JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU

TNF

Technisch-Naturwissenschaftliche
Fakultät

Examples of educating employees about IT security: How are companies doing it, what are they doing?

SEMINARARBEIT

im Masterstudium

Webwissenschaften

Eingereicht von:
Torben Försterling

Angefertigt am:
Institut für Informationsverarbeitung und Mikroprozessortechnik

Beurteilung:
Assoz.Prof. Priv.-Doz. Mag. iur. Dipl.Ing. Dr. Michael Sonntag

Linz, Mai 2013

ABSTRACT

Current security issues need to be understood in the context of an ecosystem that involves the interplay between worms and bots, as well as scams, spam, phishing, active content, browsers, usability, and other human factors. This problem is currently getting even bigger because of the increasing quantity of mobile devices used in companies, as well as more sophisticated malware or popularity of social networks like Facebook or Twitter.

Therefore employees have to be educated based on specific security programs. To have a look at companies dealing with sensitive data itself as well as those providing IT infrastructure, this paper focuses on examples from the healthcare sector as well as the networking systems industry.

KURZFASSUNG

Aktuelle Sicherheitsprobleme müssen im Kontext eines Ökosystem verstanden werden, welches ein Zusammenspiel zwischen Würmern, Viren und Bots, wie auch Betrug, Spam, Phishing, aktiven Inhalten, Browsern, Usability und anderen menschlichen Faktoren ist. Die in Firmen zunehmende Anzahl mobiler Endgeräte, aber auch die immer fortschrittlicheren Schadprogramme zusammen mit der großen Beliebtheit sozialer Netzwerke wie Facebook oder Twitter machen die Sicherheit zu einer immer größer werdenden Herausforderung.

Mitarbeiter müssen deshalb auf Basis von speziellen Sicherheitsprogrammen geschult werden. Um sowohl einen Blick zu werfen auf Firmen, die mit sensiblen Daten direkt zu tun haben, als auch auf solche die IT Infrastruktur produzieren, konzentriert sich diese Seminararbeit auf Beispiele aus dem Gesundheitswesen und im Kontext von Netzwerksystemhersteller.

CONTENTS

1 INTRODUCTION

Contents

1.1 HUMAN FACTORS IN CORPORATE IT SECURITY

Information has become one of the most precious resources. It has influence on basic enterprise's activities like searching clients, stuff and co-operators, establishing partnership or adjusting products or services to customers' needs. Reliable, up-to-date and unique information is more than a crucial competitive advantage: it is the base of running a business itself. As companies and organizations rely more on technology to run their businesses, connecting system to each other in different departments for efficiency data security is always a concern, not only for administrators. [7] Information occurs as confidential or not confidential (available for all people without limits). This division is caused by: law regulations and possible influence of the information on an enterprise or its competitors, both positive (competitive advantage) and negative (weaknesses). Information is not only collected from the environment, but it is also emitted to the environment. It means that there is a

need of building and maintaining a system which is capable to control the emitted information. If the system fails, an enterprise faces a data leak incident. The possible effects of disclosing confidential data are severe: law prosecution, reputation loss and heavy, financial losses up to bankruptcy. In some cases it is very difficult and costly to even estimate the losses. [6]

According to a survey conducted by Trend Micro Incorporated in 2008, the disclosure of confidential data becomes the second most important problem of security (after viruses) that companies in the USA, UK, German and Japan face. Furthermore only 54% of 1600 examined companies have reportedly implemented prevention measures against data leakage. The problem is currently getting even bigger because of the increasing quantity of mobile devices used in companies, as well as more sophisticated malware or popularity of social networks like Facebook or Twitter. [3] [6]

The Data Breach Investigation Report by the northern american internet service provider Verizon in 2010 confirmed that the majority of breaches and almost all (95%) of the data stolen in the year before was perpetrated by remote organized criminal groups hacking servers and applications. [4] In 2010 Chen, Paxson and Katz emphasized, that current web security issues need to be understood in the context of an ecosystem that involves the interplay between worms and bots, as well as *scams, spam, phishing, active content, browsers, usability, and other human factors*. [1]

1.2 BASIC STRATEGIES TO ACHIEVE CORPORATE IT SECURITY

Basically security can be achieved by the implementation of 3 concepts:

- Authorisation: Granting access to specific, limited resources only to a limited range of persons.
- Authentication: Verifying the identity of users.
- Accountability: Linking particular users/employees to their actions.

The polish PhD-Student Juszczyk calls this the "AAA" rule, which works on the principle of "controlling by limiting" [6]. Hackers are, however, aware of these strategies and base their attacks on trying to circumvent these restrictions by finding logical flaws in systems as well as in the users of these systems.

