THE HUMAN FIREWALL - THE HUMAN SIDE OF CYBER SECURITY

By Annamária Beláz, Doctoral School on Safety and Security Sciences, Óbuda University, Budapest, Hungary, belaz.annamaria@phd.uni-obuda.hu
and Zsolt Szabó, Doctoral School on Safety and Security Sciences, Óbuda University, Budapest, Hungary, szabo.zsoltmihaly@phd.uni-obuda.hu

Abstract

Cyber criminals are keen to exploit vulnerabilities in various software programs to gain access to users' computers and accounts and steal important data, such as credit card information. An important change in the case of digital data theft, compared to paper-based data management, is that in many cases, we do not even notice when something has gone missing. No need to go far back in time, just a few days ago, hackers had access to the Facebook profile of nearly 50 million customers, not just data, but were able to do what they wanted with the Facebook profiles, for example. They were also able to access other systems that the victim logged into with their Facebook profile. A little earlier, the credit card details of 380,000 customers who bought tickets on British Airways' website got into the wrong hands. In 2016, Tesco Bank (UK) lost the money of its 20,000 customers, also due to IT errors. And these are just some of the many events that are well known. Attacks are usually made with the use of automated methods that search for common bugs. These are the attacks you can and should defend against. It is essential to know what the potential faults of the IT system are and what you can do to prevent them. The purpose of the study is to analyze the role of humans in the information security of the digital state and society.

Keywords

Information security; IT security; human firewall; public administration; digital state and social content.

INTRODUCTION

The aim of modern on-demand government is to build effective efficient and economic public administration system and to increase client satisfaction. This is why electronic governmental services, identification and authentication processes have been developed continuously in the past few years in Hungary. The improvement programs on digital state building supported this goal as well. We cannot lose sight of the fact that during digitalisation programs, in order to build an open, safe and secure digital state, we must consider the cybersecurity aspect a priority.

Network-based information systems play a vital role in the daily lives of societies. The modernization of public administration and the process of digitization contribute to the transfer of official administration tasks from office buildings to citizens' homes and personal smart devices. Therefore the reliable operation and security of these systems are essential. At the same time, the frequency and impact of attacks that threaten the secure operation of information systems are increasing.

According to the RiskBased Data Breach QuickView Report 2019 Q3, at the end of September, there

were 5,183 breaches, exposing 7.9 billion records. Compared to the 2018 Q3 report, the total number of breaches was up 33.3 percent and the total number of records exposed more than doubled, up 112 percent [1]. A significant percentage of the leaked records are from or connected to public sector databases.

Alongside illegal data mining, other types of information security incidents are common to the public, such as denial of service attacks (DOS/DDOS), defacement, malware, phishing, spam, and unauthorized access.

Based on the Directive (EU) 2016/1148 of the European Parliament and the Council (of 6 July 2016) concerning measures for a high common level of the security of network and information systems across the Union (NIS Directive), the information system of the on-demand state public administration, the data produced, stored and transmitted by it, and the security of the persons and organizations using the system, must obtain the minimum capabilities necessary to provide an adequate level of protection.

In order to achieve the required level of protection, it is necessary that information security rules, as well as the principles and solutions of risk assessment and management related to the field, form an integral part of the development programs. The following sections briefly discuss the risk factors and the underlying concepts and principles[2].

TECHNOLOGICAL FACTOR: FIREWALLS AND ANTIVIRUS SOFTWARE

Nowadays, more and more devices can connect to the Internet, from fitness bracelets to smart washing machines to sophisticated industrial systems. While they make our lives easier and more comfortable, they are another attractive target for cybercriminals.

In 2017, various Internet-enabled devices, such as the Internet of Things (IoT) and the Industrial Internet of Things (IP), will become a significant risk factor for targeted attacks. Cybercrime targets vulnerabilities and unsafe systems and seeks to disrupt business processes – as was the case this year with Mirai malware[3].

Mobile devices are increasingly used in production and industrial control systems. In addition to the significant number of vulnerabilities in systems, this trend may expose organizations to additional threats. Cybercriminals are constantly improving their methods to circumvent the highest levels of protection and exploit the vulnerabilities of the latest technologies. According to Trend Micro's 2017 forecast, a growing number of financial professionals will try to ransack the key to the company's cash box with fraudulent emails, and no Internet-connected device can be safe from blackmail viruses.

