SAND5G

https://sand5g-project.eu/

Analysis of cybersecurity measures under NIS-2 Directive

Dedicated Courses from National Authorities

D3.1: Security training, knowledge and capacity building report

This project has received funding from the DIGITAL EUROPE (DIGITAL) programme under Grant Agreement No 101127979

NIS-2 Directive – article 21
Cybersecurity risk-management measures

1. policies on risk analysis and information system security;
2. incident handling;
3. business continuity, such as backup management and disaster recovery, and crisis management;
4. supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
5. security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
6. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
7. basic cyber hygiene practices and cybersecurity training;
8. policies and procedures regarding the use of cryptography and, where appropriate, encryption;
9. human resources security, access control policies and asset management;
10. the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Analysis of NIS-2 cybersecurity measures

1. Information security policies and procedures

Create an information security policy and topic-specific policies, to ensure protection of the confidentiality, integrity and availability of your data and systems, in accordance with applicable laws and contractual requirements

- **At the highest level: develop a general security policy**

A document written in a high level language, approved by top management and which sets out the organization's approach to managing its information security.

- **At a lower level: develop topic-specific security policies**

Documents written in a more specialized language, approved by the appropriate level of management, and which define rules and security measures for specific thematic areas of network and information systems.

1. Information security policies and procedures

Examples of topic-specific information security policies:

- ✓ Access control
- ✓ physical and environmental security
- ✓ asset management
- ✓ secure configuration and handling of user endpoint devices
- ✓ cryptography and key management
- ✓ networking security
- ✓ information security incident management
- ✓ backup
- ✓ secure development

NIST Cybersecurity Framework

Core functions	Categories
Govern	Organizational Context – Risk Management Strategy – Roles, Responsibilities, and Authorities – Policy – Oversight – Cybersecurity Supply Chain Risk Management
Identify	Asset Management – Risk Assessment – Improvement
Protect	Identity Management, Authentication, and Access Control – Awareness and Training – Data Security – Platform Security – Technology Infrastructure Resilience
Detect	Continuous Monitoring – Adverse Event Analysis
Respond	Incident Management – Incident Analysis – Incident Response Reporting and Communication Incident Mitigation
Recover	Incident Recovery Plan Execution – Incident Recovery Communication

2. Risk management framework

Establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of your network and information systems

- Select a risk management methodology (e.g., ISO 27005, NIST 800-30, EU ITSRM).
- Establish the entity's risk appetite, that is the amount of risk that the entity is strategically willing to accept to achieve its objectives.
- Define the risk tolerance level, which refers to the level of risk that an entity is willing to accept in pursuit of its long-term objectives.
- Define risk acceptance criteria.

2. Risk management framework

Risk assessment process

Identify threat sources and threat events

Identify vulnerabilities in network and information systems

Determine the likelihood of a threat exploiting a vulnerability

Determine the impact should the threat materialize

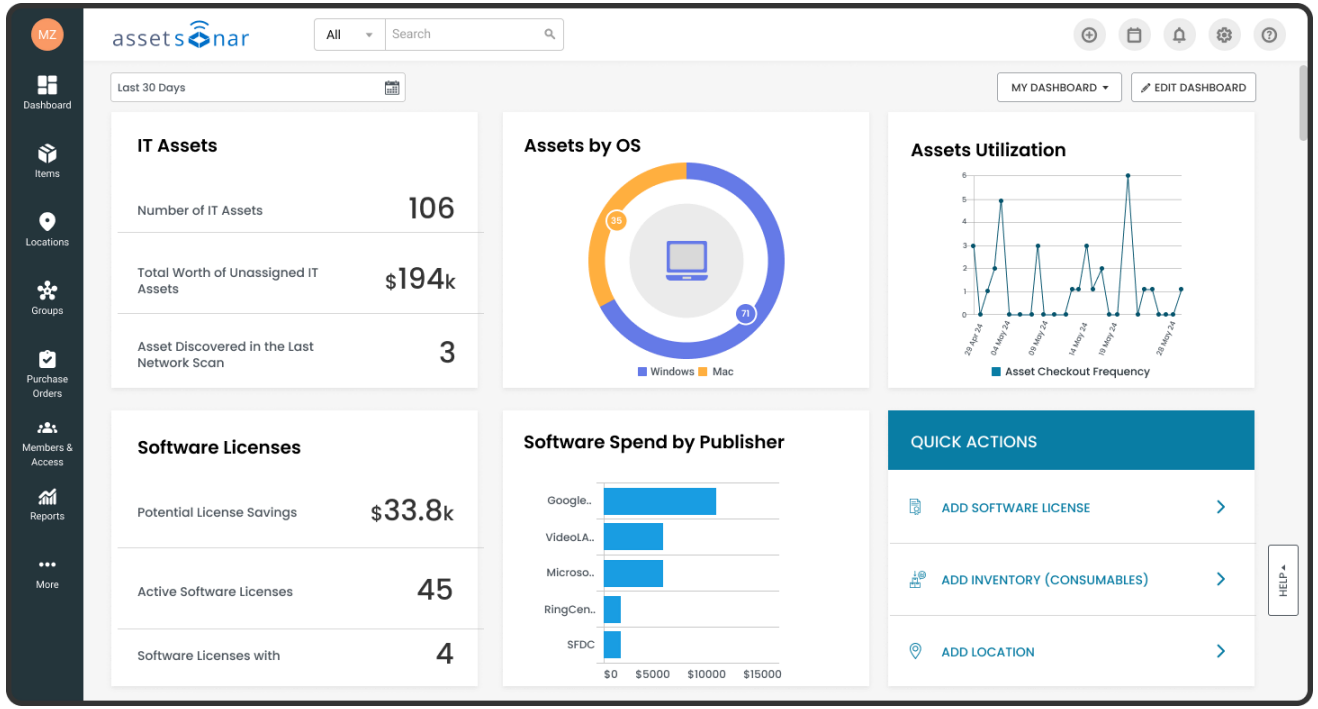
Risk = Likelihood x Impact

3. Asset inventory

Create an inventory of all IT assets (hardware and software) hosted on your physical infrastructure, as well as in cloud environments

