Network Security

Exercises Question 1

Tobias Famos
16-933-764

March 2, 2022

A) List and briefly define the three key objectives of computer security.

The key objectives of computer security are the following:

Confidentiality A communication should be confidential. This means the contents of the communication shall not be readable by any third party. A confidentiality breach must not be entirely ready and understanding the message. Also being able to guess the type of communication, or a communication partner can be seen as a breach of confidentiality

Integrity A communication should keep its integrity. This means a communication shall not be altered in any way by a third party. A breach of integrity might be altering a message, a sender or a receiver of the message.

Authenticity A communication or communication partner must be authentic. This means I want to be sure that whomever I am communicating with is acctually who he claims to be. A breach of authenticity might be phishing attack of some third party posing as a banking site.

B) Consider the Following Szenario

Consider that all data of a private clinic are handled by a server with vulnerability against a ransomware attack. In which way (with examples) could the confidentiality, integrity and availability requirements be affected in such a case? Compare the degree of their importance

Answer: I have structured my answer by the three requirements:

Confidentiality The confidentiality is usually not critical in a Ransomware Attack. The Attacker usually does not try to access information but to make access to information impossible for every party, most prominently for the victim of the attack. However, if there is a security vulnerability that enables an attacker to deploy ransomware, then the same vulnerability might also be exploited to get data dumps, at least in encrypted form. This would pose a real threat to the confidentiality, which is breached as soon as any attacker has unencrypted access to any data or communication. Given that the data dump is encrypted, the confidentiality is not yet breached, but the threat for a breach is increased as encrypted data is not impossible to decrypt but just quite hard to decrypt.

Integrity With integrity, it is the same thing as with confidentiality. Usually integrity is not a primary factor attacked during a ransomware attack but with exploiting the same vulnerability as the ransomware would, integrity might be in danger. To breach integrity, the attacker must be abler to alter any data or communication of the victim. Same as before, if the communication and or data is encrypted, integrity is not yet fully breached, but the attacker is one step closer to breaching it. A concrete scenario might be an attacker gets access to the database of with patient data via the same vulnerability and alters some data of a given patient.

Availability Now here lies the standard attack of a ransomware. The availability of the data is breached mostly via encryption. A ransomware is deployed on the server via the vulnerability and starts encrypting any data on the system. Only after paying a fee will the victim be able to access his information again (note that often after paying the fee, an attacker will still not give access to the system)