Great feedback and insight from everyone. End users in any organization are key to ensuring safety on the network, either on the Local Area Network (LAN) or connecting from a Virtual Private Network (VPN). Companies need to protect users because many of them are not tech savvy and things do fall through the cracks, even if they have had training.

Companies need to look at the bigger picture by ensuring that the various layers are protected within the network by using Web Application Proxies (WAP) (Microsoft, 2016) as one example to protect web applications such as Outlook on the Web (OWA) used by Exchange. This can assist in preventing attacks such as cross-site scripting (P. Wurzinger, C. Platzer, C. Ludl, E. Kirda., C. Kruegel., 2009). In addition to network segmentation and making use of a Next Generation Firewalls (NGFW), each of these devices do have limitations and when you are dealing with large networks, a Security person or group of people cannot monitor everything that comes in and out of the network manually.

IT departments should look at implementing additional solutions such as Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) to be one step ahead of an attacker and consider an Antivirus solution that also sends log files to an off-site location which can be a cloud based SIEM solution. Traditional SIEM solutions can also be deployed which also has its pros and cons but will help the relevant teams look at trends in the traffic and give the security and IT team insight into what is happening on the network.

If an infection does happen on an end users’ machine where they possibly plugged in a USB device or opened an email attachment that device can be isolated immediately and dealt with.

To conclude, the human factor is always the weakest link in the chain in any organization. Companies should not worry about the cost of a solution or multiple solutions as the cost of data theft out ways the cost of a security solution and a company’s reputation.

References

Microsoft. (2016) Web Application Proxy. Available from: <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn584107(v=ws.11)#:~:text=Web%20Application%20Proxy%20is%20a,from%20outside%20the%20corporate%20network> [Accessed 28 September 2021].

Wurzinger, P., Platzer, C., Ludl, C., Kirda, E. & Kruegel, C. (2009) SWAP: Mitigating XSS attacks using a reverse proxy. *ICSE Workshop on Software Engineering for Secure Systems:* 33-39. DOI: https://doi.org/10.1109/IWSESS.2009.5068456