

Vulnerability Analysis In Business Unit

Petr Doucek^{1,*}, Miloš Maryška², Jiří Hološka¹ and Lea Nedomová¹

¹ Department of System Analysis, Prague University of Economics and Business, W. Churchill sq. 4, Prague, Czech Republic

² Department of Information Technology, Prague University of Economics and Business, W. Churchill sq. 4, Prague, Czech Republic

* Correspondence: doucek@vse.cz

(Article history: Received December 01, 2025; Received in revised form January 03, 2026; Accepted February 01, 2026; Available online June 15, 2026)

Abstract: Nowadays, risk management is one of the fundamental tools for protecting the assets of business corporations. In this article, we delve into a comparison of vulnerability analyses that took place in a specific organization in the financial sector during two periods when data was collected for the article. The first period was in 07/22 and the second in 03/23. The starting point for the vulnerability analysis was the ISO/IEC 27007 concept, and the main tool for its implementation was Microsoft Center Configuration Manager. Standard tools and functions of Microsoft Excel were used for calculations on the obtained data. For more complex analyses, the programming language R was primarily used. The vulnerability of assets in the organization was then measured on a scale from 1 to 10, where values from 8 to 10 represented critical vulnerabilities. The results of the analysis showed in the first period the use of unauthorized software, a large number of vulnerabilities immediately after the installation of the software and therefore a poor use of the additional installation of security patches. Only 22% of secure computers in the organization were identified. The subsequent second period showed a very substantial improvement in the protection of the organization's assets - 85% of secure computers. The result of our research is clear evidence of the need for regular risk analysis associated with the analysis of the vulnerabilities of an organization's assets. The main causes of the increase in vulnerability or its changes may be software updates or the emergence of new threats in cyberspace.

Keywords: risk analysis, vulnerability analysis, critical vulnerability, ISO/IEC 27000

1. Introduction

The dependence of standard business processes on computing technology is becoming increasingly important in everyday and working life, reaching critical levels in some processes. This dependence and the integration of many computers into global computer

networks, which are now very difficult to manage, increases the pressure to manage the protection of the assets (investments) that companies and countries have already made in them. In line with these trends, information security and related cyber security are receiving more and more significance in everyday life and in business [1]. Increased demands for the security of information systems and cybersecurity in everyday work also bring with them a rise in demands for their reliability and management. Management aspects include an increasingly broader concept of threats to organizations and therefore also significantly growing requirements for their analysis. We all know from experience that in almost every application in operation, whether it is standard software or a on demand proprietary solution, there are imperfections that can be potential gateways for unwanted access to information systems - so-called vulnerabilities. The actual reasons and objectives why some users enter unauthorized access to other people's information systems may be different. Nowadays, it is both personal gain - the possibility of obtaining money either for stolen information or for decrypting information without which the attacked organization is unable to operate (in the Czech Republic, it was e.g. hospitals, state and public administration offices and some business corporations especially in the relation to the Ukraine war), and ideological reasons - hatred of the establishment, ethnicity, religion, economic and political system, etc. Motivation of the attackers to prove that they are good (we are champions - unfortunately, these situations are very rare – for example The Ministry of Interior of the Czech Republic) but not to cause any great damage to the attacked organization is quite in the background (except the good reputation). Cyberattacks on the security of information systems in business bring with them relatively large losses, which are expressed in financial indicators. *"Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching \$10.5 trillion USD annually by 2025, up from \$3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined"* [2]. Threats of financial loss bring with them efforts by organisations to protect themselves against them in a variety of ways. According to ISO/IEC 27001:2022 [3], these include risk avoidance, transferring the risk to another legal entity (e.g. insurance - [4]), accepting the risk and establishing countermeasures to protect assets. And it is because of risk decision making that vulnerability analysis [5] - i.e. what potential threats can be effective on the assets of the organization - is important for any organization.

The aim of this paper is to present partial results of a static analysis [6, 7] of personal computer vulnerabilities in a financial organization in two periods of measurements, to compare the results of corrective actions and to present the conclusions from this analysis. As part of the research on risk and vulnerability management in this organization, we formulated the following three research questions:

- RQ1: How long do critical vulnerabilities survive on employee PCs?