ASSET INVENTORY TEMPLATE

INV. No.	CONDITION	ITEM NAME / DESCRIPTION	CATEGORY	LOCATION	WARRANTY Info.	SERIAL No.	BANK LOAN?	PURCHASE DATE	EXPECTED LIFE in Years	ASSET END DATE	MONTHS TO REPLACE	3 MONTH END ALERT	PURCHASE PRICE	END OF LIFE EXPECTED VALUE	STRAIGHT LINE DEPRECIATION – ANNUAL	STRAIGHT LINE DEPRECIATION – MONTHLY	CURRENT VALUE	NOTES
1.1	GOOD	Description of Asset A	Computer hardware	Main office	Expires at end of Q4	12345	YES	02/02/28	2.00	02/01/30	85.4	11/03/29	$5,500	$2,500	$1,500	$125	$13,029	
1.23	FAIR	Description of Asset B	Computer software	Main office		56789	NO	02/05/28	5.00	02/03/33	122.0	11/05/32	$1,200	$1,000	$40	$3	$1,401	
1.36	POOR	Description of Asset C	Computer hardware	Main office	Expires at end of Q5	10233	YES	02/08/28	8.00	02/06/36	158.6	11/08/35	$2,850	$0	$356	$30	$4,644	
1.49	BAD	Description of Asset D	Computer software	Main office		14577	NO	02/11/28	11.00	02/08/39	195.2	11/10/38	$3,911	$500	$310	$26	$5,475	
1.62	GOOD			Main office	Expires at end of Q6	19121	YES	02/14/28	14.00	02/10/42	231.8	11/12/41	$2,800	$200	$186	$15	$3,738	
1.75	GOOD			Main office		23465	YES	02/17/28	17.00	02/12/45	268.4	11/14/44	$7,300	$0	$429	$36	$9,473	
1.88	GOOD			Main office	Expires at end of Q7	27009	YES	02/20/28	20.00	02/15/48	305.0	11/17/47	$134	$0	$7	$1	$168	
2.01	GOOD			Main office		32453	NO	02/23/28	23.00	02/17/51	341.6	11/19/50	$5,789	$8,500	-$118	-$10	$5,191	
2.14	GOOD			Main office	Expires at end of Q8	37897	NO	02/26/28	26.00	02/19/54	378.2	11/21/53	$56,348	$100	$2,163	$180	$67,349	
2.27	GOOD			Main office		41341	NO	02/29/28	29.00	02/21/57	414.8	11/23/56	$546,587	$0	$18,848	$1,571	$642,582	
2.4	GOOD			Main office	Expires at end of Q9	45785	NO	03/03/28	32.00	02/24/60	451.4	11/26/59	$54,548	$0	$1,705	$142	$63,244	
2.53	GOOD			Main office		50229	NO	03/06/28	35.00	02/26/63	488.0	11/28/62	$545	$0	$16	$1	$625	
2.66	GOOD			Main office	Expires at end of Q10	54673	NO	03/09/28	38.00	02/28/66	524.6	11/30/65	$480	$0	$13	$1	$545	
2.79	GOOD			Main office		59117	NO	03/12/28	41.00	03/02/69	561.2	12/02/68	$654	$0	$16	$1	$736	
2.92	GOOD			Main office	Expires at end of Q11	63561	NO	03/15/28	44.00	03/04/72	597.8	12/05/71	$5,498	$0	$125	$10	$6,140	
3.05	GOOD			Main office		67005	NO	03/18/28	47.00	03/07/75	634.4	12/07/74	$3,487	$0	$74	$6	$3,869	
3.18	GOOD			Main office	Expires at end of Q12	73449	NO	03/21/28	50.00	03/09/78	671.0	12/09/77	$5,450	$0	$109	$9	$6,011	
3.31	GOOD			Main office		7893	NO	03/24/28	53.00	03/11/81	707.6	12/11/80	$6,488	$0	$122	$10	$7,120	
3.44	GOOD			Main	Expires at	82337	NO	03/27/28	56.00	03/13/84	744.2	12/14/83	$4,878	$0	$123	$10	$7,513	



Excel file

Asset inventory software

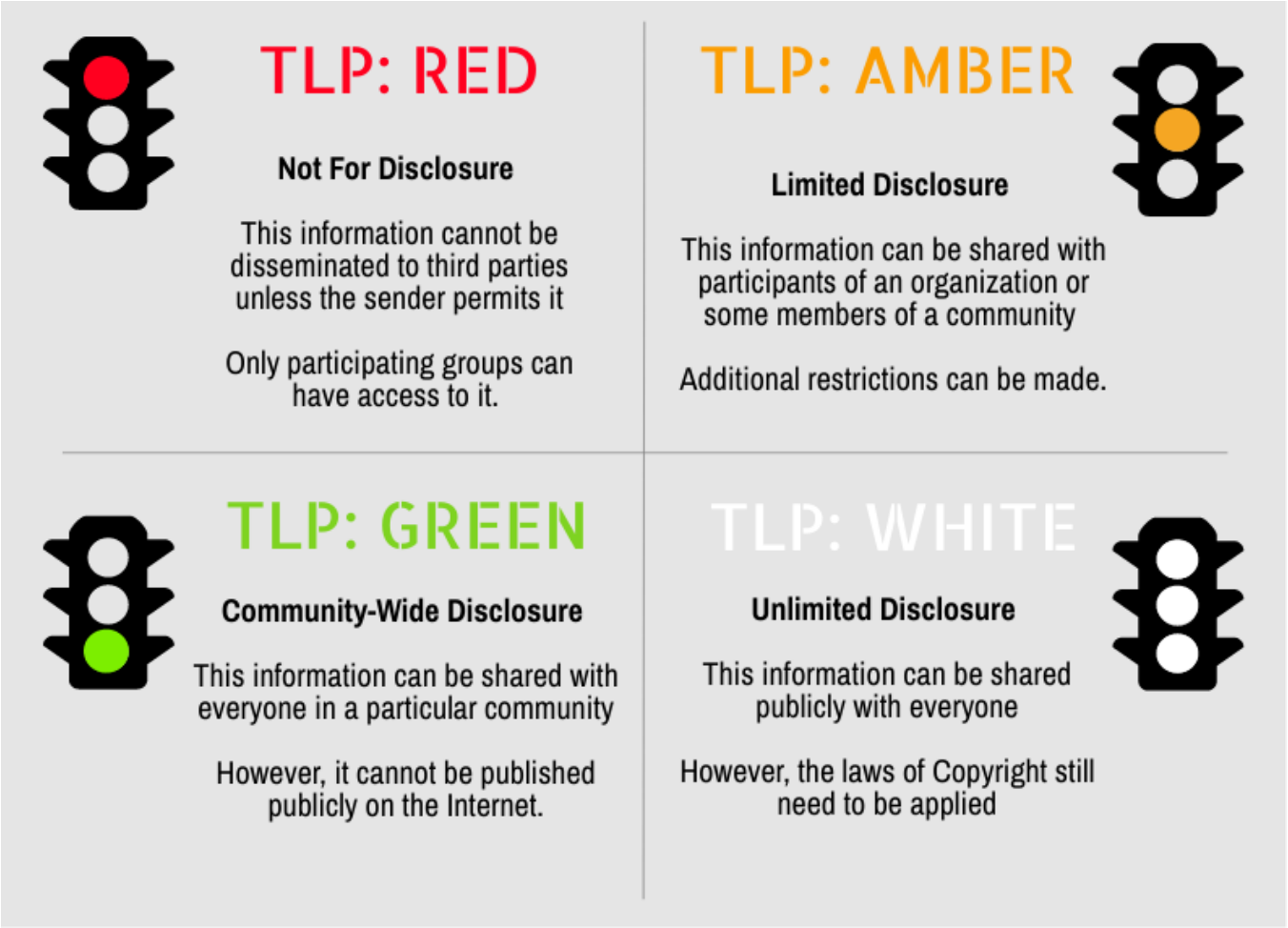
3. Asset inventory

- The asset inventory must be accurate and up-to-date.
- Define classification levels for your data (e.g., restricted, confidential, internal, public, …).
- Associate each asset with the classification level of the data it processes.
- Replace assets no longer supported by the vendor (“end-of-support”).
- Give special attention to “shadow IT” assets.

