authorities to develop and implement solutions to monitor their IT infrastructure and end-user endpoints, the weakest link in the IT security chain with the greatest vulnerability.

Specialized IT-companies will find all your vulnerability. If you hire a former hacker he/she will find your vulnerabilities fore sure. And train your staff (see above).

✔ 5. Updating and patching product servers

Don’t work with Windows XP any more in you authority or office, like the capital of German, Berlin, did till 2015.

Security updates and patches from your software producer must be installed. Before installing a update you should make a backup (see above No. 2). If you are updating your device or infrastructure be sure that the download source is an official one or from a official website of your software product.

Most software automatically inform or ask your for updating or patching your software. Trust them or ask your IT department to never miss a security update.

✔ 6. Application whitelisting

On a higher level of protection with an application whitelisting you control which user could start programs. With an application whitelisting you also control in which directory users could be working or starting programs.

The application whitelisting should be installed and controlled by the IT-department.

✔ 7. Incident response

Security incidents must be determined and evaluated fast and effective to prevent future security breaches or damages. For that reason you need a given and proofed procedure to deal with security incidents. Therefore you establish a so called “Security Incident Response” or “Security Incident Handling”.

Implement measures for detecting compromises and develop a cyber security incident response plan that includes such measures at intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), antivirus software and logs to help detect compromises in their earliest stages.

✔ 8. Business continuity

Business Continuity Management (BCM) means all organizational, technical and personal measure to continue the „main business“ of the authority or company after a security breach or incident. In addition to that with a BCM-plan your company or authority could be continuing working in case of a long disruption e.g. power is down.

Specialized IT-companies or local or state requirements will lay down a perfect Business-Continuity-Management-Plan for your office and authority.

✔ 9. Restriction administration privileges

The administrator of an IT-infrastructure is the administrator. The end-user of an IT-infrastructure is the end-user. Did you ever asked yourself why the end-user has the same rights as the administration. It's not a constitutional right – changed that today!

Most of the hacker attacks occurred through an email-attachment that the end-user opened. The sender of the email looks very official or comes from a know email-address, it could be a application form attached or an pdf- or zip file. Another examples in which a cyber hacker tries to access a computer or sensitive information stored in it is by offering to "fix" the computer. In a blog by Andrew Johnson, Division of Consumer and Business Education for the FCC, entitled *Official-sounding calls about an email hack,* April 6, 2016, at https://www.onguardonline.gov/blog/official-sounding-calls-about-email-hack, this latest form of hacking takes place when a person gets a call from a person identifying himself or herself as representing the Global Privacy Enforcement Network, in which they claim that the person's email account has been hacked and is sending fraudulent messages.

In both examples happened the same: a malware is opened from the end-user (by opening the attachment or by installing the offered "fix"-program) and the malicious software will install by the end-user just because the end-user has the user-right to install programs.

Our tip: Administrators and end-users must have different administration privileges!

Best – Practice – Step-by-step

✔ 10. Network segmentation and segregation into security zones

Implement network segmentation and apply firewalls, classifying and categorizing IT assets, data, and personnel into specific groups and then restricting access to those groups.

We will give you a simple example: If you cook at home you use different pots to segregate the food because every food needs his own attention and preparation. Do that the same way in your office or authority network. Some date a more sensitive than other. Some data doesn't match with other data. Some data are just for special group of staff or the head of the organization or authority.

It's like cooking: Different cooking zones and different pots are the guarantee for the best result. For the best result for your data security use different security zones and network segments.

Ask us for advise in both: Using different security zones and cooking!

Best – Practice – Step-by-step

✔ 11. input validation

Input validation, also referred to as data validation, is the outer defensive perimeter for a web application, a perimeter that protects the core business logic, processing and output generation. If you do not practice input validation, this can lead to application attacks such as buffer overflow, SQL infection, and cross-site scripting.
Data validation is the process of ensuring that a program operates on clean, correct and accurate data.

✔ 12. file reputation

File reputation entails checking the reputation of each file against an extensive database, typically an in-cloud database, through which users are allowed to rate each other in online communities to build trust through reputation.

Best – Practice – Step-by-step

✔ 13. Understand and using firewalls

A firewall is what it's sounds like: A wall prevents "fire" behind the wall. In our case the "fire" are the hackers, cyber attacks, cyber thefts, foreign governments, DDos-attacks (*). The firewall on your device or IT-infrastructure comes as a software or hardware solution.

