Martin Petik

ID279832

2B.P2

A client is a computer or application that sends requests to a server. In doing so, it makes services and data provided by the server available to end users. Common client applications include email programs and web browsers.

Access, Authentication, and Authorization Management. Awareness, Training, and Education. Disaster Recovery Planning and Data Backup for Information Systems and Services. Electronic Data Disposal and Media Sanitization.

Example of protecting a system is to ensure the confidentiality, integrity, and availability of clients’ sensitive information and technology assets. By implementing robust security measures, we aim to safeguard the client’s system and data from unauthorized access, misuse, modification, disclosure, or destruction

Security measures are the security controls you add to your networks to protect confidentially, integrity, and availability. These measures include firewall and antivirus protection, password management, encryption, security awareness training, and cyber security incident response. You should also back up your data regularly, use strong passwords and multi factor authentication, be Warly of suspicious emails and install anti-virus and malware protection.

P2

Back up your data because creating a copy of the data on your system that you use for recovery in case your original data is lost or corrupted. You can also use backup to recover copies of older files if you have deleted them from your system.

Use strong passwords and multi-factor authentication because it makes it so difficult for cyber criminals to breach. Both a strong password and two‑factor authentication is absolutely crucial for securing online identities

Be wary of suspicious emails because Phishing emails can often have real consequences for people who give scammers their information, including identity theft. And they might harm the reputation of the companies they're spoofing.

Install anti-virus and malware protection because Anti-virus software can identify and block many viruses before they can infect your computer. Once you install anti-virus software, it is important to keep it up to date.

**Encryption**

encoding “plaintext” into “ciphertext,” typically through the use of cryptographic mathematical models known as algorithms.

**User Education and Training**

Regularly educate users on security best practices, social engineering, and the importance of following security policies.

Provide training on how to recognize and report phishing attempts or suspicious activities.

**User Access Controls**

identifying a user based on their credentials and then authorizing the appropriate level of access once they are authenticated.

**Security Awareness**

Foster a culture of security awareness by encouraging users to be vigilant, report security incidents promptly, and stay informed about the latest security threats.

**Firewalls and Intrusion Prevention Systems (IPS)**

Deploy firewalls to monitor and control incoming and outgoing network traffic Use IPS to detect and prevent potential security threats by analysing network and/or system activities.

**Third-Party Security Assessment**

Assess the security practices of third-party vendors and partners who have access to the system or handle sensitive data.

2B.P3

a risk assessment

**Step 1 – Establish the context for risk management**

In this first step you should think about the things that might influence and direct the cyber security risk management decisions and choices you make. These things are likely to include your organisation’s business priorities and objectives, who or what those things should be protected from (for example, do you need to protect systems and services in the context of the threat model for OFFICIAL information, or is our service or system attractive to cyber criminals or state actors for some reason), any legal and regulatory obligations that apply to your organisation, and the cyber security risk red lines your organisation will and won’t cross to complete the things it needs to do.

**Step 2 – Define a scope for your risk assessment**

Before setting out on any risk assessment activity it is important that you define the scope of what you are assessing. The scope of assessment should define the boundaries of the existing system you are assessing or the new system that is being built, and your scope should clearly define all the assets that are to be contained within it.

As well as expressing the boundaries of your assessment it is also useful for any model of a system’s scope to describe:

* any interconnections both internal within your scope and externally with other systems, services, or organisations
* the boundaries within which you or your organisation can exert control over the assets and systems within it and where you cannot
* any external systems, services, or organisations which the system within the scope of your assessment relies upon in some way

**Step 3 – Understand your assets and assess impact**

This step is about building your understanding of the things you care about and what should be protected. To help with this you could build a register of assets that could include (for example) the equipment, systems, services, software, information and/or processes that are critical to the successful delivery of your business objectives. An important part of this step is to identify and to record ownership of each asset (or groups of assets) within your organisation.

**Step 4 – Assess the threat**

This step is about understanding two things,

1. Who or what might pose a threat to your organisation and its objectives?
2. How they might go about attacking or otherwise compromising the things you care about.

To achieve the first objective of this step you should seek out authoritative sources of threat information that can help you understand who might seek to do you and your organisation harm, and why. This threat information could come from national authorities such as the NCSC or NPSA,

from vendors and or industry groups or be based on historical knowledge about who has attacked organisations such as yours, or your sector.

