nuspire

WHITE PAPER

Three Proven Tips for Securing Home Networks and the Internet of Things (IoT)

The Recent Impact IoT Has Made on Your Attack Surface

During this pandemic, an estimated 75 million Americans are working from home[1] – creating tens or hundreds or thousands of remote work environments for your organization. Even though many are slowly going back to the office, the work-from-home model will remain a preference for many organizations for a long time. Everyone is on the internet – for meetings, email, shopping, home schooling, live exercise workouts, video games and entertainment. Add smart devices to the list – voice-activated music/speakers, home monitoring solutions, refrigerators, thermostats, TVs and security systems. By the end of 2019, there were 7.6 billion active Internet of Things (IoT) devices[2] — and many of them are collecting data. This new IoT frontier needs remedies for challenges introduced by today's remote work environments:

Protecting far more endpoints that require IoT cybersecurity expertise

Defending and educating unaware home office workers

Finding and fixing vulnerabilities, some of which may already be exploited

Covering all the necessary IoT endpoints with stretched IT resources

Employing managed security services addresses many of these challenges to:

- Reduce the risk of breaches and loss of sensitive information
- Keep up with changing home office conditions and personal device requirements
- Expand your cybersecurity team and capabilities without hiring additional people or increasing capital expense

WHY IS IOT A CHALLENGE?

Think of the smart home devices as eavesdroppers on your conversations and everyday life events. The riskiest IoT devices are voice activated and connected to home command central. They collect intelligence and store data for future use – on a network that is now being used for company business. In addition, the connected devices in a home are competing for bandwidth, potentially slowing down or even disrupting workflow.

IoT devices in the home are often "out of sight, out of mind" because they make our personal lives easier. Yet, IoT devices can be hacked in seconds or minutes, exposing conversations or providing entry to an organization's network.

Tip 1: Focus on Visibility

Visibility is one of the most important components of a security program. IT teams do their best, despite all the unknowns of home environments. The challenge in early 2020 was that many companies did not have solid remote work policies or guidelines. As a result, many workers chose to use personal devices that were not configured to meet company standards.

Every home likely has unique equipment and diverse configurations. Setting up remote access and troubleshooting user problems take time. Trouble tickets involve chats, calls or online meetings – potential ways that IP addresses, passwords and other intelligence can be leaked through data-collecting IoT devices. Rolling out tools for tens or hundreds or thousands of new endpoints is not a simple undertaking – home environments present a scale issue that no one saw coming for a situation that has no playbook.

IT teams need visibility to see what's on the wire and what's on each device – no matter the device origin or whether it is personal or company-issued. If a device is on the internet, it poses a risk.

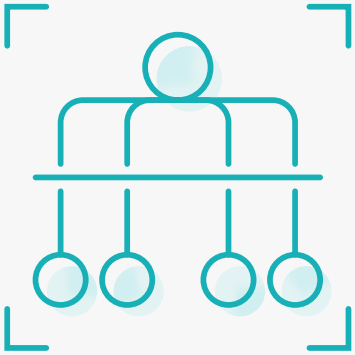
WHAT TO DO NEXT

Conduct a thorough remote breach assessment for each home environment to obtain a point-in-time picture. The findings in the assessment report show the complete stack, and a risk profile, to help you make better decisions. Along with a breach assessment, follow these best practices to improve cybersecurity:

- Engage a managed security services provider (MSSP) to provide ongoing visibility through monitoring and reporting tools that can be activated swiftly with no disruption
- Prioritize the vulnerabilities listed in the breach assessment and create a plan to fix them
- Establish a threat hunting strategy to expand visibility and strengthen your defenses by being proactive

Tip 1: Focus on Visibility

USE CASE



Effortless Remote Breach Assessment

An IT manager recently called Nuspire because his organization had an incident that needed immediate attention. Unfortunately, the company's current security services provider couldn't provide any insight into the situation, so he didn't know what to do.

Within minutes, the IT manager installed the Nuspire breach assessment application. After certifying the application, the Nuspire managed detection and response team began receiving data – no time wasted forwarding logs. Within a few hours all devices, including two key data center servers, and applications were identified and scanned.

