



The Cyber Savvy Café

Ssn 2 Ep 1: Top 3 Issues that Make Remote Workstations a Target, Pt 1

Remote working has been on the rise in recent years and exploded in 2020 during the pandemic. Find out why remote workstations are a popular target for hackers--and what you need to do to protect the corporate network from a breach through this mostly-unprotected back door.

SHOW NOTES

:47: Let's define what we mean by "remote working".

1:18: We were working remotely for years before the pandemic, but remote working has changed since 2020.

2:36: We're making an assumption that people are working on a company-provided equipment that's managed by an IT dept.

3:43: Why do remote workstations put corporate networks at greater risk than a traditional office environment?

3:50: Discussion of article about a number of laptops that were unknowingly infected with malware, and what happened when those laptops went home during the pandemic.

4:43: What are the top 3 reasons why remote workstations are a hot target?

4:55: Number One, No corporate firewall.

6:23: Discussion of best practices—and inherent dangers—when setting up your router, setting the password, and hiding the SSID.

9:25: What do people need to do in order to know if their firewall is secure?

10:00: If you have employees working remotely, what do you need to do?

10:59: What if your employees are working remotely using public wi-fi?

Downloadable pdf from media.defense.gov, "Securing Wireless Devices in Public Settings":

https://media.defense.gov/2021/Jul/29/2002815141/-1/-1/0/CSI_SECURING_WIRELESS_DEVICES_IN_PUBLIC.PDF

12:34: VPNs and inherent challenges. What is an "always on" product?

14:18: Number Two: Segmentation; dividing your network into separate networks that don't allow lateral movement, and what is lateral movement?

16:10: What happens if you're not segmented and your VPN is activated?

17:20: Discussion of an article about hackers who targeted government employees through an active online aerobics presence.

18:45: How much effort and time are hackers willing to put into gaining access into your network?

19:00: Discussion of today's hackers. Gone are the days of the solitary hacker working out of a basement.

20:20: Discussion of a guy that built a machine for reverse hacking and how he uses it.

End of Part 1. Catch Part 2 for the rest of the discussion!

Your hosts: Rex Nance and Penny O'Halloran of East Atlantic Security, LLC @ <https://EastAtlanticSecurity.com/>

Voiceover Artist: Paul Kadach at www.voices.com