- RQ2: What is the proportion of computers that can be assessed as secure, i.e. with an acceptable level of vulnerability?
- RQ3: Are corrective countermeasures implemented in time to eliminate vulnerabilities?

The answers to these questions led us to the conclusion that it is necessary to conduct regular analysis of both risks and vulnerabilities. In addition, when formulating the concept for carrying out both analyses, it is essential to take into account new trends in both information security and cybersecurity. Specifically for the mentioned organization, this necessity is discussed in the section '**Discussion – Vulnerability Analysis, Service Enhancements and Practical Recommendations**', where the question of implementing and managing the security of payment terminals arises.

2. Methodology

The methodology used by the authors of the article for the analysis of vulnerabilities and risks of the company's information system is based on the overall concept of risk analysis as presented by the ISO/IEC 27000 family of standards. Specifically, it is the ISO/IEC 27005:2018 standard [8]. The severity of vulnerabilities in terms of impact on the company's operations is organized into a standard 1-10 scale, where vulnerability level 1 represents minimal impact on the company's operations and vulnerabilities 8-10 represent critical vulnerabilities to the company's operations and processes [9]. However, we also look at the type of vulnerability as part of the analysis. For the authors of the paper, the type of vulnerability represents information not about each occurrence of vulnerability, but about the occurrence of their type. Another variable analysed is the "Vulnerability age", i.e., the total amount of time a vulnerability exists in an organization's information system without being treated. For the purpose of answering RQ2, we introduced a vulnerability index, the amount of which was checked on each individual computer connected in the internal corporate network or that it was connected to the internal corporate network through a VPN (Virtual Private Network) – in generally - used anywhere within the organization. If its value was less than 0.2, we set a value of 0.2 for this index, hereafter referred to as the Critical Index Value (CIV). In case the index value found for the analysed station was lower than the CIV mentioned above, we considered the station used within the IT environment of the organization as secure.

Commercial tools were used for the vulnerability analysis, the main one is presented in the following section.

2.1. Vulnerability Analysis Tools

Several tools were used to perform a realistic vulnerability analysis of individual devices within the organization's infrastructure. The most important of the tools used is Microsoft System Centre Configuration Manager (SCCM) [10], which is a solution that enables the

administration of all technical computing devices in the organization. SCCM is an extended and very powerful software tool that enables central management of stations (computers) within a defined environment. For the purposes of this post, we need to define the term "report". By administration, we mean the management of large groups of computers in the form of the ability to remotely control computers, the management of software patches provided by software producers on individual computers, the distribution of new software, the deployment and patching of the operating system, the deployment of bug fixes in all other software that is managed by Microsoft System Centre Configuration Manager in the organization, etc.

An important function of SCCM is to scan individual devices on the network and monitor the software installed on them. An important parameter of the solution is not only the ability to forcefully update computers on the network, but also to make various types of software available to users. The advantage of access via SCCM is the fact that users can install the accessed software themselves without the need to have local administrator rights, which are usually required for the installation of most existing software.

2.2. Vulnerability Analysis

The vulnerability analysis was conducted on more than one hundred and less than one hundred and fifty computers in real operation on 13 July 2022 - the first period and then on 8 March 2023 - the second period. Analysed computers were mainly from the set of the organization's ICT department. Any computer that was logged into the corporate network on those days was analysed and a Critical Index Value was calculated. The analysis was mainly focused on the full range of applications used on the computers. Vulnerabilities were found not only in common office software (MS Windows, MS Office, Adobe, etc.), but also in information systems development applications (Java, Visual Studio) and locally installed database systems (MS SQL Server 2017, etc.).

3. Results

The results of the vulnerability analysis are divided by period of measurement into a first period, conducted in 2022, and a subsequent second period, conducted in 2023 - about eight months after the first one.

3.1. Results of the First Period of Analysis

In the first period of vulnerability analysis, which took place in 2022, a total of more than 6,000 vulnerabilities were identified, 528 of which were in the organization-critical category - vulnerabilities in levels 8-10. Their relationship to the software used is shown in Table 1.

