RETAIL INFO SYSTEMS
POWERING INTELLIGENT COMMERCE

5 Mobile Security Steps to Take Now to Protect Your Retail Business

By Marco Nielsen - 09/11/2017

When the massive “Vault 7” leak made headlines, the world learned just how insecure many mobile devices are. In more than 8,000 documents allegedly obtained from the CIA, whistleblower Wikileaks said that the agency had turned iPhones, Windows devices, Samsung TVs and more into covert microphones – underscoring how important it is to develop a proactive mobile security policy.

The retail industry is using mobile to drive new levels of productivity, efficiency and customer satisfaction, offering in-store customers payment methods like Apple Pay and Google Wallet and tailoring specials to individual shoppers.

Unfortunately, mobile also comes with security risks, from outside threats like those detailed in Vault 7 to rogue employees who can steal your data.

Each compromised record costs retailers an average of $172, according to the Ponemon Institute’s *2016 Cost of Data Breach Study*. When retailers face large-scale breaches of thousands or even millions of records, those numbers add up fast.

There are many aspects to consider when developing a mobile security strategy, from operating systems to applications to traffic. Bring-your-own-device (BYOD) and corporate-owned programs have different requirements, so it’s important to understand the differences before choosing your mobile security route. Focus on these five areas to build a robust mobile security strategy:

1. **Secure and filter data traffic.**

Could a single Facebook scam compromise your company's systems? The answer is ... maybe.

If your employees access social media channels on their devices, you could be more vulnerable to cyberattacks. In response, many enterprises restrict access to social media or other websites where cyber threats lurk. Luckily, there are many products available to audit and monitor data traffic.

Several products can monitor and filter all data traffic to and from the mobile device. That means instead of just blacklisting a specific application, like Facebook, you can block or monitor all Facebook data traffic so potential hackers can't use other avenues, such as the Facebook web site. Businesses can also invest in products to compress and limit data usage on mobile devices.

2. **Protect your devices.**

Malware isn't just for desktops anymore: All platforms are susceptible to malware today, including Apple iOS and Google Android. There was a 153 percent increase in the number of unique Android malware samples and 70,000 total unique iOS malware samples in 2015, according to the *Hewlett Packard Enterprise Cyber Risk Report 2016*. Fortunately, businesses can invest in anti-malware screening to identify and contain cyber threats before they turn into problems.

Many of these threats come from fishy applications, making it more critical than ever to only download mobile applications from validated locations. Make sure your business is using trustworthy application vendors to avoid installing anything suspicious on your organization's mobile devices. If your business uses custom applications, you can also use third-party code validation to ensure proper data handling and secure data communications.

3. **Consider a virtual private network (VPN).**

Who's eavesdropping on your conference call? The reality is that it's pretty simple to listen in on wireless devices. Bad access points are also risky: If corporate employees log into an airport hotspot while traveling on business, for example, a hacker can easily gain unauthorized access to calls, texts or even websites by spoofing the network.

A VPN helps to ensure security for all communication between mobile devices and the enterprise. This security measure encrypts data and requires stricter authentication for

users before they access applications or services. Some enterprises also use access point names (APNs), a carrier feature, to protect data that travels to and from the company. In addition, there are options to encrypt voice and text message traffic that might be important for certain high-level employees or departments.

4. **Take extra precaution for BYOD environments.**

While BYOD offers flexibility and lets you leverage assets your workers already own, it comes with increased risks. If your employees use their own phones or tablets at work, one rogue third-party app can wreak havoc on your security and allow unauthorized access to your company's information. One option is to have separate containers on the device that workers log into, housing all company applications and data in a secured space.

5. **Don't forget your other IoT devices.**

The retail industry is fairly new to the Internet of Things, but innovations such as smart shelves that detect low inventory and systems that send digital coupons to consumers entering the store are gaining adoption by tech-savvy retailers.

However, today's IoT devices are often poorly secured and vulnerable. Late last year, hackers used security cameras to create a large denial-of-service attack that brought down large pieces of the Internet. Something similar could easily happen within your own networks. Anyone remember the old SQL Slammer worm from 2003? Make sure your Wi-Fi access points are secure and establish multiple security levels to protect critical systems. Several network access control (NAC) solutions also support mobile devices.

Keep your data secure with managed mobile services

Creating an effective security strategy takes time and resources, but the alternative – letting hackers make off with your customers' credit card information or company trade secrets – is too big a risk to take.

A managed mobile services provider can help you design a security plan that works with your devices, operating systems and company goals. MMS providers also offer consistent monthly spending and the ability to spread out security investments over multiple years, providing financial as well as mobile security.

-Marco Nielsen, *Vice President, Managed Mobility Services, Stratix Corporation*

Marco Nielsen works with enterprises across many verticals to develop mobile solutions that help them navigate the global supply chain efficiently. He understands that supply chain modernization is key to solving the challenges today's businesses face, such as end users' expectations for faster deliveries and order accuracy, all while delivering a high level of service cost-efficiently.