GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Donlon, Meaghan

Title: "IoT Risks for SMB Security and How to Manage Them"

Website: IoT World Today Blog

Organization: IoT World Today

Date: 27 June 2019

URL: https://www.iotworldtoday.com/2019/06/27/iot-risks-for-smb-security-and-how-to-manage-them/

Accessed: 19 Oct 2019

Synopsis: IoT poses a unique SMB security risk as smaller-sized organizations often deploy connected devices without the IT resources of larger enterprise companies.

As the use of Internet of Things devices continues to increase, so too does the level of security risk, especially to small business. A report by Juniper estimates that there will be 50 billion IoT devices by 2022.

There are certainly many benefits for businesses that implement IoT, including improvements in efficiency and logistics, as well as convenience. But with many small businesses operating on tight margins, the speed with which these devices are becoming standard is bringing with it a security challenge for SMB IT teams.

Operating without specific IoT security measures in place puts data at risk, but now everything, from lights, printers to speakers are multiplying the attack surface. The number and type of devices will vary according to the company, but there are a number of universal precautions that SMBs can take to minimize the risks IoT can pose.

IoT World Today

(https://www.iotworldtoday.com)

SECURITY (https://www.iotworldtoday.com/subject/security/)

IoT Risks for SMB Security and How to Manage Them

IoT poses a unique SMB security risk as smaller-sized organizations often deploy connected devices without the IT resources of larger enterprise companies.

Written by Terry Hearn 27th June 2019

As the use of Internet of Things devices continues to increase, so too does the level of security risk, especially to small business. A report by Juniper estimates that there will be 50 billion IoT devices by 2022.

There are certainly many benefits for businesses that implement IoT, including improvements in efficiency and logistics, as well as convenience. But with many small businesses operating on tight margins, the speed with which these devices are becoming standard is bringing with it a security challenge for SMB IT teams.

Operating without specific IoT security measures in place puts data at risk, but now everything, from lights, printers to speakers are multiplying the attack surface. The number and type of devices will vary according to the company, but there are a number of universal precautions that SMBs can take to minimize the risks IoT can pose.

Strong Passwords

Possibly the oldest security mantra is to make sure that strong passwords are used at all times, on all devices. IoT makes this more relevant than ever before. In many cases, device makers pride themselves on the simple setup processes of their products. As convenient as this can be, the result is that many devices are installed with default passwords.

Knowing this, all hackers would need to do is perform a quick search to find gain access. A recent report by Avast found that four out of 10 smart homes had at least one vulnerable device. If this risk is not dealt with, similar numbers of businesses could be vulnerable to an entirely preventable security threat.

Endpoint SMB Security

The makeup of the modern office space is changing rapidly. Just a few years ago mobile working was a rarity but is now set to account for 43.3% of the worldwide workforce by 2023. Alongside this, the popularity of Internet of Things (IoT) devices is projected to grow in the United Kingdom from 272 million connected devices in 2018 to 625 million in the next five years. What does this mean? More and more endpoints.

The first step is to consider carefully when adding new devices to the network if the benefit of the device is worth the SMB security risk of adding another endpoint. Any device that can connect to your network needs to be correctly set up and secured to avoid it becoming a point of entry for an attack. This includes everything from the personal devices of remote workers to smart speakers.

Next, ensure that antivirus software and firewalls are updated and in place to monitor and deal with any suspicious activity. Next, while many of IoT devices are designed to easily connect to a network, it can be easy to forget to change the default password to something more secure — the equivalent of leaving your front door unlocked.

Beyond standard security, IoT measures should go even further by including tools to identify phishing emails, WiFi scanners and encryption for sensitive files.

Patches

Regular security updates are a common sight with modern technology, and while it might be an annoyance to install when you are in the middle of something, they are a crucial security step. Aside from seasonal refreshes, numerous security patches are likely to be made available during the course of a year. Most will be produced to fix a known security vulnerability, meaning that those who click 'remind me later' are putting their data at unnecessary risk.

In addition to laptops, servers and personal devices used for mobile working, the rapid increase in IoT devices poses a challenge for SMB IT teams, which may consist of just one or two people. Many companies may adopt a cycle process to ensure every device is updated at regular intervals. But as patches could arrive at any time, this strategy could see a crucial delay between the patch's release and its implementation.

The solution is delegation. If staff take responsibility for their own devices, then IoT can be addressed as part of a reduced workload for dedicated IT staff.

Limit Access Permissions

A very simple way to protect data is to limit the number of people who have permission to access it. Hackers might be able to take control of an account using a phishing attack but if that user does not have access, the data will remain secure and the hacker will have to find another route.

The key here is for companies to not give out admin privileges to all members of staff, regardless of seniority, unless access to the data is essential to their work. This applies to freelancers, temp workers and former employees, who should all have their permissions revoked as soon as their work is completed.

Staff Training

In a majority of cases, data breaches are not the result of a targeted attack. More than 80% of data breaches are actually the result of human error. While security solutions are still important for scanning emails and removing suspicious files, effective small business security needs to adopt a multi-layered approach that includes training on cybersecurity, best practices and company policy should a breach occur.

Training must apply to all staff, from directors to freelancers, regardless of their position in the company. If everyone who has access to the company's network has the same level of basic training, it will help to ensure that passwords are strong, two-factor authentication is applied where possible, updates are installed, and potentially suspicious activity is flagged.

By providing regular training and security updates, staff will become more comfortable with best practices and will be less likely to make a mistake, but they will also be better equipped to react should a breach occur. These processes can also help to keep security as a front-of-mind concern for everyone, rather than something that is only the concern of IT staff.

Backing Up

With huge corporations, governments and travel networks as victims, most headline-grabbing cyberattacks of recent years have been ransomware, a type of attack that goes unnoticed until a message appears demanding payment for stolen files.

Faced with this situation, there is a temptation to simply pay the ransom. Yet even this is a risk as half of those who agreed to pay did not get their data back. Thankfully, one preemptive measure can mitigate this threat.

Keeping secure backups, either held in the cloud or on a separate network, will reduce the threat of losing data to a ransomware attack. Should you suffer an attack, the infected devices will need to be restored, but your data will remain secure.

Conclusion

With large companies suffering data breaches on what seems like a daily basis it can feel like there is nothing that SMBs can do other than hope they are overlooked. But the best way to improve SMB security is to build a culture of commitment to reducing human errors and building a better understanding of security.

As security companies and hackers continue to try and outmaneuver each other, the landscape can change quickly. For this reason, it is vital that SMBs keep up to date on the current security trends and best practices to help stay ahead of the curve. Not only will regularly checking the tech news help to build a broader understanding of the field, but it will help to improve your security policies and be alert to the latest threats.