Table 1. Overview of Identified Critical Vulnerabilities by Software

SW/Vulnerability Level	'8	'9	'10	Total
Adobe	12	184	8	204
Apple iTunes	3	5		8
Oracle Java	122	22	55	199
Microsoft Edge	1			1
Microsoft Office		4		4
Microsoft Windows	22	29	12	63
Silverlight			16	16
Microsoft SQL Server			28	28
Total	160	244	119	528

Table 1 provides information on the number of times a critical vulnerability was detected across all software occurrences in the organization. Thus, vulnerabilities may recur, depending on the number of times certain software is installed in the organization. The biggest problem for system administration is caused by Adobe and Java software (see [11]), which account for 76.33% of all critical vulnerability occurrences in the organization.

A different view of vulnerabilities is provided by Table 2. This lists the different types of critical vulnerabilities that have been identified in each software.

Table 2. Occurrence of Different Types of Critical Vulnerabilities According to the Software

SW/Vulnerability Level	'8	'9	'10	Total
Adobe	3	2	2	7
Apple iTunes	3	5		8
Oracle Java	3	2	5	10
Log4J	3		2	5
Microsoft Edge	1			1
Microsoft Office		1		1
Microsoft Windows	7	7	4	18
Microsoft SQL Server		1	1	2
Total	20	18	14	52

Table 2 shows that a total of 52 different types of critical vulnerabilities have been identified. At the same time, Table 2 contains information about which software has how many types of critical vulnerabilities and how they are categorized into 8-10 categories. From this perspective, Microsoft Windows and Oracle Java are the most problematic. Their type 8-10 vulnerabilities represent a total of 53.84% of all identified types of critical vulnerabilities in the organisation. At vulnerability level 10, this share is as high as 64.28%.

A very interesting result of the analysis is the existence of the Apple iTunes software in the organization's information system. It is a software that is not used to support the processes of the organization, but to play multimedia content such as music, movies, various programs of TV stations, etc. Since the software can be freely downloaded from the Internet and users in this organisation usually have administrator rights to their computers, the existence of this

software represents an unnecessary source of vulnerabilities for the organisation, including critical ones. In this case, 15.38% of the types of critical vulnerabilities are level 8 and 9.

3.2. Results of the Second Period of Analysis

Over an eight-month period, the company made significant changes to the process of deploying patch packages to applications, excluding some applications from the company's application portfolio and, most importantly, removing the oldest vulnerabilities.

In the second period, approximately 2,100 vulnerabilities were identified during the vulnerability analysis, of which 113 were in the organization-critical category - i.e. in vulnerability level 8-10. Their relationship to the software used is shown in Table 3.

Table 3. Overview of Identified Critical Vulnerabilities by Software

SW/Vulnerability Level	'8	'9	'10	Total
Adobe	0	5	1	6
Apple iTunes	N/A	N/A	N/A	N/A
Oracle Java	N/A	N/A	N/a	N/A
Oracle Java – New	2	1	0	3
Log4J	2		3	5
Microsoft Edge	0			0
Microsoft Office		10		10
Microsoft Windows	12	20	5	37
Microsoft Silverlight	N/A	N/A	N/A	N/A
Microsoft SQL Server			47	47
Total	16	36	56	108

Table 3 after re-analysis says that the Apple iTune and Silverlight applications have been removed from the application portfolio. A significant change was made to the Java application, which was replaced by other alternative software with the same functionality but with significantly lower vulnerability rates. In Table 3 this is labelled as Java - New. Currently, the problem for the company is no longer Adobe or Java, which now represent only 9% of the vulnerabilities, but now it is Microsoft SQL Server and Microsoft Windows itself, which together represent 77.78% of the critical vulnerabilities in the organization. A significant representation of Microsoft SQL Server is the fact that there has been no removal of existing vulnerabilities and new ones have been discovered. In the case of Microsoft Windows, even with regular updates, it is only a matter of chance how many vulnerabilities will be disclosed at any given time.

A different view of vulnerabilities is provided by Table 4. This lists the different types of critical vulnerabilities that have been identified in each software during the second round of our analysis.

