www.pipelinepub.com
Volume 17, Issue 5

Securing Connected Home Devices

By: Marijus Briedis

With so many people remotely working, today's typical office looks nothing like it did before. In fact, it might be corporate chaos in the living room. This new approach to working from home introduces new risk from a technological perspective, as there are now hundreds of devices accessing corporate networks.

The days of being able to control every element through Active Directory and still stay safe are over. And as the lines between work and home continue to blur during and after this period, employees will increasingly use their personal devices while working from home. Many may also switch between personal and company-issued devices to perform work-related tasks.

To add to the chaos, chief security officers for companies around the world must deal with a number of unaudited, uncontrolled, and yet interconnected Internet of Things (IoT) devices that employees own.

In 2020, home security cameras, smart TVs, fridges, robot vacuums, baby monitors, and doorbells all became a part of a company's peripherals (if we can still apply the term to today's situation). All these devices have become gateways to the corporate world—in hackers' eyes, at least. This is because, first, most of these devices are not even password protected; second, they are connected to the same network the user's computer is; and, third, there are still no standard controls or protocols for IoT developers to follow.

So, the present is a new opportunity both for IoT innovation to blossom and for cybercriminals to thrive.

Big Brother at the home office

George Orwell's dystopian concept of Big Brother might not be that far-fetched, as individuals and businesses now all rely on devices capable of interacting, recording, and tracking. And these consumer devices are keeping CSOs around the world awake at night.

Recently in Singapore, hackers broke into security IP cameras and shared the footage online, specifically on nefarious sites. The videos featured people in footage they might not have wished to be revealed, including mothers breastfeeding their babies and people working in their underwear.

The victims' faces are not blurred, which makes them easy to identify, especially with facial recognition technology. Such technology, offered by developers like Clearview.ai, is so advanced that it can scrape a decade-old picture from the Internet and link it to the person. This kind of hack poses a lifetime threat to the victims. Businesses fall under the same risk, as home cameras can be used for corporate espionage—bad actors can easily observe what employees are typing on their devices.

Gaining access to an IoT device is relatively easy. In 2019, credentials of more than 3,000 Ring users ended up online after a credential stuffing attack. People tend to use the same credentials for most of their accounts, so attackers simply had to match the previously leaked passwords to take control over the device. To make it even easier for hackers, users often keep the manufacturer's default password.

Dozens of stories about hacked baby monitors have been made public. Hacking them isn't difficult either. And, because our homes have become our offices, baby monitors are perfect for recording business calls.

Aside from privacy and security concerns, the bigger danger is the fact that hackers can harness interconnected devices to form a botnet—and IoT devices are often used for just that. One of the best-known botnets is Mirai, which caused a lot of trouble in 2016 and still exists today. When we have interconnected devices, the virus spreads from our home devices to our work devices, ultimately infecting corporate servers.

Because the IoT industry is in its infancy, such devices have the potential to become cybersecurity risks. In the rush to bring them to the market, most manufacturers simply ignore the notion of security.

Making IoT more secure

Interconnected IoT devices are expected to lead to the fast emergence of dominant digital ecosystems. As a result, a breach of a single element will present new challenges for mitigating the resulting wildfire.

That's why Japan sought to secure IoT devices before the 2020 Summer Olympics in Tokyo, to avoid malware like Olympic Destroyer and similar attacks. The government requested employees of the Japanese National Institute of Information and Communications Technology (NICT) to hack into people's IoT devices by using password dictionaries and default passwords.

The result of this Japanese initiative should have been a list of unsecured IoT devices so that the authorities and Internet service providers could take measures to secure them. What followed was public backlash.

On the other side of the universe, on July 16, the European Commission launched an IoT antitrust competition. Following this initiative, Germany, South Korea, and the United Kingdom developed policies to mitigate the harmful impact of IoT security vulnerabilities.

Governmental efforts only highlight the problem, but the solutions must come from the tech industry itself. "IoT security" is considered an oxymoron by some, yet basic protection measures are available, though rarely used by home users.

Immediate fixes

When Japan raised the specter of hacking consumer IoT devices, it addressed the most common mistake users make, namely keeping the default passwords or using the same password for multiple devices and accounts. Once leaked, the password gives access to the full ecosystem of the user's accounts, including those related to their work.

A study by the password manager NordPass revealed that there are 10 billion records on the dark web ready to be picked up by bad actors. The first thing that needs to be done is to require employees to create unique passwords for each and every device they own. To avoid the hassle of remembering them all, using a password manager is the best solution.

Network security combo

VPN minimizes the problem of vulnerability when devices use unencrypted traffic. A VPN connection set up on the router protects the network against man-in-the-middle attacks. This makes targeted botnet and DDoS attacks much harder to launch, too. On the other hand, devices might become undiscoverable when trying to manage them outside the network.

A VPN can also prevent home devices from participating in botnet attacks. If you set up a VPN on your router, you can connect and secure any number of gadgets with a single device slot. Any device that connects to it will automatically be private on the Internet.

There is one category of IoT devices that should have a native VPN app on at all times: smart TVs. These days, TVs are used to access files in the cloud, shop online, or even participate in meetings. They store massive amounts of financial data. Attackers could use your smart TV to download malware or turn on your webcam. A VPN app encrypts online activities to keep online snoopers away.

As of now, there is no silver bullet, as it's become impossible to track everything within such scattered peripheries, but these steps are a good starting point.

Advancing IoT technology

Verified Market Research estimates that the IoT market will be worth $1319.08 billion globally by 2026, at a CAGR of 25.68 percent. With technologies like digital twin, artificial intelligence, and 5G, it will receive a major boost. At least in the short term, IoT developers will focus on the core needs, such as health and safety as well as equipment monitoring.

AI-powered IoT might expect another stimulus coming from the European Union, as it's planning to force tech companies to open up their data to European SMEs that use their platform for doing business.

This is a very significant trend to follow as, if it succeeds, the EU will lay the foundation for other countries to follow suit, as they did with the introduction of the GDPR.

As of today, IoT is moving towards edge computing. More data is expected to be processed by the devices themselves or by local systems, rather than through a data center, which will be done for the sake of efficiency.

This means that IoT security will continue to be an evolving concept—and that *security* must be an integral part.