Belgian Financial Forum

Cyber Security Risk and Trends: Understanding the Current Threats and Trends

Jeroen Vandeleur
Senior Expert
NVISO

ABSTRACT

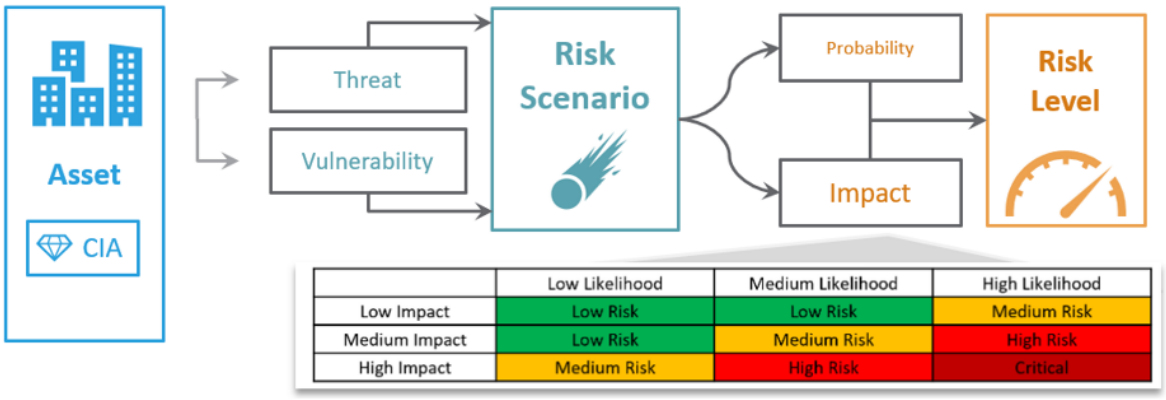
In today's digital landscape, cyber security is a pressing concern for executives and organizations. Understanding common vulnerabilities and misconfigurations is crucial for effective risk management. Weak passwords and phishing attacks pose significant threats that can be mitigated through strong passwords and user education programs. Misconfigurations, such as unchanged default settings, can be addressed through regular software updates and maintenance. Implementing secure protocols like HTTPS and VPNs safeguards against insecure network connections. The principle of least privilege and access permission reviews help prevent unauthorized access. Regular data backups, coupled with off-site or cloud storage, ensure resilience against ransomware attacks. Updating and retiring unsupported software reduces vulnerabilities. Executives must prioritize user awareness and training to foster a secure environment and protect valuable assets.

Introduction

In today's digital landscape, cyber security is an increasingly critical concern for organizations across industries. As technology advances and businesses become more reliant on digital systems, the risks and threats they face continue to evolve. It is imperative for organizations to identify potential risks and vulnerabilities to protect their valuable assets effectively. This article, based on the presentation in Gent, provides a comprehensive understanding of the current trends in cyber security, covering topics such as emerging threats, data breaches, and social engineering techniques. The importance of proactive measures is emphasized by examining specific examples of risks and vulnerabilities, while the significance of implementing practical measures to protect smaller organizations and individuals in today's digital world is also addressed. The goal is to empower readers with actionable strategies - regular software updates, the use of strong passwords, caution for and awareness of phishing attempts…- to enhance their cyber security posture.

Getting started with risk assessments and risk levels

For some organizations it's difficult to define or prioritize certain risks, therefore as a crucial preparation step you need to know your environment and your assets. For example, where is your critical data stored, are you hosting data locally or in a cloud environment. All these questions will help you to define the correct risk scenarios and to know what a potential risk level for your organization is. Below you can find a schematic view on how to start by evaluating an asset, define the risk scenario and allocate the appropriate risk level.



	Low Likelihood	Medium Likelihood	High Likelihood
Low Impact	Low Risk	Low Risk	Medium Risk
Medium Impact	Low Risk	Medium Risk	High Risk
High Impact	Medium Risk	High Risk	Critical

In essence a risk assessment involves evaluating the value of assets, identifying potential threats, and assessing vulnerabilities. By accurately calculating the probability and potential impact of various risk scenarios, organizations can determine the level of risk they face. This information is crucial for effective resource allocation and the implementation of appropriate security measures to mitigate identified risks.

Insights from the field

NVISO has gained extensive insights into the common security issues faced by organizations. Our analysis of 356 assessments revealed a total of 1,923 vulnerabilities, with 41 classified as critical and 286 carrying a high-risk level. These findings highlight the prevalence of security weaknesses, even among organizations that regularly undergo security assessments.

As mentioned, 41 critical findings were found. Critical findings represent the most severe level of risk and require immediate attention and remediation. They often indicate a failure in security controls, such as inadequate access controls, unpatched software vulnerabilities, misconfigurations, or weak authentication mechanisms. These findings demand urgent action and prioritization to address and mitigate the identified risks to minimize potential harm or damage.

