IDC ANALYST CONNECTION

Sponsored by: IBM

Organizations must shift away from trying to control all configurations and environments on the mobile endpoint. Instead, they need to deploy solutions that secure the data and the access to it based on identity and conditions of end-user context.

Managing Mobile Security Threats Facing the Hybrid Enterprise Workforce

December 2021

Questions posed by: IBM

Answers by: Phil Hochmuth, Program Vice President, Enterprise Mobility and Endpoint Management

---

Most enterprises are mobile enterprises at this point. With U.S. smartphone penetration at >90%, and 9 out of 10 enterprises allowing some form of BYOD in their organization, workers are using a mobile device for work in some fashion. With businesses now coming out of the pandemic and moving toward hybrid work environments, it is important for enterprise IT and security teams to be aware of increasing threats to mobile computing usage.

Q. According to the FBI, phishing attacks were the most common type of cybercrime in 2020. Can you provide more details on this threat and the challenges associated with it?

A. The FBI and IDC agree. According to IDC's *U.S. Enterprise Workspace Management and Security Survey, 2021*, mobile email phishing and SMS phishing were identified by U.S. IT and security administrators as the top 2 most frequently experienced mobile security threats. If you combine these threats, phishing is overwhelmingly the most frequently seen attack or incident.

Mobile phishing challenges include the ease with which attackers can spoof legitimate websites and messages in a mobile user interface (UI). The biggest issue with SMS-based attacks is that they can be sent to anyone with a phone number, allowing automated bots and systems to send out phishing attacks via text to random phone numbers. It's like robocalling on steroids but with much greater risk to the organization (such as embedding malicious links in texts that go to malware or data theft sites). Malicious SMS messages are particularly hard to stop because they do not go through corporate email antispam or messaging security solutions, which may be deployed to protect PC and mobile email clients. Carriers can take some actions on their networks to prevent malicious SMS spam, but it is still hard to catch.

There is less potential for underlying damage to a device in a mobile phishing attempt via email. However, there's still a great risk of users being tricked and entering information into false website forms or being lured into other types of fraud facilitated with mobile phishing emails.

Q. Why are mobile endpoints so vulnerable to advanced threats (spear phishing, targeted attacks), and what is the impact?

A. There are many reasons that mobile email phishing is so challenging for enterprise security teams. First, end users trust their phones and are more likely to tap on or open attachments or messages sent to their device's email app as opposed to their PC's email client. The screen on phones is smaller than the screen on PCs, which makes it harder for users to vet a mobile email message for the sender's name, domain, and address or other potential signs of a phishing attempt. Further, most corporate training around antiphishing focuses on PC-based usage of email clients and not on mobile.

Attackers have also realized that some of the most valuable data in an organization is moving to mobile devices. As enterprises open up more apps and data stores to mobile access, sensitive information is increasingly being downloaded and stored on these devices. As seen in some very high-profile attacks on social media CEOs and others, it is not impossible to spoof the mobile device of even the most monitored or closely watched end users. Hackers are exploiting vulnerabilities in mobile operating systems at rates not previously seen. New vulnerabilities in both Android and iOS are now common, and OEMs are constantly issuing updates to keep pace with security threats and challenges. Mandatory patching and security software updates on mobile are now a must-have for many organizations whose end users work primarily or even wholly on smartphones.

Q. The pandemic forced many enterprises to modernize their remote access control models around a zero trust network. Why is this so important in a hybrid environment, and do you see it continuing to be relevant in a post-pandemic world?

A. Many traditional VPN-based remote access architectures buckled, or broke, during the pandemic. Making access control universal and consistent across home/remote work is critical to ensure good user experiences and consistent adherence to corporate policy. The biggest challenge in hybrid environments is that end users are moving targets for IT teams to track, support, monitor, and protect. The pandemic made everyone a mobile worker or a road warrior to some extent; in the past, a smaller percentage of end users were traveling frequently or working from different locations on a regular basis. Switching even a couple days a week from a home/remote office to a corporate site drastically changes the attack surface of an end-user's workspace. It also requires organizations to rethink how they provide access to IT assets and systems overall. In a hybrid work environment, IT security teams need to look at employees as a mobile workforce, with worker profiles whose access needs and security requirements will change daily.

