Professional paper

Cyber-attacks as a Threat to Critical Infrastructure

Roman Domović
Zagreb University of Applied Sciences
Vrbik 8, Zagreb, Croatia
roman.domovic@tvz.hr

Summary

In today's world, hybrid warfare is present like never before. The top spot holds information operations, perception management and various types of cyber-attacks. Cyber-attacks that can be carried out via critical infrastructure can disable the normal functioning and development of a society or state for a long time. Analyzing such threats and designing solutions to reduce or eliminate these threats is a challenge for current and upcoming generations of computer security and legal experts. In this research paper, some examples of cyber-attacks on critical infrastructure from this decade are analyzed to see which attack vectors are the biggest threats and what can be done to avoid or minimize its impact.

Key words: hybrid warfare, cyber-attacks, critical infrastructure, defence strategies

Introduction

In the modern world, various states, centers of power, various activist groups and individuals are trying to spread their influence. The spread of influence can be done in two ways: through hard power and through soft power. Hard power refers to military power threats and the realization of these threats. Soft power relies on the ability to shape priorities of others by influence. Instead of pushing someone to do something, the same goal is achieved through co-operation. [1] But there is a gray zone, something that is neither purely conventional warfare, nor peaceful diplomatic and economic action. It is so-called hybrid warfare, where superiority is achieved by handling information and information and communications technology (ICT) infrastructure. Apart from the problems that may arise in private and business networks, special problems can arise out of threats on critical infrastructure. Given the role critical infrastructure has, it can have serious consequences for the stability and integrity of states. There are many different attack vectors like email attachments, insecure network connection, physical access to an insufficiently protected device, web pages, operating system ex-

[1] Joseph Nye: Soft Power : The Means of Success in World Politics, pp. 5, 2004.

ploits, social engineering and human error. The aim of this research paper is to analyze several examples of cyber-attacks on a critical infrastructure, to see which attack vector represents the greatest danger and what can be done to avoid or minimize the impact of certain cyber-attack.

Critical infrastructure

Although there is no universally agreed definition, critical infrastructure is generally understood as "those facilities and services that are vital to the basic operations of a given society, or those without which the functioning of a given society would be greatly impaired".[2] According to the directive of the Council of the European Union, "critical infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."[3]
The sectors covered by these definitions differ from country to country, but generally include transportation systems (air, rail, road, sea); energy production and shipping; government facilities and services, including, in particular, defense, law enforcement and emergency services; information and communication technology; food and water; public health and health care; financial institutions.[4] Today, all these resources are managed by means of information-communication technology, which opens up a special attack vector. What makes it an advantage for easier management and control is at the same time a weakness subject to attacks. Why is information-communication technology at the same time a weakness?

About cyber-attacks

According to Bruce Schneier, "there are a bunch of reasons for this, but primarily it's:

1. the complexity of modern networked computer systems and
2. the attacker's ability to choose the time and method of the attack versus the defender's necessity to secure against every type of attack".[5]

[2] NATO Parliamentary Assembly. Document 162 CDS 07 E rev 1 – The protection of critical infrastructures, 2007, http://www.nato-pa.int/Default.asp?SHORTCUT=1165. (Access date: 02. 04.2017).

[3] The Council of the European Union: Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. (Text with EEA relevance). http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008L0114 (Access date: 02.04.2017).

[4] NATO Parliamentary Assembly. Document 162 CDS 07 E rev 1 – The protection of critical infrastructures, 2007, http://www.nato-pa.int/Default.asp?SHORTCUT=1165. (Access date: 02. 04.2017).

[5] Bruce Schneier. Attack vs. Defense in Nation-State Cyber Operations. https://www.schneier.com/blog/archives/2017/04/attack_vs_defen.html (Access date: 09.04.2017).