The information in the assessment clarified next steps: create a threat hunting strategy and design custom alerts and custom reports. The initial threat hunt uncovered two attacks originating from two separate countries. The Nuspire remediation team leapt into action to halt the attackers and lock down entry points.

Tip 2: Secure Rampant IoT Devices

Organizations do not have control of home office networks including the DSL, cable, Wi-Fi or routers employees use. IT teams don't know if devices are patched and updates are installed. Or if a virtual private network (VPN) on a company laptop is turned off, switching the device to Wi-Fi. Or if a VPN is spoofed, creating a tunnel for bad guys to access the modem. This wild west situation presents many potential vulnerabilities.

Right now, external threat actors are more active than ever. In 2019, there was a 300% increase in IoT device hacks[3], making unprepared home network devices a potential easy target for cybercriminals. The number of IoT hacks in 2020 has surged. In Q1 2020, the Nuspire analysts saw executable and linkable (ELF) variants targeting IoT devices in attempts to spread the Mirai botnet. Often attackers scan for IoT devices with open SSH or Telnet ports to brute-force access into them. After they gain shell access, the attackers download a payload that adds the device to the Mirai botnet.[4] From one foothold, a botnet can spread rapidly throughout a network.

In addition, internal threats are on the rise because many organizations haven't educated their employees about how to be safe online and how to keep the organization protected while using the internet. For example, password hygiene is critical. Passwords may be too simple. Or the same password is used for multiple accounts or worse, shared by multiple workers. Further, COVID-19-themed offers pop up regularly, tempting people who want to stay informed or buy protective products to click on malicious links. And, phishing has increased 100% since December 2019.[5]

Not all risk can be removed, of course. But it is possible to define your organization's acceptable level of risk, allowing you to make cybersecurity decisions based on cost-benefit.

A recent Nuspire breach investigation uncovered a compromised Google email account ID on a client's company laptop that was used for both business and personal email. The user, not knowing the ID was compromised, used it to access the employer's conferencing application, which was highjacked. The conference room exposure opened the door to malware that eventually took over the phone system.

ABOUT THE MIRAI BOTNET

Mirai is malware that infects networked devices and turns them into bots. Infected devices scan the internet for IP addresses of IoT devices, searching for vulnerabilities such as factory-default usernames and passwords. Using the power of thousands or millions of IoT devices, Mirai is behind some of the largest distributed denial of service (DDoS) attacks perpetrated since 2016.

Tip 2: Secure Rampant IoT Devices

WHAT TO DO NEXT

Patch devices to update signatures and operating systems and be sure to provide workers with security awareness training that covers topics such as social engineering attack types, password rules, breach etiquette, reference documentation, applicable regulations and roles/responsibilities.

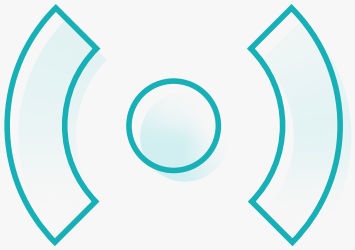
Additionally, implement 24x7 managed detection and response, along with remediation runbooks, to give your IT team the tools they need to defend against threats. The right tools provide:

- Visibility all the way through to each endpoint, making sure each one is the actual endpoint and not an unknown source disguised as a known endpoint
- Continuous monitoring of networks, devices and applications (another overlooked target), allowing security events to be ingested and analyzed to speed response
- Consistent device scanning to make sure data isn't exposed

Imagine learning, like one Nuspire client, that 1,000 company devices had 2,100 IoT communication points. The best way to bring these vulnerabilities to light? Endpoint protection – which reveals risks ranging from laptops communicating with the internet via undetected open ports to hackable crock pots.

Tip 2: Secure Rampant IoT Devices

USE CASE



Protecting Remote Workforce Endpoints

An IT director migrated to a remote workforce with 1,100 endpoints. A single IT person dedicated to overseeing the company's managed detection and response (MDR) was experiencing alert fatigue. Then the organization was hit with a ransomware attack. A multi-million-dollar demand was negotiated to $75,000, but the IT director wasn't confident that his network tools could perform an adequate job and reduce risk sufficiently.