This change is why it's important to rethink how users are going to access systems and create access control architectures that are flexible and not tied to specific sites, devices, or locations.

As we come out of the pandemic, some organizations are moving back to full-time onsite work. During this transition period, forward-looking businesses will move toward access controls that are identity based and zero trust focused to help strengthen and modernize their perimeter security capabilities and enable future resiliency.

Q. Why are the tools in place for traditional network threats inadequate for safeguarding mobile devices and a hybrid workforce?

A. The traditional enterprise security approach assumes end users are attached to corporate networks and behind a company firewall. Mobile introduces a major blind spot in corporate visibility and control. The 4G and 5G cellular data networks that connect most smartphones are not visible or manageable from an enterprise security standpoint. Instead, organizations must rely mostly on carriers to provide security and enforce policy on these networks. Even with corporate cellular plans that can be managed and controlled, there are limited capabilities available to enterprises for enforcing network and security policies across traditional data networks and wireless networks.

The challenge increases with BYOD users, who bring their own cellular services to work. Basically, every worker in the organization could potentially have their own private internet connection to do whatever they want, mixing files and data downloaded from this insecure network with data and devices controlled by the corporate LAN and WAN.

The lack of security software running on mobile endpoints is also an issue. Generally, mobile devices are more secure than traditional PCs from an operating system perspective and an app distribution perspective. Controlled access to the underlying kernel, sandboxed environments for individual apps and data, and the controlled App Store model for downloading software prevent a lot of the challenges that organizations face with PC users. However, most enterprises do not use mobile threat management on the majority of their endpoints. This is another blind spot that many organizations think they're covering with mobile device management (MDM) tools. However, these tools do not actively look for threats on endpoints. They merely remediate threats that are identified by other platforms. Organizations are beginning to deploy more endpoint security on mobile to match what they do on the PC side, but more needs to be done.

Q. What should an ideal secure mobile enterprise focus on to protect a hybrid workforce?

A. Start by focusing on controls that tie policy enforcement to virtual/digital factors — identity, apps, data, and observable end-user behavior and context. Rely less on controls tied to specific networks, devices, or physical locations. Controlling mobile endpoints is still important. In addition, deploying MDM or unified endpoint management tools to lock down, configure, and control users' devices remains a critical function. The deployment of security software on those endpoints is also becoming more of a requirement.

However, organizations must shift away from trying to control all configurations and environments on the mobile endpoint. Deploying different standalone tools is also a challenge. Instead, organizations need to deploy solutions that are tightly integrated end to end. One example would be MDM integrated with threat management that is further integrated with the overall IT security platform. Such a solution would provide end-to-end visibility into IT security threats — including phishing — and be able to leverage this integration to enable real-time and targeted actions based on a threat's risk level. This integrated approach is required to truly eliminate the mobile blind spot and allow administrators to act on these threats based on identity and conditions of end-user context. Zero trust is called what it is for a reason: Its modus operandi is not to trust any underlying device, network, or user.

About the Analyst

Phil Hochmuth, *Program Vice President, Enterprise Mobility and Endpoint Management*

Phil Hochmuth is the Program Vice President on IDC's Enterprise Mobility team. His research provides insights into how enterprises deploy mobile devices and applications as well as management and security platforms.

MESSAGE FROM THE SPONSOR

In today's work from anywhere culture, enterprises require a hybrid strategy that enables employees to be both productive and secure. Companies are challenged to find new ways to combat the latest phishing attacks and need to strengthen their existing controls at both endpoints and mobile devices. IBM is dedicated to helping our customers meet this challenge through a *Zero Trust* approach to unified endpoint management. IBM MaaS360 was designed to both secure and manage resources and data in an integrated approach. This cloud-based solution supports a hybrid environment through a single console. Find out how MaaS360 can help your organization's digital business transformation. Click this link to find out more about MaaS360.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com