Why can we consider that Schneier is right? In the protection of information-communication systems it is essential to keep its functionality, easy manageability, scalability and supervision of the system. In the data security it is essential to stick to the classical principle of cryptography, i.e. to preserve the confidentiality, authenticity and integrity of the data. If we look at the examples, we can see that this is a very demanding task. For example, GSM technology and its upgrades are the world's largest security system. There are more than four billion active security features in it.[6] The implementation of GSM technology for practical purposes leads to a number of large and complex information systems. Since the information and communication system consists of not only software and hardware, but also the people who manage it and protocols and procedures under which it is being operated, it is obvious that there are many points where an error or omission may occur. Attackers who actively monitor what is happening can take advantage of it. Smaller systems, even the smallest, are subject to the same.

The attackers in front of them have a concrete system with concrete technological solutions. They have advantage over defence which has to anticipate attacks, which is practically impossible because the attacks are enhanced by the development of technology and knowledge. And it requires time that defence doesn't have at its disposal. At the time of launching a system in operation, attacks on it or its parts may be completely unknown and impossible to predict. In addition, sharing knowledge in computer security is often hampered by business secrets and the secrecy of scientific discovery until its publication in a journal or at a conference. This benefits the group of attackers who unite resources in an attempt to attack a newly discovered weak point in a system.

In general, cyber-attacks can be divided into four categories according to the type of the attack:[7]

a. hacktivism – political propaganda and protest, fun or self-proving,
b. cyberespionage – strategy aimed at obtaining critical governmental or corporate information by breaking into computer networks and systems,
c. cybercrime – motivated by economic gains through illegal penetration of computer networks and relatively non-violent in nature,
d. cyberwarfare – actions by a nationstate to penetrate another nation's computers or networks for the purpose of causing damage or disruption.

Whoever runs the attacks, needs resources to do it. Resources cost. But equally, resources also cost the defense. Rebecca Slayton in her detailed analysis of the balance between cyber offense and cyber defense balance says that improvement of various defensive practices "will not produce invulnerable organiza-

[6] Dan Forsberg, Gunther Horn, Wolf-Dietrich Moeller, Valtteri Niemi. LTE Security, pp.28, 2010.

[7] Tobby Simon. Critical Infrastructure and the Internet of Things, 2017. https://www.cigionline.org/sites/default/files/documents/GCIG%20no.46_0.pdf (Access date: 09.04.2017).

tions, but they can increase the costs to attackers and decrease the costs of defenders". And also that "innovation in software development processes and technologies can make attack much more difficult". She concludes that "offensive advantages are not inevitable in cyberspace, and they cannot be eliminated by a technological fix. Instead, gaining defensive advantage will require persistent investments in technological management, innovation, and skill".[8] All this applies to cyber-attacks on critical infrastructure. By analyzing the cyber-attacks on critical infrastructure, it is possible to draw conclusions about which attack vectors are currently the most common and which critical points of the system within critical infrastructure are the most vulnerable.

Threat analysis

For the purpose of this paper five major cases of cyber-attacks on critical infrastructure from this decade have been analyzed.

1. In 2010. Stuxnet worm was detected and it was a first worm known to attack Supervisory Control And Data Acquisition systems (SCADA). It destroyed a number of Iranian nuclear centrifuges. Symantec Security Response team did a thorough examination of Stuxnet and concluded that it was created with the aim "to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment". To increase chances of success, Stuxnet authors implemented various components such as zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface.[9] Stuxnet was created to attack specifically Siemens S7-300 system running centrifuges in Iran's nuclear-enrichment program. It installs malware on the PLC that monitors the Profibus of the system and under certain conditions it periodically modifies that frequency, which results in that the connected motors change their rotational speed.[10] Eventually, it leads to destruction of centrifuges. Infection starts by plugging in a USB flash drive or from the internal network if an infected machine exists. In this case, the attack vector is a human error, an error made by the operator that works in the nuclear facility complex, who inserts the infected USB into the computer connected to the facility network.

