CYBER 2022
Group number: 11
Group members: Josefin Chenon, Lovisa Krantz, Johan Olausson, Duaa Al-Kebsi

Case 2: Cyber Security Modeling

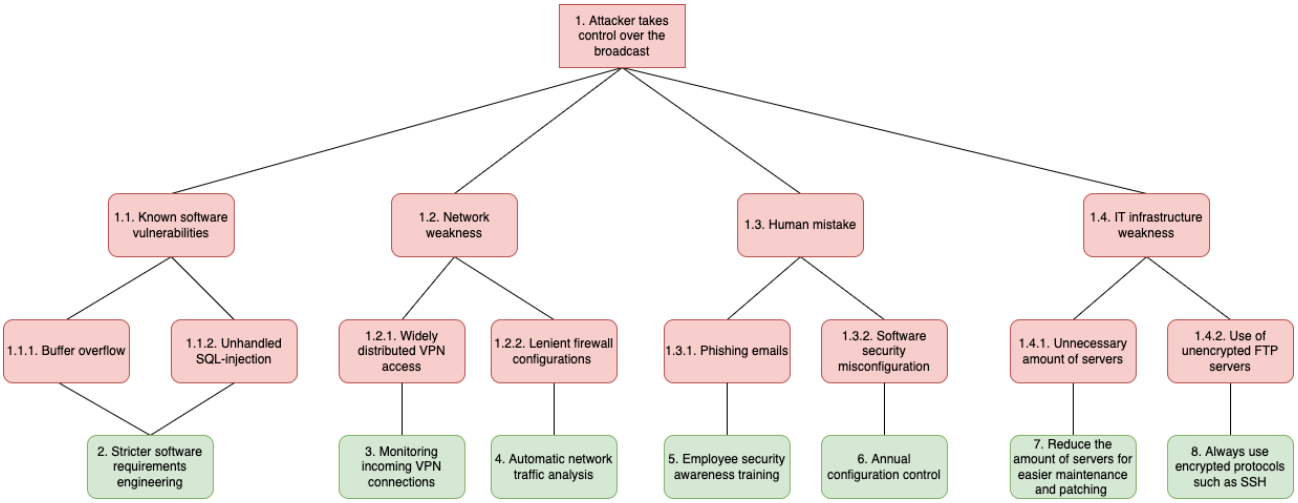

Figure 1. Attack Tree

Figure 1 above presents identified threats and attack vectors illustrated in an attack tree for Radio Sweden.

1. The root threat is someone taking control of the broadcast which would enable an attacker to shut down the communication or spread false information through the radio station.

1.1 Known software vulnerabilities include unhandled weaknesses from the software provider. For example, buffer overflow (1.1.1) and unhandled SQL injection (1.1.2). The countermeasure is stricter software requirements engineering (2).

1.2 Network weaknesses that might allow unauthorized access to the internal network. For instance, widely distributed VPN access (1.2.1) and lenient firewall configurations (1.2.2). The countermeasure for 1.2.1 is to monitor incoming VPN connections (3) to track their activity. The countermeasure for 1.2.2 is automatic network traffic analysis (4).

1.3 Human mistakes consider actions made by employees due to a lack of security awareness. For example, act upon phishing emails (1.3.1) and software security misconfigurations (1.3.2). The countermeasure for 1.3.1 is to increase security awareness among employees by education and training sessions regularly (5). The countermeasure for 1.3.2 is annual configuration controls of software (6).

1.4 IT infrastructure weaknesses include vulnerabilities in the hardware architecture. For instance, unnecessary amount of servers (1.4.1), which creates maintenance issues and use of unencrypted FTP servers (1.4.2). The countermeasure for 1.4.1 is to reduce the number of servers for easier maintenance and patching (7). The countermeasure for 1.4.2 is to always use encrypted network protocols such as SSH (8).