Collaborative Discussion 2 – Summary Post – Michael Geiger

Personal firewalls have the task of ensuring the protection of an end device, as well as blocking applications that should not be used. An issue that personal firewalls could have, is that they are not optimally set up because of security gaps or they block the intended applications of the user, which leads the user to turn off the firewall or to modify it in such a way that security gaps arise. This enables attacks in the form of adware, malware, spyware or ransomware (Herzog, 2007).

Network firewalls, on the other hand, can be divided into three sub-categories, packet-filtering firewalls, circuit-level firewalls and application-level firewalls (Noonan, 2006). They are aimed at protecting LAN (Local Area Networks). While they offer good protection when properly configured, this is often accompanied by disadvantages in terms of usability in relation to network delays (Andress, 2014). For example, proxy firewalls can reduce the flow of data and generate jitter (Hayajneh et al., 2013). In the event of a bad configuration, the connection with other desired communication partners can also be prevented (Firkhan, 2011). A compromise must therefore be found between security concerns and usability.

As noted with personal firewalls, the human factor also plays a comprehensive role. Careless use of and interference with the firewall system enable attacks and make systems vulnerable to them. Since every development of security systems arouses the commitment of attackers to circumvent this, for example through encryption or spoofing, LAN should be set up under the aspect of "Zero Trust" (Klein, 2021). It is assumed here that a network or its users are already infected and therefore they are also a potential source of danger.

It can be concluded that single firewalls do not offer sufficient protection and can only offer the greatest possible protection through a sensible combination with other security systems. The human factor plays a decisive role in relation to firewalls and their security and should be limited by companies through restrictions and internal regulations.

References:

Andress, J. (2014) *The Basics of Information Security, Understanding the Fundamentals of InfoSec in Theory and Practice*. 2nd ed. Massachusetts: Syngress Publishing. Available from: https://www.sciencedirect.com/book/9780128007440/the-basics-of-information-security?via=ihub= [Accessed 29.09.2021]

Firkhan,A. (2011) A study of technology in firewall system. IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA). 232-236. Available from: https://ieeexplore.ieee.org/document/6088813 [Accessed 29.09.2021]

Hayajneh, T., Mohd, B.J., Itradat, A. & Quttoum, A. (2013) Performance and information security evaluation with firewalls. *International Journal of Security and Its Applications 7*(6): 355-372. Available from: http://article.nadiapub.com/IJSIA/vol7_no6/37.pdf [Accessed 29.09.2021]

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. IFIP International Federation for Information Processing. Springer, Boston, MA. Available from: https://link.springer.com/content/pdf/10.1007%2F978-0-387-72367-9_4.pdf [Accessed 28.09.2021]

Noonan, W. & Dubrawsky, I. (2006) Firewall fundamentals. Cheswick: Pearson Education. Available from: https://read-download-books.com/v6/preview/?pid=6&offer_id=522&ref_id=2acb793e0c1094d0a2eb125e14JbDbHZ_541a0fad_c28f910b&sub1=541a0fad&keyword=firewall-fundamentals-wes-noonan-ido-dubrawsky.pdf&sub8=firewall-fundamentals-wes-noonan-ido-dubrawsky.pdf&m=firewall-fundamentals-wes-noonan-ido-dubrawsky.pdf [Accessed 28.09.2021]

Klein, D. (2021). Relying on firewalls? Here's why you'll be hacked. *Network Security 2021*(1): 9-12. Available from: https://www.sciencedirect.com/science/article/pii/S1353485821000076?via%3Dihub [Accessed 30.09.2021]