Cybersecurity threats of on-premise systems in small and medium-sized enterprise environment

Dávid János Fehér

david.janos.feher@gmail.com

Abstract: *Small and medium-sized enterprise environments are less resilient than large enterprises. SMEs have much less budget to spend on IT security, but they sometimes feel even more the cybersecurity attacks. This paper examines the common weakness and threats against SMEs through two Hungarian Companies.*

Keywords: *SME, Security, Open Source, SIEM, Log management,Elastic Stack*

1 Introduction

Multinational companies usually spend huge sums on reducing the impact and amount of IT incidents, using more and more IT tools, set up dedicated teams, or hire external experts to protect their trade secrets and their users 'data. They are aware of what data they handle and to what extent they need to protect it. Based on my own professional experience and on the preliminary survey, smaller organizations receive less attention to cybersecurity threats, as they use fewer IT tools, and they are less known, and maybe less exposed to targeted attacks. They can be even more vulnerable - precisely because of their smaller size and more limited resources - than large companies with the right security tools, systems and with the right governance. As a cybersecurity analyst for several multinational companies, I have gained experience in cybersecurity incidents involving organizations, including on a 24/7 information security incident management team. My colleagues in my environment, working in other spheres, and my personal acquaintances, who work in a smaller company or company, surprisedly listened to my reports on the operation of such organized intervention groups. During our conversations, it became clear to me that they are all different from the IT threats affecting organizations, and the size of the company strongly influences the opinions they form. This pattern is a phenomenon barely explored in the literature, so I focus on this under-researched area in my research. The dissertation aims to assess and investigate the threats affecting small and medium-sized enterprises in Hungary. [1], [2]

2 Research process.

During the research process, I examined a Software development company with around 200 office employees and a Logistics company with around 20 office employees. Both companies are small, and mediums size enterprise categories and are located in Hungary. I picked these companies to reveal the two extreme characteristics of the SMEs; the clearest common attribution is probably the pursuit of cost-efficiency. Relevant domestic and international literature was processed to gather more information about the cheap way to improve the environment's security. Consulted with local security auditors to find cost-efficient best practices. Complete security review based on ISO 27001 requirements. Collected existing information security log files and shreds of evidence. The information collection happened via several different streams; it started with enterprise mapping and employee discussions. Collected information about the everyday work from the end-user employees and the managers and network and IT information from the system administrators and planned the further network scanning and mapping with their involvement, and we installed a network vulnerability scanner. After I get the full picture of the enterprises' structure and their IT systems, we started to deploy the open-source tools to collect near-time information about the enterprise. Based on the collected information and the review of the available books, websites, the information collection happened with the Elastic Company's open-source tools. The core is the Elasticsearch product, which is a multitenant-capable full-text search engine with an HTTP web interface. The Elasticsearch instance is the collection and store point of our log files, and this product provides advanced search capabilities. The following tools are extensions for Elasticsearch. The Kibana is an open-source data visualization tool that generates informative dashboards with near-time information. The Logstash product is a log-parsing engine and data collecting tool which can transform and manage any data on the fly; it is used as a man in the middle between the Elasticsearch instance and log source systems like Beats, Syslog, or any agents which are capable for log forwarding. The mentioned Beats product bouquet is used for the data collection on the agent end. During the research, the opensource Filebeat, Packetbeat, Winlogbeat, Metricbeat, Heartbeat, Auditbeat, Journalbeat were used to collect the data. The used Elasticserarch, Kibana, Beats architecture shown below in figure 1. [3]–[5]

