Proschinger, Christian

Conference Paper

StuxNet, AnonAustria, DigiNotar & Co: What they teach us about operating IT systems in a secure way

23rd European Regional Conference of the International Telecommunications Society (ITS), Vienna, Austria, 1st-4th July, 2012

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Proschinger, Christian (2012) : StuxNet, AnonAustria, DigiNotar & Co: What they teach us about operating IT systems in a secure way, 23rd European Regional Conference of the International Telecommunications Society (ITS), Vienna, Austria, 1st-4th July, 2012, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/60354

StuxNet, AnonAustria, DigiNotar & Co - what they teach us about operating IT systems in a secure way

Christian Proschinger, BSc; Mag. Otmar Lendl

e-mail:[nachname]@cert.at

Abstract

Information technology (IT) is no independent technology island anymore. Today it is an essential part of our society. Critical functions of countries are based on information technology. For example there is no electricity without IT and there is no IT without electricity. Our civilization is reliant on processes that are IT driven. This critical infrastructure, especially the critical information infrastructure, is often operated by private companies. With the development of IT networks, the integration of the business processes between organizations has increased, too. Thus the protection of the critical information infrastructure has become a high priority topic for the governments in Europe and all over the world. It can only be handled in cooperation between public and private stakeholders.

IT security is a quality aspect of operating IT infrastructure. The availability, integrity and confidentiality of the systems and processed data have to be guaranteed.

StuxNet has been the successful proof that malware can attack industrial control systems. Such systems are used to control a wide variety of machinery, from power plants to assembly lines.

DigiNotar was a Certificate Authority – part of the critical information infrastructure of the Netherlands. Its compromise in 2011 is a prime example of an attack of a (inter-) national relevant IT system and demonstrates the wide-reaching impact such an event can have.

Last summer the attacks by AnonAustria generated a lot of publicity. The Austrian national Computer Emergency Response Team – CERT.at and the Government CERT – GovCERT Austria have been involved in the handling of these incidents. Our experience shows how important it is for an organization to know how to deal with “Hacktivism”.

All these attacks have shown various technical and organizational aspects which have to be considered to guarantee a secure IT operation. This paper gives an overview about the lessons learned.

Introduction

Compared to other engineering disciplines, information technology is a very young area, but it has changed our daily life as profoundly as electricity or cars. Without IT, the productivity gains in almost all sectors of the economy would not have been possible. The establishment of the Internet has further accelerated this change. The use of information technology has made “just-in-time” production possible. All this brought the dependency on information technology from the production of virtual goods to the manufacture process of real goods like cars.

A reliable IT infrastructure is thus one of the foundations of a modern economy.

To process data in a reliable and secure way three main properties have to be fulfilled:

- Integrity
- Availability
- Confidentiality

The importance of these factors depends on the sector of industry. In the finance area the integrity and confidentiality is very important, concerning electricity the availability is one of the highest priorities. For the Domain Name System the integrity and availability is essential.

As early as 1988 (the outbreak of the Morris worm) IT administrators around the world realized that security incidents on the Internet can only be solved by cooperation. So the first Computer Emergency Response Team (CERT) was found: CERT/CC at the Carnegie Mellon University. (Carnegie Mellon University, 2012)
CERTs can be categorized by their constituencies.

- National CERT: contact point and/or responsible for a whole country
- Military CERT: operated by and/or for the military IT
- Governmental CERT: responsible for the Government and public authorities IT
- Organizational CERT: for example for companies.

CERT.at is the Austrian national CSIRT[1]. It’s constituency is the Austrian Internet space (IP addresses, *.at). It is also the fallback CERT for Austria – if the issue is not handled by a team directly responsible for the problem, then CERT.at will take up the issue and coordinate a solution. CERT.at is a joint project of the Austrian domain name registry nic.at (a company owned by a private foundation) and the Federal Chancellery.
(CERT.at, 2012)
The Austrian Federal Chancellery and CERT.at are also operating the Governmental CERT called GovCERT Austria as a Public-Private-Partnership.
(Austrian Federal Chancellery, 2012)

[1] Computer Security Incident Response Team (CSIRT) and Computer Emergeny Response Team (CERT) are used as Synonyms. CERT is a protected trademark by the Carnegie Mellon University.

