Collaborative Discussion 1 – Initial Post – Michael Geiger

As a basis for the Attack – Defense Tree of vulnerabilities of a small business, the study by Bastarelli et al. (2012) was used.

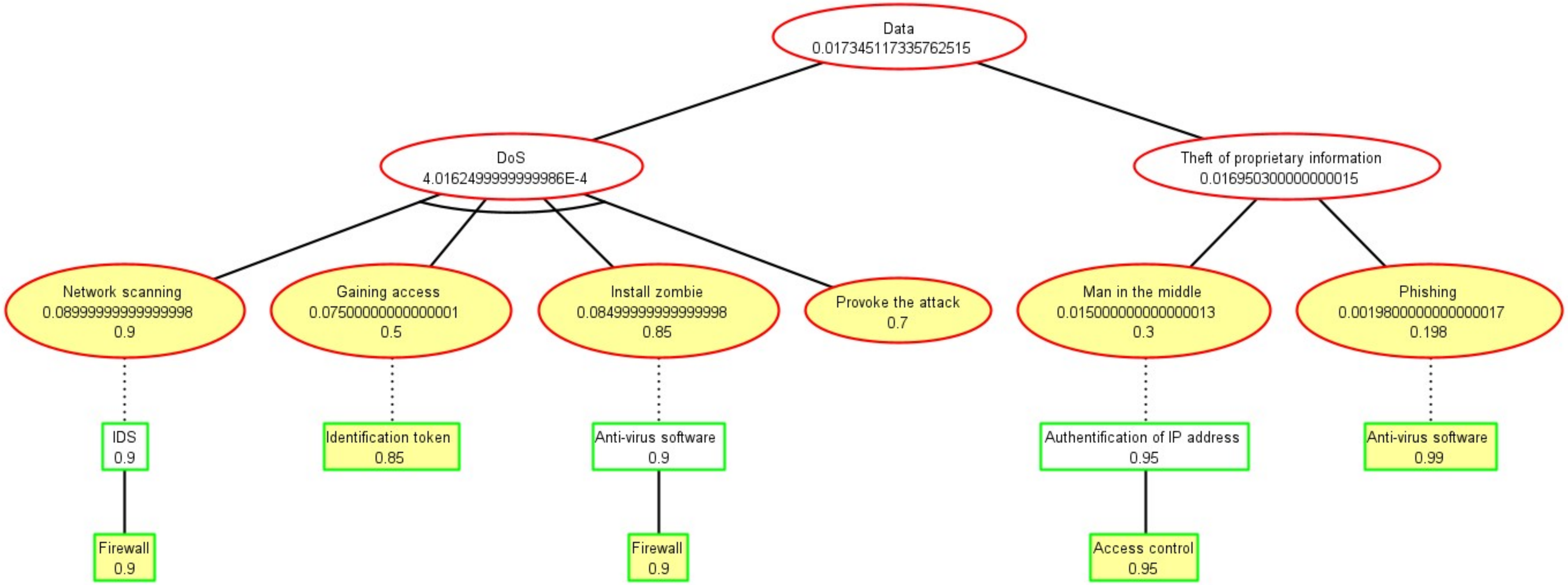
Two key threats considered here are DoS attacks and theft of proprietary information. The probability of a successful attack was chosen as a meaningful quantitative investigation (see diagram below), as this can cause the positive influencing factors of mitigation measures.

Since networks can be sniffed quickly and easily without security measures using pentesting tools such as Nmap, Burp Suite or Metasploit, a high probability of 90% was selected. This probability can be reduced by an intrusion detection system (IDS), since these are often coupled with an intrusion prevention system (IPS) and thus not only detect unwanted access, but also protect sensitive information of the network from unauthorized access (Samson, N.D.) .

Gaining access can take place without security measures using simple brute force attacks, which is why a successful probability of this attack was determined at 50%. Identification tokens can significantly increase security, which can reduce the probability of success to 7.5%. Installing malware via malicious emails for example is also a factor which without a firewall is just a matter of time and repeated attempts as human error will eventually arise.

The threats mentioned, man-in-the-middle attack and phishing, for information theft are also based on human error, whereby detecting dangerous networks can be difficult for the untrained staff. A study by Terranova Worldwide Corporation (2021) found that 19.8% of participants clicked on a phishing email link and 14.4% downloaded documents in the phishing simulation. The human factor is therefore a serious vulnerability. However, anti-virus software and spam filters can prevent over 99% of phishing attacks (TitanHQ, 2020).

It should be emphasized that the cumulative prevention measures in the DoS attack in particular clearly illustrate the benefit. In this example, the probability of a successful DoS attack drops from 26.8% without security measures to 0.0004% with mitigation measures.


Data
0.017345117335762515
DoS
4.0162499999999986E-4
Theft of proprietary information
0.016950300000000015
Network scanning
0.08999999999999998
0.9
Gaining access
0.07500000000000001
0.5
Install zombie
0.08499999999999998
0.85
Provoke the attack
0.7
Man in the middle
0.015000000000000013
0.3
Phishing
0.0019800000000000017
0.198
IDS
0.9
Identification token
0.85
Anti-virus software
0.9
Authentification of IP address
0.95
Anti-virus software
0.99
Firewall
0.9
Firewall
0.9
Access control
0.95

References:

Bistarelli, S., Fioravanti, F., Peretti, P. & Santini, F. (2012) Evaluation of complex security scenarios using defense trees and economic indexes. Journal of Experimental & Theoretical Artifical Intelligence. 24(2): 161-192. Available from: https://www.sci.unich.it/~fioravan/papers/BFS-JETAI12.pdf [Accessed 06 Mai 2022].

Samson, R. (N.D.) Top 10 Intrusion Detection And Prevention Systems. Clearnetwork. Available from: https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/ [Accessed 07 Mai 2022].

Terranova Worldwiede Corporation (2022) Gone Phishing Tournament. Available from: https://terranovasecurity.com/gone-phishing-tournament/?utm_campaign=en_gpt_report2021&utm_medium=cpc&utm_source=google&gclid=Cj0KCQjwsdiTBhD5ARIsAIpW8CJsJXkKQo9CHcB6IF-sExDaKcOXPjtbSIjC5XNoxqEpMjj4A31k8WAaAoIDEALw_wcB#tournament [Accessed 07 Mai 2022].