Collaborative Discussion 2 – Peer Response 5 – Thomas Ranson

Thank you Thomas for your very interesting post on EDR software and multi-factor authentication.

Two-factor authentication, which can be seen as a pioneer of MFA, is a relatively long-known technology that was patented by AT&T in 1995 (Blonder et al., 1995). While the MFA was initially limited by a lack of technical possibilities, this type of securing authentication is now a common method. Since 01.01.2021, the European credit institutions have been obliged to offer customers strong customer authentication (The European parliament and the council, 2015). This is made possible by confirming transactions through two independent characteristics from the categories of knowledge, ownership and inheritance.

The most common method here is authentication using the knowledge category in the form of a password and the possession category in the form of a confirmation of entering a confirmation code sent to the mobile phone. It should be noted, however, that the frequent authentication by SMS can be bypassed in various ways. For example, under the Android operating system, fake apps can gain access to received SMS in order to forward them to fraudsters (Markert et al., 2019).

In addition, attacks can target the Singnalling System No 7 protocol (SS7) used in the cellular network. In this way, the attackers can redirect the SMS, which is intended for authentication, to a mobile phone they control and thus undermine the security factor of ownership (Gibbs, 2016). In this way, during an attack on the customers of the mobile operator O2-Telefonica, which operates in Europe and Latin America, in 2017, they were defrauded by unauthorized withdrawals from their bank accounts (Price, 2017).

It should therefore be stated that although MFA increases the security of customers, this technology does not represent absolute protection either.

References:

Blonder, G., Greenspan, S., Mirville, R. & Sugla, B. (1995) Transaction authorization and alert system. United States Patent. Available from: https://web.archive.org/web/20190415174426/http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=5708422.PN.&OS=PN/5708422&RS=PN/5708422 [Accessed:01.10.2021]

Gibbs, S. (2016) SS7 hack explained: what can you do about it?. The Guardian. Available from: https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls [Accessed: 02.10.2021]

Markert, P., Farke, F. & Dürmuth, M. (2019) View The Email to Get Hacked: Attacking SMS-Based Two-Factor Autentification. Available from: https://www.mobsec.ruhr-uni-bochum.de/media/mobsec/veroeffentlichungen/2019/08/19/way2019-5-view-the-email-to-get-hacked_v3.pdf [Accessed: 02.10.2021]

Price, R. (2017) Hacker used a long-neglected vulnerability in phone networks to empty victims' bank accounts. Markets Insider. Available from: https://markets.businessinsider.com/news/stocks/hackers-ss7-vulnerability-steal-cash-german-back-accounts-2017-5 [Accessed: 02.10.2021]

The European parliament and the council (2015) Revised rules for payment services in the EU. Available from: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366 [Accessed: 01.10.2021]