Table 4. Occurrence of Different Types of Critical Vulnerabilities According to the software

SW/Vulnerability Level	'8	'9	'10	Total
Adobe	0	2	1	3
Apple iTunes	N/A	N/A	N/A	N/A
Oracle Java	N/A	N/A	N/A	N/A
Oracle Java - New	1	1		
Log4J	2		2	4
Microsoft Edge	0			0
Microsoft Office		2		2
Microsoft Windows	3	4	1	8
Microsoft Silverlight	N/A	N/A	N/A	N/A
Microsoft SQL Server			2	2
Total	6	9	6	21

Table 4 presents that the number of types of critical vulnerabilities has significantly decreased and there are currently 21 of them in the organization. In terms of the largest share of unique vulnerabilities, Microsoft Windows leads as expected, but it is followed by Log4J. In the case of the highest level of criticality (level 10), Microsoft SQL Server and Log4J are tied for first place, representing 33% of the level 10 vulnerabilities.

Given the replacement of Oracle Java applications with a new solution and the uninstallation of Apple iTunes and Microsoft Silverlight and the update of Adobe, there has been a significant decrease in unique vulnerabilities.

3.3. Research Questions - Answers

RQ1: How long do critical vulnerabilities survive on employees' personal computers?

The answer to the first of the research questions can be seen in Figure 1 below. There was a significant decrease in vulnerabilities with ages of 100-199 days, 200-299 days, and over 400 days. The increase in the age of vulnerability indicator from 0 to 22% is due to the fact that the other values have decreased and at the same time there has been an increase in the number of vulnerabilities in this indicator. The original value of the indicator was 8 vulnerabilities and the new value is 15 vulnerabilities, which significantly affects the observed percentage when the total number of vulnerabilities decreases.

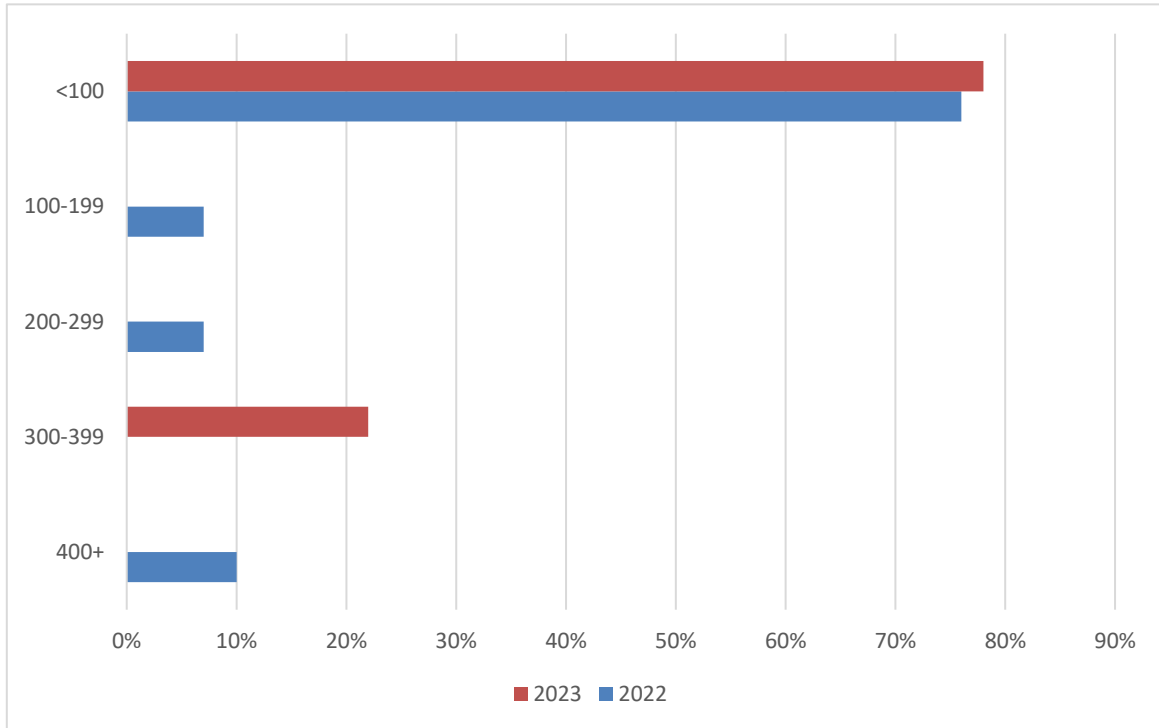


Figure 1. Persistence Time of Vulnerabilities in Information System Source: authors

Note: Figure 1 contains data on the percentage of occurrence of all vulnerabilities by duration in the company's information system.

