Case 2 - Threat Model

CYBER Security

2020-04-08

**Submitted by:**

Group 15

Ranjana, Efstathios, Justas

|  |  |
| --- | --- |
| **Application name** | Threat analysis and Threat model for Radio Sweden |
| **Application Version** | 1.2.1 |
| **Description** | This document provides the report of threat analysis and presents the analysis in the thread model |
| **Document Owner** | Group 15 |
| **Participants** | Ranjana, Efstathios, Justas, IT of Radio Sweden, CEO of Radio Sweden |
| **Reviewer** | Legal Representative of Radio Sweden |

# 

# External Dependencies

|  |  |
| --- | --- |
| **ID** | **Description** |
| 1 | The internal servers for finance, internal communication and systems are running in windows server 2008, the patching of the system is not available because of outdated Operating system. |
| 2 | The backup server is Solaris, this will be maintained as per Oracle maintenance plans with updates and patches. This will include the application of the latest operating system and application security patches. |
| 3 | The Web Server is behind a firewall and the only communication available is TLS. |

# 

# Entry/Exit Points

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Name** | **Description** | **Trust Levels** |
| 1 | VPN login portal | This is the connection page where user enters credentials to connect to company resources via browser/app | (1)IT Administrator (6) User with Valid Login Credentials (7) User with Invalid Login Credentials |
| 2 | POP portal | This is the email server connection where the user connects to emails from internal colleagues to external sources | (1)IT Administrator (6) User with Valid Login Credentials (6) User with Invalid Login Credentials |
| 3 | Company Main page | This is the main page of Radio Sweden’s website with entry points to all users which does not need any credentials to access from any point. | (8) Anonymous Web User |

# 

# Assets

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Name** | **Description** | **Trust Levels** |
| **1** | Employees and Freelancers | Base information of employees and freelancers |  |
| **2** | Login Details | The login details of employees working in Radio Sweden for email access | (6)User with valid login credentials  (1)IT administrator  (5) Email server user process  (4) Web server administrator |
| **3** | Backups | The backups of the servers/laptops performed throughout the time period | (2)Backup Administrator |
| **4** | Create/Disable Users | The new users and freelancers accounts are created when they join the company and disabled when they leave the company | (1)IT Administrator |
| **5** | Access to FTP server | The file transfer occurs through FTP inside the internal network | (6)User with valid login credentials  (1)IT administrator |
| **6** | Access to surveillance camera footage | The surveillance footage is checked via clarified personnel during emergencies | (1)IT administrator  (3)Surveillance administrator |

# 

# Trust Levels

|  |  |  |
| --- | --- | --- |
| **ID** | **Name** | **Description** |
| 1 | IT Administrator | Administrator in charge of the Radio Sweden IT infrastructure |
| 2 | Backup Administrator | The backup administrator in charge of the backup server to read/write and make other changes that are needed |
| 3 | Surveillance Administrator | The surveillance administrator has access to setup surveillance cameras, read the content of the camera and apply necessary camera accessories. |
| 4 | Web Server Administrator | The web server administrator had read/write/modify and delete privileges to the web server. The administrator is responsible for management and maintenance of the web server. |
| 5 | Email Administrator | The administrator in charge of emailing services |
| 6 | User with Valid Credentials | A user who can connect to the Radio Sweden internal network and components within the network |
| 7 | User with Invalid Credentials | A user who can not connect to the Radio Sweden internal network and components within the network without valid credentials |
| 8 | Anonymous Users | A user who can connect to the companies website, but has no credentials to make adjustments or view sensitive data |

# 

# Stride Threat & Mitigation Techniques List

|  |  |
| --- | --- |
| **Threat Type** | **Mitigation Techniques** |
| Spoofing Identity | 1. Appropriate authentication 2. Protection of secret data by not storing it 3. Encrypted network |
| Tampering With Data | 1. Appropriate authorization 2. Hashes 3. Digital Signatures 4. Tamper Resistant Protocols |
| Repudiation | 1. Digital Signatures 2. Timestamps 3. Audit logs |
| Information Disclosure | 1. Authorization 2. Privacy-enhanced protocols 3. Encrypted protocols |
| Denial of Service | 1. Appropriate authentication 2. Appropriate authorization 3. Filtering 4. Defining the limiting parameters |
| Elevation of Privilege | 1. Defining user permissions based on roles 2. Run with least privilege |

# 

# 

# Threat Model

# 

# References

CRV2 App Threat Modeling, Open Web Application Security Project, Accessed on: 8th April 2020 <https://owasp.org/www-community/CRV2_AppThreatModeling?fbclid=IwAR3imeXOzmyrfgsPIQU7PQ_4Ddgj44CdW9KtzoZhiIFdA2Kz7-byjvTslTE>

Hello Group 3,

The document is well formulated and presented. The details of the threats and their countermeasures are praise worthy. We just found some minor things and have presented them as our questions:

1. **Why were Backup server and FTP server not identified as assets?**
2. **Was there any specific reason for not addressing the data flow model in your document?**
3. **Which threat model did you use to mitigate the defined risks, STRIDE or DREAD?**

Regards,

Group 15

Comments:

The report has a very good structure with contents, list of figures and list of tables.

The figure of threat is quite nice and clear.

Mitigation techniques can be more detailed.

Questions:

1. Do you have any threat type like phishing? And any mitigation technique for it?

2. Do you think Radio Sweden has any vulnerability? And any remediation plan for it?

3. Can you describe if it is necessary to estimate the values of assets?

Sincerely,

Group 9

Hi Group 9,

Thank you for your comments. Please find the answers to your questions below:

**1. Do you have any threat type like phishing? And any mitigation technique for it?**

Phishing attack constitutes a potential threat to Radio Sweden and it is considered as one of “Spoofing Identity” threat types described in our STRIDE threat list. Appropriate authentication, up-to-date firewalls and employees sufficient information security awareness level are considered as mitigation techniques ,specifically, for phishing attacks.

**2. Do you think Radio Sweden has any vulnerability? And any remediation plan for it?**

One of the vulnerabilities we identified is Windows 2008 server. As of January 2020, Microsoft has stopped patches for it, therefore the only way to mitigate this vulnerability is to upgrade the OS of the server.

Another vulnerability is that the backup server, internal windows server, and employee/journalist laptops are all connected to one subnet (router). If any of the servers in the subnet is attacked, everything will be exposed, therefore employee/journalist laptops should have a separate subnet from the servers. It is more beneficial to create a demilitarized zone for backup servers and other internal servers.

**3. Can you describe if it is necessary to estimate the values of assets?**

The value of the assets define how much the company is going to lose when the assets are attacked via different threats. This will give companies a base idea of how much they are willing to spend on resolving those problems. The value of assets provides a baseline for cost-benefit analysis.

Not having value of assets might be troublesome, as the company will not be able to distinguish which asset to prioritize on while creating the security model. Based on the value of assets, the mitigation techniques for the vulnerabilities should be tailored.

BR,

Group 15