[8] Rebecca Slayton. What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. International Security, 2017(41), No. 3, pp. 72-109.

[9] Nicolas Falliere, Liam O Murchu, Eric Chien. W32.Stuxnet Dossier, 2011. /w32_stuxnet_ dossier.pdf (Access date: 16.04.2017).

[10] Stamatis Karnouskos. Stuxnet Worm Impact on Industrial Cyber-Physical System Security, 2011, http://papers.duckdns.org/files/2011_IECON_stuxnet.pdf (Access date: 16.04.2017).

2. In 2011 there was an attempt made to breach the Information Technology (IT) systems of Lockheed Martin, the American global aerospace, defense, security and advanced technologies company. But story begins earlier when the so-called Advanced Persistent Threat (APT) attack was carried out on United States security company RSA, consisting of three phases. The first phase of such attack is studying the targets and conducting social engineering over the target by which it is fooled, causing it to install malware. The second phase is a breakthrough in the network and the search for the appropriate parts of the information system, such as a user with as many administrator access rights to servers as possible. The third phase is the ultimate activity such as data gathering, data modification, data deletion, etc. In this attack, the attacker sent two different phishing emails within two days to two small groups of employees, who at the first glance were not worth the effort, just doors to higher levels. The assumption is that the attacker had previously gathered information about these employees. The email subject was "2011 Recruitment Plan". One employee opened an Excel file that was in the email attachment, entitled "2011 Recruitment plan.xls". The Excel document contained a zero-day exploit that installs backdoor through Adobe Flash vulnerability (CVE-2011-0609). After that, Poison Ivy malware was installed on the computer, which enabled the attacker to supervise the employee's computer and break in further into the company network. The attacker found certain RAR files on one server and sent them via an FTP server to an external server.[11] There were indications that a database was stolen which links serial token numbers called RSA SecureID and "seed" that each token fills so it becomes unique. There are also indications that this data was used to attack Lockheed Martin. The attack was possible because Lockheed Martin employees, along with thousands of employees from other companies, use RSA SecureID tokens to log onto computers and other sensitive parts of information systems. In this case, the attack vector is also human error, an error made by the operator that works in the company, who opened infected file on a computer connected to the internal company network.
3. In 2014 a hacker group known as Dragonfly or Energetic Bear attacked companies from energy sector in Europe and United States. In the attack they used malware "Havex" to run into the control system of the attacked companies.[12] When Havex infiltrated these systems, he sent sensitive

[11] RSA FraudAction Research Labs. Anatomy of an Attack, April 1, 2011, URL: http://blogs.rsa.com/anatomy-of-an-attack/ (Access date: 16.04.2017).

[12] Trend Micro. Report on Cybersecurity and Critical Infrastructure in the Americas, 2015, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf (Access date: 29.04.2017).

information back to hackers. Havex is known to be distributed to targeted users through three arrival vectors: spam emails, exploit kits and trojanized installers planted on compromised vendor sites. Security experts from F-Secure company discovered that the main components of Havex malware are a general purpose Remote Access Trojan (RAT) and a server written in PHP. They also discovered how Havex operates. "Once the Havex malware has been delivered to the targeted users and installed on a machine, it scans the system and connected resources accessible over a network for information of interest. This information includes the presence of any Industrial Control Systems (ICS) or Supervisory Control And Data Acquisition (SCADA) systems present in the network. The collected data is then forwarded to compromised websites, which surreptitiously serve as remote Command and Control (C&C) servers."[13] In this case, the attack vector is also human error, an error made by certain users who have released malware into the networks.