Important to note is that these numbers are based on organizations that have the budget and resources to perform security assessment and invest in security controls. However smaller companies

often face challenges due to limited resources and a lack of awareness regarding the risk levels associated with their assets.

Common vulnerabilities found in these assessments

Below follows a description of some of the common vulnerabilities found during our assessments. A security vulnerability refers to a weakness or flaw in a system, network, application, or process that could be exploited by attackers to compromise the confidentiality, integrity, or availability of the system or its data. Organizations typically perform vulnerability assessments and penetration testing to discover vulnerabilities and take appropriate measures to mitigate them.

1. Weak Passwords: Weak passwords lacking complexity and diversity pose a significant vulnerability. Implementing password policies that enforce strong passwords, regular password changes, and multi-factor authentication (MFA) provides a robust defense against this vulnerability. MFA adds an extra layer of security by requiring users to provide additional verification factors beyond passwords, such as unique codes or biometric authentication.

2. Vulnerable Software: Outdated or unpatched software often contains known vulnerabilities that cybercriminals exploit. Organizations must establish a robust patch and update management process to ensure the timely installation of security patches and software updates. By regularly monitoring software updates and patches, testing them for compatibility, and deploying them promptly, organizations can significantly reduce the risk associated with vulnerable software.

3. Phishing: Phishing attacks are social engineering tactics that exploit human vulnerabilities to deceive individuals into revealing sensitive information or installing malicious software. Comprehensive employee training and awareness programs are crucial in educating staff about phishing techniques, enabling them to identify phishing attempts and implement best practices to prevent successful attacks.

4. Unsecured Network Connections: Unsecured network connections, particularly those transmitting sensitive data, expose organizations to significant risks. Implementing encryption protocols, such as Transport Layer Security (TLS) or Virtual Private Networks (VPNs), ensures secure communication. Additionally, organizations should enforce secure Wi-Fi standards, such as WPA2 or WPA3, to mitigate risks associated with unsecured network connections.

5. Unsecured External Access: The widespread adoption of remote work has increased the vulnerability of unsecured external access points. Organizations must implement secure remote access solutions, such as VPNs or secure remote desktop protocols, with strong authentication measures. Regular monitoring and logging of remote access activities enhance visibility and aid in detecting potential security breaches.

6. Backup and Recovery Processes: Inadequate or non-existent data backup and recovery processes can result in significant data loss and prolonged downtime. Implementing comprehensive backup

strategies, including regular backups, offsite storage, and testing data recovery procedures, ensures business continuity and minimizes the impact of potential data loss or system failures.

Common misconfigurations found during our assessments

Security misconfigurations can arise from various sources, including human error, lack of awareness, inadequate knowledge of secure configuration settings, or failure to implement appropriate security controls. They can occur at different levels, such as the operating system, web server, database, network devices, or application frameworks. Below some common misconfigurations are described that have been found during our assessments. Some of these misconfigurations are also heavily linked to the vulnerabilities found. This also indicates that a misconfiguration can lead to a vulnerability within your environment.

1. Weak or No MFA: MFA adds an additional layer of security beyond passwords by requiring users to provide additional verification factors. Implementing MFA strengthens authentication measures and mitigates the risk of unauthorized access.

2. Patch and Update Management: Regular patching and updating are crucial to maintaining a secure environment. Organizations should establish a robust patch management process, which includes identifying systems and software that require updates, testing patches for compatibility, and deploying them promptly. Automating patch management can streamline this process, ensuring timely updates and reducing the window of vulnerability.

3. Application and Mail Filtering: Effective application and mail filtering mechanisms are essential for mitigating the risks associated with malicious software and phishing attacks. Implementing robust filtering mechanisms that prevent the execution of unauthorized applications and filter out malicious emails enhances overall security posture.

4. Encryption of Data at Rest and in Transit: Encrypting data both at rest and during transmission safeguards against unauthorized access. Organizations should implement encryption mechanisms, such as disk encryption and secure communication protocols, to ensure the confidentiality and integrity of sensitive information.

5. Segmentation and Access Control: Proper network segmentation and access control measures restrict unauthorized lateral movement within networks and limit access to critical systems. Implementing network segmentation and robust access controls reduces the impact of potential security breaches and unauthorized access.

6. Disaster Recovery Plans: Developing comprehensive disaster recovery plans is crucial for minimizing downtime and restoring operations after a security incident or data loss event. Organizations should establish procedures for data backup, replication, and recovery, ensuring timely recovery and minimizing the impact on business operations.

7. Vulnerable Third Parties: Engaging with third-party vendors that lack adequate security measures introduces risks to an organization's overall security posture. Conducting thorough vendor risk assessments and due diligence, including evaluating their security practices and certifications, helps mitigate the potential risks associated with vulnerable third parties.