In addition, cyber-propaganda and vulnerabilities are expected to continue to grow, in line with previous trends. Also, almost every day, new attack methods emerge and threaten organizations, newer tactics are deployed, and more devices are attacked. According to experts, another risk is misinformation: with 46% of the world's population having an Internet connection, cyber-propaganda will increase with the appointment of new leaders in the world, potentially providing the public with misinformation[4].

Thycotic has been surveyed by hackers at one of the most significant IT security events of the year at the Black Hat 2017 conference in Las Vegas[5]. According to the research, traditional border security technologies (firewalls, anti-virus software) are outdated, and sensitive data is most easily accessed through privileged (administrative) accounts.

According to a survey of 250 hackers, the easiest way to access company confidential information is

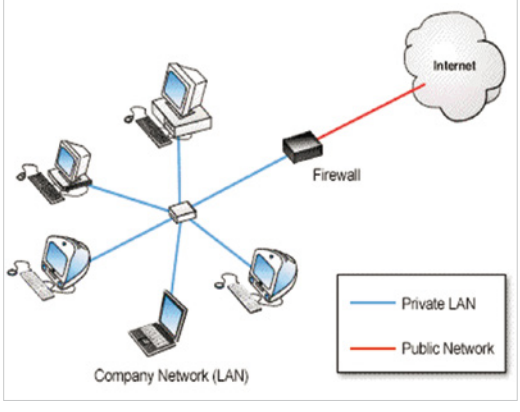

Figure 1. Firewall.

through administrative accounts (32%), followed by email accounts (27%) and endpoints (21%). 73% of participants say that traditional border protection tools such as anti-virus software and firewalls are outdated and easily circumvented.

According to those surveyed, cybercriminals' activities are mostly hampered by multifactor identification and encryption, and the most ineffective are intrusion prevention systems (IPS). 85% of hackers say human error is behind data loss. The reason for this is that there is increasing pressure on users, who eventually become tired of complying with security rules.

35% of average users said that keeping their passwords in mind and changing them is the biggest concern, but too much information (30%), ongoing updates to protect (21%), and constant cyber threats (15%) are also a problem[5].

HUMAN FACTOR: EMPLOYEE AS THE WEAK POINT

Information leaks are events that make information available to otherwise unauthorized parties by creating an opportunity for accidental or intentional data access.

According to much international and domestic research, the most common and costly damage caused by data leakage is caused by employees, not by external attackers:

"Companies can spend millions of dollars on firewalls, encryption, and secure access devices, but it's a waste of money because none of the measures address the weakest link in the security chain: it's the person who uses, administers, operates, and is responsible for these systems" [6].

György Vasvári, one of the pioneers of Hungarian information technology, and an active scientist throughout his life, formulated important and up-to-date ideas on one of the most pressing issues of information technology (IT) security:

"(...) I can say that Internet users are very proud that their system is protected by a firewall from various hacker attacks. But the hackers and the terrorists, are clever and turned to the weakest point, the user. Therefore, state-of-the-art computing says that the whole chain of people, employee security awareness, is all about the human firewall - and besides the technical firewall (Figure 1), we need to do the human firewall (Figure 2)" [7].

Most employees do not feel responsible for corporate IT security, and a quarter of large companies do not have security policies in place. It was revealed, among other things, by Cisco's security research conducted in 13 countries, interviewing more than 12,000 employees [8].

Cisco has conducted a survey in the Europe, Middle East, Africa, and Russia (EMEAR) region, which shows that large and small and medium-sized companies' IT security policies and resources are primarily protective against external threats; however, threats within the company receive little attention. The main findings of the research highlighted the following trends:

- 69% of respondents are unaware of major vulnerabilities or threats (such as Heartbleed or the recent Shellshock)
- Respondents considered cybercrime the main risk (60%), while user behavior was ranked second as a risk factor. 58% of those surveyed know that their company has an IT security policy, but 23% do not know it at all.
- 44% of respondents show little or no compliance, and every 14 people actively work around IT security.
- 31% of surveyed employees say that IT security is a barrier to innovation and collaboration or complicates working.