The IT director's peace of mind has improved considerably since the company rolled out the following Nuspire solutions:

- **24x7 endpoint detection and response**
- **Security information and event management (SIEM) technology**
- **Security operations center (SOC) and network operations center (NOC) expertise**
- **Always-on MDR, incident response and unlimited remediation**

Tip 3: Close IoT Cybersecurity Gaps Without Hiring Additional IT Staff

Just when cybersecurity is more important than ever, already lean IT staffs are facing potential budget cuts. One survey found that 49% of companies are considering layoffs, more than one-third are freezing new hires, 11% have conducted permanent layoffs and another 7%, temporary layoffs.[6]

Organizations need to manage costs, but at the same time, cybersecurity specialists need help. Most companies have few unplanned IoT devices in office settings, but IoT considerations in home environments are uncharted territory. Your chief information security officer (CISO) or IT director should be prepared to educate decision-makers by answering these questions:

- Why is it important to understand that the IoT is comprised of more than devices?
- How is IoT operating in our business environment?
- What does the attack surface look like now that employees are working from home?

WHAT TO DO NEXT

Implement managed security services to close gaps in tools and skills – the most efficient way to gain IoT security expertise without hiring more people or purchasing new technology. Your inhouse IT experts can focus on what they do best while the MSSP backs them up by:

- Monitoring all endpoints 24x7 using the latest scanning and detection tools
- Customizing runbooks to increase efficiency and effectiveness
- Offering flexible OpEx billing arrangements – approximately 46% of managed IT service users cut their annual IT costs by 25% or more[7]

SWIFT, CLOUD-BASED REMEDIATION

A breach is stressful. Structured, cloud-based remediation services are reassuring and efficient – and can include:

- Activating a security and emergency response (SERT) team
- Assigning a commander to coordinate the efforts of specialists in threat intelligence and threat hunting
- Returning to a stable, pre-breach state should a zero-day event or ransomware attack occur
- Changing processes, wiping drives and reinstalling software
- Engaging with the appropriate law enforcement officials to maintain the custody chain of forensic evidence

Apply IoT Best Practices Within Hours

During this unprecedented time, IoT is an overlooked challenge. Securing home environments filled with IoT devices is not business as usual. Managed security services provide capabilities and experience that help you immediately tackle this vast new attack surface and reduce the risk of breaches. Keep cybersecurity as simple and easy as possible by:

Aligning services to your unique environment, risk profile and objectives – customized security programs are the most effective

Applying best practices based on firsthand knowledge of securing IoT environments

Ensuring you have access to the right expertise at the right time

ENDNOTES

1. Global Workplace Analytics.

2. Transforma Insights, Global IoT Market Will Grow to 24.1 Billion Devices in 2030.... May 19, 2020.

3. Forbes, Cyberattacks on IoT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims. September 14, 2019.

4. Nuspire research.

5. Nuspire research.

6. CNBC, Coronavirus Jobs Survey. March 30, 2020.

7. CompTIA, Fourth Annual Trends in Managed Services Study, 2016.

AUTHOR:

John Ayers

Chief Strategy Product Officer and SecOps Leader

Mr. Ayers is responsible for organizational leadership specific to technology and security innovation, operations and threat intelligence at Nuspire. His role is to ensure the alignment of Nuspire's business and managed security product strategy across all domains of information networking and security. Additionally, Mr. Ayers currently serves on product advisory councils for FireEye, Palo Alto, Sophos, Cisco, Intel-McAfee and Symantec.down entry points.

ABOUT NUSPIRE

Nuspire is a leading managed security services provider (MSSP) that is revolutionizing the cybersecurity experience by taking an optimistic and people first approach. Our deep bench of cybersecurity experts, world-class threat intelligence and 24x7 security operations centers (SOCs) detect, respond and remediate advanced cyber threats. We offer comprehensive services that combine awardwinning threat detection with superior response capabilities to provide end-to-end protection across the gateway, network and endpoint ecosystem. Our client base spans thousands of enterprises of all sizes, across multiple industries, and achieves the greatest risk reduction per cyber-dollar spent. At Nuspire, we are laser focused on delivering an extraordinary cybersecurity experience that exceeds client expectations. For more information, visit www.nuspire.com and follow @Nuspire.

nuspire