Case 2 Threat Model - Group 9

Melina Bernsland - mebe2625
Melina Lagerstedt - mela9606
Kevin Lindén - keli1001
Arvin Moshfegh - armo2982

Radio Sweden - Threat Model

Overview

Radio Sweden is a public service national radio station that is owned by the government of Sweden. They provide investigative journalism, documentaries and news on several radio frequencies. Since Radio Sweden is owned by the government, it is also used for Public Service Announcements (PSA) and communicating national emergencies. This means that Radio Sweden is an important service provider for the entire nation of Sweden. Due to recent threats and attacks (threats against employees, ransomware attacks) it is of importance to get an overview of what threats Radio Sweden is facing - and how to mitigate and prevent these threats.

Valuing Assets

The identified assets of Radio Sweden have been assigned a value, which follows the scale Low - Moderate - High. This scale is based on the three levels from FIPS 199, and the values are decided in regards to how the loss of confidentiality, integrity or availability would impact Radio Sweden and/or its involved parties.

The table below describes the meaning of each value and their implication.

Low	**Moderate**	**High**
The loss of confidentiality, integrity or availability of assets could be expected to have a **limited** adverse effect on Radio Swedens organizational operations, assets or individuals.	The loss of confidentiality, integrity or availability of assets could be expected to have a **serious** adverse effect on Radio Swedens organizational operations, assets or individuals.	The loss of confidentiality, integrity or availability of assets could be expected to have a **severe** or **catastrophic** adverse effect on Radio Swedens organizational operations, assets or individuals.

Information Assets

The table below presents identified information assets of Radio Sweden. Radio Sweden handles a lot of different information that is related to their public service objectives. The table contains a description of the asset and why it should be protected, who has access to it and its perceived value.

ID	Name	Description	Trust Level	Value
1	Sources Personal Data	Information about sources, such as names, contact details, etc. This information is vital to protect to maintain the confidentiality and privacy of sources or whistleblowers. Their personal information also needs protection to be compliant with GDPR and Swedish law.	(1) Journalists	High
2	Journalist Personal Data	Information about journalists, such as their private contact details, requires protection due to previous cases of threats. This can threaten journalistic work by causing fear of publishing investigative reports. It is also needed to be compliant with GDPR.	(1) Journalists (2) HR (3) Administrators	High
3	Other Employee Data	Other employees', such as external production companies and freelance journalists, data needs protection to ensure the safety and fearlessness to work with Radio Sweden with investigative reports and productions.	(1) HR (2) Contract Lawyers (3) Administrators	High
4	Journalistic Research Material	Journalistic research material is important to protect since it is the foundation of writing journalistic reports. Without this, it could halt or damage Radio Sweden's work and news reportage.	(1) Journalists (2) Publishing Team (3) Head of Journalism Dep.	Moderate
5	PSA Procedure Guidelines	The procedural guidelines on what, when and how to act during national emergencies requires protection so that this information is correct and available incase of a national emergency.	(1) Journalists (2) Head of Journalism Dep. (3) Top Management	High
6	Radio Broadcasting Tower Information	Locations and information about radio broadcasting towers are important to protect so that they are not easily targeted by malicious actors - whether it be disruptive attacks from individuals or nation backed attacks.	(1) Top Management (2) Technicians (3) Maintenance Personnel	High
7	Tips from Sources	Tips from sources are sensitive information that should not be tampered with, or disclosed before publication. Disclosure before censoring certain tips If this happens, it could damage the trust behind tips or impact the competitive nature of journalism.	(1) Journalists	High

4. Assets

ID	Name	Description	Trust Level	Value
1	Employee laptops 172.18.0.1/24	Windows 10 Professional (64 bits) without full disk encryption	(1) Employees	Moderate
2	Journalist laptops 172.16.0.1/21	Windows 10 Professional (64 bits) with full disk encryption	(1) Journalists	High
3	Internal Windows servers 172.17.0.1/28	14 Windows servers 2016 for internal systems (finance, internal communication, systems)	(1) Head of IT (2) Technical Administrators (3) Employees	Moderate
4	Backup server 172.17.0.18/30	2 Solaris 11.1 servers for backups	(1) Head of IT (2) Technical Administrators (3) Employees	High
5	HP Proliant Switch	HP Officeconnect 1850 Gigabit switch accessible after internal firewall	(1) Technical Administrators	Moderate
6	Cisco 7301 router	Cisco 8808 router accessible after internal firewall	(1) Technical Administrators	Moderate
7	VPN Controller 172.19.0.1/30	VPN directly give access to Cisco 7301 router	(1) Technical Administrators (2) Employees (3) Freelance journalists	Low
8	Bridge network 172.18.0.1/24	Bridge network give access directly to Cisco 7301 router	(1) Technical Administrators	Low
9	Bridge network 172.16.0.1/21	Bridge network give access directly into Cisco 7301 router	(1) Technical Administrators	Low
10	WiFi Controller 172.16.8.1/30	Cisco Catalyst 9800 controller accessible after internal firewall	(1) Technical Administrators	Moderate
11	WiFi access points	Aironet 3800 access points accessible after internal firewall	(1) Technical Administrators	Low
12	WiFi network 172.16.8.4/24	Internal and guest network/ one guest WiFi, one restricted internal WiFi accessible after internal firewall	(1) Guests (2) Employees (3) Technical Administrators (4) Head of IT	Moderate
13	Firewall 192.168.11.1/30	Cisco ASA 5500 firewall next to Cisco 7301 router inside of internal network	(1) Technical Administrators (2) Head of IT	High
14	Cisco router	Cisco 8808 router outside of internal firewall	(1) Technical Administrators	Moderate
15	HP Proliant Switch	HP Officeconnect 1850 Gigabit switch outside of internal firewall	(1) Technical Administrators	Moderate