In the PwC 2019 survey, 9,500 respondents from 122 countries were interviewed. Simple business e-mail abuse remains the biggest business impact, and frontline employees continue to be the primary reason for security incidents [9].

As can be seen from the above, employee behavior and lack of awareness are the Achilles heel of enterprise IT security, which is becoming a growing risk factor. As companies isolate users from daily IT threats, most expect their corporate security systems to eliminate all potential risks.

User behavior should be considered. As part of the research, Cisco identified four typical behavioral

patterns related to IT security. Although one hundred percent security is never achieved, the following behaviors make it possible to develop security strategies that take into account different user behavior. In each case, the level of threat is different, and each user requires a different approach to minimize risk to companies, while not limiting the freedom of employees, allowing them to perform their day-to-day tasks with optimal efficiency. The four types of users can be described as follows:

- Conscious: is aware of security threats and does everything possible to stay safe online.
- Well-intentioned: makes an effort to comply with security rules, but occasionally fails, without any purpose.
- Irresponsible: expects the company to take all necessary security measures and does not assume any responsibility for data security.
- Bored and cynical: say security threat warnings are excessive and even that security measures discourage efficient work, so they prefer to bypass the rules for their own benefit.

The research points out the need to rethink security regulations in order to continue providing adequate protection against external attacks, while also adapting to employee behavior and expectations.

The development of user-centred control means that the former point security solutions will be replaced by centrally controlled, automatic controllers and applications. Enterprise mobility trends and employee expectations force IT executives to apply user-specific protocols to the tools employees use. This flexible security control enables the company to react quickly while reducing users and the company's vulnerability.

Lack of awareness is the biggest problem. According to the research, the most significant internal risk factor is the false sense of security that causes employees to believe that their company protects them from possible threats. 35% of respondents expect the company's security settings to protect against all kinds of threats, with nearly half (42%) saying it is their responsibility to keep their data safe, while 62% of respondents believe that their behavior has only a moderate impact.

This attitude results in a reduction in the effectiveness of security rules. While 59% of employees believe that a company has a valid security policy, nearly a quarter (23%) of respondents do not know whether there is any regulation. More than half (46%) of those surveyed believe that regulators have no effect on their activities, and 38% only see it when security settings prevent it.

However, in response to another question, 17% of employees said that IT security hinders innovation and collaboration within the company, and 14% feel restricted in their daily workflow. 17% of respondents believe that missed business opportunities cause the company to lose more than the loss due to a data leak.

Because nearly three-quarters (69%) of employees are unaware of problems affecting many users, such as Heartbleed or the recent Shellshock vulnerabilities, nearly one-third (32%) do not consider changing their security habits. More than half (55%) of users use the same password for all applications and websites, and 60% do not change their passwords regularly.

HUMAN FIREWALL: THE BEST PROTECTION

Last year was a year of blackmail viruses, and all indications are that this type of threat has reached its peak. However, cybercriminals are not expected to give up this lucrative source next year, and will even expand the pool of opportunities. Experts predict that the number of newly discovered blackmail virus families will increase as criminals look for new targets: POS terminals, ATMs and industrial systems will be targeted.

Even the best-built enterprise system cannot be protected if only one person is responsible for security. Experts believe that the only solution is to regulate users. The most significant vulnerability is the human side.

The enterprise data body is fundamentally complex, and it has become even more extensive and intricate with the appearance of smart devices. With the spread of the BYOD (Bring Your Own Device) model, some users and devices who hardly have any connection to the company can get access to its systems[10]. This is also the reason why there is no harmonized security in IT; people start using the system after "plugging in" their own devices, and therefore become the hole in that system.

Figure 2. Human firewall.

There are no asset systems that are both secure and quality-assured, so the business manager's problem to overcome. Continuous and immediate change monitoring would be necessary. Although developers repair systems, it is difficult for business executives to fix them on the go. However, reports of bugs also reach hackers; therefore, those who do not immediately use the new patches are at an increased risk, as criminals can identify these vulnerability holes.

