ActZero

THREAT INSIGHT

Mobile Device Vulnerability

You only need to look around you at the office or out in public to understand that mobile devices are ubiquitous today. There are approximately 6.37 billion smartphones in the world as of October 2021—and only 7 billion people.

Not surprisingly, mobile devices are everywhere in business, too.

More than 60% of endpoints accessing enterprise data today are unsecured mobile devices, increasing the enterprise attack surface. The average smartphone runs 80 apps, each of which is its own potential security risk. Nearly a quarter of Android apps have API exposures and key leaks, close to half (48%) lack data encryption, and 53% of apps would outright fail data and privacy compliance. Moreover, an average of 65% of enterprise-connected mobile devices are running an OS with critical vulnerabilities.

With mobile devices increasingly functioning as digital ID to access enterprise services and data through two-factor authentication (2FA), the threat plane is expanded. Whereas previously you would have protected access to a laptop, now a secondary device is in play.

Mobile devices have never before been such a source of vulnerability or the target of such directed attacks, because if you can gain access to them you gain access to a system.

Security Implications of Mobile Devices

So, what are the security implications of mobile devices for SMBs?

Consider that in 2020, 75% of organizations around the world experienced a phishing attack, with that number rising each year. Of the 51 zero-day vulnerabilities discovered in 2021, 16 were mobile-specific and there are over 35 million samples of mobile malware known to exist.

Moreover, 90% of all breaches start with a phishing email...and 60% of all business emails are now read on mobile devices. Given the current reality of a workforce that divides its time between in-office and at-home working, a mobile device becomes a go-to for responding quickly to work email wherever you are. And due to lack of securoity awareness, or simply being rushed,, it becomes easy for people to accidentally respond to phishing attacks or SMishing attacks (SMS-based phishing) without realizing until it’s too late.

Three Core Cybersecurity Functions

There are many ways to protect mobile devices and many companies have responded to the vulnerability of mobile devices with Mobile Device Management (MDM).

MDM allows compliant devices to access corporate email, apps, and data, secures data-in-transit between mobile devices and the corporate network, and separates business from personal data, even where there is a 'bring your own device' (BYOD) policy in place.

While a useful step to take, MDM isn't necessarily a threat protection tool. MDM is far more focused on access management and making sure that devices accessing the network are compliant with general password policies, timeout policies, and screen lock policies, for example.

MDM's biggest blind spot is in its lack of active threat detection.

Security Implications of Mobile Devices

If you're allowing mobile devices on your network and you've put MDM in place, you've done the right thing and taken the first step to protecting your network. From there, however, you need to take your protection to the next level. You need to step it up and find a way to actively detect threats on those mobile devices because threats on those devices can easily worm their way back into your network.

That's why ActZero's latest offering, ActZero MDR for Mobile - a Mobile Threat Detection (MTD) solution, is a level-up on the protection offered by MDM, providing around the clock, scalable threat coverage that seamlessly integrates with existing MDM coverage. Offering superior detection and remediation, MDR for MobileMDTD provides machine learning-enabled detection for mobile threats and on-device automatic response options, including tailored guidance and detailed remediation advice for all alerts.

MDR for MobileMTD blocks reconnaissance scans of your network, Mas well as Man-in-the-Middle attacks, SSL stripping, SSL decryption attempts, and rogue access points. It protects devices from OS/kernel exploits, profile and configuration modifications, system tampering, and physical USB/SD card exploits. Applications are scanned for malicious code, known and unknown malware, download abuse, and other exploit techniques. MTD also detects and protects against cyber threats like phishing and SMishing attacks by blocking attempts on mobile devices, email, SMS, and messaging apps.

Interested to learn more about how ActZero MDR for Mobile can boost your existing mobile device endpoint security? Reach out today to start a conversation. **[LINK HERE]**