In this functions CERT.at has been involved in many large scale security incidents in different ways, from analyzing and distributing information to the right stakeholders and affected organization in Austria, working as clearinghouse up to taskforces handling incidents on-site.

In this paper a recap of the biggest security issues of the last 2 years is given. The lessons learned there give some clues to what is needed for secure operation of IT systems.

StuxNet stands for the first famous malware which targeted industrial control systems. It was discovered in July 2011 and analyzed in detail by many malware laboratories. In the first step it infects the computers, which are used to program the programmable logic controllers (PLCs). These are typically Microsoft Windows desktop computer. Stuxnet manipulates the program code which is pushed on the PLCs in a way that it can hardly be detected by the operator. It is a kind of rootkit for PLCs. The most infections have been seen in Iran. The malware has used four Microsoft Windows vulnerabilities, two of them are zero-day exploits[2]. (Falliere, Murchu, & Chien, 2011)

DigiNotar
In September 2011 the information about the compromise of the Certificate Authority (CA) DigiNotar became public (DigiNotar noticed the hack already in July). The attackers generated certificates for popular websites like google.com. This was used to intercept communication of users. By analyzing the logfiles of the Online Certificate Status Protocol Server have shown that these fake certificates have been used around the world, but especially in Iran.
DigiNotar was also operating the sub-CA of for the government.
This incident killed DigiNotar: it had to declare bankruptcy and was subsequently liquidated. (FOX-IT & Prins, 2011) (ENISA, 2011)

Anonymous and AnonAustria
Anonymous is a new actor in the IT security landscape. It is a mixture of hacking and activism. While old-fashioned activism might block employees from enter the office building, Hacktivism uses denial of service attacks against the company's Websites. Instead of putting provocative posters at the outside wall of office buildings, web defacements are done.
Anonymous uses social media in a very professional way. So they find a lot of media echo. Companies often don't know how to react to this threat. (Lendl, Bundeskanzleramt, & BVT, 2011)

Lessons Learned for secure IT Operations

The security incidents and events of the past years have demonstrated some essential aspects of secure IT operations.

Don't follow security myths

Some flawed assumptions are used again and again to justify security decisions.

[2] If the vulnerability is exploited before the vendor has been notified and the vulnerability and exploit become public on the same day, this called a zero-day exploit

- Myth: “Industrial Control Systems and Embedded Systems don’t have to be patched.”

Usually Industrial Control Systems have a lifetime cycle of up to 20 years and more. Many of these devices are running on commodity operating systems. Just like any other software, it is likely that critical security vulnerabilities will be found every now and then. It is thus necessary to have a vulnerability- and patch management in place.

- Myth: “It is in a separate network, so it is secure”

Also networks without connection to the internet or corporate network have contact with the environment. The assumption of the distribution way of StuxNet is the maintenance technician (Notebook or USB-Stick). If systems are not patched for years, they can get infected in a very easy and successful way.

- Myth: “It is proprietary, so it is safe, because it is too complex to understand”

Security by obscurity is a bad idea. Motivated security researchers have shown many times, that nearly everything can be reverse engineered[3]. To be secure it has to be designed in a secure way. For example, it is a well-accepted rule that the security of a cryptographic system must lie in the strength of the algorithm and not in its obscurity.

- Myth: “Security problems can be kept secret”

If vulnerabilities exist, they are found by security researchers, in many times not only by one.
DigiNotar has shown that the hesitant behavior has made the situation worst. Users have been attacked and the company was liquidated. (FOX-IT & Prins, 2011)

Social Media and security
Social media, and in particular Twitter, have decreased the reaction time of the traditional media dramatically. If security issues get reported by a person who has journalists as followers (like Anonymous and AnonAustria have) press inquiries reach companies within minutes. At this time organizations already have to be prepared.