**Step 5 – Assess your vulnerability**

Vulnerabilities can exist in people, processes, places and technology and these vulnerabilities may be exploited by threat actors to achieve their aims and objectives. There are several techniques and resources that can help you assess your vulnerabilities:

* you could use good guidance such as the NCSC’s Secure system administration guidance, secure design principles or cloud security guidance to help you think about where vulnerabilities might exist in the systems and service you use
* you could build attack trees to help you understand the steps a threat actor would need to take in order to achieve their aims and objectives
* you could make use of catalogues or databases of publicly disclosed technology vulnerabilities (for example MITRE’s Common Vulnerability Enumeration [CVE] database) to help you understand the vulnerabilities that are known about affecting the technology you use
* you could use the knowledge bases of threat information, such as MITRE ATT&CK to help you understand more about the vulnerabilities that are exploited as part of a real world and known attack
* you could assess vulnerability in terms of the ease by which a vulnerability could be exploited, how widespread a vulnerability is across your organisation and its systems, and how easy it is for a threat actor to know or assume that you have a vulnerability affecting your systems and services

a summary of protection measures covering technology and tools and techniques.

1. **Stop giving away your personal information**

Step one is easy. Stop giving it away. A common and effective way to get people’s information is to simply ask for it, whether buying at a retail cashier, joining an online group or through a phishing email. Because we are polite or in a hurry to get to the objective, we often just give it up.

Be suspicious of unsolicited e-mails that have a “sense of urgency” and warn that your accounts will be closed or your access limited if you don’t reply.

1. **Check your mobile app permissions**

Mobile apps also have implications for personal data. Many force you to accept certain permissions (access to contacts, photos, GPS location, etc.) to download the app. In many cases, the permissions have nothing to do with the app’s functionality.

1. **Review your security and privacy settings**

While we’re talking mobile, make sure your smartphone locks automatically when not in use. If you lose your phone, anyone who finds it shouldn’t be able to gain access. Many new smartphones have fingerprint authentication, which is better than a simple passcode or swipe pattern.

If possible, configure “Find my phone” to locate your phone if it is lost or stolen.

Each social media platform has a privacy and security policy. If you’re going to use social media, you should know what is being collected and shared. If you use Facebook extensively, take the time to review and understand the privacy settings to make sure you’re comfortable. It is a powerful data collection machine.

1. **Use Antivirus software and install the latest software patches**

There is a potential for contracting a computer virus or other type of malware. This can cause damage to your computer, provide access to your confidential information or even cause a ransomware attack. Criminals look for vulnerabilities within software. It’s important to install software updates (patches) when made available by the vendors.

Risk assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk number | threat | Risk description | Risk level | Risk loss |
| 01 | Virus | can attack your computer via the following means: Opening infected email attachments such as .exe, msi files. Opening infected files from web-based digital file delivery companies for example google disk and drop box | Medium risk | The risk of losing data due to computer viruses is a serious thread for any computer user |
| 02 | Adware | various pop-up advertisements that show up on your computer or mobile device. Adware has the potential to become malicious and harm your device by slowing it down, hijacking your browser and installing viruses or spyware. | relatively harmless  (Low risk) | Data Theft: Adware commonly collects information about users and their browsing habits to serve more targeted advertisements that have a higher probability of receiving clicks. |
| 03 | Fileless Malware | gain access to data they can either steal or use to sabotage the operations of an organization. Fileless malware hides by using applications, such as Windows script programs, or PowerShell. | High risk  (Can bypass antivirus software) | they can either steal or use to sabotage the operations of an organization. |
| 04 | Ransomware | a type of malicious software designed to block access to a computer system until a sum of money is paid. | High risk  (Financial loss, data loss) | encryption causes loss of data availability. |
| 05 | Trojans | a type of malware that downloads onto a computer disguised as a legitimate program | Hight risk  (A Trojan horse can break through all security polices in a network) | Ransom Trojans seek to impair a computer's performance or block data on the device so that the user can no longer access or use it. |

2B.M2

Alternative’s solutions

Alternatives solutions for protecting the client’s system and reduce security risks by using tools such as: Network Segmentation because it is a network security technique that divides a network into smaller, distinct sub-networks that enable network teams to compartmentalize the sub-networks and deliver unique security controls and services to each sub-network. This allows network administrators to control the flow of network traffic between subnets based on granular policies. Organizations use segmentation to improve monitoring, boost performance, localize technical issues and – most importantly – enhance security.