The “vulnerability age” of vulnerabilities in the company's information system has **decreased significantly and except for the 200-399 category**, where the largest number of vulnerabilities is Microsoft SQL Server, the number of vulnerabilities has decreased and they have remained mainly with an age of up to 99 days, which can be considered acceptable.

RQ2: What is the proportion of computers that can be assessed as secure, i.e. with an acceptable level of vulnerability?"

As part of the vulnerability analysis, we also sought to answer the second question. Here, we assumed a uniform index where we assigned weights to individual computer vulnerabilities and if the vulnerability index value was found to be less than 20.00% when other criteria are met as the identified vulnerabilities are in the lower level than 4, we consider the computer to be secure. The observed percentage of secure computers in the organization is shown in the following Figure 2.

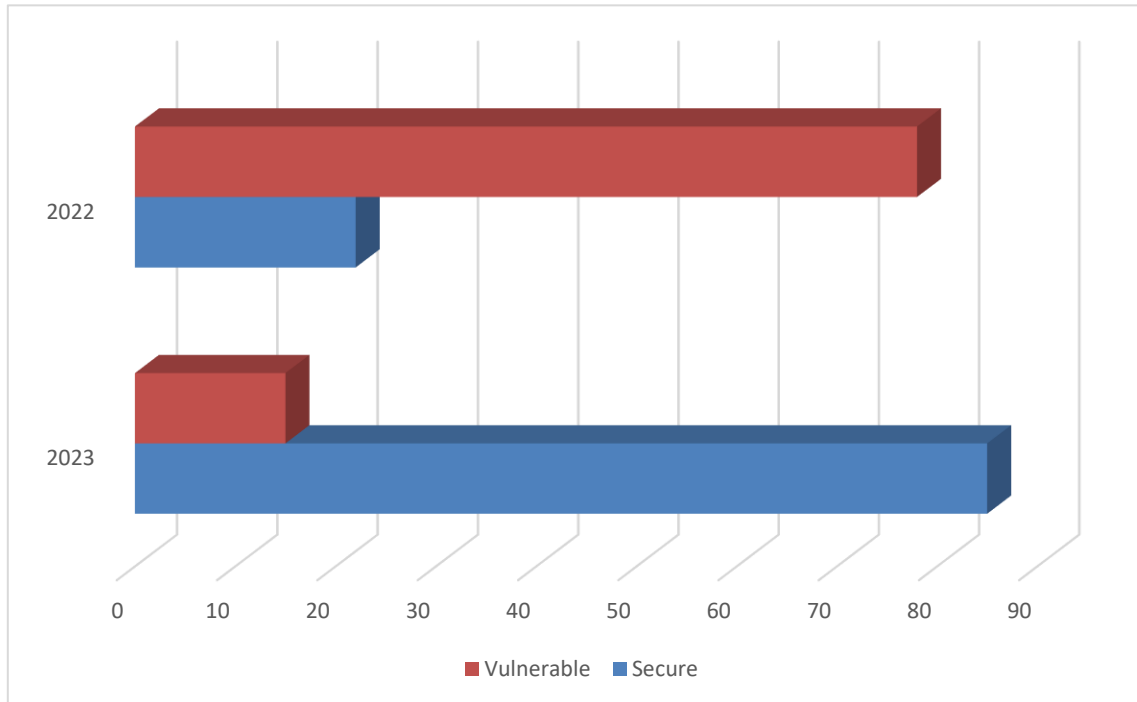


Figure 2. Proportion of Secure Computers in the Information System Source: authors.

Figure 2 shows that the **number of secure computers has significantly improved** due to the conducted vulnerability analyses.

RQ3: Are corrective countermeasures implemented in time to eliminate vulnerabilities?

The 85% share found is a significant improvement on the original 22%. Figure 1 and Figure 2 are both responses to RQ3, where it can be concluded that the company **has significantly improved the level of updates and vulnerability risk reduction between the two measurements performed.**

4. Discussion – Vulnerability Analysis, Service Enhancements and Practical Recommendations

During the next cycle of conducting risk and vulnerability analysis, another request emerged for expanding services to include payment terminal services.

This, of course, means an expansion of the concept of the analyses being carried out, which led to the changes and experiences mentioned below.

