Inventory of All Connected Assets Can Thwart Cyber Attacks

As businesses use more and more devices in their operations, their vulnerability to cyber attacks increases exponentially.

Some employees may have a work smartphone, a laptop for the road and a desktop unit for when they work in the office. And there may be other systems and assets that are connected to the company network and the internet.

That's why it's important for all organizations to have a thorough inventory of everything that may be connected to their network. Every device is essentially another door for hackers to exploit.

Not only that, but you likely subscribe to multiple cloud services, which can also be used to gain entry into your database.

If you don't have a full accounting of all your connected devices and services, you leave your business exposed to a cyber attack. You may be slow to detect an attack, as well — and the longer you wait to respond, the more damage the hackers can cause.

To protect your organization, you can start by making a list of all of the following that may be connected to your network and the internet:

- Computers and other hardware
- Software
- Devices like smartphones and tablets
- Data
- Cloud services like storage and accounting systems
- Internet of Things devices
- Industrial IoT devices.

Once you have a full inventory of the above, you can take steps to secure them and set up each device and service for monitoring. For example, you can ensure that each service and device is up to date on its latest security updates and patches.

Obstacles

It may seem like a simple task to put your list together, but it's important to understand the factors that can result in gaps, such as:

Employee turnover — If you are not thorough and fail to retrieve all of the devices a former employee was assigned, you may have items out there that still have access to your network.

Also, if you allow employees to use their own devices, you'll need to take steps to ensure they can't access your database after they leave. Additionally, failing to disable an outgoing employee's accounts also leaves you vulnerable to a possible attack.

Remote work — With more employees working from home, more company-owned devices are away from the office. And you may not know who is accessing your system from those devices.

Additionally, remote workers are more likely to connect to an unsecured network and send company data to their personal e-mail, computer or smartphone.

Lack of resources — Many companies may not have the personnel or the time to monitor and analyze each device and service they have out there. And some tools for monitoring devices can be expensive.

What you can do

The most straightforward way to keep track of a business's network devices is to do it manually, but this is only an option for small firms that don't have many connected items. Walk around the office and take note of each device that is on the network.

You'll know too which employees have company smartphones or which ones are connecting to your database using their own phones.

The main benefit to manually managing network devices is that you get to save money, but it can often get tedious. If you want to check the detailed status of a network device, then you'll have to do so directly through the computer that it is connected to.

Larger firms with multiple devices and accounts can use software that monitors all connected devices. The software will regularly scan all of devices connected to the organization's network and will catalog all of them. This can be extremely efficient for companies that have many items connected to the networks.

###