ZONES

Endpoint Security Technical Paper

Shine a light on every endpoint security risk.

Securing your IT environment can feel a bit like playing a game of Whac-A-Mole.™ Just when you think you've secured your network infrastructure from all the potential intruders out there, another one pops up to taunt you. With the proliferation of internet-enabled devices saturating the market, nearly any type of technology can be considered an endpoint security risk.

In this increasingly complex environment, it can prove challenging to defend your business against the full range of attacks it faces. That's why we've compiled three of the most commonly overlooked endpoint security risks, so you can learn how to secure them all.

1. Don't forget about your printers and copiers.

Businesses tend to regard printers as "set it and forget it" devices. In other words, devices that don't harbor any serious security vulnerabilities. In fact, just 53% of IT managers realize their 2% of printers are secure.[1]

This lax approach to printer security is a serious liability. Why? When determining their path of attack, hackers target the endpoint that's easiest to penetrate. Since many overlook the importance of defending it, digital criminals often exploit the print environment. From there, they can pillage a corporate network and help themselves to whatever data or information they want.

Fortunately, there are many ways you can bolster the business's defenses against these attacks. Newer printers feature real-time threat detection, automated monitoring, and software validation to head off potential assaults. Some models can even heal themselves after an attack. Printer administration tools also streamline the process by setting company-wide security configuration policies and automatically validate settings for every printer in the fleet. You can partner with Zones for an expert assessment of vulnerabilities in your print environment.

2. Stay one step ahead of connected devices.

Connected devices represent another massive endpoint security risk. This category includes a huge variety of devices ranging from wearable gadgets, like smart watches, to industry-specific appliances, like medical devices. The IoT market will keep expanding and is expected to hit $661.74 billion by 2021.[2] Further, IoT device manufacturers have been criticized for rushing devices to markets that collect a lot of sensitive data, yet lack even basic information security standards in their design.[3] Some devices even fail to require complex passwords or use strong encryption. Poor IoT device security has already threatened the stability of the internet.

Remember the outage in which major services, such as Twitter, Spotify, and PayPal, went offline for a long stretch of time? A major source of the attack was IoT devices compromised by Mirai botnet malware without their owners' knowledge.[4] Meanwhile, hackers recently targeted a hotel in Austria with IoT ransomware that compromised its key card system, locking the company out of its own computer network and preventing a dozen guests from entering their rooms until the company paid the ransom.[5]

How can your businesses defend against this growing threat? Before deploying any devices, determine whether hackers can easily identify existing user accounts or steal personal data. You should also stay current with patches issued by the manufacturer. If any of your IoT data is stored in the cloud, then you should carefully review how your cloud vendor secures that data.

You may also consider an IoT management solution that incorporates security protections, like those you might expect to find in a mobile device management (MDM) solution. If your IT team is crunched for time, it may prove beneficial for Zones to conduct an in-depth IoT security review that provides actionable follow-up steps tailored for your business.

3. Lock down your mobile devices.

Mobile malware has been approaching the same level of sophistication we've seen in desktop and laptop computers for some time. As with IoT devices, hackers increasingly target mobile devices in malware attacks. A recent report from Nokia's Threat Intelligence Lab found that mobile infections increased 83% in the second half of 2016.[6] However, 64% of respondents to a recent survey on mobile security reported they're unprepared for a mobile attack.[7]

To improve your mobile security, consider investing in an MDM solution that keeps your mobile devices current with security patches and applies security policies (for example, preventing them from connecting to unsecured wireless networks). Make sure to carefully vet the apps installed on company devices, including BYOD devices. Although app stores are becoming more vigilant in screening out malicious apps, some bad actors still slip through undetected. Remember the Pokemon Go craze? Opportunistic hackers piggybacked on the game's popularity and released copies of the app injected with malware.

Conclusion.

There's no getting around it: The number of endpoint security risks is skyrocketing. In some cases, a business will face unique risks due to the nature of its work or the vertical in which it operates. For this reason, a comprehensive security assessment performed by Zones experts can prove useful in helping your company identify and prioritize which vulnerabilities to secure. This can allow you to leverage the tremendous benefits new technologies offer while ensuring your network environments and mission-critical data are safe, sound, and secure. Best of all, it's as easy as 1, 2, 3.

1. "The Insecurity of Network-Connected Printers: Executive Summary," *Ponemon Institute*, (September 2015).
2. "Internet of Things (IoT) Market by Software Solution, Platform, Service, Application Domain, and Region—Global Forecast to 2021," *MarketsandMarkets Research*, http://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html, (April 2016).
3. Andrew Tannenbaum, "Why Do IoT Companies Keep Building Devices with Huge Security Flaws?," *Harvard Business Review,* https://hbr.org/2017/04/why-do-iot-companies-keep-building-devices-with-huge-security-flaws, (April 27, 2017).
4. Andrea Peterson, "'Internet of Things' Compounded Friday's hack of major websites," *The Washington Post,* https://www.washingtonpost.com/news/the-switch/wp/2016/10/21/someone-attacked-a-major-part-of-the-internets-infrastructure/, (October 21, 2016).
5. Dan Bilefsky, "Hackers Use New Tactic at Austrian Hotel: Locking the Doors," *The New York Times,* https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html, (January 30, 2017).
6. Kevin McNamee, "Mobile threats on the rise: What's to blame?," *ITProPortal,* http://www.itproportal.com/features/mobile-threats-on-the-rise-whats-to-blame/, (May 2, 2017).
7. "The Growing Threat of Mobile Device Security Breaches," *Dimensional Research,* http://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf, (April 2017).