UNIT V

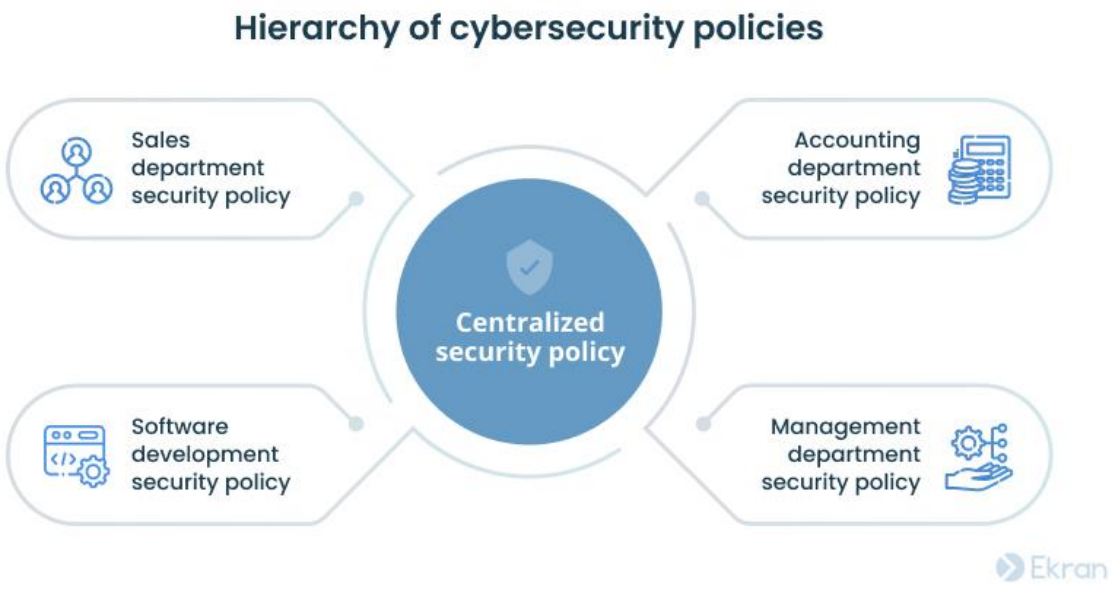
SECURITY ASSESSMENT

Security Monitoring and Improvement Best Practices

Cyber security best practices:

1. Establish a robust cybersecurity policy

A cybersecurity policy serves as a formal guide to all measures used in your company to improve cybersecurity efficiency. The policy helps your security specialists and employees to be on the same page and describes essential and company-wide information security practices. Consider implementing a hierarchical cybersecurity policy that consists of a single centralized policy and additional policies uniquely designed for each department within your organization. A hierarchical cybersecurity policy takes into account each department's unique needs, helping you increase overall cybersecurity policy effectiveness and avoid disrupting departments' workflows.



2. Secure your perimeter and IoT connections

Present-day organizations' perimeters extend far behind firewalls and DMZs, as remote work, cloud environments, and IoT devices significantly extend the attack surface. IoT is a rising trend — the IoT market is expected to grow to about $567 billion in 2027 from around $384 billion in 2021. Security cameras, doorbells, smart door locks, heating systems, and office equipment — many of these are connected to the internet and can be used as potential attack vectors. A compromised printer, for instance, can allow malicious actors to view all printed or scanned documents. Consider securing your perimeter by protecting your border routers and establishing screened subnets. To enhance the enterprise database security, you can also separate sensitive data from your corporate network and limit access to such data. You can combine conventional protection measures such as firewalls and VPNs with the zero trust model to protect yourself. Based on the concept never trust, always

