Cyber 2 Threat Model Group 1

Karin Säberg
Carl Sundelin
Hamid Farajisarkati

Terms

CVE - Common Vulnerabilities and Exposures: a collection of known and published vulnerabilities and exposures in cyber security.
CVSS - Common Vulnerability Scoring System, a scoring system to reflect the severity of vulnerabilities. The scores can be translated into three levels of low, medium and high.

Current flaws

Our review of the current setup has revealed a number of flaws, technical, policy-related and organisational.
Among the technical flaws we have found issues, such as, a multitude of vulnerabilities in the hardware used.

- The Cisco 8808 routers have 11 CVEs with most having **High** CVSS.
- The Cisco ASA 5500 firewall has 60 CVEs with mostly **High** CVSS.
- The Cisco Catalyst 9800 has 12 CVEs with mostly **High** CVSS.
- The Windows Server 2016 has 2896 CVEs, most of them **High** and **Medium** CVSS.
- The F-Secure Client Security anti-malware can cause performance issues

We also noticed a lack of firewalls on the laptops themselves which is problematic, especially when the device is brought from outside the network and can have been connected to insecure sites and devices leading to potential attack vectors.

A lack of password policy was noted, strong passwords are a good start to protect against attacks. There is also no policy or process presented on how to handle downloading of files, while we understand the need to download, and access, resources and tips a process should be in place to ensure that no malicious files get access to the network.

There is no education of the users about cyber security. We also noticed that there is no process of how to verify freelance journalists when they get access to the VPN.

Journalists are expected to travel far and wide, and into high risk areas at times. This puts their devices at risk of being injected or infected with malware, especially if they leave their devices unattended or let someone else handle them. Journalists returning from such high risk areas may jeopardise the network by connecting an infected device.

Attack vectors

- Social engineering/Spear Phishing
    - Employees being tricked to give sensitive information to outsiders or make security mistakes

- DDoS
    - Cisco ASA 5500 firewall has a flaw which can lead to denial of service(DoS) attacks and result in disconnection from the internet and or local network.

- Drive-by Malware/rogue USB device
    - Employees can install malware by receiving emails from untrusted sources or visiting websites and this could lead to allow attackers gain access to the internal data and systems
    - Malware could be disguised as legitimate tips

- Insider - Access, Control, Knowledge
    - Freelance journalists have access to the internal systems using VPN which can allow attackers to gain access to these systems by gaining access to the freelance journalists' laptop
    - A malicious person masquerading as a freelance journalist could gain access to the VPN

Consequences

A DoS/DDoS attack would be very damaging to the reputation of Radio Sweden and would directly compromise your goal of being available to make broadcasts in the event of an emergency. This lack of availability is damaging to the consumers since they are not able to get the information that they may need, and damages your reputation because people would see the institution as a failure, leading to less trust being placed in it and fewer people using the service.

Since there were many possible ways for a malware attack to take place, there are many possible consequences for them. In the event of a ransomware attack, the servers and data on the servers could be locked away and not accessed by Radio Sweden until a large ransom is paid. It is always uncertain whether this data is stolen by the attackers or if the data is completely locked away so no-one can access it. By not having a backup, this data would be lost and many stories and confidential data could be lost forever. By losing the contact details of trusted sources, they may not continue to trust you in the future and may choose to work with other news organisations instead.

Other malware that might be installed on a device in the network might steal and access the confidential data that is being stored on the network. This information could be sold to criminal organisations that are angry at Radio Sweden and want to do them harm; other governments that may want to target sources that are in their countries, and others that want to see Radio Sweden fail. Such a breach of data would lead to a lack of trust from both potential sources, since they can no longer be certain that their identity will be secure, and from the public, because they can no longer be certain if the data that is in their system is actually what the reporters have found or if it is something that has been planted by malicious actors. Creating this lack of integrity means that the lack of trust would be difficult to come back from.

Countermeasures

In light of these flaws, attack vectors and consequences we propose the following solutions:

- Upgrade outdated and vulnerable hardware
- Hire a CISO or similar to be responsible for cyber security
    - Create and implement cyber and information security policies
    - Update and upgrade soft- and hardware as necessary
    - Educate your users on cyber security
- Implement secure method for tips (For example: SecureDrop or similar instead of emails)
- When returning from high risk areas where the risk of devices being infected by malware, implement a process to check devices before they are connected to the network

These are ordered in our suggested order of action, your current hardware puts you at great risk and thus we suggest hardening these as a first step while you get started on bringing in a CISO, or similar person, to take over cyber security responsibility. As this will be an iterative process we strongly suggest having a dedicated position and team. We judged the potential risks from malicious files being disguised as tips to be major and recommend you implement alternative ways to receive tips and information. We also recommend implementing a process of checking devices returning from high risk areas, and/or devices left unattended, to be checked for malware before connecting to the network.