Restricted	• Highly-sensitive information
Confidential	• Sensitive information
Internal	• Non-sensitive information that is not released to public
Public	• Information has been approved for public access

3. Asset inventory

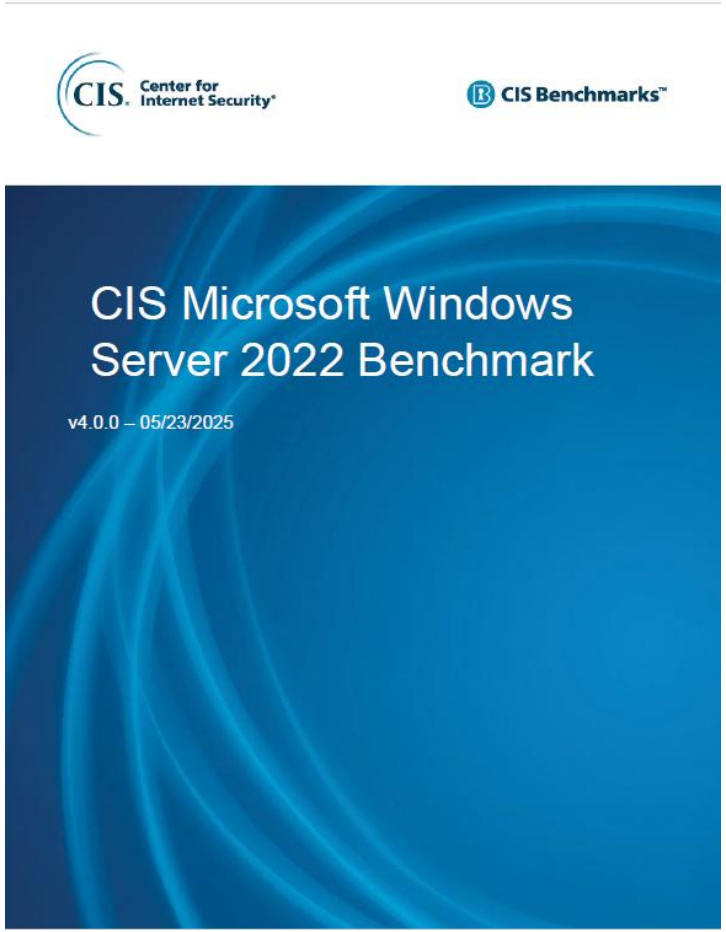
Information classification:
Traffic light protocol for information sharing



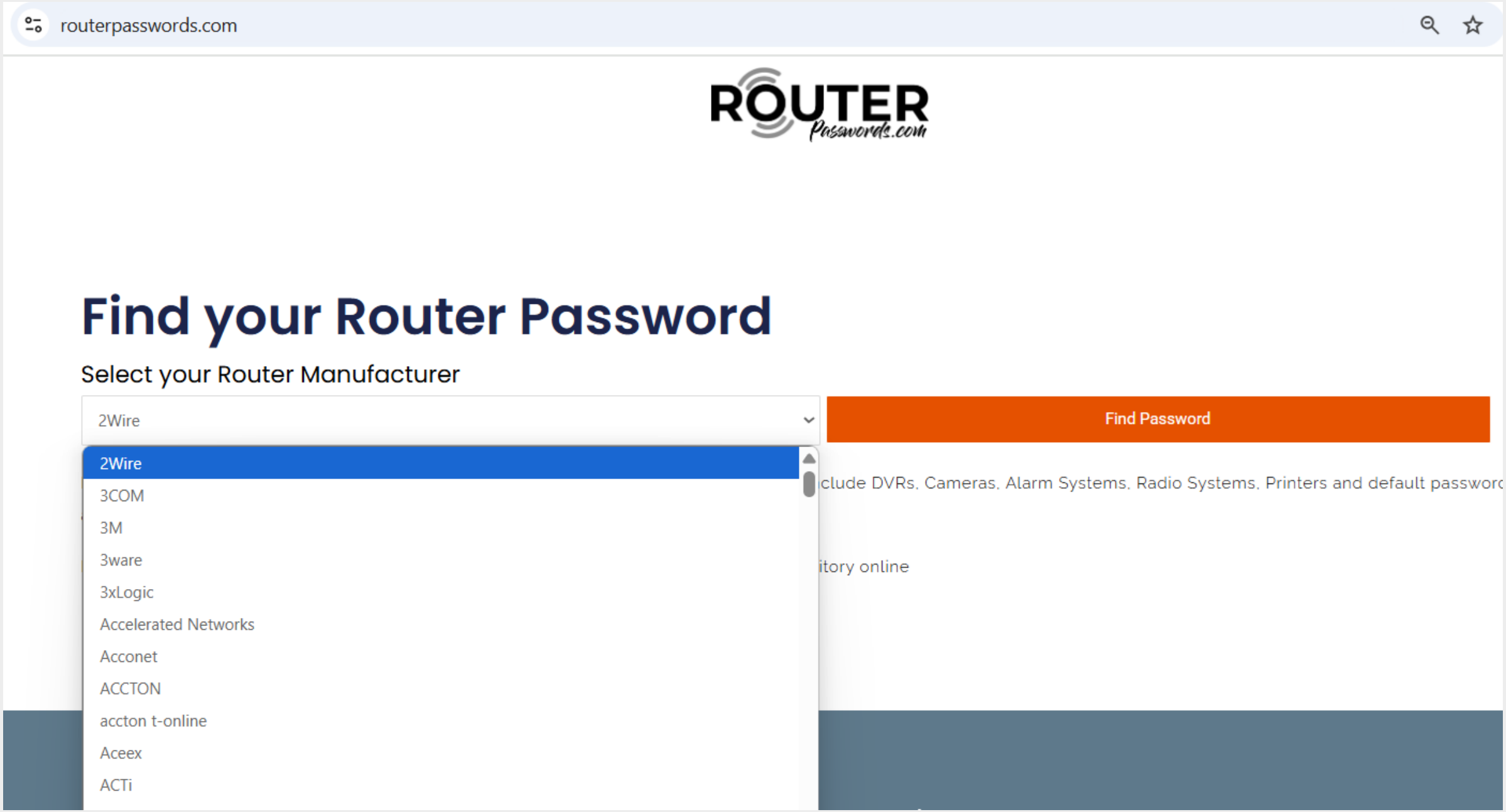
4. Secure configuration of enterprise assets and software

Regularly implement secure configuration on workstations (desktops, laptops), servers, network devices (routers, switches, wireless access points, firewalls) and applications.