4. In 2014. an attack was launched on a steel factory in Germany. According to a report by Germany's Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI), the attackers first infected the steel factory office network by spear-phishing emails and smart social engineering. From there, they progressed through a network and other systems including systems that control the plant's equipment, to cause frequent falls of individual control components and various systems. Consequently, the operators were unable to adequately regulate and immediately turn off a blast furnace. BSI stated that final result was "massive damage to the plant".[14, 15] In this case, the attack vector is also human error, an error made by certain employees who have activated backdoor and released malware into the network.
5. On December 23, 2015 an event that according to gathered evidence points to a cyber-attack at three regional electric power distribution companies, called Oblenergos, has caused a power outage in Ukraine and made impact on approximately 225,000 customers. According to ICS-CERT report, "the cyber-attack was reportedly synchronized and coordinated, probably following extensive reconnaissance of the victim networks. According to company personnel, the cyber-attacks at each company occurred within 30 minutes of each other and impacted multiple

[13] F-Secure. Backdoor:W32/Havex : Threat description, 2014, URL: https://www.f-secure.com/v-descs/backdoor_w32_havex.shtml (Access date: 29.04.2017).

[14] Trend Micro. Report on Cybersecurity and Critical Infrastructure in the Americas, 2015, (Access date 29.04.2017.). URL: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf (Access date: 29.04.2017).

[15] F-Secure. Backdoor:W32/Havex : Threat description, 2014, URL: https://www.f-secure.com/v-descs/backdoor_w32_havex.shtml (Access date: 29.04.2017).

central and regional facilities. During the cyber-attacks, malicious remote operation of the breakers was conducted by multiple external humans using either existing remote administration tools at the operating system level or remote industrial control system (ICS) client software via virtual private network (VPN) connections. The companies believe that the actors acquired legitimate credentials prior to the cyber-attack to facilitate remote access." Attackers executed the KillDisk malware and wiped some systems, probably in the way that "KillDisk malware erases selected files on target systems and corrupts the master boot record, rendering systems inoperable". More damage has been done by KillDisk's overwriting of Windows-based human-machine interfaces (HMIs) embedded in remote terminal units, corrupting firmware of Serial-to-Ethernet devices and making them inoperable and scheduling disconnects for server Uninterruptable Power Supplies (UPS) via the UPS remote management interface. Companies also reported that they had been infected with BlackEnergy malware which was delivered via spear-phishing emails with malicious Microsoft Office attachments. It is suspected that it may have been used as an initial attack vector to acquire legitimate credentials.[16] ICS-CERT report does not confirm that BlackEnergy played a role in this cyber-attack, but it looks so and other sources support it.[17, 18] In this case, the attack vector is also human error, an error made by certain employees who have activated backdoor and released malware into the network.

Discussion

Attacks have occurred and the damage is done. Based on the performance of the attacks and the spotted defects in defense it can be analyzed which scenarios should occur so that the attacks are unsuccessful and without or with less damage. Unfortunately, all essential attacks detail and countermeasures needed for thorough in-depth analysis are not available. Therefore, after the analysis carried out on the basis of available information, a synthesis of the necessary defense countermeasures can be made.

Particularly interesting case is a Stuxnet breach into the uranium enrichment plant in a desert outside Natanz in central Iran. This facility is buried more than

[16] ICS-CERT. Alert (IR-ALERT-H-16-056-01) : Cyber-Attack Against Ukrainian Critical Infrastructure, 2016. URL: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (Access date: 30.04.2017).

[17] Trend Micro. Frequently Asked Questions: BlackEnergy, 2016. URL: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy (Access date: 30.04.2017).

[18] F-Secure. Backdoor:W32/BlackEnergy: Threat description. URL: https://www.f-secure.com/v-descs/backdoor_w32_blackenergy.shtml (Access date: 30.04.2017).