Social Media allows discussion. A company which tries to downplay a problem basically taunts the attacker to prove his claim. This is not a good idea.

Crisis communication
An organization has to be prepared how to handle security incident. Crisis Management also includes Public Relations.
Make sure your press speaker knows how to handle Hacktivism. He should try to de-escalate the situation.

Reporting of security issues
In many cases security problems or vulnerabilities are reported by the person who found it direct to the organization.

[3] For example: at the Computer Chaos Congress 2008 reverse engineering an algorithm from the microchip was shown. http://events.ccc.de/congress/2008/Fahrplan/attachments/1182_nohl.pdf

There are different channels:

- Telephone
- Email
- Social Media (Twitter, Facebook, …)
- Personally

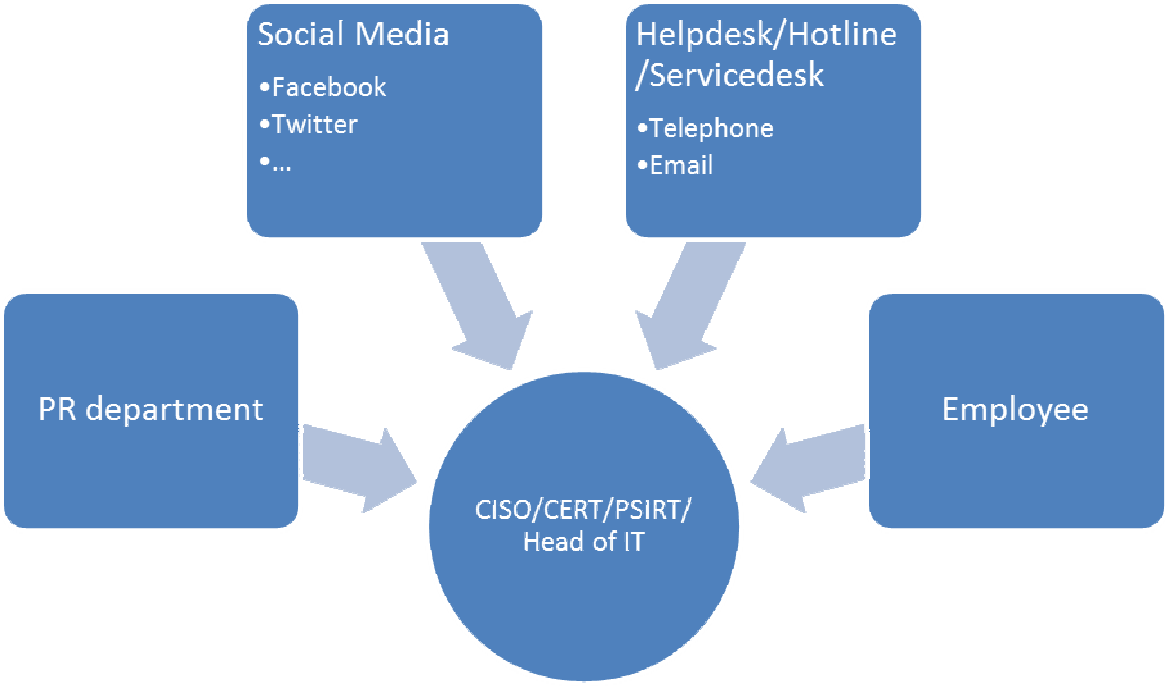

Figure 1: Sources of security relevant reports

Organizations have to define one technical competent single point of contact, which is also visible to the outside world, for example a CERT.
The call-center agents and marketing department has to be coached to report security related messages to this single point of contact. For example they should know what XSS and SQL Injection stands for. Reporting vulnerabilities using Twitter is already a common way.

The own employees have to be made aware of reporting security issues to this point of contact.