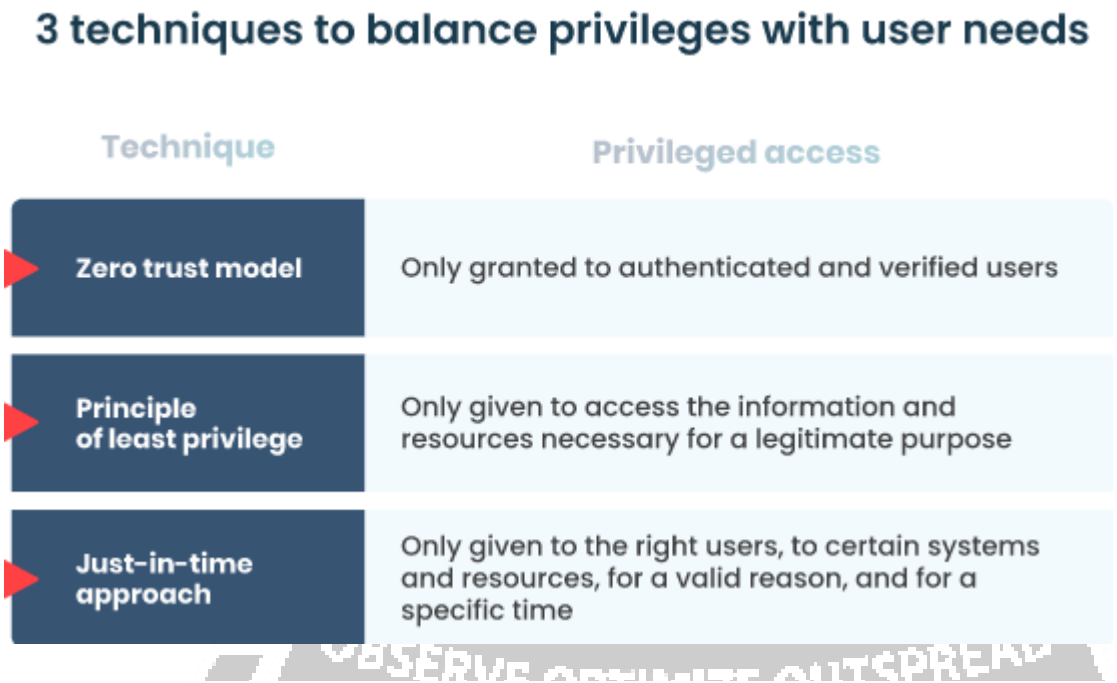
verify, zero trust requires users and devices in your organization to be continually validated to prevent unauthorized access.

3. Employ a people-centric security approach

A technology-centric approach to cybersecurity isn't enough to ensure all-around protection, since hackers often use people as entry points. According to Verizon's 2023 Data Breach Investigations Report, 74% of breaches involve a human element. A people-centric approach can help you reduce the chance of human-connected risks. In people-centric security, an important perimeter is the workers themselves. Educating and monitoring employees are the main things to consider for a secure people-centric environment.

4. Control access to sensitive data

Granting employees many privileges by default allows them to access sensitive data even if they don't need to. Such an approach increases the risk of insider threats and allows hackers to access sensitive data as soon as they compromise an employee's account. Applying the least permissions model (also called the principle of least privilege) is a much better solution. It means assigning each user the fewest access rights possible and elevating privileges only if necessary. If access to sensitive data is not needed, corresponding privileges should be revoked.



5. Manage passwords wisely

Employee credentials give cybercriminals direct access to your sensitive data and valuable business information. Brute force attacks, social engineering, and other methods can be used to compromise your employees' credentials without your employees knowing. Organizations often use specialized password management tools to prevent such attacks. Such solutions can give you control over your employees' credentials, reducing the risk of account compromise.

Give preference to password management tools that provide passwordless authentication, one-time passwords, and password encryption capabilities. If you still trust employees to manage their own passwords, consider

adding the following recommendations to your cybersecurity policy: Use a different password for each account Have separate accounts for personal and business use Create lengthy passwords with special symbols, numbers, and capital letters Use mnemonics or other tactics to remember long passwords Use password managers and generators Never share credentials with other employees Change passwords at least once every three months

6. Monitor the activity of privileged and third-party users

Privileged users and third parties with access to your infrastructure have all the means to steal your sensitive data and go unnoticed. Even if these users don't act maliciously, they can unintentionally cause cybersecurity breaches. To reduce the risks posed by privileged users and third parties, consider the following measures:

The most useful way to protect your sensitive data is by monitoring the activity of privileged and third-party users in your organization's IT environment. User activity monitoring (UAM) can help you increase visibility, detect malicious activity, and collect evidence for forensic investigations.

