ivanti

Protecting the Enterprise: Best Practices in Mobile Device Security

Attacks are on the rise—for the third year in a row.
Here's what you need to know to protect against them.

Cybersecurity attacks targeting mobile devices are on the rise. More than one in three companies suffered a security breach targeting mobile devices in the past year, according to the 2020 "Verizon Mobile Security Index"—the third year in a row the number has increased.

In the 2020 report, 39% of the survey respondents admitted that their organization had suffered a mobile breach, up from 33% last year and 27% in 2018. Of those whose organization was compromised, two-thirds said the impact was "major" whereas 36% said it had had lasting repercussions. More than one-third said remediation was "difficult and expensive."

The consequences of a mobile security breach are numerous, with the most common being downtime, cited by 59% of the survey respondents. Other issues include loss of data, compromise of other devices, damage to reputation, regulatory penalties, and loss of business (see Figure 1).
One reason why attacks are on the rise is that hackers are getting more clever in their techniques, such as successfully hiding telltale URLs on the small screen typical of many mobile devices. Hackers are also not above exploiting events such as the global pandemic to get the attention of unsuspecting victims.

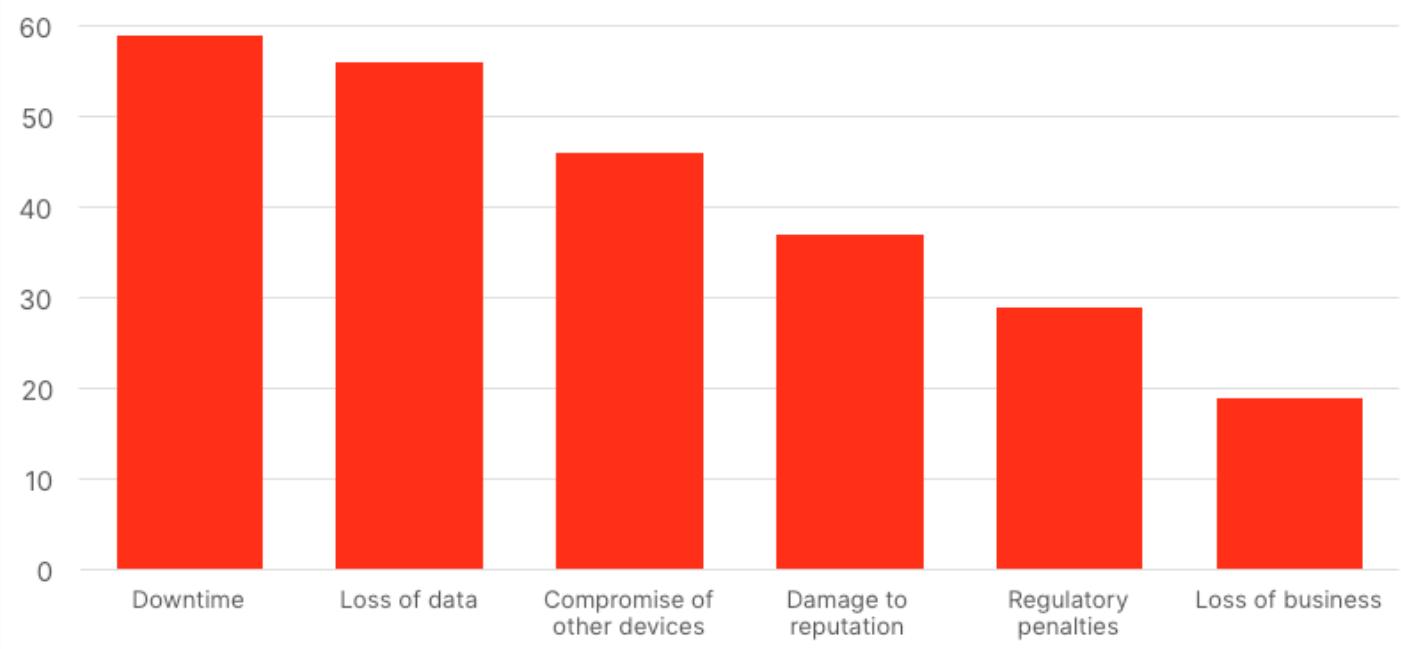
The pages that follow examine the rise of mobile attacks, explore the challenges of securing mobile devices in the enterprise, and offer best practices to protect against attacks.

The rise of mobile attacks

Hackers are increasingly targeting mobile devices, for at least one good reason: There are simply an awful lot of them—even more than desktops.

Worldwide mobile internet use surpassed that of desktops in 2016 and has been steadily rising since, according to BroadbandSearch, which collects data on internet service providers. Mobile phones account for 51.33% of all device market share, compared to 45.9% for desktops and laptops and 2.78% for tablets, according to Statcounter.

Figure 1: Consequences of mobile-related compromise



Source: Verizon Mobile Security Index: 2020 Report

Another reason is that hackers have multiple potential attack vectors they can exploit on a mobile device.

Phishing attacks

Among the attack vectors is the phishing attack, where hackers essentially trick users into clicking on a malicious link. They have numerous ways to entice users, including preying on coronavirus fears. With many employees working from home, without many of the usual protections they have in an office setting, hackers have seen new opportunities.

In April 2020, the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) issued a joint statement with the UK's National Cyber Security Centre (NCSC) warning of the issue. It cited use of email subject lines containing COVID-19–related phrases in phishing emails.

"To create the impression of authenticity, malicious cyber actors may spoof sender information in an email to make it appear to come from a trustworthy source, such as the World Health Organization (WHO) or an individual with 'Dr.' in their title," the CISA wrote. "In several examples, actors send phishing emails that contain links to a fake email login page. Other emails purport to be from an organization's human resources (HR) department and advise the employee to open the attachment."

