Top Ten Insider Cybersecurity Threats and How To Handle Them

Here are the top 10 insider cybersecurity threats you should be worried about:

1. UNAUTHORIZED ACCESS TO A COMPUTER

Some computers have sensitive information on them, and access is limited for a reason. Any unauthorized access should be noted and looked into promptly to ensure there's a valid reason for someone to login.

If it turns out this individual should have access, it should be done via the IT department following standard procedures. If the unauthorized access is suspicious, then an investigation should ensue.

2. UNAUTHORIZED COMPUTERS ACCESSING THE INTERNET

Not every system should have unfettered access to the Internet, particularly if they house sensitive data or mission critical functions. Scanning for this activity and either blocking access or restricting it to approved connections prevents the bad guys from getting in and data from leaking out.

3. UNAUTHORIZED DEVICES ON THE NETWORK

Whether it's someone logging into the WiFi on their personal device or installing a networked printer without following proper IT protocols, these seemingly innocuous actions could allow uninvited guests into the network or facilitate the escape of private data.

Clamp down on extracurricular devices by monitoring the network for any new IP addresses and alerting IT when they make an appearance.

4. UNAUTHORIZED LOCAL ADMINISTRATORS

Local administrator accounts may be used to bypass domain-level security. With administrative access, all kinds of bad things can happen. Unauthorized or unlicensed software could be installed (including accidental or intentional execution of malware), profiles of other users can be accessed, and important settings can be changed that could both impact performance and create security risks.

Verify if the new local administrator account is authorized and lock down access in the future to prevent local administrative access from causing trouble.

5. UNINSTALLED SECURITY PATCHES

Vendors are constantly rolling out updates to patch security holes and shore up defenses, but if they haven't been installed on every single applicable device within the corporate network then you're operating with major weak points.

Perform regular automated scans comparing the current version of each device's operating system and software to what should be installed. If anything is lagging behind the current versions and patches, upgrade things as soon as possible to limit exposure.

6. IRREGULAR LOGIN ACTIVITY

Even if an employee has authorized access to a particular device or application, logging in afterhours may be a red flag that they're up to no good and are trying to hide this activity from coworkers.

Monitoring for anomalous logins outside standard timeframes can initiate an investigation into whether this was harmless and justified behavior or if something more nefarious is afoot.

7. ADDING NEW USERS TO THE NETWORK

While this is often 100% legitimate, each new account should be vetted and confirmed as a standard preventative measure. Getting alerts about any new user raises the visibility of these account creations and trigger a check in with the authorizing administrator.

8. ADDING A NEW PROFILE TO A COMPUTER

Similar to the previous potential threat, a new profile may be totally on the up-and-up, but additional profiles being created may be a sign that an employee is accessing a computer they shouldn't be using. Scanning for these events and investigating them ensures the access is warranted.

9. SPOTTING NEW BROADCAST WIRELESS NETWORKS

With routers small enough to fit in your pocket and the ability for almost any smartphone to also serve as an access point, it's simple for someone to introduce a new WiFi network within an environment. Proactively scan for these network events and block access unless they're authorized.

10. OPEN PORTS

While an open port itself isn't problematic, it opens the environment up to a number of risks. It increases the "attack surface" of the network while allowing the programs listening and responding to them to transmit sensitive information or expose information about system architecture or security protocols.

Detecting these ports and locking them down strengthens network security and plugs holes before they become problems.

Keeping up with internal threats

With so many potential threats that could emerge within the networks you're managing, it may seem like a daunting task to keep up with them all and commit the time and resources to continually checking up on these items.