For companies it is thus crucial to use security strategies, that prevent social engineering and other attacks that happen on the employee level.

2 EXAMPLES ON HOW COMPANIES EDUCATE EMPLOYEES

Abstract. How security programs can be structured and which philosophies and methods are key to success in the healthcare sector and the network production.

Contents

2.1 APPROACHES FOR THE HEALTHCARE SECTOR

2.1.1 Conceptualizing a security program

Since informations on diseases, treatment, medication are nowadays recorded digitally in almost any healthcare system, strict data security is a critical factor for hospitals, doctor's offices, pharmacies and other institutions. Therefore the United States congress signed the *Health Insurance Portability and Accountability Act (HIPAA)* in 1996

[5]. Among others it states, that every procedure must be documented and include every required action, activity and assessment that is relevant to security. The healthcare environment does mainly have problems with IT security that result from system failure, data breaches and improperly altered applications, reported the director of professional practices at the Institute of Internal Auditors in 2009. He furthermore suggests that companies should at first answer a checklist of questions and then take steps to encounter the remaining problems effectively. [8]

- Has the organization implemented a comprehensive information security program?
- Does the organization have approved information security policies, procedures, and controls? Are they enforced?
- Does the information security program reflect the risks and complexity of the organization? Are risk assessments occurring regularly and are improvement efforts an ongoing everyday way of life?
- Does the program actively identify new ways of protecting the organization from harm based on emerging threats?
- Are the security measures and controls regularly tested for operational effectiveness, and are corrective actions occurring?
- Is performance being measured and reported to senior leadership and other key stakeholders? And how does the organizations security compare with other well-run similar organizations?
- Has the security program been formally evaluated in the past 12 to 18 months?

- Does the program include ongoing security awareness efforts?
- Do management and staff members get security education appropriate for the jobs they perform?
- Do members of the management team and workforce understand what good security practices are?
- Is the organization assessing and measuring the results of security education and awareness efforts on a regular basis?

2.1.2 Implementing a security program

To properly implement a security program on a sustainable basis management and staff need to be regularly informed of *emerging* threats and risks and quality training should be be provided for each employee. Education is the formal training class that a system administrator might attend to learn how to better apply, e. g. Microsoft Profiles to controlling changes to the desktop.

1. A good method to deliver that security awareness message to the workforce can be to first to educate them on the actions they can take to *protect themselves personally* from the issues that individuals face today. These include such things as identity theft, phishing attacks and proper precautions to take when sharing personal health information online. Providing this information in the training sessions makes the process more personal.

2. Updated threat informations should be regularly provided to management and staff. Some common concerns today include: password theft, laptop theft, infected e-mails, "shoulder surfing," and dumpster diving. With clear communication channels that allow everyone to be more

informed on the latest threats, and changes in previous threats, it encourages the workforce to be better prepared and, where beneficial, to consider new security measures. An /empheducated and motivated workforce is the key to defend attacks.

3. *Explaining the possible consequences* of security incidents in business terms can be another critical option. An organization or its workers could encounter identity theft, equipment theft, loss of productivity, loss of competitive advantage, increased staff turnover, penalties due to compliance fines, loss of reputation, loss of data, and eroded customer confidence. While the list is long, the workforce absolutely must understand what the effects on the organization could be. By making it personal and demonstrating the possible hit to operations, increased support for good information security practices can be reinforced.

4. Providing comprehensive, *role-based courses* to selected management and staff members that require the *latest* knowledge regarding good security practices. Here, the issue is ensuring that an investment in skills and staff competencies is happening on a regular basis.

5. Regularly providing *leading practice information* for various IT security and IT management processes. Some important processes include: patch and change management, configuration management, security architecture, fraud prevention and detection and physical security. Not just the how, but the why of various security procedures should be explained to the staff. And a wise first step is to focus on educating the influencers of your management and staff ranks, and then let them set the example for the rest.

6. A complete and periodic survey of management and staff. This is to assess how well they understand the information security policy, procedures and controls as well as to identify major opportunities for improvement. [8]

2.2 THE NETWORKING AND TELECOMMUNICATION SYSTEMS INDUSTRY

2.2.1 Analyzing a social engineering attack

In 2009, the CSO security magazine published an article that featured the security vulnerability expert Chris Nickerson, who performed a successful social engineering attack by explaining himself to be a Cisco expert and thus entering an unnamed Internet company. He states, that a social "penetration testing" requires intelligent information gathering on the target. When he is doing this, he likes to find holiday or time-relative events. In this particular exercise, there was a large horserace going on in this specific area. In the town where the target was located, it was popular to go to this horse race. Many people in the city and around it would gear up and leave the office to go to it and that was the time Nickerson chose for the attack, which he had planned and prepared weeks ago.

