LO2: Risk Consultant

Contents

[1 – Security Threats 2](#_Toc88568796)

[2 – IT Risk Analysis & Business Continuity 5](#_Toc88568797)

# 1 – Security Threats

* **To get a better understanding of these threats and attacks find articles on internet about malware, spam, phishing, adware, ransomware, DDOS attacks, Advanced Persistent Threats what it is, how they work and how to protect. Give a brief description of what it is, how it works and how to protect your 'company X' in your portfolio.**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Definition | Way of working | How to protect |
| Malware | Software intentionally designed to cause damage to a computer, server, client, or computer network. There are several types of malwares, such as viruses, trojan horses, or worms. | Virus-> It requires user action to transmit from one system to another and attaches bits of its own malicious code to other files.  Trojan horse->it can hide in cracked software, in shady websites, etc. Trojan is a way for the attackers to send malicious software. | Virus-> Learn to spot phishing, invest in security, do not click suspicious links, check their authenticity  Trojan-> run periodic diagnostics scans, get a firewall, use complex passwords, avoid suspicious websites. |
| Spam | The use of messaging systems to send multiple unsolicited messages to large numbers of recipients | Malware can be sent via these messages through phishing, the victim can fall to a scam or simply have malware installed on their device. | Learn to spot phishing, install security, report found spam, use two-factor authentication |
| Phishing | An attack in which the attacker poses as a trusted person or organization to trick the victim into sharing sensitive information or giving away their money | The email invites the victim to click on a link and take an action or download an attachment. This can lead to the victim giving away sensitive information or downloading malware on their device. | Do not open e-mails from senders you are not familiar with. Don't ever click on a link inside of an e-mail unless you know exactly where it is going. Mouseover the link to see if it's a legitimate link. |
| Adware | Unwanted software designed to throw advertisements up on your screen, most often within a web browser. | Adware generates revenue for its developer by automatically displaying online advertisements in the user interface of the software. | Practice safe computing. Proceed carefully when downloading software, install security |
| Ransomware | Type of malware that prevents users from accessing their system or personal files and demands money in order to give back access. | The attacker uses spam, advertisements, or phishing, attaching malicious files to as many people as possible. | Prevent it from happening in the first place, invest in security, create backups of your data regularly |
| DDOS attacks | Form of attack consisting of sending large amounts of traffic from multiple sources to a service or website, intending to overwhelm it. | A huge amount of traffic all at once can block the site and deny access to its legitimate users. | Plan ahead of such an attack, have protection turned on at all times |
| Advanced Persistent Threats | Covert cyber-attack on a computer network where the attacker gains and maintains unauthorized access to the targeted network and remains undetected for a significant period. | During the time between infection and remediation the hacker will often monitor, intercept, and relay information and sensitive data.  The malware searches for vulnerabilities in the system and exploits them. | Multiple layers of security working together, constant network monitoring, install a firewall, install antivirus software. |

* **Describe the organization you are implementing your network for and use the CIA matrix to describe each item in a (few) line(s) of text in the context of information relevant for your example company. This will be input for the next Body of Knowledge subject.**

I am going to use an imaginary example company named DartsMasters. This is the name of the website I created during the third semester, and it is a forum for darts enthusiasts to share content and discuss topics related to this sport.

Text

Description automatically generated

Resources:

* <https://www.malwarebytes.com/malware>
* <https://en.wikipedia.org/wiki/Malware>
* <https://www.malwarebytes.com/spam>
* <https://www.malwarebytes.com/phishing>
* <https://www.malwarebytes.com/adware>
* <https://www.malwarebytes.com/ransomware>
* <https://www.malwarebytes.com/ddos>
* <https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html>
* <https://www.malwarebytes.com/computer-virus>
* <https://www.malwarebytes.com/trojan>

# 2 – IT Risk Analysis & Business Continuity

* + **Perform a qualitative risk analysis for the company environment that you are analysing and developing this semester.   
      
    1. List and describe the threats for your company in terms of possible attackers (threat actors) and their motivations.  
    2. For each threat determine and explain the probability (likelihood) on a qualitative scale.   
    3. For each threat determine and describe the possible impacts if it occurs.**

The impact will be determined by the following factors:

Graphical user interface, text, application

Description automatically generated

Determining the impact level per event:

Table

Description automatically generated

Determining the probability for each event:

Table

Description automatically generated

Determining the risk (probability \* impact):

Chart, table

Description automatically generated

Table

Description automatically generated with low confidenceText

Description automatically generated with medium confidence

* **Take your top 5 risks from the Risk analysis assignment and think of as many mitigating measures as possible. Determine physical, technical, and organizational measures that are needed and find a good balance in preventive, detective, repressive and corrective measures.**

The 5 biggest risks are:

1. Ransomware
2. Malware infection
3. Personal data breach
4. Phishing
5. DDoS attacks

A good prevention method for phishing, ransomware and malware infection is raising awareness to the problem by instructing the employees to pay maximum attention to suspicious emails and websites. They should always check the email address, not click links, and not download suspicious attachments.

In order to prevent data breaches, the code surrounding data should be as secure as possible. The information in the database has to be encrypted and security measures need to be put in place, such as 2 factor authentication, protection against cross site request forgery, or protection against SQL injection.

A famous backup strategy is 3-2-1. It has 3 principles. The first one is that the employee should keep at least 3 copies of their data, including the original copy and 2 backups. Also, in order to improve safety, the backups should be stored in different places. The second principle states that the backup data should be kept on 2 different devices, in case one of the devices gets corrupted. It is suggested to store the two backups on 2 different storage types, such as external hard drives, or USB flash drives. The third and final principle addresses the importance of keeping at least one of the copies offsite. Storing the data in another distance remotely significantly increases the security.

Redundancy is an engineering term which means “the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or fail-safe, or to improve actual system performance”. In ICT there are four main forms of redundancy: Hardware, software, information, and time, with hardware redundancy being the most common one. This means adding a duplicate device or component in the system with the goal to ensure zero downtime. Server redundancy means creating a replica of the company server. It is kept offline and in case of failure, downtime, or excessive traffic, likely cause of a DDoS attack at the primary server, the redundant server can be turned on and take a share of the primary server’s load. This is a very good disaster recovery option, but it comes with doubling the cost of the server solution, along with doubling the storage space.

RTO and RPO are part of the business impact analysis, which differentiates critical and non-critical organization functions. For each function, two values are assigned: Recovery Point Objective (RPO) and Recovery Time objective (RTO). RPO is the acceptable amount of data that will not be recovered. RTO is the acceptable amount of time to restore the function.

* + **Resources:**
* <https://www.ubackup.com/3-2-1-backup-strategy.html>
* <https://www.your-itdepartment.co.uk/knowledge-bank/what-is-redundancy/>
* <https://en.wikipedia.org/wiki/Business_continuity_planning#Maximum_RTO>