16	Intranet servers 192.168.10.1/29	7 GNU/Linux Red Hat servers for intranet, web servers, email, intrusion detection systems, log, FTP servers.	(1) Technical Administrators (2) Head of IT	Moderate
17	Firewall 134.25.4.10	Cisco ASA 5500 firewall next to Internet and intermediate cisco router	(1) Technical Administrators (2) Head of IT	High

STRIDE Threat Model

The STRIDE model has been used to identify the threats against Radio Sweden. The STRIDE model focuses on threats such as spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privileges. The table below gives an overview of these threats and examples of how it threatens Radio Sweden as an organization.

	Threat	**Property Violated**	**Definition**	**Threat Examples**
S	Spoofing	Authentication	Impersonating something or someone else.	Claiming to be a rightful user of Radio Sweden's assets and/or information assets, e.g. login with an employee's username and password. By doing this, an unauthorized person can gain access to sensitive and internal information/systems.
T	Tampering	Integrity	Modifying data or code.	Altering information assets coming from outside the internal network. This threat can result in journalistic material being wrong and/or not trustful. The same goes for tampering and modifying data within the internal network, such as backup servers.
R	Repudiation	Non-repudiation	Claiming to have not performed an action.	Deleting signs of modifications of assets and/or information assets. By doing this an attacker may delete or modify sensitive information and/or gain access later by altering internal information/systems. In case of such events, it needs to be clear who has done what so that no one can deny their involvement in malicious events - such as leaking sources information or deleting research material.
I	Information Disclosure	Confidentiality	Exposing information to someone not authorized to see it.	Publishing a list of journalists' sources could result in harm to the source. Similarly, disclosing information about employees or work being done could make them targets for threats and intimidation.
D	Denial of Service	Availability	Deny or degrade service	Sending data packets and occupying internal servers. This could result in harm

			to users.	to time critical assets and/or information assets. DoS could also lead to difficulties for Radio Sweden to communicate PSAs.
E	Elevation of Privilege	Authorization	Gain capabilities without proper authorization.	Allowing guest/limited/remote users to run commands and/or give them access to internal information/systems. This could result in modification, deletion or publication of sensitive or critical internal information.

Countermeasures and Mitigation

The following countermeasures and mitigations are recommended to prevent or minimize the realization of these threats. It also provides some examples of implementations and how it can countermeasure/mitigate the threat.

	Threat	**Countermeasure/Mitigation**	**Examples of Implementation**
S	Spoofing	(1) Boundary Protection (2) Firewall Rules (3) Strong Authentication	As an example, by using stronger authentication (such as 2FA) it can make it harder for adversarial actors to spoof their identity. Similarly, firewall rules can be used to detect whether someone is claiming to be from the inside, but in reality the connection is coming from the outside.
T	Tampering	(1) Hash-Based Message Authentication Code (2) ACLs (3) Digital Signatures	HMAC can be used for information that is processed, stored and transmitted to ensure that their integrity is intact. ACLs can be implemented so that unauthorized insiders and/or outsiders do not access certain data/information. Using digital signatures on all data also helps detecting whether someone is trying to tamper with data.
R	Repudiation	(1) Digital Signatures (2) Audit Logs (3) Timestamps	Digital signatures and timestamps make it easier to attribute certain actions to an entity and time. Audit logs can also be used to monitor different types of events and get an overview of what has happened.
I	Information Disclosure	(1) ACLs (2) Encryption	By dealing with access to data with ACLs, it is harder for unauthorized individuals to access sensitive data and exfiltrate it. By using strong encryption - even if data is exfiltrated, it is unreadable by unauthorized parties.
D	Denial of Service	(1) System Time Synchronization (2) Unsuccessful Logon Attempts (3) Firewalls (4) Denial-Of-Service	Synchronize system clocks within and between systems and system components in order to identify misuse of internal systems. This can be used together with limitation of consecutive invalid logon attempts by a user in order to prevent misuse of internal systems.

		Protection	Furthermore, the firewalls can be used to stop data packets coming from specific sources or entries whose purpose is to occupy internal servers. Monitoring system resources in order to determine if sufficient resources exist to prevent effective denial-of-service attacks can be an effective Denial-Of-Service Protection together with these implementation approaches.
E	Elevation of Privilege	(1) Account Management (2) Least Privilege Principle (3) RBACL	Employees and other actors should have the least privilege needed to perform their work, so that accounts cannot be misused to elevate one's privileges. Similarly, by managing accounts and using RBACL, it makes it harder for someone to gain higher privilege by accessing someone else's account, and accesses in general are related to role membership. User and accounts should be prohibited from using certain systems that is not needed, and remote access to certain systems/services should be managed to protect unauthorized access to sensitive systems/data from outside.