Case 2

Threat Model
Group 10

Participants

Athanasios Ntales (atnt3398)
Bilal Riaz (biri9477)
Chanchala Fernando (chfe1432)
Emad Abdulsamad (emab9908)
Lekhaz Adapa (lead3201)
Muhammad Usama Younas (muus4313)

Threat Model for Radio Sweden's Cybersecurity:

- Application Name: Radio Sweden's IT Infrastructure
- Application Version: 1.0
- Description: The threat model aims to detect potential attack scenarios and weaknesses in Radio Sweden's IT infrastructure, including personal computers, servers, firewalls, switches, and wireless networks. It will examine Radio Sweden's possible dangers and attack vectors in light of recent cases of anonymous threats and ransomware assaults. The threat model will also offer countermeasures and defensive tactics to reduce the detected risks.
- Document Owner: Mark Taylor
- Participants:
    - CEO of Radio Sweden
    - Head of IT at Radio Sweden
    - External Security Consultant (The person who is creating the threat model)
- Reviewer: James Oliver

Entry Points:

ID	Name	Description
1	Employee computers	Employee computers running Windows 10 Professional (64 bits) serve as access points to Radio Sweden's information technology infrastructure. Employees, including journalists, utilize these computers for day-to-day work and can access the internet, a VPN connection, and email services. If they are not adequately protected, they may be subjected to malware, ransomware, and other cyber dangers.
2	Servers	Servers, such as Windows servers (2016), GNU/Linux Red Hat servers, and Solaris 11.1 servers, are critical components of Radio Sweden's IT infrastructure, handling internal systems, web servers, email, backups, and other services. They are linked to the internet and, if not protected with suitable security measures such as firewalls, intrusion detection systems, and regular patching, may be possible entry sites for cyber assaults.
3	Wireless Networks	Radio Sweden has two wireless networks, one for guests and one for employees, which are handled by a Cisco Catalyst 9800 controller with Aironet 3800 access points. These networks enable wireless connectivity to personnel, including freelance journalists, and if not adequately protected, can serve as entry points for unwanted access or assaults. Because it is intended for external guests, the guest WiFi may offer a larger danger.

4	Firewalls	By monitoring and filtering incoming and outgoing network traffic, Cisco ASA 5500 firewalls safeguard Radio Sweden's IT infrastructure from external attacks. They are an important protection tool against potential cyber assaults and illegal internet access. Yet, because of the lax firewall restrictions that enable journalists to do research and receive tips through email, there may be possible vulnerabilities that may be exploited.
5	Switches	HP Officeconnect 1850 Gigabit switches connect numerous components in Radio Sweden's IT infrastructure, such as servers, firewalls, and wireless access points. They enable network connectivity and, if not adequately protected, can provide entry points for illegal access or assaults.

Assets:

ID	Name	Description	Trust Levels
1	Journalist	Journalists utilize workstation computers to generate news material, including sensitive information about sources, articles, and interviews.	
1.1	Journalists' data	Personal information, such as names, contact information, and other sensitive data, is retained on their computers.	(2) Authenticated User (5) VPN User
1.2	Research Data	Research data collected by journalists, including audio recordings, video footage, and documents related to news stories.	(2) Authenticated User (5) VPN User
1.3	Email accounts Journalists	Email accounts are used for communication, receiving tips, and exchanging sensitive information.	(2) Authenticated User (1) Unauthenticated User (for receiving tips) (4) VPN User
1.4	Files and documents	Files and documents related to news stories, interviews, and research are stored on journalists' workstations.	(2) Authenticated User (4) VPN User
1.5	Journalist personal devices (BYOD)	A journalist may use their personal mobile phones or laptops to generate data and then move this data to work computers or storage	(2) Authenticated User

		server	
2	Servers	Servers are used for various internal systems, communication, and data storage.	
2.1	Finance server	The server used for financial transactions and data storage related to Radio Sweden's financial operations	(5) Finance Department User (6) Server Administrator (7) Database Read User (8) Database Read/Write User
2.2	Intranet Server	The server used for internal communication, document sharing, and collaboration among Radio Sweden employees	(2) Authentication User (6) Server Administrator (7) Database Read User (8) Database Read/Write User
2.3	Email Server	The server is used for sending and receiving mail communications among Radio Sweden employees, including sensitive information.	(2) Authentication User (1) Unauthenticated User (for external email communication) (6) Server Administrator
2.4	Web Servers	Servers hosting Radio Sweden's website and other web-based applications for news publishing and content management.	(2) Authentication User (1) Unauthenticated User (for public access) (6) Server Administrator
2.5	Backup Servers	Servers used for backing up critical data and systems to ensure data integrity and disaster recovery	(6) Server Administrator
2.6	IDS Server	The server is used to monitor data transmission and behavior on the network to detect any misbehaving or intruders.	(6) Server Administrator
2.7	Log Server	The server stores all logs from network servers and employees' computers.	(6) Server Administrator (10) IDS Server
3	Network Equipment	Network equipment used for connectivity, communication, and security of Radio Sweden's IT infrastructure.	
3.1	Routers	Routers are used for routing network traffic between different networks and providing connectivity to external networks, including	(6) Network Administrator

