Save yourself from mobile hacking - Q&A with Simeon Tassev

By Lauren Hartzenberg

30 Mar 2016

The age of 'connected everything' is here and mobile devices are becoming extensions of our physical selves. Of paramount importance in many businesses today, these devices are now critical access tools for employees at all levels of an organisation and the Bring Your Own Device (BYOD) trend shows little sign of ceasing.

Simeon Tassev

But for all their convenience, the ubiquitous use of mobile devices in the workplace and beyond has brought a variety of new security risks that require greater security implementations. Simeon Tassev, director at Galix, offers some expert advice on combating the new wave of cyber attacks.

What has brought about the surge in mobile attacks?

Simeon Tassev: The use of smartphones has increased significantly and is often adopted en masse by end-users for convenient email access as well as by managers and executives who need access to sensitive business resources from their device of choice. Smartphones and tablets have even become critical access tools for a wide variety of production applications from Enterprise Resource Planning (ERP) to project management. For all of their convenience, however, the pervasive use of mobile devices in the workplace and beyond has brought a new set of security risks.

Where do the biggest vulnerabilities lie?

Tassev: Combine the lack of security with the fact that mobile devices are being targeted by cybercriminals and you have a dire situation. For example, the number of variants of malicious software aimed at mobile devices has reportedly risen from about 14,000 to 40,000 or about 185% in less than a year.

Mobile devices face an array of threats that take advantage of numerous vulnerabilities commonly found in such devices. These vulnerabilities can be the result of inadequate technical controls, but they are more likely to be the result of poor security practices of consumers.

How have attack methods evolved over recent years?

Tassev: Attack methods have evolved in a few key ways, namely:

• Cybercriminals have embraced Advanced Persistent Threat (APT) tactics for targeted attacks.
• APT groups fragment and diversify their attacks.
• There has been an escalation of Automated Teller Machines (ATM) and Point of Sale (PoS) attacks.
• Phishing attacks have turned into whaling attacks, targeting larger scale organisations.
• Mobile OS vulnerabilities have been exploited and malware software is on the rise.

How do you suggest an organisation protects itself from attacks?

Tassev: To secure an organisation from an IT perspective, IT security professionals and business executives need to look at the effect mobility has on the business risk profile. This requires examining the device, data, applications and transactions that will be utilised and performed while mobile as a whole, rather than examining them individually. Together, IT and business need to find a balance between usability and mitigating risk in creating a practical mobile security

framework that will facilitate productivity gains and enhance employee satisfaction while limiting the exposure to business-critical information and assets.

Combine this with the BYOD challenges and the only way to secure the mobile devices used for business is to secure the data on the device. Latest trends are to use secure data containers for this. A secure data container is a third-party mobile application that is used to separate and secure a portion of a device's storage from the rest of the device.

©langstrup via 123RF

How can individuals protect themselves?

Tassev: Most individuals have no idea how vulnerable they are when they use their cellphones. So how do you protect yourself? The minimum one can do is to protect one's mobile device by enabling PIN protection and biometrics security where possible. Pulling out your phone's battery is probably the only way to interrupt the flow of information if you suspect you are already under surveillance but unfortunately that is not always an option depending on the mobile device you use (you can do this with an Apple device).

As for prevention, a common rule for making a man-in-the middle attack is to send the target a text message that claims to be from his or her cell service provider asking for permission to 'reprovision' or otherwise reconfigure the phone's settings due to a network outage or other problem. Don't click 'OK'. Call your carrier to see if the message is a farce.

Individuals need to be more proactive in terms of their mobile security. They need to be aware of the networks that they log onto and check if they are open and if other individuals have access to their information on their phone via this entrance. Also checking the permission on apps downloaded onto your phone is important to establish what information you are sharing online.

ABOUT LAUREN HARTZENBERG

Managing editor and retail editor at Bizcommunity.com. Cape Town apologist. Dog mom. Get in touch: lauren@bizcommunity.com
- The secrets behind Israel's rise as a 'Startup Nation' - 8 Aug 2018
- Israel's plan to accelerate innovation in sports tech - 31 Jul 2018
- #DesignMonth: Chatting molluscs and mobile gaming with Thoopid - 16 Feb 2017
- #BizTrends2017: Reimagine work, redefine productivity - 31 Jan 2017
- #BizTrends2017: People-powering the digitalisation process - 27 Jan 2017

View my profile and articles...