Are Unknown Devices the Way in to Your Organisation?

Forward-thinking businesses are embracing new tech with open arms. As a result, they're seeing business efficiency, staff satisfaction, and profits soar, but what about when things go wrong? Your team could be carelessly plugging unknown devices into your network, lowering the drawbridge and inadvertently giving threat actors access to your data.

According to the Online Trust Alliance, 2017 was the 'worst year ever' in terms of data breaches, increasing from 82,000 incidents in 2016 to over 160,000.

Yet, we still see organisations, small and large, failing to make the necessary security improvements.

Many of these attacks could have been prevented with even the most basic security measures, such as implementing patching schedules, training staff on the dangers of poor passwords and phishing attempts, or limiting access to sensitive data. However, even with the most robust security measures in place there still may be a potential security issue: the issue of the unknown device.

The security issues surrounding connected devices

The number of internet-connected devices is growing rapidly. Everything has suddenly become 'smart', from your TV and fridge to your light bulbs and doorbell. The business world has also been quick to adopt these devices: printers, scanners, CCTV, coffee machines and voice assistants have all benefited from added connectivity.

Companies are more than willing to plug these directly into their networks in anticipation of the possibilities.

However, such devices may offer a point of entrance for a cyber-attack that compromises sensitive data or financial information. An unnamed American casino, for example, had its confidential high roller list stolen after a hacker broke in through the internet-connected thermometer in a fish tank.

More and more organisations are also starting to embrace 'bring your own device' policies: if an infected personal device was to connect to your internal network then malware could potentially spread across it and attackers may be able to access your company's sensitive information.

With so many assets connected it's easy to lose track.

Uncovering the unknown

Uncovering any unknown devices is an essential first step to keeping your business protected. You can do this manually, but you'd be surprised how many tests we've conducted where we've found that a supposedly disconnected device is not only connected, but also extremely susceptible to attack.

Cybersecurity companies can assist with this and estate discovery tools have been developed to uncover what is actually connected to your network, showing not only the devices you may not have known about but also the potential vulnerabilities within them.

Improving your situation

Making the necessary security improvements is the next step and keeping core systems running, as well as protecting your company's critical information, is key. Ask yourself: what can't my business live without in the event of a cyber-attack?

You must prioritise your budget accordingly to ensure business continuity. This could include implementing more robust privilege controls throughout your organisation, segregating important information from the main network, isolating any vulnerable devices behind firewalls, increasing employee cybersecurity training or by patching and changing default passwords on any rogue device.

Testing yourself

It's then essential that you test these security measures to ensure they are robust. There are a number of options available, ranging from a vulnerability scan to a penetration test, right up to a full scale red team exercise, which combines physical and IT-based attacks.

A good cybersecurity firm should work with you to understand your needs, then provide clear instructions on remedial action, as well as helping you to translate any wider recommendations for upper management.

No matter which method you choose, when it comes to protecting your business against the threat of cyber-attack, you don't want to be left in the dark.

For more information about uncovering unknown devices, and other cybersecurity advice, contact a member of our team.

This blog originally appeared in Business Cloud