Initial post: Moving beyond firewalls

Network firewalls identified as a key cyber security component in the early 1990s (Ranum, 1993) are still essential but should not be prioritized over other security investments. Infrastructure protection and identity and access management (IAM), lag behind network security investments (Gartner, 2020). Failure to prioritize these areas potentially exposes organizations to greater risk because many technology assets are no longer consistently behind organization-controlled network firewalls (Sangster, 2020).

Two specific technologies within the infrastructure protection and IAM categories (Deshpande, et al., 2018) that every organization should consider implementing are endpoint detection and response (EDR) agents and multi-factor authentication. The 2021 Verizon data breach report (VDBR) confirms user actions, endpoints and credentials are still responsible for, or the precursor to, 85% of the data breaches analyzed (Verizon, 2021). Users and endpoints continue to be targeted because once an organization's endpoint is compromised, a great deal of improperly protected data (Varonis, 2021) is now accessible.

Legacy antivirus products search for byte patterns of known malicious software, EDR solutions monitor for malicious behaviour within real time processes on the endpoint. EDR agents can be configured to block suspicious actions without security analyst intervention, preventing attacker gaining a foothold or elevating privilege levels. Leading EDR solutions also incorporate large scale data collection and machine learning analysis; data sources are now too complex for human comprehension alone (Sjarif, et al., 2019).

Sixty one percent of the VDBR analyzed breaches involved compromised credentials (Verizon, 2021). Implementation of multifactor authentication adds cost, complexity and may still be bypassed but creates a much larger key space than passwords alone(O'Gorman, 2003). Single factor authentication is vulnerable to numerous attacks and was first identified as a MITRE common weakness 2006 (MITRE, 2021).

References:

Deshpande, S. et al. (2018) Market Definitions and Methodology: Information Security and Risk Management Products and Services Forecast. Available from: https://www.gartner.com/en/documents/3885567/market-definitions-and-methodology-information-security- [Accessed 12 June 2021].

Gartner. (2020) Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020. Available from: https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem [Accessed 12 June 2021].

MITRE. (2021) CWE-308: Use of Single-factor Authentication. Available from: https://cwe.mitre.org/data/definitions/308.html [Accessed 12 June 2021].

O'Gorman, L. (2003) Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE* 91(12): 2021-2040. Available from: http://0-eds.b.ebscohost.com.serlib0.essex.ac.uk/eds/detail/detail?vid=0&sid=5a6e549d-5dd4-4e44-b760-133da96580cc%40sessionmgr103&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=edseee.1246384&db=edseee [Accessed 12 June 2021].

Ranum, M. J. (1993) 'Thinking about Firewalls', *Second International Conference on Systems and Network Security and Management (SANS-II).* Arlington, April. Bethesda: SANS. Available from: http://web.cs.ucla.edu/~miodrag/cs259-security/ranum94thinking.pdf

Sangster, M. (2020). When it comes to cyber security, ignorance isn't bliss – it's negligence. *Network Security* 2020 (12): 8-12. Available from: **https://doi.org/10.1016/S1353-4858(20)30140-9**

Sjarif, N. N. et al. (2019) 'Endpoint Detection and Response: Why Use Machine Learning?', *2019 International Conference on Information and Communication Technology Convergence (ICTC 2019).* Jeju Island, 16-18 October, New York: Institute of Electrical and Electronic Engineers (IEEE). *283-288*. Available from: https://doi.org/10.1109/ICTC46691.2019.8939836

Varonis. (2021) 2021 Data Risk Report Financial Services. Available from: https://info.varonis.com/hubfs/docs/research_reports/2021-Financial-Data-Risk-Report.pdf [Accessed 12 June 2021].

Verizon. (2021) DBIR 2021 Data Breach Investigations Report. Available from: https://www.verizon.com/business/resources/reports/dbir [Accessed 12 June 2021].