- Implement the principle of least functionality.
- Disable unused open ports, protocols and services.
- Implement software execution control (application blacklist / whitelist).
- Change default passwords in internet-facing assets (routers, access points, etc.) after first installment.



Major security risk: router default credentials per vendor public on the Internet



5. Vulnerability management

Implement procedures to identify, assess and address technical vulnerabilities in your network and information systems.

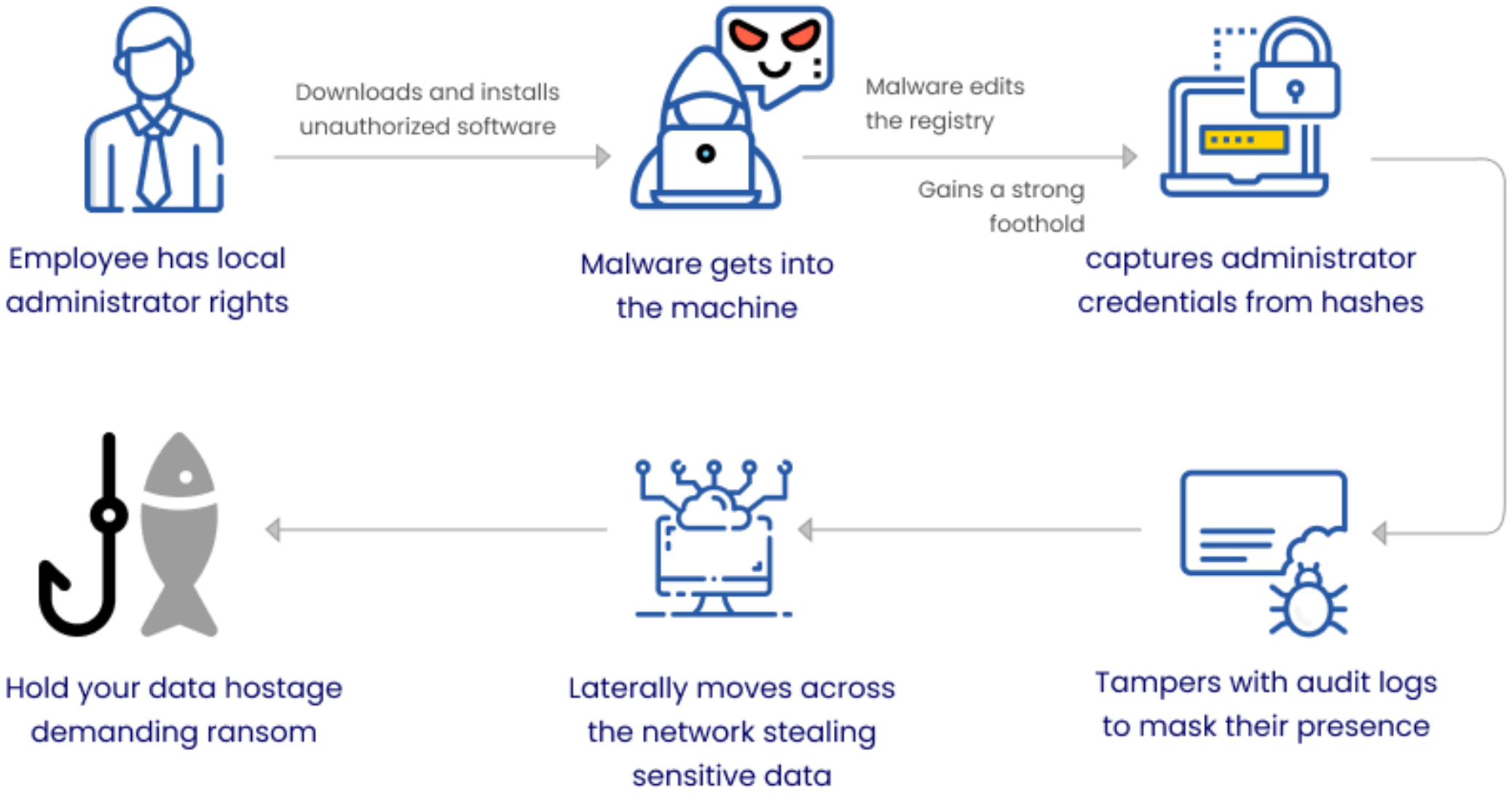
- Apply security patches within a reasonable time frame as they become available. Prioritize Internet-facing assets.
- Test security patches before applying them to production systems.
- Perform periodic vulnerability scans using automated tools.
- Implement a vulnerability remediation process based on a clear prioritization plan.

6. Identity management and access control

Restrict access to your information systems based on the principles of least privilege, need-to-know, and separation of duties.

- Create unique identities for all human and non-human users.
- Restrict admin privileges.
- Implement secure authentication.
- Implement multi-factor authentication, where feasible.

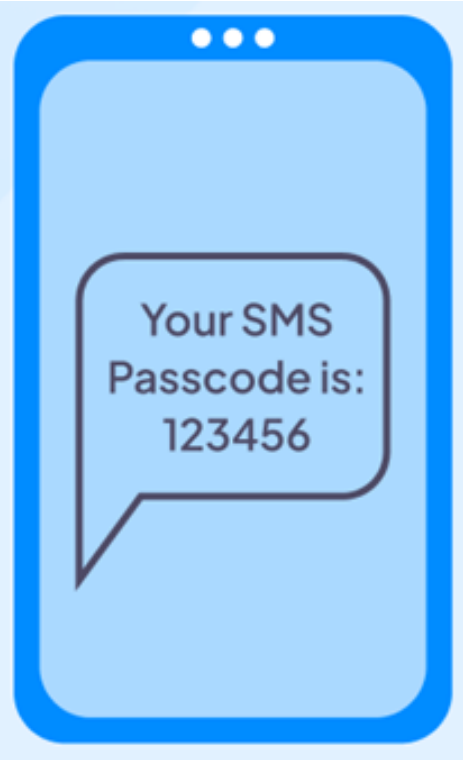
Example of the impact of not restricting administration privileges



6. Identity management and access control

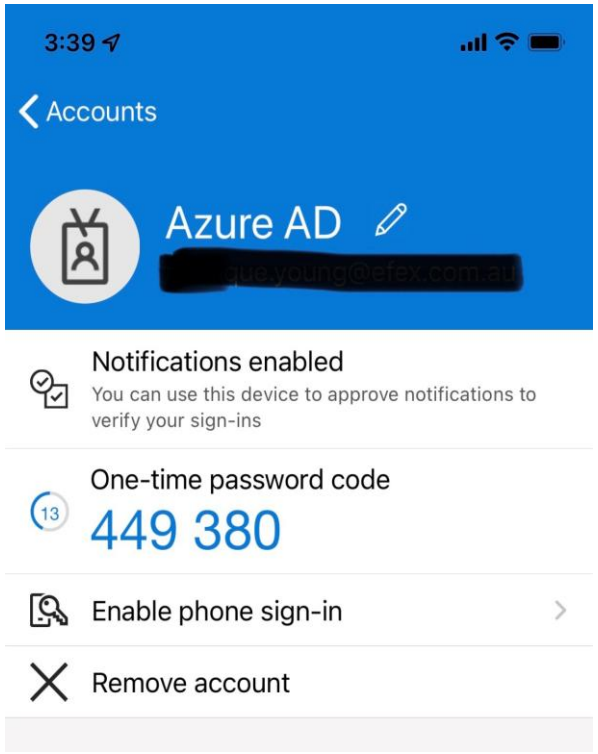
- **Authentication:**
  - Enforce strong passwords or passphrases.
  - Enforce MFA (Multi-Factor Authentication) for access to your critical applications.
  - Enforce MFA in all privileged accounts.
  - Enforce MFA for remote network connections.
  - Enforce session lock-out after a predefined number of continuous unsuccessful log-ins.