He explained at the reception of the company, that he had to meet with Nancy, a person he researched and found out to be going to said horse race. He knew she wasn't going to be in the office since on her MySpace profile it said she was getting ready to go to the race. Then her Twitter profile said she was getting dressed to go to the event. So he knew exactly, that she wasn't in the office at that time just by using social media.

Before he went to the office, he bought a cheap Cisco shirt from a thrift shop. Then he went in and said "Hi. I'm the new representative from Cisco. I'm here to see Nancy." As expected, the front desk attendant in this situation said "She's not at her desk."

He replied "Yeah. I know. I've been texting back and forth with her. She told me she is in a meeting and the meeting is going over."

This was right around lunch time and he said "Since I'm waiting, is there anywhere around here where I can go get some food?" The attacker knew very well that after surveying the area the closest thing was about five miles away because they were sort of out in the sticks.

The receptionist said "Four or fives miles down the road there is a McDonalds. But we have a nice cafeteria here. If you want, you can just eat in there."

Being allowed to go to the cafeteria gave him full access to the facility because the only thing that was guarded was the door and the cafeteria lead right into the rest of the building.

So the attacker went into the cafeteria and ate, but he also did what he called "USB key drops". That means, he dropped USB sticks with names like 'Payroll' or 'Strategy 2009' throughout the entire cafeteria. The USBs had rootkits on them and many contained an autorun rootkit. Others had Hacksaw, which is a little piece of tech that you can use with a U3 drive. It is plugged into a machine and, if the machine has auto run on the CD-Rom running it, it will just start dumping all the passwords, usernames, and other sensitive data. It will also put a hook into the machine to start emailing that information out to a previously specified email account, which takes about 30 seconds to enable itself.

When Nickerson did this kind of exercise, he made sure to put USBs in areas that people are in, where they might forget something, e. g.the bathroom. Another potentially useful area could be near a coffee machine and other Areas where people naturally put things down where they might not remember to pick it back up. This attacker claims to have never done USB key drops without success.

Meanwhile, he had a complice go in through the smoking door in the back. He hung out, waited, had some cigarettes with people who came out to smoke on break, and when they were done, the door opened and he just walked with them inside. Yet another exercise to prove how easy it is to get inside.

Eventually, once Nickerson, the attacker, and his complice met, they went out of the cafeteria inside an office room. They made it appear on the security tapes as though someone was coming to get Nickerson out of the cafeteria to escort him to whatever meeting he was going to attend. They went through and found inside of this 100,000-square-foot cube farm a few seats that were open and just sat down.

There was no one around them because of said horse race taking place at that very moment, so they started pulling keys. They used tools like Ophcrack to start cracking Windows passwords and dump them into Linux, they started putting their machines on the networks so they could start doing pen testing and hacking active servers in the environment. They put up WRT 54G routers and put Unix on them and opened WRT. That resulted in them having a wireless access point they could hit not only from the parking lot, but it also beacons and calls home so they had a Unix box that sits inside their network.

In the end, what they exposed for their client was the vulnerability of their physical access and they showed them some of the blended techniques they used to get in. They were able to demonstrate how, with social engineering, someone could be able to hack the SQL Server and dump the whole data base of everybody's account information. This kind of breach could have cost them multiple billions of dollars.

Nickerson finally states that companies need to run a general social engineering *awareness* campaign. Companies need to tell employees what to look for and how to look for it and teach employees that it's not that the company doesn't trust the people within the organization, it's that there are people out there trying to do this every day. It is just a good awareness technique to do it.

If someone is coming to work on the environment, employees should probably know who they are. If they think of your company like your home, they would do things differently. They are not going to just let someone walk into their house. That is the kind of philosophy companies need to inject into *corporate culture*. [3]

2.2.2 Realizing a culture of security awareness

The networking hardware producer Cisco Systems Inc. states in an article on how to "Protect Against Social Engineering" on their website, that "technology solutions, security policies, and operational procedures alone cannot protect critical resources". Therefore they aim to achieve a *Security-Aware Culture* in each company that uses their routers, network switches and other critical hardware components. [2] This culture should contain:

1. Top-Down Security Culture: Executive commitment is vital to a security-aware culture. When security awareness is emphasized by the top levels of management, employees are more likely to view security as a business enabler instead of a hindrance to productivity. An executive staff that takes the initiative to be informed and involved in security issues, rather than off-loading responsibility to a security team, will encourage a security culture that is collaborative, structured,

and ingrained throughout the organization's processes and people.

