Collaborative Discussion 2 – Initial Post – Michael Geiger

In order to protect computer systems from harmful interference from outside, there are various options that act on different levels.

A firewall software installed locally on the computer is referred to as a personal firewall. Their job is to prevent unwanted external access to network services on the computer. It can also be used to prevent applications from communicating with the outside world without the user's authorization. The personal firewall offers an advantage in the case of computer worms that exploit a security flaw in a network service in order to spread (Herzog & Shahmehri, 2007). They can only infect the computer if appropriate network services are available for the worm. Here a personal firewall can restrict remote access to the network service and thus make infection more difficult or prevent it.

Personal firewalls can protect against some computer worms which spread over the network, but they do not protect against the installation of any other malware. Programs that run on the same hardware as the personal firewall software have far more options for manipulating and circumventing them than with an external firewall (Alfayyadh et al., 2010). A crash or even permanent deactivation of the firewall software due to a software error or malware results in unrestricted access to the previously filtered network services, sometimes without the user noticing.

A network firewall is predestined to prevent unauthorized external access to the internal system. In contrast to the personal firewall, the internal system does not necessarily consist of a single computer, but can be based on a network of several computers form the internal network (LAN). One such firewall is a Proxy firewall. It is characterized by the fact that, in addition to the pure traffic data such as source, destination and service, it typically also scan the user data, i.e. the content of the network packets (Zalenski, 2002). The typical Proxy filter does not simply pass the network request from the source system on to the target system. Rather, it establishes itself own connection to the target system. Since it communicates with the target system on behalf of the requesting client, it can analyze the packets coherently and influence the connection. From a technical point of view, such a filter works as a communication partner who intervenes in the traffic and terminates the connections on both sides instead of passing the network packets through. The filter itself is a utility program for computer networks that mediates data traffic. As an active mediator, it behaves like a server towards the requesting client, and towards the target system like a client (Herbert, 2021). Since the Proxy firewall must know the communication protocol, there is a separate filter for each higher communication protocol (e.g. HTTP).

This could be a problem. In principle, any service can work on any port number. If a port for HTTP for example, is enabled in the set of rules, a different protocol can still run over it. Only both communication partners (the client in the internal network and the service on the server from the external network) have to be configured accordingly. In addition, a poorly configured Proxy can be dangerous because it allows third parties to act on the Internet via the Proxy address. As an example, the proxy could be misused for an attack or to send spam. In the event of misuse, the Proxy is then determined as the source, which under certain circumstances can have unpleasant consequences for the operator (Herbert, 2021).

References:

Alfayyadh,B., Ponting, J., Alzomai, M., & Jøsang, A. (2010) Vulnerabilities in personal firewalls caused by poor security usability, IEEE International Conference on Information Theory and Information Security, 2010, pp. 682-688, doi: 10.1109/ICITIS.2010.5689490

Herbert, K. (2021) proxy firewall. Available from: https://searchsecurity.techtarget.com/definition/proxy-firewall [Accessed 15.09.2021]

Herzog A., Shahmehri N. (2007) Usability and Security of Personal Firewalls. In: Venter H., Eloff M., Labuschagne L., Eloff J., von Solms R. (eds) New Approaches for Security, Privacy and Trust in Complex Environments. SEC 2007. IFIP International Federation for Information Processing, vol 232. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-72367-9_4

Zalenski, R. (2002) Firewall technologies, in *IEEE Potentials*, vol. 21, no. 1, doi: 10.1109/45.985324