MFA types – from weakest to strongest



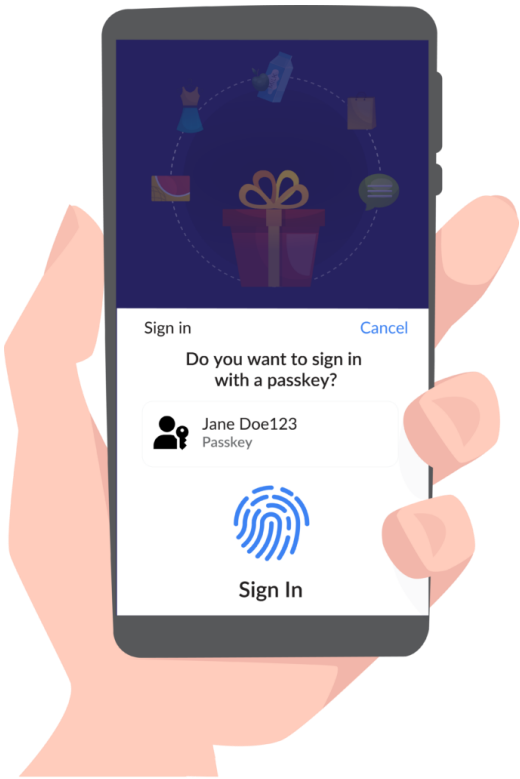
1. SMS based MFA

Vulnerable to phishing, SS7, and SIM swap attacks



2. App-based authentication

Vulnerable to phishing. SS7, and SIM swap attacks are not applicable



3. Phishing-resistant MFA

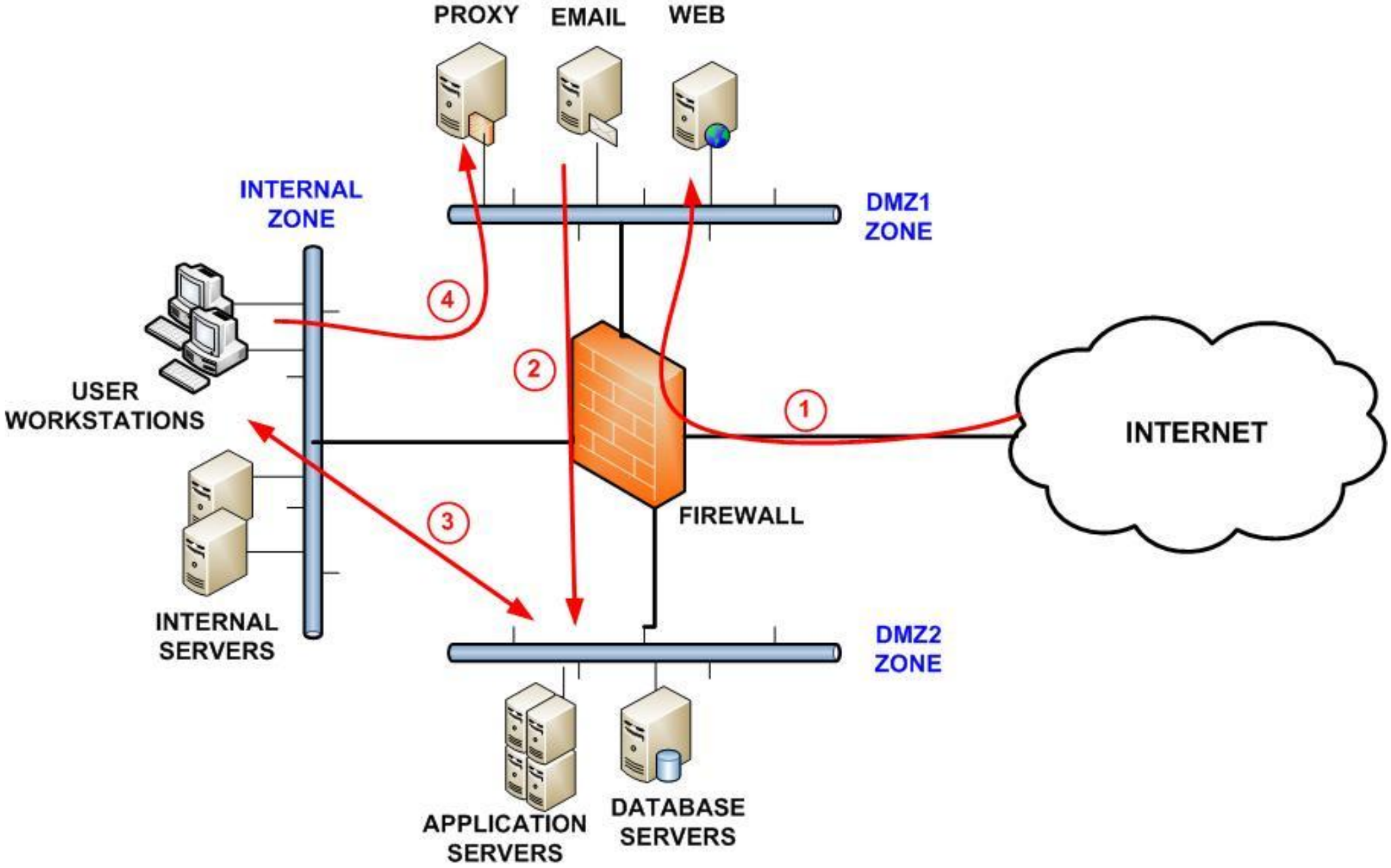
Resistant to phishing. Implements FIDO/ WebAuthn authentication

7. Network security

Implement appropriate security measures to protect your network from cyber threats.

- Place a firewall in your network boundary.
- Network segmentation: segment your network into distinct subnets based on the level of criticality of your business operations.
- Implement traffic filtering between subnets.
- Implement monitoring technologies in your network.
- Implement best practices for the security of DNS.
- Implement measures against distributed denial-of-service attacks.

Network segmentation example



8. Malware protection

Implement technologies that detect and prevent the installation, execution, and transmission of malicious software or commands on your devices and network.