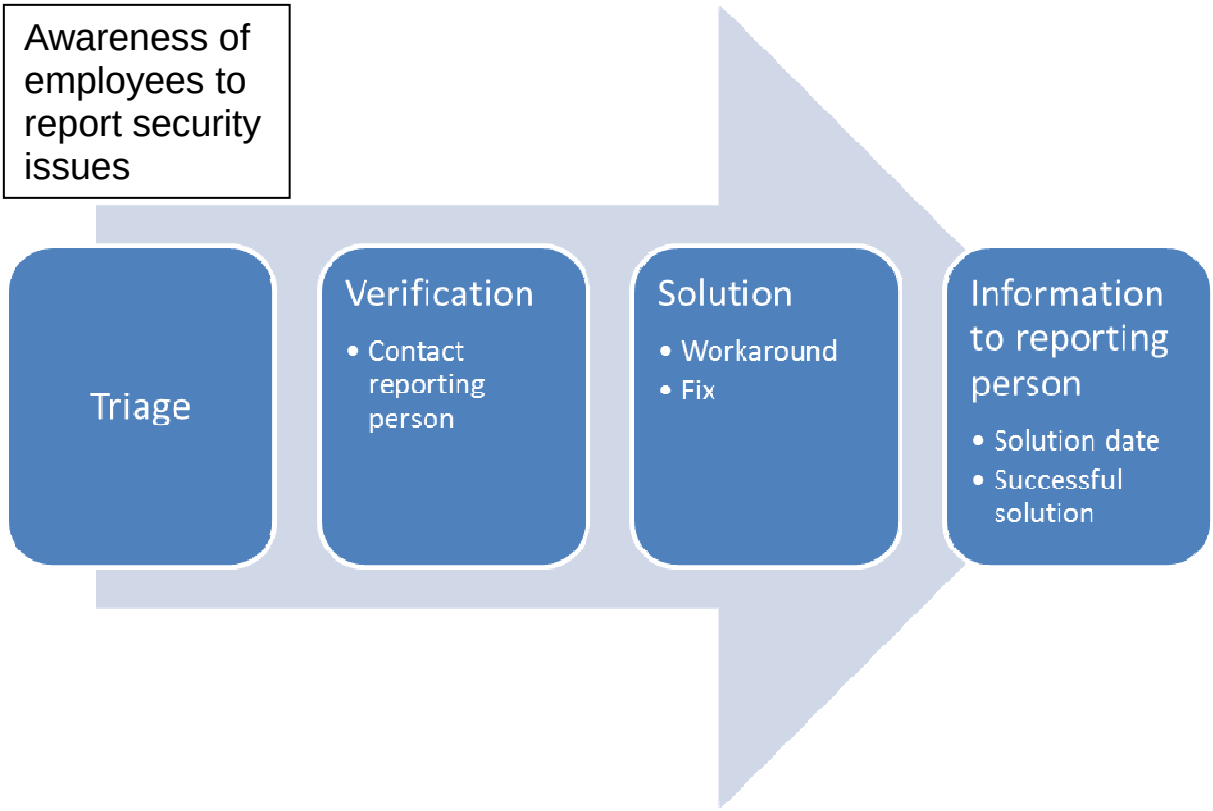

Figure 2: Solving security issues

These are recommended steps solving reported security problems:

- Talk to the person that reported the issue in a friendly way. You can get more information about the problem which makes it easier to verify it.
- Verify it.
- Make a triage to define how critical is this issue
- Find a solution/workaround
- Communicate to the finder until when you can fix it
- Think about the information policy to your affected customers.
- Fix It
- Tell the finder that you have solved it.
- Say “Thank You”.

(Lendl, Bundeskanzleramt, & BVT, 2011)

Technical issues

First some organizational aspects have to be considered.

