COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 4. April 06, 2023 Security Checklist: Four Strategies to Keep Ransomware at Bay

By Jane Anderson

Ransomware is a huge problem: some two-thirds of 5,600 IT managers surveyed across all industries in 31 countries said they had been hit by ransomware in the past year.

Of those who had been hit, 65% said the attackers succeeded in encrypting the data, with an average cost of $1.4 million for remediation, said Chris McCormack, network security specialist at security firm Sophos.

Still, companies can deploy strategies that are effective against network penetration and ransomware, McCormack explained in a recent webinar.[1] He recommended four strategies to guard against ransomware attacks: (1) switch to Zero Trust Network Access (ZTNA) from a virtual private network (VPN), (2) micro-segment the network, (3) block remote desktop protocol (RDP) access, and (4) require multifactor authentication

Of those strategies, McCormack's top recommendation is to employ ZTNA: "No one solution can do more for your network security than switching from old-school VPN to ZTNA if you have remote workers outside your corporate perimeter," McCormack said.

Understand How Attacks Unfold

In order to protect an organization from ransomware attacks, it's imperative to understand how they work and how they can be stopped, McCormack said.

"So first, these attacks need to get onto your network. And this is typically done in a few ways," he said.

Intruders can make it onto an organization's network in the following ways:

- Exploiting a vulnerability, possibly in a VPN client or server.
- Exploiting a system or an Internet-of-Things device that's exposed to the internet.
- Harvesting legitimate credentials obtained by brute force attempts to guess a password.
- Leveraging legitimate credentials purchased on the dark web.
- Obtaining legitimate credentials via a phishing or malware attack.

Once the bad actors have gained entrance to the network, their next step is to move around inside of it, McCormack said. "Once they get an entry point, the focus becomes one of moving laterally to explore the network, figure out what's there, where is the data, how is the network structured, and really just do some network reconnaissance."

Finally, they will strike, he said. "After disabling or carefully bypassing security measures, which is what they are going to do on most networks, then it all becomes about stealing data, encrypting it, and extorting the organization to pay a ransom to get their data and systems back."