The CISA noted that phishing attacks may also come via SMS text message, not just email.

The text messages often use a COVID-related financial theme, such as a promise of government payments, in order to steal banking information. Other attacks seek to steal user login information and to deploy malware, the CISA warned.

Device, network, and app-level attacks

Another type of attack targets the device itself, with the goal being to actually gain control of the user's device. Device-level attacks are often caused by common vulnerabilities in the mobile operating system that can be exploited to gain access to the device. Other examples include compromising mobile devices via physical hardware such as USB charging ports or remote attacks via Bluetooth/near-field-communication vulnerabilities.

Network-level attacks involve an attacker setting up a rogue Wi-Fi access point (AP), such as in a coffee shop or other public place. When an unsuspecting user connects to the AP, the attacker can launch a man-in-the-middle attack to intercept communications coming from the device. Should the user then proceed to log into a corporate network, for example, the attacker could intercept a valid username and password and use them later to gain access to corporate resources.

As the name implies, an application-level attack uses an app that users download from sources outside of the official Apple or Google app stores. Apps embedded with malware can cause faults in the device operating system or one or more applications, enabling the attacker to gain control of an application or the entire device.

Challenges to securing mobile devices

Defending against attacks on mobile devices presents several challenges.

Phishing attacks, for example, are often more successful on mobile devices than they are on desktops, because their smaller screens make it less likely that a user will detect a malicious URL. The user may not detect that the URL ends in something odd, like www.yourcompany.io instead of .com. Hackers may also employ such tricks as using shortened URLs, from TinyURL or Bitly, for example,

as well as using an I instead of the numeral 1 or the letter O instead of a zero.

While in the thick of the moment on a mobile device, many users won't think to drill down and closely inspect the URL.

A hacker has to be successful only once to do damage, whereas users have to be vigilant all the time to escape it.

Educating end users is another challenge. They need to be brought up to speed about the various types of attacks and reminded not to click on any links unless they're 100% sure they're legitimate. During the pandemic especially, with so many people working from home, it's easier for users to fall prey to phishing attacks, given that there's nobody around to warn against them.

"In the last six months, we've seen growth in apps being installed from malicious sources, outside of the Google Play or Apple App stores," says Mirko Bulles, senior lead market technical advisor for Ivanti. "They tend to be malicious apps that could take over the device. If the mobile device is also used for business purposes, you have an issue."

Use of personal devices presents another challenge, as they may not be up to date with the latest operating system and therefore the latest security patches—making the devices more susceptible to attack.

Best practices: simplicity and a tiered approach

In terms of how best to ensure security for mobile devices, you must first make security simple for users. If you have to rely on users to download agents, register, adjust settings, and the like, you will inevitably not achieve 100% adoption. Whatever mobile device security solution you choose, it should require no action on the user's part to install and configure.

Another best practice is to implement a tiered approach to compliance actions. In some instances, you may want to send users a message alerting them to a potential problem. If the security solution detects someone trying to steal a password in a coffee shop, for instance, you should have options for how to respond. Maybe your policy is to send users an alert message encouraging them to disconnect, or perhaps you want to simply shut down the Wi-Fi connection and send users a note explaining why.

Similarly, if a security setting is disabled on a device, a tiered response would enable you to give a user a few hours to fix it before the device is disabled from the network. The point is to give IT a level of control that enables it to ensure security while still enabling employees to stay productive when the threat is not immediate.

Multivector, holistic protection

A mobile security solution should also offer protection against not only email-based phishing but also SMS/texts, messenger apps, and social media sites—and even be able to handle whatever future modes of communication arise. In other words, it should block threats no matter where they come from.

The solution also needs to strike a balance between being able to detect threats on its own and using cloud-based resources to detect the latest threats. That's important, because about 5,000 new malicious links are created every hour, Bulles says. So the device needs to have a database on board that can catch the vast majority of malicious links and then connect with the cloud-based database to be updated every few hours.

Some organizations will be sensitive about sending potentially personal information to a cloud service, so they may opt to use only the on-device database. Others may decide that at least some devices are so sensitive that they need to check with the cloud-based database every time. Again, it gets back to the tiered approach and giving IT options.

Conclusion

With so many employees working from home and the number of mobile devices they use continuing to rise, it's never been more important to address the security challenges these devices present.

Ivanti Mobile Threat Defense is one solution that addresses mobile security challenges head-on while enabling organizations to successfully drive 100% user adoption and giving IT the flexibility it needs to balance privacy with security requirements (see sidebar).

Ivanti: 100% Adoption for Antiphishing Plus Flexibility for IT

Ivanti Mobile Threat Defense (MTD) combines protection and remediation for mobile security attacks with the simplicity required to achieve 100% user adoption and a tiered security strategy that enables IT groups to find the right balance between privacy and protection for all users in their organization.

MTD offers protection against not only email-based phishing but also SMS/texts, messenger apps, and social media sites—and can even handle whatever future modes of communication may arise. Its multivector protection includes an on-device machine learning database lookup as well as a cloud-based URL database lookup for the most recent threats. You decide which vector to use for each user, depending on your needs and the balance you want to strike between privacy and security.

No user interaction is required to activate MTD, so you can ensure 100% adoption. A tiered incident response structure also enables you to determine how to handle security events, depending on their severity, the user's location, and more, helping ensure adoption among users.

To further reduce risk, Ivanti's zero-sign-on technology provides secure authentication to enterprise cloud services from any device, by using the mobile device and biometrics for authentication rather than passwords.

MTD offers a complete mobile security solution based on best practices. It's just the ammunition you need in the battle against mobile cybersecurity threats. To learn more, visit: **https://www.ivanti.com/products/mobile-threat-defense**