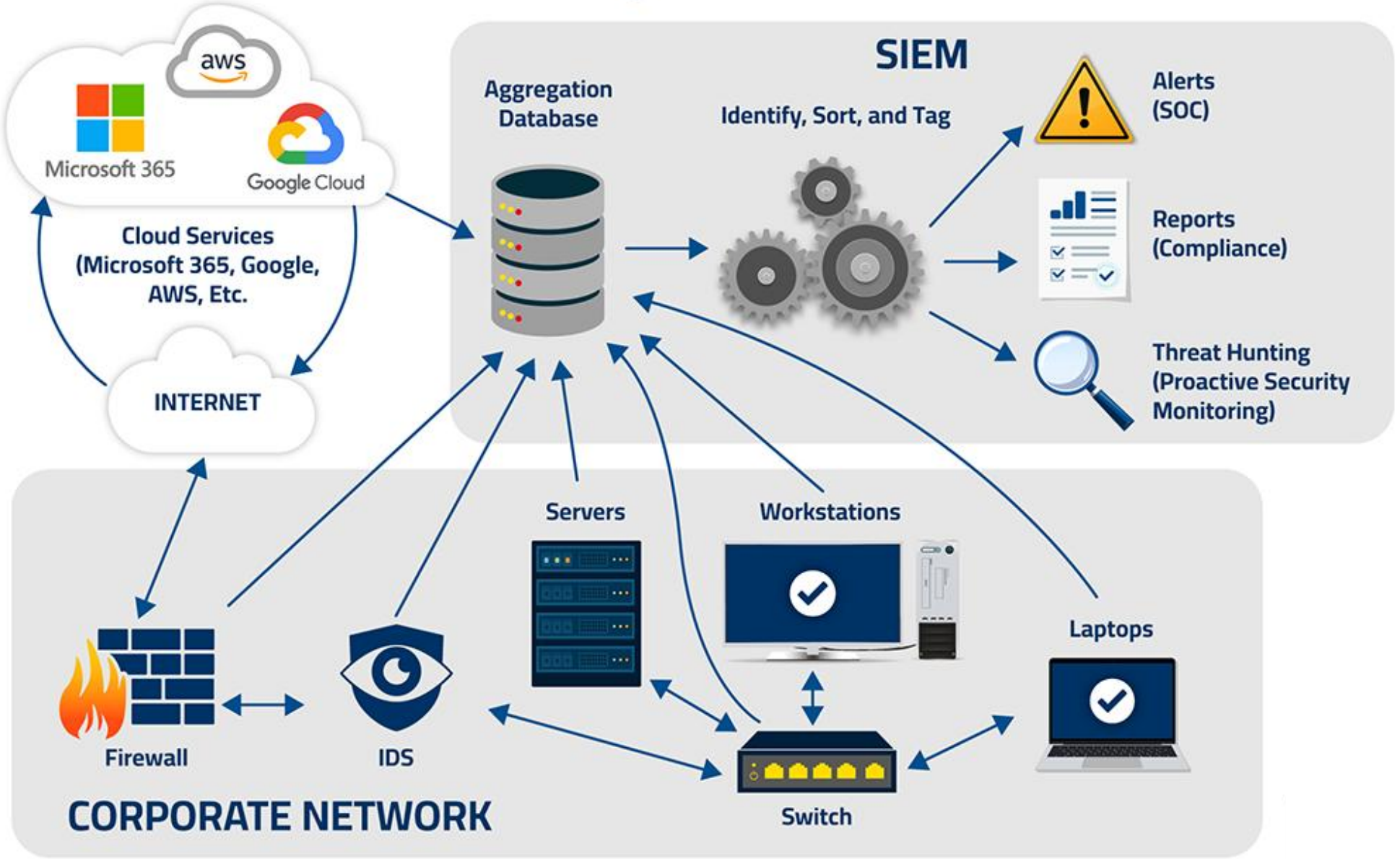
- Implement malware detection and protection software on every workstation and server, which will operate in an automated manner through central management.
- Implement DNS filtering to block access to known malicious domains.
- Implement rules that control the execution of applications (application whitelist / blacklist).
- Implement content filtering to control malicious incoming emails.
- In your email infrastructure, configure the following: a) enable STARTTLS, b) enable SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail), c) enable DMARC (Domain-based Message Authentication, Reporting and Conformance)

9. Logging and monitoring

Implement procedures and tools to monitor and log activities on your network and information systems to detect events that could be considered as incidents and respond accordingly to mitigate the impact.

- Enable logging in every workstation, server and network device.
- Ensure that logs include: a) creation, modification or deletion of users, b) authentication-related events, c) all privileged access to systems and applications and activities performed by administrative accounts, d) activation, stopping and pausing of the various logs, e) access or changes to critical configuration and backup files.
- Ensure the clock synchronization in every device.
- Implement SIEM (Security Information and Event Management), which correlates events from multiple sources and identifies patterns to detect possible cyber threats.