In identifying vulnerabilities and misconfigurations, it is crucial to discuss specific mitigation techniques tailored to address each issue and lower the associated risk level. By focusing on practical solutions, we can effectively tackle a range of security concerns, such as weak passwords, outdated software, insecure network settings, and more. Through our discussions, we will provide actionable guidance on how to remediate these issues, emphasizing the importance of following secure configuration practices, implementing proper access controls, regularly updating software, applying encryption protocols, and adopting other relevant security measures. By implementing these mitigation techniques, organizations can significantly enhance their security posture and minimize the risk of exploitation.

Mitigation Techniques

In cybersecurity, mitigation refers to the process of reducing or minimizing the impact of security risks, threats, vulnerabilities, or attacks. It involves implementing measures and taking actions to prevent, detect, respond to, or recover from security incidents effectively. The primary goal of mitigation is to lessen the likelihood of successful attacks or minimize the potential damage they can cause.

Mitigation strategies can vary depending on the specific context and nature of the security issue at hand. The list below provides an overview of common mitigation techniques based on the vulnerabilities and misconfigurations described earlier.

1. Enforcing strong password policies and implementing multi-factor authentication (MFA)
Context: Weak passwords are a common entry point for attackers. Password policies that enforce complexity and regular changes significantly strengthen the authentication process. Implementing MFA provides an additional layer of security by requiring users to provide multiple verification factors, reducing the risk of unauthorized access.
Importance: Password-related vulnerabilities are exploited in a significant number of cyber-attacks. Strengthening password policies and implementing MFA greatly reduces the likelihood of successful credential-based attacks and unauthorized access to sensitive systems and data.

2. Establishing a robust patch and update management process:
Context: Outdated or unpatched software often contains known vulnerabilities that cybercriminals exploit. Regularly applying security patches and software updates closes these security gaps, mitigating the risk of exploitation.
Importance: Vulnerabilities in software are frequently targeted by attackers. Timely patching and updates ensure that known vulnerabilities are addressed, reducing the organization's exposure to potential attacks and minimizing the risk of data breaches or system compromises.

3. **Deploying effective application and mail filtering mechanisms**:
Context: Malicious applications and phishing emails are common vectors for cyber-attacks. Application and mail filtering help prevent the execution of unauthorized or potentially harmful software, as well as identify and block malicious emails.
Importance: Filtering mechanisms play a vital role in preventing the infiltration of malicious software and reducing the risk of successful phishing attacks. By proactively filtering out suspicious content, organizations can minimize the likelihood of malware infections, data breaches, and compromises resulting from socially engineered attacks.

4. Ensuring encryption of data at rest and in transit:
Context: Unencrypted data is vulnerable to interception and unauthorized access, whether it is stored or transmitted. Encryption protects sensitive information, rendering it unreadable to unauthorized individuals.
Importance: Encryption safeguards the confidentiality and integrity of data. By encrypting data both at rest (e.g., on storage devices) and in transit (e.g., during network communication), organizations significantly reduce the risk of data breaches and unauthorized disclosure of sensitive information, ensuring compliance with data protection regulations.

5. **Implementing network segmentation and access control measures**:
Context: Network segmentation divides a network into separate zones, limiting access to specific resources and systems. Access control mechanisms authenticate and authorize individuals to access specific network resources based on predefined policies.
Importance: Network segmentation and access control help contain potential security incidents and limit lateral movement by separating critical systems and sensitive data from less secure areas. By enforcing access controls, organizations reduce the risk of unauthorized access and minimize the potential impact of successful attacks, enhancing overall network security.

6. Developing comprehensive disaster recovery plans:
Context: Disruptions caused by security incidents or data loss events can have severe consequences. Disaster recovery plans outline procedures for data backup, replication, and recovery to minimize downtime and restore operations.
Importance: Disaster recovery plans are essential for business continuity. They enable organizations to recover quickly from security incidents, minimize the impact on operations, and ensure the availability of critical systems and data. By having a well-defined plan in place, organizations can reduce the duration and costs associated with recovery efforts.

7. Conducting thorough vendor risk assessments and due diligence:
Context: Vendor risk assessments and due diligence involve evaluating and analyzing the security posture and practices of vendors to assess the potential risks they pose to an organization's data, systems, and overall security. This process helps organizations understand the level of risk associated with engaging a particular vendor and enables them to make informed decisions regarding vendor selection, contract negotiation, and ongoing vendor management.
Importance: Conducting thorough vendor risk assessments and due diligence has multiple benefits. It can incentivize vendors with weak security measures to enhance their security practices.

Additionally, comparing and evaluating multiple vendors allows for the selection of more mature and reliable organizations to collaborate with. A shared responsibility model, often provided in cloud environments, clarifies the specific responsibilities of both the vendor and the organization, ensuring transparency and accountability.

By implementing these mitigation techniques, organizations can enhance their overall cyber security.