15 meters beneath the desert surface. Its wall and roof are reinforced with concrete and covered with layers of earth and it is heavily guarded.[19] This prevents unwanted surveillance over the facility, physical entry into the facility and partially protects it from missiles and different kinds of armed attacks. Regarding to cyber-attacks, it prevents side channel attacks on the internal electronic devices and communication. Internal network, computers and various electronic devices such as International Atomic Energy Agency (IAEA) digital surveillance cameras installed inside the facility are all air-gapped. It means that they are isolated from the internet or any other external network, which prevents direct intrusion by remote attackers. Policies and procedures are arranged so that the air-gap could not be bypassed. It looks like all the necessary protection measures have been taken so that any type of cyber-attack taken from the outside is not possible. But still, the successful attack has been done. How? Since it is impossible to access internal devices from the outside because of the air-gap, the air-gap needs to somehow be bypassed. Now, components inside the plant must be updated from time to time. Whether it is updating of operating systems, software, hardware or firmware, whether it is adding new components to a facility that should be connected to others, these operations are usually conducted by outside contractors. Technicians who are employees of companies who as outside contractors collaborate with a nuclear facility, have the ability to enter the plant and perform upgrades of the system. For the upgrade, it is necessary to add new parts of the upgrade to the existing components. To do this, it is necessary to connect existing components to a laptop, tablet or USB flash drive of an external technician, or to insert a CD / DVD into it. And there is the air-gap bypass.

Because of the need for upgrading, an absolute air-gap is not possible. Stuxnet was sent to spread across the world to increase the possibility of breach, with the main target – USB flash drives of four carefully selected companies that were outside contractors of Natanz nuclear facility, dealing with "manufacturing products, assembling components or installing industrial control systems".[20] These companies were a gateway and its infected technicians were carriers which passed Stuxnet inside Natanz facility and bypassed the air-gap. So, a scenario in which no air-gap bypass comes up includes a thorough check of every device entering the plant, conducted on separate pieces of equipment that are also air-gapped. It is time consuming and requires additional resources but reduces the possibility of breach. For such cases, an optimal solution should be found, but it cannot be presented in this paper because any such solution depends on the specific situation in a specific environment.

[19] Kim Zetter: Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (2015).

[20] Ibid.

In four other cases, there were procedures under which employees should not open suspicious files or click on suspicious links. Despite this, the breaches occurred by phishing emails and compromised web sites which download payloads to an access computer. A scenario in which such breaches cannot occur involves administrator procedure of blocking every incoming file on the email server, sending message to a recipient that there is a file for him and that it should be checked on the air-gapped machine before being delivered to a specific computer. But this procedure can create a massive queue on email checking which can affect working efficiency and cause harm to operational capabilities of certain critical infrastructure. There can be other solutions and again, an optimal solution depends on the specific situation in a specific environment.

From all analyzed cases it is possible to extract elements of cyber-attacks that represent the greatest threat. The greatest threat that cannot be entirely resolved will remain the existence of zero-day exploits and carefully programmed malware which can remain undetected despite sophisticated digital-forensic equipment, all-rounded procedures, staff knowledge and experience. Secondary to that is the impact of social engineering. If the precautionary measures are intensified, it may be significantly reduced.[21] It would be irresponsible to say that it can be completely eliminated.

Also, it is possible to extract elements of cyber-attack countermeasures that are usually implemented, but must be improved. These are:

- incomplete procedures > that should be all-rounded to be able to prevent the air-gap bypassing,
- insufficient education of employees who are subject to social engineering > there must be constant raising of awareness of the methods of social engineering, data protection, information-system security and above all awareness of the need to protect critical infrastructure as a whole,
- insufficient coordination with outside contractors > there must be service level agreement (SLA) which determines the course of action in accordance with the defensive strategies of a particular critical infrastructure.

Critical infrastructure must be protected physically and procedurally from all known types of attack. In addition, as much as possible, new types of attacks must be foreseen and accordingly there has to be a modular defense strategy. Implementation of defensive strategies depends on certain type of critical infrastructure, its business operation and cost/benefit analysis of cyber security investments. Due to the importance of critical infrastructure for the functioning of a society, defence strategies must be fully met.

[21] For an example see Bullee, Montoya, Pieters, Junger and Hartel: The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of Experimental Criminology, March 2015, Volume 11, Issue 1, pp. 97-115.