		the Internet.	
3.2	Switches	Switches are used for connecting devices within the internal network and managing network traffic.	(6) Network Administrator
3.3	Firewalls	Firewalls are used for securing the network parameters and controlling incoming and outgoing network traffic.	(6) Network Administrator
3.4	Access Point	Access points are used for providing wireless connectivity to internal and guest networks within Radio Sweden's premises	(6) Network Administrator

Trust Levels:

ID	Name	Description
1	Unauthenticated User	External entities who have not been authenticated or authorized by the application
2	Authenticated User	External entities who have been authenticated by the application and have valid credentials
3	External Partner	Entities who are trusted partners of the application, such as third-party integrations or APIs
4	VPN User	External entities who have established a secure VPN connection with the application.
5	Finance Department User	Authorized users from the finance department who have specific access rights within the application
6	Server Administrator	Authorized administrators who have administrative access rights to the servers or network equipment
7	Database Read User	Authorized users who have read access to the database
8	Database Read/Write User	Authorized users who have read and write access to the database
9	Network Administrator	Authorized administrators who have administrative access rights to the network equipment
10	IDS Server	The authorized IDS Server analyzes all network and system logs to detect any misbehaving or intruder in any machine on the network.

External Dependencies:

ID	Description
1	The operating system that hosts the program, including its version and patch level.
2	The version and settings of the web server software used to host the application.
3	The database server software, including its version and configuration, is used to store application data.
4	All third-party libraries or modules that the program makes use of, including their versions and any known vulnerabilities.
5	The application and its environment are protected by the firewall setup and rules.
6	The load balancer setup and policies are used to distribute incoming traffic to the application's numerous servers.
7	The intrusion detection or prevention system is in place to detect and prevent possible application assaults.
8	The processes and policies are in place to protect the application and its data from data loss or system failures.
9	Any external authentication and authorization services or systems, including their setups and interface with the application.
10	The network and infrastructure components are crucial to the application's functioning, such as routers, switches, and DNS servers.

Threat Categorization:

STRIDE:

STRIDE can be used to determine the goals of an attacker, such as:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

STRIDE Threat List

Type	Description	Security Flow Type
Spoofing	Threat action aimed to use deception to appear as another person or source information. Examples: Impersonation, forgery, falsification	Authentication
Tampering	Threat action is an intentional but unauthorized act resulting in the modification of a system or components of a system. Examples: Modifying, altering	Integrity
Repudiation	Threat action happens when an application or system does not adopt controls to properly track and log users' actions. Examples: Denying actions, claiming actions were not performed	Non-repudiation
Information Disclosure	Threat action occurs when a website unintentionally reveals sensitive information to its users. Examples: Data leaks, Unauthorized access to sensitive information	Confidentiality
Denial of Service	Threat action describes the ultimate goal of cyber-attacks designed to render a service inaccessible. Examples: Disrupting, degrading, or denying access to the system or service	Availability
Elevation of Privilege	Threat action describes a type of network attack used to gain unauthorized access to systems within a security parameter.	Authorization

Threat Analysis & Rating

Type	Threat Analysis	Rating score
Spoofing	Unauthorized users attempt to gain access through the global network or the organization's wireless network. Also, some employees try elevation privileges. Secret information disclosure to the public affects the overall system's truthfulness. A spoofing attempt is a continuous attack vector, and a system will face this attempt all the time. Internal spoofing attempts can be detected and handled, while attempts from global networks	8

	can only be detected.	
Tampering	Some employees try to access sensitive data, system configuration, or organization departments. Sensitive data disclosure is lost or manipulated. Tampering is a continuous attack vector for both physical and digital data. Physical attempts can easily be detected, while a digital attempt by employees is hard to be detected.	7
Repudiation	Repudiation of failed access attempts can easily be detected and network repeat attack can be easily handled by firewall and IDS.	3
Information Disclosure	Unauthorized users may physically access employees computers to do some work or lose device status. Information disclosure affects specific employees' work and the whole business of the organization. Information disclosure is hard to be detected by digital systems.	10
Denial of Service	Radio Sweden can be attacked for different reasons, political, tampering, financial, or reputation.	9
Elevation of Privilege	Some organization employees try to elevate their privileges to access sensitive information or sections to copy, delete or manipulate. Elevation of privileges inside the network can be easily detected. Unauthorized access affects specific employees' work and the whole organization business.	6

