Cybersecurity threats of cloud and third-party services in small and medium-sized enterprise environment

Dávid János Fehér

david.janos.feher@gmail.com

***Abstract**: Small and medium-sized companies typically use the advantages of cloud solutions to run their business; moreover, they can use the cloud to decrease their responsibility. Some of the on-permisses threats can easily eliminate and transform by moving to the cloud environment, but some of the threats will remain. This paper examines the common threats of cloud and third-party services in the SME environment.*

***Keywords**: SME, Security, Cloud threats, Third-party service threats*

1 Introduction

The most popular cloud providers focus on smaller companies and try to help them with special packages tailored for small and medium-sized enterprises. Using cloud solutions is very accustomed to SMEs, as there is no need for well-educated technical persons to manage these servers and care about the availability and settings. There is much important advantage of the cloud, like less operational tasks needs for these, and it is highly scalable, and the availability of these systems is really high. The most common components are easily accessible from any device without a special jump-server, and there is no need for a higher one-time investment as it is available as a monthly subscription. Sadly, moving to the cloud is not solving every security problem and make the dependencies disappear; it is just transforming the threat to something different. The dissertation aims to assess and review the threats related to cloud solutions in small and medium-sized enterprises in Hungary. [1], [2]

2 Research process

I examined a Software development company with around 200 office employees and a Logistics company with around 20 office employees during the research process. 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 use cloud solutions to reduce its operational task-related responsibility and improve the environment's

security. Consulted with local security auditors and company members 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 managers later gathered more information about the system administrators' network and IT. The Logistics company CEO and one first-line manager from the Software development company kindly answered all of my questions during the examination.

3 Common cloud panorama in the world of SMEs

There are great advantages of the Cloud, accessibility, scalability if the business grows, no need for technical maintenance, built-in disaster recovery, redundant storage, decreased responsibility, short term cost savings, tailored packages for SMEs. The main advantage of using Cloud is to delegate responsibility to let the companies focus on their business, not on their systems. It is common to use the Cloud's advantages nowadays; most people use Google Drive and Gmail in their private life. Nowadays, in the word of SMEs, it is common to use Google Workspace or using Microsoft's Outlook, OneDrive or Office with Cloud subscription, but the use of Google Cloud Platform or Microsoft Azure is not really obvious, neither any another Cloud Computing provider's solution, so mostly the Software as a Service is used by SMEs. [3]

With the SaaS, there is no need to care about the updates or the vulnerabilities; the company's few responsibilities are to handle the accounts with the right passwords and backup settings and make and keep the used device safe. Another important part of the SaaS to know what is uploaded and shared with whom via these platforms; it needs. It sounds simple but still needs education and security awareness on the user end. These enterprise cloud solutions could make it even easier to review the team's security readiness with well-tailored audit procedures or with the management consoles. The commonly used cloud characteristic defines the responsibility of the customer in each service model. Table 1 shows that in the case of an on-premise system, it is the customer's responsibility to care about everything about the environment and go from the Infrastructure as a Service through the Platform as a Service to the Software as a service the responsibility of the Customer is decreasing.[4]

Responsibility of Custumer	SaaS	PaaS	IaaS	On-prem
Information and data used	Yes	Yes	Yes	Yes
User devices to use these services	Yes	Yes	Yes	Yes
Accounts and identities	Yes	Yes	Yes	Yes
Identify and directory infrastructure	Mostly	Mostly	Yes	Yes
Applications		Mostly	Yes	Yes
Network controls		Mostly	Yes	Yes
Operating system			Yes	Yes
Physical hosts				Yes
Physical networks				Yes
Physical datacenter				Yes

Table 1 - Responsibility of the Costumer [4]

In the case of a Platform as a Service, there are some special cases where the responsibility mostly depends on the scenario. Based on the companies' review, the most problematic parts are the physical host, physical network, and server operation. In table 1, the responsibility model clearly shows the usage of Software as a Service solutions are the best as the user company's responsibility is limited. In the logistics company's case, they could use most of their system as SaaS; most of their tools are available as cloud subscription. Their ERP, CRM tools are already available as Cloud, and they have alternative billing providers who have a cloud subscription option, and as they have only 20 office employees, it could be thrifty. The Software development company is in a different shoe as they have 200 employees; however, they already have Google's Gmail as enterprise mailing and using Google Drive with well-managed accounts. The software development company uses services that are available as PaaS or IaaS in the portfolio of Cloud companies, but it could be cheaper to use the on-premises solutions for testing purposes. The employees mostly use their own enterprise notebook to host any virtual machine and test their developed programs, but they have to use a more powerful resource to test and run their codes in some cases. With both companies, we started developing a complex solution to collect user activity-related events and feed a Security Information Event Management solution. The used Elasticsearch instance and the visualization Kibana tools are available as SaaS. However, the log forwarder that collects the logs from the end-user devices is only available as Linux or Docker installer, so we have to use IaaS to meet these requirements, which means responsibility for us is still just a fragment of the whole project.[1], [2], [5], [6]

Services	Logistics company	Software development company
Microsoft Office	Office 2019 (non-cloud)	Office 365
File share	Google Drive	Google Drive
Document share	Google Drive	Google Drive, Office365
Email provider	Hungarian domain provider	Google Gmail
Online meetings	Google Meets	Google Meets
Calendar	Outlook calendar	Google Calendar
Servers in use	2 – internal hosting	10 –development, global hosting