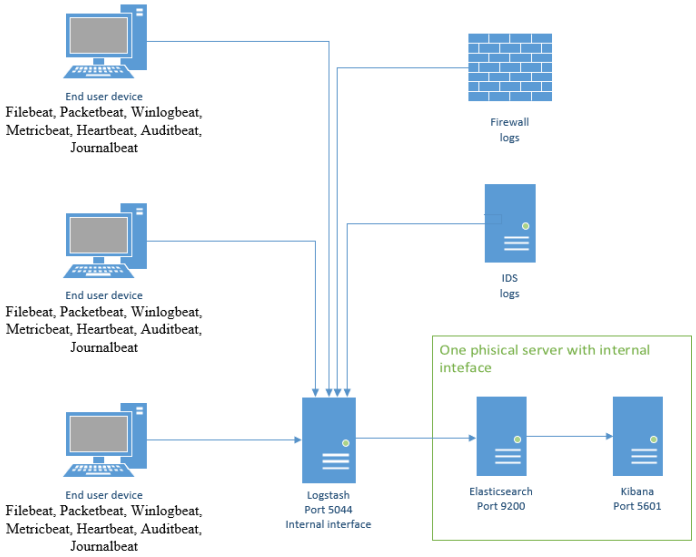

Figure 1

Log collector architecture

This setup with Elasticsearch, Kibana, and Logstash is mentioned on the Elastic Company's site as Elastic Stack, and it is usually used for security information and event management (SIEM) purpose; in this case, it is outstanding, but the main goal is the threat hunting in the environment. This was the core of our monitoring system; also, we installed RDP, SSH, VNC honeypots, and forwarded the logs to the Elasticsearch instance from the firewalls and network devices. I have to mention here as the Security module of Kibana, which is responsible for encryption, and user access management is not available for free. To avoid any extra cost here, I did extreme hardening with the Elastic search and Kibana instances. This final setup is the outcome of several integrations, tests, reviews, and based on the actual threat campaigns and the findings of our threat hunting and findings.[6], [7]

3 Discussion of Findings

Data collection period from 1st of February 2020 until the 20th of April 2020. Several findings from bot company's RDP, VNC, SSH honeypots, and the attackers tried to download and run several malicious scripts on the servers. There were similar attacks from several different IPs, so it is not efficient to block these IPs one by one as the attackers can easily find other devices to use as jump-server. After a review, most of the initiated scrip on the honeypot environment could significantly damage the servers or user devices as they were vulnerable against them.

Based on the user browsing activity, both company's employees visit non-recommended, suspicious, or malicious webpages. However, the Software developer's history was way more significant for their daily work even though most of the more suspicious sites where related to programming forums, while the Logistic company's employees' suspicious traffic was more unpredictable. Most of them came from spam or scam emails and browsing. For example, one of the Logistics company's employees opened a phishing mail on the enterprise device and provided her bank card details on the phishing site; happily, with the monitoring system, it was noticed on time, so she was able to ask the bank to block her credit card.

Based on the network logs, we found APT activity in the Logistics company's employee device.

- Communication catched towards the following malicious site: alibaba[dot]zzux[dot]com
    - IBM X-Force Exchange: Risk score 10/10 - APT41 Using New Speculoos Backdoor to Target Organizations Globally[8]

Several malicious software found on the device's, so an OS re-install was the answer for us to solve the problem; the antivirus softer has been deactivated on the device; happily, other devices had no problem with it.

From the vulnerability scanner results and the enterprise device reviews in the Logistician company, we found several non-supported outdated software or tools and found deactivated or non-frequently updated antivirus solutions and non-installed OS and application updates. The software developer company's conditions were much better, with centrally managed Antivirus solution and forced OS updates, but they neither patched their servers with special tools, while they use much of them.

4 Conclusions

The Logistics company sees the IT systems as a necessarily bad thing to deal with; if it works and can run their business, they do not care about it, and as there is no real IT management, the main problem is the lack of security awareness. Without the frequent security awareness pieces of training and control, people use their company devices as their other private devices, and without the proper security awareness, the reckless web surfing and email link or attachment opening by employees could go wrong. Expired paid applications open new vulnerabilities when the OS and application updates are not forced and are commonly postponed. If someone using USB drives, then mostly unaware of the related threats, and common to charge private mobile via USB while attaching the device's storage. The antivirus solution is not managed centrally, and they have poor Network and Firewall configuration, and they did not have IDS/IPS or any network monitoring.

