CYBER VT2022

Case 2 Policy Group #10

Jawdat Kour
Anas Kwefati
Hideo Tommaso Nishimura
Munish Sharma

1. Threat Model

Business Objectives:

Radio Sweden is a government national radio that focuses on news and political matters. The company needs help for an overall assessment of the possible attack vectors towards them, and different countermeasures against these threats. In this document, we will present the different assets, and do a risk assessment of the strengths and weaknesses of IT/information infrastructure. Then, a threat model following STRIDE will be presented with its countermeasures.

Business Assets:

- Data (Documents, images, videos, documentaries, sensitive information etc.)
- Employees, journalists,
- servers for intranet, web servers, email, intrusion detection systems, log, FTP servers, servers for internal systems (finance, internal communication, systems), servers for backups
- Network devices routers, switches, firewalls

Threat Agents: (internal/ external authorized or unauthorized users)

- Malicious Hackers
- Organized Crime/Terrorist
- External freelance Journalists
- Internal (Employees, journalists, System administrators, developers)
- Nation states

Strengths and weaknesses of the IT/information infrastructure:

Strengths:

- Anti-malware policy
- Disk encryption policy
- Email encryption
- Two layers of trust by incorporating two firewalls
- IDS (Intrusion Detection System)
- Backups
- Log handling
- Network segmentation

Weaknesses:

- Lack of CISO / CERT
- Potential access to confidential information (unencrypted tips via email)
- Email security gateway and filter is not presented

- Ransomware incident shows that the anti-malware is not efficient or was not running properly.
- Lack of identity check for freelance journalists (potential social engineering attack, to get access to the internal network)
- Potential Modification attack vector
- VPN access by freelance journalists
- Lenient firewall

Potential threats to the system and solutions following STRIDE model:

Spoofing → Malicious actors can disguise themselves as freelance journalists using different methods such as Social Engineering, and then they would access the VPN, and so access to the internal network.

- ***Countermeasures***: Do enough background checks on the freelance journalist, in order to prevent any fake freelancers. Sign a document between both parties. Also, train the employees against any other kinds of social engineering attacks (e.g., phishing email). Any potential suspicious spoofing attack should be reported back to the IT department, and ideally the cybersecurity team.

DDoS → Malicious actors may try to overload the traffic in order to disrupt a company's network, which would affect its availability. The problem is also due to lenient firewall protection and obsolete firewall model (CISCO ASA 5500).

- ***Countermeasures***: The company should implement different DDoS mitigation techniques. For instance, it should implement filtering like connection tracking, packet inspection, rate limiting, blacklist IPs etc.

Tampering → Malicious actors may tamper the data, and so affect the integrity of the information. As the information should be kept integral and accurate. The company does not seem to be using any digital signature, or any other methods to make sure that the sent and received data has not been tampered. Hence, there is a likelihood that received or sent emails may be modified.

- ***Countermeasure***: Enable virtual execution of email attachments in a sandbox environment to prevent malware propagation throughout the internal network. Alternatively, different channels of communication between journalists and sources could be set up (i.e. using SecureDrop software). Implement a digital signature policy between different actors within the company, in order to drop the chances of tampered data.

Repudiation -> Malicious actors may be able to delete data, or erase any logs within the company.

- ***Countermeasure:*** The company should implement a log system, and a cybersecurity as well a network management system that would notify administrators for any deleting.

Information Disclosure → Malicious actors may have access to the confidential data. According to the company, journalists can receive tips via email, where data can be unencrypted. This may raise issues, in case of someone intercepting the data that could be sensitive. Furthermore, the company disclosed confidential data, which lead to the journalist to receive threats.

- ***Countermeasures***: Every communication should be encrypted, as well as encrypting the full disks in case someone gets access to these data. Furthermore, when disclosing sensitive information, the company should anonymize the journalist name, in order to prevent any kind of blackmailing, or further social engineering on the journalist.

Elevation of Privilege -> Malicious actors may gain access to the network, or computers which could lead to a potential privilege escalation. The company has several equipment and servers that are connected to the Internet. Moreover, the company has contacts with freelance journalists. These can provide potential threat, and lead to elevation of privilege if the attacker manages to exploit the connected servers to the Internet if misconfigured. Or can use social engineering and try to obtain higher level information within the company by acting themselves as freelance journalists.

- ***Countermeasures***: The company should implement protection to their servers, and equipment that are connected to the Internet. For instance, it should put a firewall that would implement rate limit, but also, would block access to suspicious IPs etc. Furthermore, adding an IDS/IPS to the network could improve company's security, as it would be able to detect any potential threats, and prevent it from accessing the network or could notify the administrator in time, in order to prevent the potential threat.

Ransomware → The ransomware main purpose is to affect the availability of data, in exchange of money. However, ransomwares are becoming more and more complex, and now a ransomware attack on a company may also bring the potential risk on confidentiality and integrity. Thus, we have decided to put it outside the STRIDE model.

The company has noted that an employee's device was affected by ransomware, and was connected to the internal network. Thus the likelihood that it may have also infected other internal devices increases.

- ***Countermeasures***: The company should do an intensive security check on all internal devices within the company, and also update every anti malware tool. Furthermore, it should isolate the backup server from the rest of the network by installing an additional firewall between subnetworks. Every sensitive data, or important data should be a priority and backed up outside the network. In addition, a system for screening mobile devices returning from an ‘unsecured’ environment should be put in place.

GENERAL SOLUTION

- Appointment of a CISO or similar figure
- Security awareness education for all employees accessing internal network
- Revision of obsolete hardware devices (i.e. The Windows Server 2016, CVEs count: 2359)