While ISO/IEC 27007 (aligned with ISO/IEC 27001 and 27002) provides broad, flexible guidelines for auditing and managing information security risks within an Information Security Management System (ISMS), PCI DSS (Payment Card Industry Data Security Standard) [12] offers prescriptive, detailed requirements explicitly designed for securing cardholder data. PCI DSS introduces specific technical mandates such as encryption standards for data at rest and in transit (AES and TLS), mandatory quarterly vulnerability scans by Approved Scanning Vendors (ASVs), annual penetration testing, explicit multi-

factor authentication requirements, detailed logging/audit trail management, rigorous network segmentation guidelines, and precise incident response measures tailored specifically to cardholder data breaches.

Therefore, even if your vulnerability management approach is driven primarily by ISO/IEC 27007, integrating PCI DSS controls adds significant value beyond merely ensuring compliance for payment card systems. PCI DSS fills critical gaps by explicitly addressing payment-specific threats and vulnerabilities with defined frequencies, mandated technologies, and clear, actionable steps tailored specifically to securing and managing cardholder data, which are not thoroughly covered or mandated within ISO's more generalized security standards. An Organization that handles cardholder data, integrating PCI DSS controls alongside ISO/IEC standards is not just about compliance, it's essential for explicitly securing the specific risks associated with payment systems. ISO/IEC provides a solid foundation, but PCI DSS complements it with prescriptive and specific controls tailored to secure payment transactions explicitly and robustly.

Table 5. Summary Table PCI DSS and. ISO/IEC 27001/27002 Controls [13]

Control Aspect	ISO 27001/27007	PCI DSS
Explicit Cardholder Data Protection	Broad coverage	Specific coverage
Encryption at Rest (Specific Standards)	Broad guidance	Mandatory AES-128/256
Encryption in Transit (Explicit Requirements)	Broad guidance	Explicit TLS standards
Multi-factor Authentication (Explicit Scope)	Recommended	Explicitly mandatory
Mandatory Vulnerability Scans (Quarterly)	Recommended	Mandatory, ASV required
Penetration Tests (Annual Mandatory)	Recommended	Explicitly mandatory
Incident Response (Specific to CHD Breach)	Broad guidance	Explicitly prescribed
Network Segmentation (Explicitly Mandated)	Recommended	Explicitly mandated
Logging/Audit Trails (Explicit Retention)	Broad guidance	Explicit retention/review

4.1. Vulnerability Assessment Process

- Analysing vulnerabilities in managed applications distributed through Microsoft Endpoint Configuration Manager (formerly SCCM) provides an essential baseline for maintaining system security. However, managing vulnerabilities in operating systems and user-installed applications presents additional challenges, particularly when users possess the autonomy to install or request third-party software. User-installed software significantly expands the organization's attack surface, necessitating a comprehensive approach to vulnerability management.
- Agent-based vulnerability scanners, such as Qualys [14] or Tenable, offer a robust solution by performing comprehensive (360-degree) vulnerability assessments

multiple times per day. These scanners thoroughly evaluate the security posture of endpoint devices, including both servers and personal desktops, by examining installed applications and their configurations. By running frequent scans, organizations achieve near-real-time visibility into potential threats, significantly reducing the window of opportunity for attackers.

- In addition to agent-based solutions, network-based scanning appliances further enhance the visibility and scope of vulnerability management. These appliances are particularly valuable for identifying vulnerabilities on devices that do not support software agents, including network hardware such as firewalls, switches, printers, and various network services. Beyond identifying security vulnerabilities, network-based scanners also detect system or service misconfigurations and identify unauthorized assets, often referred to as "shadow IT." Identifying rogue or unauthorized systems proactively reduces potential threats posed by unmanaged or unapproved devices and software.
- Adopting a comprehensive vulnerability management practice requires anticipation of software applications or services that may evade standard asset management or inventory processes. Such untracked software can appear for numerous reasons, ranging from testing and evaluation to unauthorized deployment by users. Regular, daily vulnerability scans enable IT teams to rapidly detect and respond to security issues, enabling prompt reconfiguration, disabling, or patching of vulnerable applications as soon as remediation becomes available. This responsiveness is crucial, especially when vulnerable systems or services are exposed directly to the internet or exist within unsecured environments, such as guest networks or public-facing segments.
- Modern patching solutions are typically designed with a hybrid infrastructure, combining the strengths of both on-premises and cloud-based tools. An on-premises Microsoft Endpoint Configuration Manager server allows organizations to achieve granular control and highly customizable patch deployment processes, particularly beneficial for critical infrastructure such as servers. On the other hand, cloud-based solutions, like Microsoft Intune, offer scalability, accessibility, and reliable availability for managing laptops, mobile devices, and remote endpoints. This combination of on-premises and cloud-based solutions forms the core of an effective and flexible patch management strategy, essential for meeting internal compliance standards and enabling timely response to both scheduled updates and emergency patches.
- Furthermore, effective vulnerability and patch management practices indirectly contribute to robust license management, an often overlooked but critical aspect of organizational security and compliance. Vulnerability scanners and agents generate detailed software inventory data, which provides insight into software deployment across an organization's network. This inventory capability enables IT and