The Software developer company performed much better, but they have significant shortcomings. The IT and the IT systems are much more in their lives. They have much better security user awareness, but they handle the IT services way too confidently, maybe even irresponsibly. Some of the employees use their enterprise device as just a remote desktop protocol server, and they log in from their personal device for their daily work; with this, they bypass most of the company's security intention. It is ubiquitous in the company to use their device to read enterprise mailing and use the enterprise chat solution. They neither have the right network and firewall configurations, and they did not have the IDS/IPS or any network monitoring.[2]

4.1 Recommendation for the small and medium size companies

Organize security awareness training and measure the results. Based on the results, plan the further strategy to improve user awareness in the company. Harden the network tools and the OS of every used device, check the publicly available hardening guides reflecting on the trending and previous threats. Use a „Deny by default" setting for everything on the firewalls and add the user applications' exceptions. Patching, patching, patching. Patch every OS and application; if the support is not available anymore, do extra hardening to compensate for the vulnerabilities. Run vulnerability tests periodically or after any significant change in the environment. Do security assessments periodically or after any significant change. Hire an IT security expert or make a contract with an IT security company to improve the company in cybersecurity. If It is not possible or not worth to cover the necessary maintenance tasks and cares about the security shortcomings, then review the possibility to use the cloud solutions like the cloud is not just someone else's server; it is operated by someone else's as described in the contract.[9]–[12]

4.2 Recommendation for the individual employees

Year by year, people are moving to the online era more and more. Most people banking, ordering, working online with this responsibility after our online being is rising. The internet is full of free user awareness training and recommendations. It is everyone's responsibility. Learn more about social engineering techniques and how to avoid these attacks. Update the OS and the applications. It is unpleasant to close all of our works and wait for the patching, but it is important, as this is necessary to maintain and update our defense lines against the threats. Plan the patching and frequently create backups about our important files.[13]–[15]

References

[1] R. Thompson, „The small business cybersecurity blindspot”, *Risk Manage.*, köt. 61, sz. 5, o. 8–9, 2014.

[2] M. Bada és J. R. Nurse, „Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs)”, *Inf. Comput. Secur.*, 2019.

[3] E. L. Opitz, „Cybersecurity for the board of directors of small and midsized businesses”, *Board Leadersh.*, köt. 2018, sz. 159, o. 4–5, 2018.

[4] C. Gormley és Z. Tong, *Elasticsearch: the definitive guide: a distributed real-time search and analytics engine*. O’Reilly Media, Inc., 2015.

[5] I. Kotenko, A. Kuleshov, és I. Ushakov, „Aggregation of elastic stack instruments for collecting, storing and processing of security information and events”, 2017, o. 1–8.

[6] J. Turnbull, *The Logstash Book*. James Turnbull, 2013.

[7] S. Chhajed, *Learning ELK stack*. Packt Publishing Ltd, 2015.

[8] „IBM X-Force Exchange”. https://exchange.xforce.ibmcloud.com/ (elérés okt. 27, 2020).

[9] B. Armstrong, P. England, S. A. Field, J. Garms, M. Kramer, és K. D. Ray, „Computer security management, such as in a virtual machine or hardened operating system”, 0 2008.

[10] R. E. Todd Sr, A. C. Glahe, és A. H. Pendleton, „Method for network self security assessment”, 0 2001.

[11] Y. Wang és J. Yang, „Ethical hacking and network defense: choose your best network vulnerability scanning tool”, 2017, o. 110–113.

[12] R. Kushe, „COMPARATIVE STUDY OF VULNERABILITY SCANNING TOOLS: NESSUS vs RETINA”, *Secur. Future*, köt. 1, sz. 2, o. 69–71, 2017.

[13] T. Caldwell, „Making security awareness training work”, *Comput. Fraud Secur.*, köt. 2016, sz. 6, o. 8–14, 2016.

[14] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, és M. Pattinson, „Individual differences and information security awareness”, *Comput. Hum. Behav.*, köt. 69, o. 151–156, 2017.

[15] C. Valli, I. C. Martinus, és M. N. Johnstone, „Small to medium enterprise cyber security awareness: an initial survey of Western Australian business”, 2014.