Table 2 – Used services matrix by the examined companies

The Table 2 shows the common used cloud and non-cloud services by companies. Based on the day-to-day life of the companies, the most common cloud part of their life is the Google Workspace environment such as Google Drive, Google Documents, Gmail, Google Calendar, Google Meets, and they are using the Microsoft Cloud Environment as well as One Drive, Microsoft Office 365, Outlook. Based on the first survey, the Google Cloud Environment and the Microsoft Cloud environment were known by everyone before they joined the companies, and because of it, the management did not think they should provide appropriate user training on how to use it in this environment. I found great shortcomings in this area; for example, some of the employees do not know how to check the access settings of different folders or files in these cloud environments, and most of the employees never check the access for these, and there is no process to review the accesses of these files. It is a ubiquitous way in the environment to upload their documents to Google Drive or One Drive to reach these via Mobile or Tablet or to share it with their team members; I found some case when users shared a public link to a folder or a file if another participant does not have a Google account. At least every member of the software development company uses the enterprise version of the Google Workspace environment, so the related accounts are linked together to make any further improvement while most of the users use shared accounts in the logistics company. I found non-reviewed and considered security, privacy, compliance questions during the assessment. During the devices' examination, we found some advanced persistent threat on one of the logistics company's devices, a sinister indicator of the user awareness shortcomings. Suppose the SaaS is perfectly secured on the provider end. That does not mean anything if the customer side end-user computer is infected, and the attacker can reach the SaaS data via one infected device. The Software development company with their more aware users and their centrally managed antivirus software performed much better during the examination, and they are located in the heart of Budapest where more internet service providers (ISP) are available moreover these ISPs are much more reliable than in case of the logistics

company which is located in the countryside in the industrial area of a town. The logistics company sometimes have serious local bandwidth limitations, as these ISP networks are not well maintained, and they are based on ADSL technology. This company did not have any business continuity plan for the ISP outage and did not have any aggregator or uninterruptible power supply. This ISP outage could stop the company's work if the company moved to the cloud, if there is no plan B for this scenario. In 2020 during the COVID-19 pandemic, most of the world changed their ways of working to work from home, and with it, the magnitude of an ISP outage decreased, but now it needs to cover on the user end. With the globally available cloud solutions, there is no way to separate it from external threats, so this risk mitigation option is not possible here, a these publicly available it is even more vulnerable for threads, and even the biggest names like Google can suffer from a data breach or 0-day vulnerabilities too. Companies could save a lot or waste a lot with the Cloud subscriptions; it depends on the company's actual profile and plans.[7]–[10]

4 Conclusion

The examined companies are already using cloud solutions, and they are open to using new cloud services if they decrease their costs or make their business more effective. During the COVID-19 pandemic, they are even more interested, as these cloud solutions make them even more resilient again the changes, and now it needs much less to invest. The companies' most important uncovered task is to improve the companies' user awareness with special attention to the right usage of the cloud services and the user's involved devices.

5 Recommendation

The most important thing is to improve the user's awareness and properly cover the right secure way of using their devices to avoid any malicious content and cover the secure usage of the Cloud services. Important to create control processes for data management and access management, as it is more exposed to the publicly available cloud environment. Do regular review on shared items to avoid unauthorized access to customer and business data and review the cloud and third-party provider related contracts for legal and compliance risks. Provide the necessary equipment for business continuity in case of an ISP outage with backup lines and 4g/5g subscription and know the provider's right escalation process and the SLA.

References

[1] I. Mikkonen and I. Khan, 'Cloud computing: SME company point of view', *Manag. Chall. 21st Century Digit. Soc. Econ. Mark. Curr. Issues Chall.*, 2016.

[2] N. M. Alsharari, M. Al-Shboul, and S. Alteneiji, 'Implementation of cloud ERP in the SME: evidence from UAE', *J. Small Bus. Enterp. Dev.*, 2020.

[3] A. Pucihar, M. K. Borštnar, C. Kittl, P. Ravesteijn, R. Clarke, and R. Bons, 'Use of Facebook and Google Platforms for SMEs Business Model Innovation', *30TH Bled EConference Digit. Transform. Connect. Things Transform. Our Lives*, p. 169, 2017.

[4] K. K. Tucker, 'Shared Responsibility Matrix For Cloud Services', *Infused Innovations*, Sep. 23, 2019. https://www.infusedinnovations.com/blog/secure-intelligent-workplace/shared-responsibility-matrix-for-cloud-services (accessed Apr. 03, 2020).

[5] 'Elastic Stack: Elasticsearch, Kibana, Beats & Logstash', *Elastic*. https://www.elastic.co/elastic-stack (accessed Mar. 10, 2020).

[6] 'Logstash: Collect, Parse, Transform Logs | Elastic'. https://www.elastic.co/logstash (accessed Mar. 20, 2020).

[7] H. Fadinger and J. Schymik, 'The costs and benefits of home office during the covid-19 pandemic: Evidence from infections and an input-output model for germany', *COVID Econ. Vetted Real-Time Pap.*, vol. 9, pp. 107–134, 2020.

[8] M. M. Alani, 'Securing the cloud: Threats, attacks and mitigation techniques', *J. Adv. Comput. Sci. Technol.*, vol. 3, no. 2, p. 202, 2014.

[9] S. Aljawarneh, 'Cloud security engineering: Avoiding security threats the right way', in *Cloud Computing Advancements in Design, Implementation, and Technologies*, IGI Global, 2013, pp. 147–153.

[10] K. Dahbur, B. Mohammad, and A. B. Tarakji, 'A survey of risks, threats and vulnerabilities in cloud computing', in *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications*, 2011, pp. 1–6.