DDoS (Distributed Denial of Service) is a form of brute force attack in which the attacker buys access to a botnet system that directs thousands or even millions of computers to access the network, email system or website. Cyber security vendors have used several approaches in an effort to prevent DDoS attacks on municipal governments. Cyber security firms or the IT-department can build a firewall that analyzes incoming traffic in real time and blocks incoming traffic when certain characteristics trigger a response. Hosting and network vendors offer cloud and hardware devices that range from $500/month for three million packets per second to $2,500 per month for twelve million packets per second that would protect most municipalities. Larger cities may need the services of companies like Akamai, IBM, Microsoft, and Amazon that can run into the hundreds of thousands or millions of dollars depending on the level of DDoS protection needed. Cyber security firms or the IT-department can also build a firewall to minimize the risk of a cyber attack.

Ask your IT-department officer or take a training tour like conferences to understand how firewalls work. With every rule you implement yourself on the firewall system (instead of a central implementation and control of the firewall system) you open your device like a piece of Swiss cheese.

✔ 14. Penetration testing

Local government can implement security efforts in the form of security audits and penetration tests. These measures call for paying ethical hackers to try to breach the local government's system and reporting their findings.
The government officials can use this information to take pre-emptive action. Officials, from the highest to the lowest levels, must understand the long-term cost of a data security breach, and they must understand, in context, the great expense of a security audit or audits. They must count the cost not only in monetary terms, but officials must also count it in terms of the loss of trust that citizens and customers have in their governments. Further, officials must decide whether an annual or biennial security audit is sufficient in the present and future cyber landscape. Attention should be given to such emerging trends as hiring 24/7 managed professional security service providers. These professional can operate from remote security operations centers with fully dedicated certified security teams. The teams watch the local government's network, inside and out, and can identify real time security threats and help develop preventive counter measures.

It is not cheap, but its cost in relative terms may make it a bargain.

Best – Practice – Step-by-step

- *EXTRA*

It's one of the most important point to know. We talked about that on IMLA-conference in Washington, DC in April 2017. Because it's so important, we add that as an extra on your step-by-step-handout as No. 15.

✔ 15. Effective password management policies

The cat-and-mouse game that seems to be taking place constantly between the perpetrators and victims of cyber security breaches, practices and measures is daunting. It has spawned a number of practices that can be implemented by municipalities to help protect their networks and systems. Some of these practices have been implemented by the private sector and are listed in a 2015 report from Online Trust Alliance (OTA). According to OTA, if the affected organizations and entities had implemented basic cyber security best practices, they could have prevented 90% of recent breaches. See Security & Privacy Best Practices (Jan. 21, 2015), https://otalliance.org/resources/security-privacy-best-practices.

That's why we highly recommend an effective password management policy, including:

a. multi-factor authentication;

b. unique password for external vendor systems;

c. strong passwords comprised of an 8-character;

d. login abuse detection system monitoring connections, login counts, cookies, and machine IDs;

e. Avoid storing passwords;

f. Remove or disable all default accounts from all devices and conduct regular audits to ensure that inactive accounts can no longer access your infrastructure; and

g. Remove access immediately for any terminated employees or any third parties or vendors that no longer require access to your infrastructure.

Examples of bad passwords:

12345	your name	your birthday
67890	qwerty	asdfg
mom	dad	apple

Example of a good password:

Tyfya@ic10-2017iNF!

(Thank you for your attention @ IMLA conference 10-2017 in Niagara Falls!)

Cybersecurity Best Practices for Local Government – Best – Practice – Step-by-step

Feel free to contact us for advice, training or help:

Benjamin E. Griffith	**Sven Kohlmeier**
	
Griffith Law Firm IMLA International Committee ABA Board of Governors	Kohlmeier Law Firm Attorney at Law specialized in IT law Member of Berlin House of Representatives
Griffith Law Firm	KANZLEI KOHLMEIER FACHANWALT · MEDIATOR
2086 Old Taylor Road, Suite 1023 **Oxford, MS 38655** **Phone: + 1 (662) 238-7727** **www.glawms.com**	**Friedrichstrasse 61** **10117 Berlin** **Germany** **Phone: +49 (30) 2260 5000** **www.kanzlei-kohlmeier.de**