2. Security-Awareness Training: Most employees do not cause security problems intentionally. Accessing unsecure Websites, deploying unauthorized wireless access points, or falling victim to social-engineering ploys are common employee actions that result in security breaches. The best way to avoid unintentional security problems is to provide all employees with regular security-awareness training. This training must inform employees of new threats and refresh their understanding of how to identify and avoid social-engineering attacks. An annual seminar or occasional memo is not an effective approach; organizations must treat security-awareness training as a normal, enduring aspect of employment. [3]

With proper training, every employee should understand the company's physical security measures and know how to handle and protect confidential data, as well as to be able to recognize and respond appropriately to social-engineering attempts. Employees in higher risk positions for social-engineering attacks, such as help-desk staff and network administrators, could benefit from emphspecialized training. An ongoing risk assessment that tests the resistance of employees to social-engineering attempts and techniques can help assess the validity of the training program and further raise security awareness.

3. Security Policies and Procedures:

- Password Management: Guidelines such as the number and type of characters that each password must include, how often a password must be changed, and even a simple declaration that employees should not disclose passwords to anyone (even if they believe

they are speaking with someone at the corporate help desk) will help secure information assets.

- Two-Factor Authentication: Authentication for high-risk network services such as modem pools and VPNs should use two-factor authentication rather than fixed passwords.
- Anti-Virus/Anti-Phishing Defenses: Multiple layers of anti-virus defenses, such as at mail gateways and end-user desktops, can minimize the threat of phishing and other social-engineering attacks.
- Change Management: A documented change-management process is more secure than an ad-hoc process, which is more easily exploited by an attacker who claims to be in a crisis.
- Information Classification: A classification policy should clearly describe what information is considered sensitive and how to label and handle it.
- Document Handling and Destruction: Sensitive documents and media must be securely disposed of and not simply thrown out with the regular office trash.
- Physical Security: The organization needs to have effective physical security controls such as visitor logs, escort requirements, and background checks.

3 CONCLUSION

While the healthcare sector is an example of a domain working with very sensitive data, the networking sector is relevant in every sector, because the networks are key to the data.

Summarizing the suggested education of employees within the *healthcare sector*:

- Management and staff need to be regularly informed of *emerging* threats and risks and quality training should be be provided for each employee.
- Employees should be educated on actions they can take to *protect themselves personally* from the issues that individuals face.
- Clear communication channels that allow everyone to be more informed on the latest threats, and changes in previous threats.
- Explaining the possible consequences of security incidents in business terms.
- Providing comprehensive, *role-based courses* to selected management and staff members that require the *latest* knowledge regarding good security practices.
- Regularly providing *leading practice information* for various IT security and IT management processes. Some important processes include: patch and change management, configuration management, security archi-

tecture, fraud prevention and detection and physical security.

- A complete and periodic survey of management and staff to constantly assess, reevaluate and improve the quality of the information security system.

Summary for the network industry with key being the "Awareness culture" suggested by both Cisco as well as the mentioned security expert:

- A Top-Down Security Culture that
  - explicitly includes top management level staff and
  - consists of a collaboration throughout all processes and employees instead of a single security department or team.
- A Security-Awareness Training
  - to regularly inform the staff of current threats and
  - to prevent unintentional security problems.
- Security Policies and Procedures
  - Password Management
  - Two-Factor Authentication
  - Anti-Virus/Anti-Phishing Defenses
  - Change Management
  - Information Classification
  - Document Handling and Destruction
  - Physical Security

An *educated and motivated* workforce is considered key to a high level of security, thus not just the how, but the why of various security practices should be explained.

BIBLIOGRAPHY

[1] Chen, Y., Paxson, V., and Katz, R. What's New About Cloud Computing Security? *Electrical Engineering and Computer Sciences, University of California at Berkeley* (2010), 1–7.

[2] Cisco Systems, Inc. http://www.cisco.com/web/about/security/intelligence/mysdn-social-engineering.html. Last visit: 2013-03-22.

[3] Goodchild, J. Social engineering: Anatomy of a hack. *CSO Online* (2009), 1–3.

[4] Grossman, J. 10 Important Facts About Website Security and How They Impact Your Enterprise. *A WhiteHat Security Whitepaper* (2011), 1–10.

[5] HIPAA. http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html. Last visit: 2013-03-22.

[6] Juszczyk, M. Impact of Human Factor in Data Security. *Actual Problems of Economics 6* (2011), 359–363.

[7] Shirandula, A., Wanyembi, G., and Karume, M. Evaluation of Data Security Measures in a Network Environment Towards Developing Cooperate Data Security Guidelines. *International Journal of Advanced Computer Science and Applications 3*, 3 (2012), 106–109.

[8] Swanson, D. Improve IT Security: Educate Staff. *Journal of the Association of Healthcare Internal Auditors, Inc. 6* (2009), 43–45.