compliance teams to proactively manage software licenses and reduce risks associated with improper software licensing. Many software products and development frameworks may be free for personal or educational use but require costly licenses for commercial deployment or use within corporate environments. Improperly licensed software can lead to significant financial penalties, sometimes comparable to the monetary losses incurred from security breaches. Thus, the proactive identification of software installations via vulnerability scanning tools not only mitigates security risks but also safeguards the organization against potential financial and legal repercussions related to software licensing.

- In summary, comprehensive vulnerability management and patching extend beyond managing baseline deployments via SCCM or similar tools. Organizations must deploy a layered approach that integrates both agent-based and network-based scanning, effectively covering endpoints and network devices alike. Regular and frequent scanning significantly reduces response times to vulnerabilities, allowing immediate remediation actions to be implemented. The strategic use of hybrid patch management solutions ensures both granular control and flexibility. Additionally, leveraging vulnerability scanning tools to manage software licenses effectively helps organizations maintain compliance and avoid financial risks. Together, these practices establish a resilient and responsive security posture, significantly reducing the risk associated with vulnerabilities and enhancing the organization's overall security and compliance capabilities.

4.2. Patching policy

Establishing effective patching Service Level Agreements (SLAs) requires categorizing assets based on vulnerability criticality, business asset criticality, and the degree of infrastructure exposure [15]. Critical vulnerabilities on assets that are highly critical to business operations and exposed to the internet or in DMZ environments require immediate attention, typically within 24 hours or less. High or medium-severity vulnerabilities affecting moderately critical business systems or internal infrastructure should have slightly more flexible SLAs, generally ranging from a few days to a week [16]. Low-severity vulnerabilities or those affecting non-critical internal assets may be scheduled for remediation within a month or as part of the regular patch cycle.

Table 6. Strategy for Patching Policy

Vulnerability Severity	Business Asset Criticality	Infrastructure Exposure	Recommended SLA
Critical	High	Internet/DMZ	Within 24 hours
Critical	Medium/Low	Internal	Within 72 hours
High	High	Internet/DMZ	Within 72 hours
High	Medium/Low	Internal	Within 1 week

Vulnerability Severity	Business Asset Criticality	Infrastructure Exposure	Recommended SLA
Medium	High	Internet/DMZ	Within 1 week
Medium	Medium/Low	Internal	Within 2 weeks
Low	Any	Any	Within 1 month

Properly structured approach ensures vulnerabilities are addressed in alignment with risk-based priorities and business continuity needs.

5. Conclusions

Vulnerability analyses conducted in the financial institution clearly demonstrate the necessity of periodically repeating the analysis of security risks, including the analysis of vulnerabilities. By repeating the analyses, the organization is forced to address the identified security issues.

Another significant conclusion is that there are several reasons for the dynamic concept of such analyses. The first reason is the changing environment in both information security and cybersecurity (in Europe, this benchmark is represented by the ISO/IEC 27000 family of standards and the relevant directives of the European Parliament). The second reason is the changing software and also the threats that compromise their weak points and vulnerabilities. The third reason is the development of the organization itself. As stated in the article, there is a need, for example, to implement payment terminals.

Another conclusion of our research is the fact that despite the conducted vulnerability analyses, some vulnerabilities of assets within the organization remain unaddressed, and this can last for a considerable time. The reason is often the necessity to replace key software, which can mean a fundamental change in the organization's operations and also significant costs.