What is the solution to the restructuring of the existing system? The answer seems obvious: on the one hand, new rules are needed, and, on the other, compliance with the rules needs to be promoted (see point V for details). Some systems have strict rules that apply to everyone who becomes part of the system – see traffic rules. There is no standard set of IT rules, but at least within companies, you have to implement one that you need to adhere to. We need solutions, not technology!

People, technology and policy (regulation) have to work together, but we have to put together a system that makes these three things work. The "human firewall" is more effective than anything else. It is not enough to deal with the "human factor" at one level only; in fact, the three groups need to communicate appropriately.

Secure corporate IT has more human aspects than you might think. So we need to look not only at machines, but also at people and on three levels. The product you buy does not protect itself, even if you buy the best on the market. IT security is not a product but a state. It must be achieved, and, very importantly, further sustained through action; it must be operated. For proper regulation, information security must be ensured from hardware, software and communication, i.e. systems (physical layer), people (personal layer – training, what to do and why it is important) and processes (organizational layer – broken down into specific corporate actions; who pulls the plug, if necessary, who reports, etc.)

Of the possible incidents, only one is due to viruses and malicious code. The critical issues are data leakage (when a colleague, for example, accidentally takes out sensitive data, e.g. sending a complete customer list instead of a quote) or denial of service. The latter can be crucial in the age of cloud computing. So the "human factor'' is an integral part of IT security. To increase the level of IT security in the organization, we need to keep our colleagues as well as the machines operating as necessary.

THE SERVICE STATE MODEL AND INFORMATION SECURITY

In his book 'On Demand Government: Continuing the e-government Journey' Todd Ramsey[11] states that on-demand government, in contrast to previous state government models (e.g. night watch state, welfare state), provides proactive, on-demand services that

Figure 3. Objectives of the application of technical practices.

meet customer expectations, while relying frequently on partners and suppliers. In his quoted work, Ramsey defines the service state according to the level of administrative modernization. He identified the following six interrelated criterions:

- conception,
- organizational culture,
- the operation model,
- the technological infrastructure,
- the conversion schedule and
- perspective thinking.

In connection with information security risk assessment and management, the most important aspects of the on-demand state are the operation model and the technological infrastructure. The values created by an organization are the result of operational processes. In a service provider organization, activities and processes are optimized for maximum customer satisfaction.

Today's development trap, however, is often not the modernization of core processes and core activities that are overlooked, but the development of complementary processes and activities (non-core), with the complete absence of risk management. This is the reason why a seemingly advanced office is close to collapse and unable to perform its duties [12].

It is important that the development of the technological infrastructure should always follow the elaboration of the operating principles and processes of the organization. The bigger the government, and wider its range of tasks, the more it is exposed to attacks. This statement is even more applicable to the on-demand state model, as the scope of public administration is widening and the focus of operation and administration shifts from the offline to the online space.

The customer orientation of the on-demand state can lead legislators to only focus on the goal of achieving the fully developed digital state, resulting in neglecting the time-consuming questions of information security and risk assessment.

As was highlighted in the previous heading, the human firewall is the best solution for improving information security. The on-demand government therefore must ensure the creation of a reliable, enforceable set of information security rules and a continuous training platform for public sector employees. Moreover, the training opportunity on a long term should be open to all citizens by incorporating information security and cyber security courses in the public education system from the earliest age.

The purpose of training is to represent a personnel education program beyond awareness raising by competence building. The education programs have different types. The most common according to[13] are the following:

- **Exercise**: the instrument to measure and improve the capability of elements or processes (such as personnel, system, communication, and organization) that are essential for performing a fast recovery and mitigating the impact caused by a disruption. The exercise is conducted based on a scenario that requires a knowledge-based decision action and decision-making, such as that required in a situation that is not scripted in the incident handling manual, or one involving a highly disrupted core business process.
- **Test:** the validation process of a system's operability and capability.
- **Drill:** the repetitive practice of skills within a recreated situation.
- **Training:** theoretical education of the personnel about their responsibilities and skills, which prepares them for exercises, tests and actual emergencies.