Conclusion

Hybrid warfare is a present danger. Cyber-attacks are being carried out frequently and the consequences are very expensive. Especially when it comes to attacks on critical infrastructure. From analyzed examples it can be concluded that the attacks are executed according to the APT attack pattern. In all cases, such attacks began by gathering information about certain employees who are then manipulated and deceived by social engineering which forces them to unconsciously install malware into the computer. That action allows attackers further penetration into the network and causing damage.

Part of the package of solutions that provide resilient critical infrastructure, in addition to high-quality security specialists and technology solutions, must include a scenario in which vital part of information systems must be procedures that prevent air-gap bypassing as well as continuing education of personnel in terms of computer security and how to not become a victim of social engineering who makes fatal errors.

For a thorough study on this topic, more examples should be analyzed with in-depth look at targeting infrastructure and types of cyber-attack methods.

References

Bullée, Jan-Willem H.; Montoya, Lorena; Pieters, Wolter; Junger, Marianne; Hartel, Pieter H. The persuasion and security awareness experiment: reducing the success of social engineering attacks. // Journal of Experimental Criminology. March 2015, Volume 11, Issue 1, pp. 97-115.

Falliere, Nicolas; O Murchu, Liam, Chien, Eric. W32.Stuxnet Dossier: Version 1.4. Symantec Security Response, 2011.

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers /w32_stuxnet_dossier.pdf (16.04.2017).

Forsberg, Dan.; Horn, Gunther.; Moeller, Wolf-Dietrich.; Niemi, Valtteri. LTE Security. Wiley; 2 edition, 2012.

F-Secure. Backdoor:W32/BlackEnergy: Threat description. https://www.f-secure.com/v-descs/backdoor_w32_blackenergy.shtml (30.04.2017).

F-Secure. Backdoor:W32/Havex: Threat description, 2014. https://www.f-secure.com/v-descs/backdoor_w32_havex.shtml (29.04.2017).

ICS-CERT. Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure, 2016. URL: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (30.04.2017).

Karnouskos, Stamatis. Stuxnet Worm Impact on Industrial Cyber-Physical System Security. // IECON 2011 – 37th Annual Conference on IEEE Industrial Electronics Society / Institute of Electrical and Electronics Engineers (IEEE), 2012, pp. 359-364 http://papers.duckdns.org/files/2011_IECON_stuxnet.pdf. (16.04.2017).

NATO Parliamentary Assembly. Document 162 CDS 07 E rev 1 – The protection of critical infrastructures, 2007, http://www.nato-pa.int/Default.asp?SHORTCUT=1165 (02.04.2017).

Nye, Joseph. Soft Power: The Means of Success in World Politics. 2004, New York: Public Affairs, 2004.

RSA FraudAction Research Labs. Anatomy of an Attack, April 1, 2011, http://blogs.rsa.com/anatomy-of-an-attack/ (16.04.2017).

Schneier, Bruce. Attack vs. Defense in Nation-State Cyber Operations. https://www.schneier.com/blog/archives/2017/04/attack_vs_defen.html (09.04.2017).

Simon, Tobby. Critical Infrastructure and the Internet of Things. Centre for International Governance Innovation, Chatham House, 2017, https://www.cigionline.org/sites/default/files/documents/GCIG%20no.46_0.pdf (09.04.2017).

Slayton, Rebecca. What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. International Security. Winter 2016/17, Vol. 41, No. 3, pp. 72-109.

The Council of the European Union. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. (Text with EEA relevance). http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008L0114. (02.04.2017).

Trend Micro. Frequently Asked Questions: BlackEnergy, 2016, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy (30.04.2017).

Trend Micro. Report on Cybersecurity and Critical Infrastructure in the Americas, 2015, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf (29.04.2017).

Zetter, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Broadway Books; Reprint edition (September 1, 2015).