How Security Information and Event Management (SIEM) Works

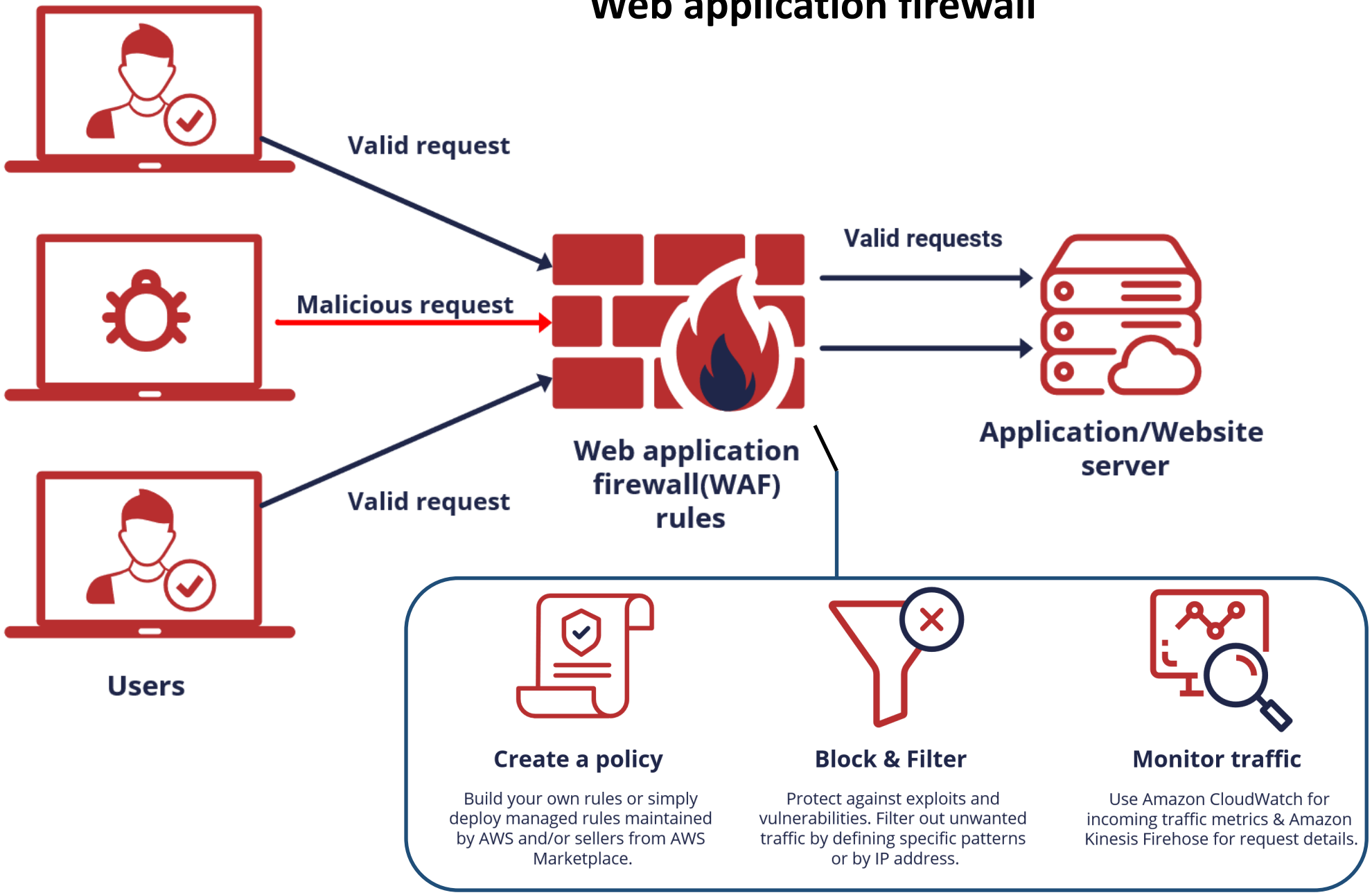


10. Application security

Implement information security principles in the full life cycle of your applications (design, development, tests, production, maintenance).

- Implement the principle of “security by design and by default” in every critical application.
- Implement secure software libraries and respectable development frameworks.
- Implement secure coding practices.
- Ensure that a vulnerability assessment / penetration test is conducted before the application goes into production.
- Implement a web application firewall, which operates at layer 7 (application layer), filters HTTP/HTTPS traffic and protects against attacks like SQL injection, cross-site scripting, etc.

Web application firewall



11. Use of cryptography

Implement policies and procedures related to cryptography to protect the confidentiality, authenticity and integrity of your data.

- Encrypt sensitive data at rest. Example implementations include Windows BitLocker (for full-volume encryption), Apple FileVault, Transparent Data Encryption (TDE) for SQL Server, etc.
- Encrypt sensitive data in transit. Example implementations TLS/HTTPS (Transport Layer Security), SSH (Secure Shell) and VPN (Virtual Private Networks).
- Encrypt data on removable media.
- Set up a mechanism (either manual or automated) for the selection, establishment and management (including updating) of cryptographic keys.

12. Cybersecurity and awareness training

Offer to all employees, including members of management bodies, cybersecurity and awareness raising programs.

- Train all users, and members of management bodies, in basic cyber hygiene practices, such as: a) protection from phishing and social engineering, b) safe email use and web browsing, c) secure use of mobile devices, d) use of relevant strong authentication means and methods, such as strong passwords and multi factor authentication, e) backup practices.
- Train network and system administrators in advanced cybersecurity issues, such as secure configuration of assets, zero trust concepts and detailed incident response activities.

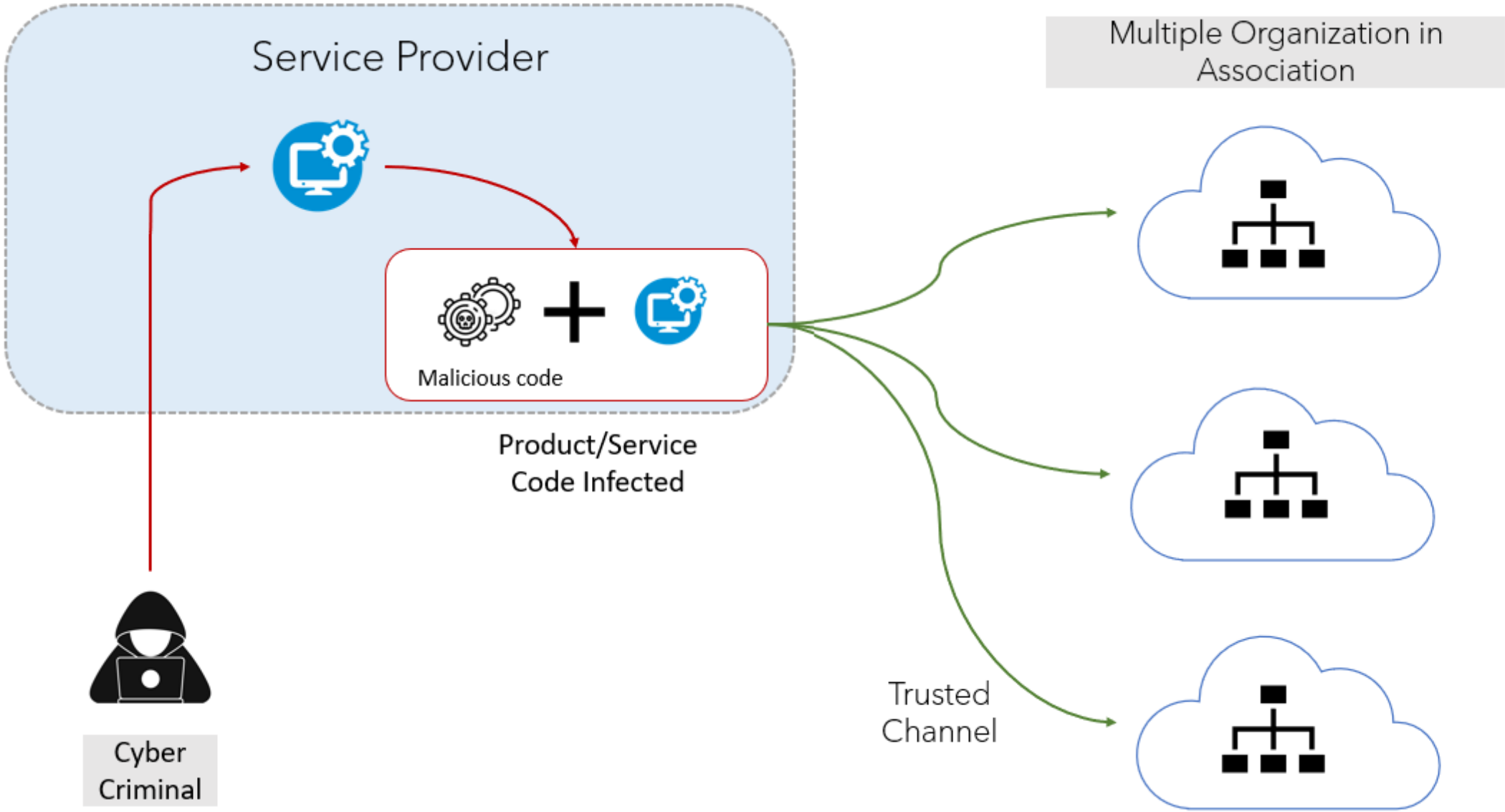
13. Supply chain risk management

Implement policies and procedures to govern the relations with your direct suppliers and service providers to mitigate the identified risks to the security of your network and information systems.

