COM-402 exercises 2024, session 9: Network Security

Exercise 9.1

Consider the following two options for letting remote users access your company's e-mail:

- They use a VPN access to the company's network. Then, they can use their preferred mail client to access the mail server of the company.
- You install a web server with a web-mail program (like ewa.epfl.ch) such that the users can access their e-mail with any web browser.

Which of the two options is more secure? Why?

Exercise 9.2

Which option is safer:

- Specifying what is forbidden (deny list) and allowing the rest.
- Specifying what is allowed (allow list) and denying the rest.

Explain why.

Exercise 9.3

- Describe the difference between a (direct) proxy and a reverse proxy.
- Describe one security related function that each proxy can provide.

Exercise 9.4

The web proxy of your company keeps a log of all connections that are made to all websites.

- Describe a situation where these logs can be used to help secure the company's network.
- Describe a situation where these logs could be a problem for the company's security.

Exercise 9.5

Describe a possible Disaster Recovery Plan (DRP) that will make possible to start over after your data center has burned down.

Solutions to the Exercises

Solution 9.1

Typically, a VPN connection gives access to all of the internal network for any type of traffic. Thus, if the user's machine was infected by a malware or under control of a hacker, the attack could propagate to all of the internal network. The web-mail program only gives access to e-mail. In case of an attack, only the e-mail would be compromised. This is a typical application of the principle of *least privilege*.

Solution 9.2

Using an allow list is safer. Indeed, if you forget to put something on the list you do not create a security risk. This is called the principle of *default deny*.

Solution 9.3

- A direct proxy is located close to the client. It receives all the connections of the client for a given application (e.g. HTTP) and forwards them to the corresponding server on the internet.
- A reverse proxy is located close to the server. It receives the connections of all clients and forwards them to a server.
- A direct proxy can be used to block access to known dangerous websites (e.g. phishing campaigns). It can also scan for malware in the documents downloaded from the Internet.
- A reverse proxy can detect and block web based attacks against a web server (e.g. SQL injections).

Solution 9.4

- If one workstation of the company was infected by a malware downloaded from the Internet, the logs could help the company find out which other workstations also downloaded the same malware.
- If the logs contain passwords or access tokens used to access protected information, an attacker who gains access to the logs would be able to access the protected information. The company could be breaking the law if the logs contain sensitive personal information that can be linked to employees (e.g. which employee accessed which political website). Such logs should only exist if there is a valid reason and they should be protected in order to prevent abuse.

Solution 9.5

A typical DRP could contain the following steps:

- Buy new machines.
- Play back the full images of all servers to get the machines working with all applications as installed before the fire.
- Use the database backups to populate the databases with the data they contained before the disaster.
- Restore the files of all the users.
- Write a report of which parts of the recovery worked and which didn't. Adapt your backup strategy accordingly.