Discussion – 1 Peer Response:

Re: Initial Post

by Demian Berisford-Maynard - Saturday, 25 June 2022, 4:10 PM
Hi Gokul

I really loved your initial post. Perfectly phrased, and I loved your bullet-point list.
I have a question though. What is the best methodology to identify and address insider threats within small-medium sized enterprises?

I have noticed a sustained threat from it over the last ten years or so. Me personally I don't trust the neural network / A.I. approach to identifying insider threats (Yuan et al, 2018; Kim et al, 2020)

Kind regards
Demian

References

Kim, A., Oh, J., Ryu, J. & Lee, K., (2020) A review of insider threat detection approaches with IoT perspective. *IEEE Access*.

Yuan, F., Cao, Y., Shang, Y., Liu, Y., Tan, J. & Fang, B. (June, 2018) Insider threat detection with deep neural network. In *International Conference on Computational Science* : 43-54. Springer, Cham.

In reply to Gokul Kurunthasalam

Re: Initial Post

by Amit Pahuja - Monday, 27 June 2022, 7:14 AM
Hello Gokul,

I liked your detailed post covering digital enterprise and Cyber challenges to bricks and mortar SME wanting to go digital.

I second you regarding the Insider Threats - Businesses of all sizes face a serious security risk from internal staff. Employees make workplace files easily accessible by using the same password for both their personal and professional accounts, and fall victim to phishing scams that deceive them into divulging their login credentials.

Also, would like to go couple more attacks to the list for bricks and mortar SME wanting to go digital – Internet of Things (IOT) and Point of Sale (PoS) attacks.

Thanks and Regards

-amit

In reply to Gokul Kurunthasalam

Peer response

by Ashok Kumar Shanmugam - Wednesday, 29 June 2022, 3:03 AM

Hello Gokul,

I liked your detailed post, and more importantly highlighting the mobile security threats.

Mobile security protects smartphones, tablets, and laptops using strategy, infrastructure, and software. Mobile device cybersecurity includes protecting device data, endpoints, and networking equipment. As mobile devices replace desktops, attackers will target them more.

Why Is Mobile Security Important?
As more people travel and work from home, mobile devices have become more common, even among corporate employees. Internet use was once limited to desktops, and only travelling employees had laptops. Mobile devices are the preferred way to browse the internet, and mobile traffic has surpassed desktops.
Mobile devices have a larger attack surface than desktops, making them a bigger security threat. Mobile devices are vulnerable to physical and virtual attacks, but desktops are immobile. Administrators must worry about physical attacks (theft and loss) and virtual threats from third-party apps and Wi-Fi hotspots (e.g., man-in-the-middle attacks). Administrators can better control network and endpoint security on stationary desktops. Users can root, add, and lose mobile devices.

Reference:
Proofpoint.com why is mobile security important. Available at: https://www.proofpoint.com/us/threat-reference/mobile-security [Accessed 27 June 2022]