- Create an inventory of your direct suppliers and service providers and classify them in levels of criticality.
- Ensure that the contracts with your suppliers and service providers specify several issues, such as:

  - cybersecurity requirements for the suppliers and service providers,
  - the right to audit or right to receive audit reports,
  - requirements regarding subcontracting,
  - obligations of the suppliers and service providers at the termination of the contract, such as retrieval and secure deletion of data obtained by the suppliers and service providers in the exercise of their tasks.

The SolarWinds incident



14. Cybersecurity assessments

Periodically assess the effectiveness of your cybersecurity risk management measures.

- Implement methods of assessing the effectiveness of your cybersecurity risk management measures, such as:

  - vulnerability assessment,
  - penetration testing (e.g. internal, external, red / blue team),
  - audit (e.g. internal, external, compliance),
  - source code review.

- Implement procedures to remediate vulnerabilities and flaws, based on a prioritization plan.

15. Environmental and physical security

Implement protection measures against physical and environmental threats, based on risk assessments.

- Consider physical access controls measures, such as: smart cards, locks, security personnel to restrict access to high-criticality areas, segmentation of spaces or creation of zones according to authorization levels and their contents, CCTV cameras and monitoring systems.
- Consider supporting utilities, where relevant, that ensure the continuous operation of network and information systems, such as (indicative, non-exhaustive list):

  - power supply / electricity to keep systems running (UPS),
  - water for cooling and other operational needs,
  - gas for heating or backup power generation,
  - HVAC to maintain optimal operating conditions,
  - telecommunications – internet and network connectivity

16. Backup management

Implement backup technologies and procedures to protect systems and information against loss.

- Implement backup procedures by appropriately combining the available technologies (full, incremental, differential).
- Ensure that critical backups are stored in at least one offline destination.
- Perform backup integrity checks on a periodic basis.
- Perform a backup restoration test once a year.
- Store backups in a safe location, which is not in the same network as the system and are at sufficient distance to escape any damage from a disaster at the main site.

17. Incident response management

Establish a program to develop and maintain an incident response capability to prepare, detect, and quickly respond to an attack.

- Assign roles and responsibilities for incident management.
- Develop a communication plan with relevant stakeholders (staff, service providers, competent authorities, …).
- Develop a detailed incident response plan, outlining actions for each stage of the incident (containment, eradication, recovery, post-incident reviews).
- Implement SOC (Security Operations Center) capabilities, either on-premises or outsource the service to a specialized managed security service provider.

18. Business continuity and disaster recovery

Implement measures and procedures to ensure the business continuity of your operations after an adverse event or disaster.

- Lay down and maintain a business continuity and disaster recovery plan to apply in the case of incidents.
- Carry out a business impact analysis (BIA) to assess the potential impact of severe disruptions to your business operations. The BIA will establish continuity requirements for your network and information systems.

  - RPO (Recovery Point Objective): The maximum allowable data loss measured in time.

  - RTO (Recovery Time Objective): The target timeframe to restore business processes after a disruption to prevent unacceptable consequences.

  - MAO (Maximum Acceptable Outage): The absolute limit of time a service can be unavailable before the impact is catastrophic.

- Implement an alternate storage and/or processing site (backup/disaster recovery site) that is located at a sufficient geographical distance from your primary infrastructure.

Thanks for your participation

Questions and answers

1. In which core function of the NIST Cybersecurity Framework does the “continuous monitoring” category belong? (choose one answer)

☐ a. Protect

☐ b. Detect

☐ c. Respond

☐ d. Recover

Correct answer: b

2. In the traffic light protocol for information sharing, what does TLP: AMBER mean? (choose one answer)

☐ a. Community-wide disclosure: the information can be shared with everyone in a particular community

☐ b. Unlimited disclosure: the information can be shared publicly with everyone

☐ c. Limited disclosure: the information can be shared with participants of an organization or some member of a community

☐ d. Not for disclosure: the information cannot be disseminated to third parties unless the sender permits it

Correct answer: c

3. Which of the following measures is an example of secure configuration of assets? (choose one answer)

☐ a. The change of default passwords in internet-facing assets (routers, access points, etc.) after first installment

☐ b. The drafting of a network security policy

☐ c. The implementation of an antivirus solution

☐ d. The development of advanced cybersecurity trainings

Correct answer: a

4. What is the most secure method of multi-factor authentication (MFA)? (choose one answer)

☐ a. SMS-based MFA

☐ b. App-based MFA

☐ c. Sending a 6-digit code in the user's email address

☐ d. Phishing-resistant MFA

Correct answer: d

5. Which of the following is true about the web application firewall? (choose one answer)

☐ a. It operates at layer 7 (application layer) of the OSI model

☐ b. It operates at layer 3 (network layer) of the OSI model

☐ c. It encrypts data in the network

☐ d. It performs vulnerability analysis in web applications

Correct answer: a

6. Which of the following methods or protocols can be used for encrypting data in transit? (choose one answer)

☐ a. Windows BitLocker

☐ b. HTTP protocol

☐ c. VPN (Virtual Private Network)

☐ d. Telnet

Correct answer: c

7. Which of the following methods can be used for assessing the effectiveness of cybersecurity measures? (choose one answer)

☐ a. Developing an incident response plan

☐ b. Performing an incremental back-up

☐ c. Implementing secure configuration in a wireless access point

☐ d. Performing an external penetration test

Correct answer: d

8. Which of the following is the meaning of RPO (recovery point objective)? (choose one answer)

☐ a. The number of offline back-ups in an enterprise

☐ b. The maximum allowable data loss measured in time

☐ c. The target timeframe to restore business processes after a disruption to prevent unacceptable consequences

☐ d. The security objectives of the access control policy

Correct answer: b

9. Which of the following is good practice for an organization regarding its supply chain risk management? (choose one answer)

☐ a. The organization doesn't have to apply certain policies, because suppliers and service providers implement due care regarding cybersecurity

☐ b. Conducting discussions at board level every 6 months

☐ c. Developing a network security policy

☐ d. Documenting cybersecurity requirements in the contracts with suppliers and service providers

Correct answer: d

10. Which of the following is true about software patch management? (choose one answer)

☐ a. In user workstations (Windows PCs), Windows updates should be installed automatically

☐ b. In some environments software patches should be first tested before deployment, due to dependency issues

☐ c. Software patches in Internet-facing assets should be prioritized

☐ d. All the above

Correct answer: d