Thanks to the wide range of publicly available exercises and training materials, continuous training of the personnel can be carried out without excessive costs.

SUMMARY

In the future, it is expected that security experts will often hear the term multi-layer protection. It is no coincidence that we need to be prepared for complex threats that are no longer sufficient for traditional security technologies or protection systems that operate in isolation.

The emergence of a service-state model and efforts to build a digital state would require risk management guidelines to be included in Country Strategy Papers, but unfortunately, there is a complete lack of risk management provisions not only in the area of information security.

The absence of risk management aspects in the Country Strategy Papers results in a lack of a unified view, mission and target in the field of information security in the public administration, and thus a heterogeneous structure and approach to the risk management plans of individual public administrations.

National threats to information security risk analysis and assessment are required to substantiate threats and objectives. The NIS Directive (Figure 3)[14] identifies key issues for national cyber-security strategies. The provision indicates the preparation of a risk assessment plan to disclose risks and the presentation of risk management principles as a separate point. A statutory risk assessment and risk management plan at the national level could provide a solution to the problem identified in the study.

An adequate security level can only be achieved if different levels of protection work in concert with one another. This aspect should be considered when purchasing and deploying new tools. There is no single magic weapon, an all-in-one security solution. The key to multilevel protection and collaboration lies in advising professionals and researchers as well. ■

REFERENCES

[1] Risk Based Security - Data Breach QuickView Report 2019 Q3 https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112

[2] B. Annamária, Information security and the digital state: the role of the risk management principles in the strategic documents, Bánki Report Vol 1 No 3 (2018), pp. 56-60.

[3] Md Sahrom bin Abu & Sharifah Roziah binti Mohd Kassim, Mirai Botnet Infection in Malaysia: Impact and Countermeasures. e-Security | Vol: 43 - (2/2017) CyberSecurity Malaysia 2017. pp. 55-57.

[4] Trend Micro, THE NEXT TIER Trend Micro Security Predictions for 2017, https://documents.trendmicro.com/assets/rpt/rpt-the-next-tier.pdf pp. 1-20.

[5] Thycotic, Black Hat Hacker Survey Report 2017, https://thycotic.com/wp-content/uploads/2013/03/BlackHat_ Hacker_Survey_Report_2017.pdf pp. 1-6.

[6] Kevin Mitnick, William L. Simon: A legendás hacker 2. - A behatolás m?vészete - A behatolás m?vészete. Perfact-Pro Kft. 2006. pp. 1-312.

[7] Vasvári György videó portré (2014. okt. 6.): https://www.youtube.com/watch?v=ewslw1ez0_U

[8] Cisco: How to be agile and secure - the fundamental challenge facing organizations today, https://www.cisco.com/c/dam/assets/global/UK/products/security/How_to_be_agile_and_secure.pdf pp. 1-18.

[9] PwC: The Global State of Information Security® Survey 2018. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

[10] Zs. Szabó, Cybersecurity issues in industrial control systems, IEEE 16th International Symposium on Intelligent Systems and Informatics: SISY 2018. IEEE Hungary Section, 2018. pp. 231-234.

[11] T. Ramsey, On Demand Government: Continuing the e-government Journey, Lewisville: IBM Press, 2004.

[12] Budai Balázs Benjámin: Az E-közigazgatás elmélete, Akadémiai Kiadó, Budapest, 2009. pp. 1-474.

[13] Tomomi A. et al.: On the Complexity of Cybersecurity Exercises Proportional to Preparedness, Journal of Disaster Research Vol. 12. No. 5., 2017

[14] Directive (EU) 2016/1148 of The European Parliament and of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=HU pp. 1-30.

ABOUT THE AUTORS

Annamária Beláz is a third-year doctoral student at the Doctoral School on Safety and Security Sciences at Óbuda University.

Her research areas include research on the organization of information security in public sector bodies and legal-strategic issues in cybersecurity and cybersecurity.

Zsolt Szabó is a fourth-year doctoral student at the Doctoral School on Safety and Security Sciences at Óbuda University.

His research interests include the economic effects of global aging on pension security (micro- and macro-simulation), information security issues on retirement disbursements (IT security, information security, cybersecurity).