Security Mechanism & Countermeasures:

Security Mechanism	Countermeasure
Authentication	1. Implement strong password regulations, such as mandating passwords to be of adequate length and complexity, as well as to be changed on a regular basis 2. Multi-factor authentication should be used for all user accounts, especially privileged ones. 3. To prevent unwanted access, encrypt credentials and authentication tokens in storage and transport. 4. Account lockout restrictions should be enforced to avoid brute-force assaults. 5. Instead of depending entirely on SQL authentication, use trusted server authentication. 6. To securely store passwords, use password hashing techniques such

	as salted hashes. 7. To avoid social engineering attempts, avoid disclosing password clues and genuine usernames during password rests. 8. Force information security training to all employees to recognize social engineering attack and other attack types.
Authorization	1. Use powerful Access Control Lists to enforce allowed resource access. 2. To limit access to certain operations depending on user roles, employ role-based access controls. 3. Follow the concept of least privilege, which states that users and service accounts should only be given the access necessary to complete their responsibilities. 4. To avoid unwanted access and privilege escalation, appropriately configure privilege separation within the presentation, business, and data access levels. 5. Deny access for all personal devices inside the work environment.
Configuration Management	1. To prevent unwanted access to configuration files, use the least privileged processes and service accounts with no administrative capabilities. 2. Allow auditing and tracking of all administration operations in order to detect and respond to illegal modifications. 3. Use proper access controls to limit access to configuration files and administrator interfaces to authorized administrators only. 4. Review and update configuration settings on a regular basis to verify that they are in line with security best practices and standards
Data Protection in Storage and Transit	1. To safeguard data in storage and transit, use conventional encryption techniques with appropriate key sizes. 2. To maintain data integrity, use hashed message authentication codes. 3. Secrets, such as keys and private data, can be cryptographically protected in transport and storage. 4. To protect keys, use built-in secure storage techniques such as key vaults. 5. Encrypt passwords and sensitive data before transmitting them over the wire to avoid sending them in clear text.
Data Validation/Parameter Validations	1. To validate all data provided by clients, enforce data type, format, length, and range checks. 2. To avoid SQL injection, cross-site scripting, and other injection threats, validate and sanitize all user input. 3. Avoid basing security decisions on factors that may be changed by attackers, such as URL parameters. 4. Use input filtering techniques, such as list validation, to accept

	anticipated input while rejecting all extraneous input. 5. Enable output encoding to protect against cross-site scripting and other code injection threats.
Error Handling and Exception Management	1. Handle all exceptions in a structured manner to prevent information leakage and minimize the impact of errors. 2. To avoid privilege escalation attacks, restore privileges to the proper level in the event of faults or exceptions. 3. Error messages should be scrubbed to ensure no sensitive information, such as system specifics or user data, is given to attackers. 4. Implement appropriate error logging and monitoring to discover and respond to problems and exceptions as soon as possible.
User and Session Management	1. Avoid strong sensitive information in cookies in clear text, such as passwords or Personally Identifiable Information. 2. To prevent unwanted access, encrypt the contents of authentication cookies 3. To reduce the danger of session hijacking, set cookies to expire after a specific length of time. 4. Implement anti-replay measures such as session token renewal and timestamp-based validation. 5. To prevent authentication cookies from interception, use secure communication routes such as HTTPS.

STRIDE Threat & Mitigation Techniques:

Threat Type	Mitigation Techniques
Spoofing Identity	1. Implement strong authentication 2. Protect sensitive data 3. Avoid storing unnecessary secrets and access tokens
Tampering with Data	1. Implement appropriate authorization mechanism 2. Cryptographic techniques, such as hashes, message authentication codes, digital signatures, and storage encryption for all employees devices 3. Tamper-resistant protocols or technologies, such as secure key management practices
Repudiation	1. Digital signatures or other cryptographic techniques to ensure the integrity and authenticity of data and prevent repudiation 2. Time stamps and audit trails to capture all relevant user activities and changes to data

Information Disclosure	1. Authorization mechanisms to control access to sensitive information 2. Privacy-enhances protocols 3. Data masking 4. Encrypt data in transit and at rest
Denial of Service	1. Authentication and Authorization mechanisms to prevent unauthorized access and misuse that could lead to denial of service attacks 2. Filtering and Throttling mechanisms 3. Quality of Service mechanism 4. Redundancy for internet connection to ensure continuous and reliable connectivity in case of any unintended failure or attack on one connection.
Elevation of Privilege	1. Principle of least privilege 2. Strict access control 3. Role-based access control