7. Manage supply chain risks

Your organization's vendors, partners, subcontractors, suppliers, and other third parties with access to your organization's resources may be susceptible to supply chain attacks.

In a supply chain attack, cybercriminals infiltrate or disrupt one of your suppliers and use that to escalate the attack further down the supply chain, which may affect your organization. During the Solarwinds hack, cybercriminals managed to access the networks and data of thousands of organizations by inserting malware inside a Solarwinds software update. Some of the fundamental practices for handling supply chain risks are:

8.Enhance your data protection and management

How you manage your business data is critical to your organization's privacy and security. You may start by documenting information management processes in a data management policy. Consider describing how data is collected, processed, and stored, who has access to it, where it's stored, and when it must be deleted. It's also vital to outline your data protection measures in a data protection policy. Consider building your data protection measures around the key principles of information security: Confidentiality — protect information from unauthorized access

Integrity — make sure unauthorized users can't modify data at any stage of the data lifecycle

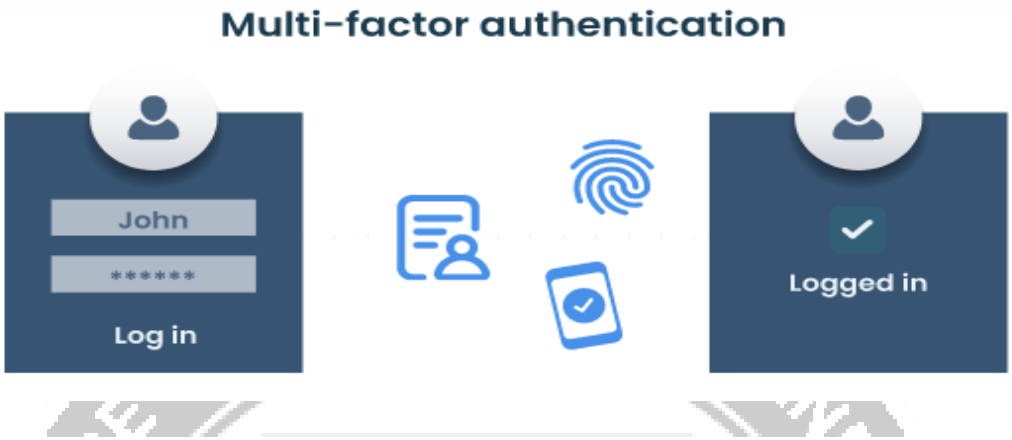
Availability — ensure authorized users always have access to data they need

9.Employ biometric security

Biometrics ensure fast authentication, safe access management, and precise employee identification. Biometrics are a reliable way to verify users' identities before providing access to valuable assets, which is vital for your organization's security. That's why the biometrics market is growing rapidly. Biometrics provide for more reliable authentication than passwords, which is why they are often used for multi-factor authentication (MFA). However, authentication isn't the only use for biometrics. Security officers can apply various biometrics-driven tools to detect compromised privileged accounts inrealtime.

10. Use multi-factor authentication

Multi-factor authentication helps you protect sensitive data by adding an extra layer of security. With MFA activated, malicious actors cannot log in even if they possess your password. They would still need other authentication factors, such as your mobile phone, fingerprint, voice, or a security token.



11. Conduct regular cybersecurity audits

Conducting audits regularly helps you assess the state of your organization's cybersecurity and adjust it if needed. During audits, you can detect: Cybersecurity vulnerabilities Compliance gaps Suspicious activity of your employees, privileged users, and third-party vendors

12. Simplify your technology infrastructure

Deploying and maintaining a large number of tools is expensive and time-consuming. Moreso, resource-demanding software can slow down your organization's workflows. Consider having one or a few comprehensive solutions that contain all the necessary functionality. This way, you'll streamline and simplifyyoursecurityinfrastructure.