A good asset management is the basis for a number of actions. A company needs to have an inventory about the equipment and software used, of all websites it operates (in-house and externally), of all interfaces it offers to other firms, and even all X.509 certificates used. (Lendl, Bundeskanzleramt, & BVT, 2011)

If parts of the infrastructure are outsourced the responsibilities have to be defined in a written contract, including security topics like patch management and security incident handling.
(Lendl, Bundeskanzleramt, & BVT, 2011)

Regular technical security audits (penetration tests) should be done for in- and outsourced IT systems and software. Especially before the launch of a new system, for example a website, it should be audited by a penetration test. (Lendl, Bundeskanzleramt, & BVT, 2011)

Mission creep has caused the problems in some incidents we have seen in the context of AnonAustria. IT-Systems that are intended for a limited task can become – over time – business critical systems processing sensitive information. A regular review of the initial assumptions versus the current reality is needed. (Lendl, Bundeskanzleramt, & BVT, 2011)

Organization should take care about their certificate handling. It is important to operate an up-to date inventory about the used X.509 certificates. For business critical applications buying "spare" certificates from a second Certificate Authority can be a risk prevention measure. (Lendl, Bundeskanzleramt, & BVT, 2011)

A good baseline security can be established if developers, system architects administrator are trained to conduct internal technical audits. This raises the awareness for security and improves their understanding about security problems. Many open source projects can be leveraged for this.[45] (Lendl, Bundeskanzleramt, & BVT, 2011)

Some data leaks form Anonymous attacks have been caused by old logfiles on servers. Introduce a clean server policy to mitigate this risk. Logfiles should be stored on a separate device and only be kept as long as necessary. Productive IT systems have to be cleared from not compiled source code and unused script code (Lendl, Bundeskanzleramt, & BVT, 2011)

Organization should think about what they are logging and how long the store it. Devices like firewalls, webserver should be included. It has to be done on a separate, centralized server. For the forensic analyze is important that the system time of all the devices is synchronized. (Lendl, Bundeskanzleramt, & BVT, 2011)

Google Hacking offers the organizations an easy way to check their outside appearance in the internet. Regular searches for leaked information or vulnerable systems in context of the organization should be done. (Lendl, Bundeskanzleramt, & BVT, 2011)

Before restarting service on a compromised machine, it is imperative to be absolutely sure that you can answer the following question:

- Which data has been manipulated / copied?
- Which system rights did the attacker gain?
- Could the attacker compromise any further systems?
- Are all identified vulnerabilities fixed?
- Has the server passed a detailed technical security?

(Lendl, Bundeskanzleramt, & BVT, 2011)

[4] Open Web Application Security Project (OWASP): www.owasp.org provides training material and tools for secure programming. WebGoat is a free training platform for the top ten web application security vulnerabilities.

[5] Backtrack (www.remote-exploit.org) is a free penetration testing Linux distribution.

If there are any doubts, a re-installation is recommended.

Conclusion

The attacks of 2011 have affected the critical infrastructure of countries. The DigiNotar case had the potential to disrupt the e-government processes. StuxNet affected the uranium-enrichment process of Iran. In many cases basics of secure IT operations have been ignored. The appearance of Hacktivism is a new challenge including social media and crisis communication.
Implementing baseline security can prevent organization and their clients form becoming a victim. Companies should harvest the low hanging fruit before someone else does it for them.

References

CERT.at. (30. 5 2012). Abgerufen am 1. 6 2012 von www.cert.at

Austrian Federal Chancellery. (1. 5 2012). *GovCERT Austria*. Abgerufen am 2. 5 2012 von GovCERT Austria: www.govcert.gv.at

Carnegie Mellon University. (01. 05 2012). *CERT/CC*. Abgerufen am 21. 5 2012 von CERT/CC: www.cert.org

ENISA. (2011). *Operation Black Tulip: Certificate Authorities lose authority.* Crete: ENISA.

Falliere, N., Murchu, L., & Chien, E. (2011). *W32.Stuxnet Dossier.* Symantec.

FOX-IT, & Prins, J. (2011). *DigiNotar Certificate Authority breach "Operation Black Tulip".* Delft.

Lendl, O., Bundeskanzleramt, & BVT. (2011). *Erfahrungswerte aus den Webserver Sicherheitsvorfällen von 2011.* Wien.