Acknowledgments: Paper was processed with support from institutional-support fund for long-term conceptual development of science and research at the Faculty of Informatics and Statistics of the Prague University of Economics and Business (IP400040).

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results. All authors declare that there are no competing interests.”

References

- [1] Wei, Y., Bo, L., Sun, X., Bin, L., Zhang, T., Tao, C.: Automated event extraction of CVE descriptions. *Information and Software Technology* 158, 107178. (2023). <https://doi.org/10.1016/j.infsof.2023.107178>.

- [2] Morgan, S.: Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>, last accessed 2023/05/21.
- [3] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. International Organization for Standardization Switzerland.
- [4] Maryska, M., Doucek, P., Nedomova, L.: Cyber Insurance/Re-Insurance and Impact of Covid-19. In: Proceedings of the 15th International Conference Liberec Economic Forum 2021, pp. 577-588. Technical University of Liberec, Faculty of Economics, Liberec (2021).
- [5] Murray, A. T., Matisziw, T. C., Grubestic, T. H. : A Methodological Overview of Network Vulnerability Analysis. *Growth and Change* 39(4), 573-592 (2008). <https://doi.org/10.1111/j.1468-2257.2008.00447.x>.
- [6] Wang, C., Li, Q., Wang, X.H., Ren, T.Y., Dong, J.H., Guo, G.X., Shi, E.J.: An Android Application Vulnerability Mining Method Based On Static and Dynamic Analysis. In: Proceedings of IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), pp. 599-603. IEEE345 E 47TH ST, NEW YORK, NY 10017 USA, ELECTRONIC NETWORK, (2020).
- [7] Zhao, J., Lu, Y., Zhu, K., Chen, Z., Huang, H.: Cefuzz: An Directed Fuzzing Framework for PHP RCE Vulnerability. *Electronics* 11(5), 758 (2022). <https://doi.org/10.3390/electronics11050758>.
- [8] ISO/IEC 27005: 2018 Information technology - Security techniques - Information security risk management. International Organization for Standardization Switzerland.
- [9] Liu, B., Shi, L., Cai, Z., Li, M.: Vulnerability Discovery Techniques: A Survey. In: Proceedings of IEEE 4th International Conference on Multimedia Information Networking and Security (MINES), pp. 152-156. IEEE345 E 47TH ST, NEW YORK, NY 10017 USA, Nanjing, China, (2012). <https://doi.org/10.1109/MINES.2012.202>.
- [10] Microsoft Corporation. Co-management for Windows devices – Configuration Manager and Microsoft Intune. Microsoft Learn, updated 4 December 2024. Available: <https://learn.microsoft.com/en-us/intune/configmgr/comanage/overview>.
- [11] Jawalkar, M., Gokhale, P.S., Dixit, A. M.: JIID: Java Input Injection Detector for Pre-deployment Vulnerability Detection. . In: Proceedings of IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), pp. 444-449. IEEE345 E 47TH ST, NEW YORK, NY 10017 USA, Kolkata, India (2015).
- [12] PCI Security Standards Council. Payment Card Industry Data Security Standard: Requirements and Testing Procedures, Version 4.0.1. PCI SSC, June 11 2024, pp. 1–379. Available: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf.
- [13] Comparison of PCI DSS and ISO/IEC 27001 Standards. Available online: <https://www.isaca.org/resources/isaca-journal/issues/2016/volume-1/comparison-of-pci-dss-and-isoiec-27001-standards>.
- [14] Qualys, Inc. Qualys Cloud Platform: One stack to consolidate traditional enterprise security and compliance solutions and secure the digital transformation. Qualys White Paper, 2023. Available: <https://cdn2.qualys.com/docs/mktg/qualys-cloud-platform-whitepaper.pdf>.
- [15] Islam, C.; Prokhorenko, V.; Babar, M.A. Runtime Software Patching: Taxonomy, Survey and Future Directions. arXiv 2022, preprint arXiv:2203.12132.
- [16] Shimizu, N.; Hashimoto, M. Vulnerability Management Chaining: An Integrated Framework for Efficient Cybersecurity Risk Prioritization. arXiv 2025. doi:10.48550/arXiv.2506.01220.