Another solution is: Multi-Factor Authentication because it requires users to authenticate using multiple factors (e.g., passwords, biometrics, tokens) to add an extra layer of security beyond just passwords. Because of that Is harder to commit Identity fraud so your personal information is more at safe. If we but in scenario for example: (Microsoft Authenticator or Google Authenticator)

If somebody else tries to sign in as you, however, they'll enter your username and password, and when they get prompted for that second factor they're stuck! Unless they have YOUR smartphone, they have no way of getting that 6-digit number to enter. And the 6-digit number in Microsoft Authenticator changes every 30 seconds, so even if they knew the number you used to sign in yesterday, they're still locked out.

Another alternative solution is Endpoint Security is a solution that’s enables to quickly detect malware and other common security threats. It can also provide endpoint monitoring, detection and response, which enables the business to detect more advanced threats like fileless malware, polymorphic attacks, and zero-day attacks. because Endpoint security uses a range of processes, services, and solutions to protect endpoints from cyberthreats. Is harder for hackers to get into your system. also, Endpoint security has since evolved to include more advanced, cloud-powered, and comprehensive solutions that help detect threats, investigate, and respond to threats, and manage apps, devices, and users. So is even harder.

Uses Examples:

examples of endpoint security: solutions include: Firewalls: Firewalls can control traffic between endpoint devices and the network. They can help to block malicious traffic and protect endpoint devices from attackers.

Another example is Endpoints are physical devices that connect to and exchange information with a computer network. Some examples of endpoints are mobile devices, desktop computers, virtual machines, embedded devices, and servers. Internet-of-Thing’s devices—like cameras, lighting, refrigerators, security systems, smart speakers, and thermostats—are also endpoints. When a device connects to a network, the flow of information between, for instance, a laptop and a network, is much like a conversation between two people over the phone.

An explanation of how the system will be protected, covering users, technology, and tools and techniques.

educate users on security best practices, social engineering, and the importance of following security policies.

Use IPS to detect and prevent potential security threats by analysing network and/or system activities.

Utilize encryption for sensitive data to protect it from unauthorized access, both in transit and at rest.

Keep all software, operating systems, and applications up to date by applying security patches promptly to address known vulnerabilities.

Implement network segmentation to isolate different segments of the network, limiting the potential impact of a security breach.

Establish regular backup procedures and a disaster recovery plan to ensure the availability and integrity of data in the event of a system failure or data loss.

Also Security technology helps mitigate risk by preventing unauthorized access, identifying potential incidents, allowing fast responses, deterring criminal behaviour and capturing crucial evidence in the event that a breach occurs.

2B.D2

Justify final decisions, explaining:

how the system will fulfil the stated purpose and ‘client’ requirements

any constraints on the plan.

Our final decisions are justified based on the client's stated purpose and requirements. User requirements define the results and qualities the user wants; system requirements define what the system must do to achieve this. User requirements are owned by the users, whereas system requirements are owned by the developers.

The security plan also needs to consider any legal, regulatory, or compliance constraints that may impact the implementation of certain security measures.

Risk Assessment: organise a comprehensive risk assessment to identify potential threats, vulnerabilities, and risks to the system.

User Training and Awareness: User awareness training allows employees to identify, avoid, report and manage cybersecurity threats facing your organization. By protecting your business with good practices, instil company values that foster a culture of safety.

Constraints in plan

Tailored Security Measures: The inclusion of continuous monitoring not only enables real-time visibility but also ensures proactive issue resolution and data-driven decision-making.

Budgetary Constraints: Consider budget limitations that might affect the selection and implementation of security technologies and training programs.

Resource constraints: are limitations on the resources, such as personnel and materials, available to the project manager. This type of constraint can also be imposed by external project resources, such as the client or the vendor, or by internal resource availability, such as your own company.

constraints Technological Compatibility: come in a wide range depending on how interoperable the product needs to be with its environment and how big an installed-base it needs to support. In principle, the problem is confined to finding a representative set of configurations needing to maintain compatibility.