5 Mobile Security Trends and Actions to Consider

Dan Lohrmann | November 26, 2012

Governments are aggressively going mobile with new devices, app development projects and system integration efforts. Whether buying proven off-the-shelf products or developing mission-critical apps from scratch, there's little doubt that the future interface for delivering customer service will be tablets and smartphones. Estimates suggest that at least 50 percent of users will access the Web via mobile devices by the end of 2013.

Meanwhile, many governments that implemented cloud-first policies over the past few years are developing new "mobile-first" edicts to match. Indeed, tech experts described our customer data landscape to business leaders with a triangular diagram containing three interacting puzzle pieces: cloud computing, mobile devices and security.

Some of these new apps are being acquired for public-sector workers to use on government-owned devices to improve efficiency. Other apps are citizen-centric, and they must be usable on the many new devices and operating systems now available and those coming soon.

So what security issues are associated with mobile devices and app development? Here are five mobile security trends and some actions to consider as you become more mobile:

More Mobile Data Than Ever. For years, sensitive enterprise data has leaked via USB drives and lost or stolen laptops, but the number of smartphones, tablets and other mobile devices has exploded.

Actions: Establish policies that encrypt mobile data on devices or keep all sensitive data off mobile devices. If accessing sensitive information is required, consider data loss prevention products and keeping all personally identifiable information on protected enterprise servers and off the endpoint devices.

More Mobile Malware. The bad guys are following the crowds, who are buying smartphones and tablets with more power than PCs of a decade ago. The DroidDream and Gemini malware attacks were launched in early 2012, and some call this the “Year of Mobile Malware.” Mobile botnets are also growing.

Actions: Mobile device management services can protect devices by locking down permissions and offering anti-malware software and tools. Training end users is also essential via formal awareness programs that explain how to think before clicking.

Growing Use of BYOD to Work. Some security experts see the BYOD trend as “bring your own disaster.” Nevertheless, one top industry expert predicted that 80 percent of global enterprises will adopt this approach by 2016.

Actions: Meet with business customers about mobile device preferences. Consider piloting BYOD in areas with nonsensitive data. Develop policies for the use of personal devices under different scenarios, even if some business areas opt out.

Authentication Complexity Growing. Despite the push for single sign-on, many enterprises still struggle with more credentials for more apps and devices. Users are tiring of more complex passwords, and the use of biometrics is growing.

Actions: Streamline credentials with federated identity management across government systems, mobile apps and legacy programs. Consider using federal health IT dollars as anchor tenants. Apply government policies to personal devices, if they store business data — after getting employee buy-in.

Mobile Platform Support Is Complex. Whether you’re writing apps for Apple’s iOS, Google’s Android, BlackBerry’s BES or Microsoft’s Windows 8, secure coding is hard work. One technology CEO said, “You’d be hard pressed to find application developers who actively try to mitigate against cross-site scripting attacks, SQL injection attacks and cross-site request forgery attacks.”

Actions: HTML5 is growing as an industry standard across mobile platforms — consider adopting it. Train staff in secure coding. And before deploying a code, test it for holes.

Final Thoughts

Government executives must consider having vendor partners manage specific services or assist with mobile activities. IT consumerization makes this a difficult area

to keep up with. The National Institute of Standards and Technology issued draft guidance on mobile security. Many state and local governments issued RFPs in this area, and NASCIO issued several helpful papers on architectures with secure mobile implementations.

http://www.govtech.com/pcio/5-Mobile-Security-Trends-and-Actions-to-Consider.html