THE THREAT FROM WITHIN -WHEN MOBILE IMPERILS YOUR

BUSINESS SECURITY

By Philip Whitchelo

In today's business world, data security is as important to small startups as it is to enormous multinationals. In the highly digitized 21s t century, a single digital document, which in reality is made up of no more than intangible zeros and ones, could represent millions of dollars worth of company assets. Unlike traditional assets, this digital data is infinitely reproducible, and at a time when more business is being conducted on mobile devices than ever before, infinitely portable.

The benefits of online technologies and big data are vast and varied, and it's nearly impossible to grasp the full extent of the online threats we're exposed to on a daily basis. According to Fortinet in a security survey, the levels of ignorance of complex hazards is dangerously high.

Whether caused by inadequate safety measures or human error, the high number of leaks and security breaches reported in the news can make us wonder just how vulnerable our data really is. The evolution of cloud computing and the boom in tablet and smart phone sales leaves little room for doubt: the remote access phenomenon is moving ahead full steam.

"The access of data anywhere from any device or platform poses a very challenging security environment for organizations," says Bala Venkat, chief marketing officer at Cenzik, a security solutions provider. "BYOD [Bring Your Own Device] further complicates the matter [by] driving companies to develop air tight security policies. Mobile security has thus become an urgent mandate on every company's technology roadmap."

This now poses the question: What should businesses take into account? Here are data security concerns to consider as businesses shift away from in-house office computing to "business on the go."

The access of data anywhere from any device or platform poses a very challenging security environment for organizations," says Bala Venkat, chief marketing officer at Cenzik, a security solutions provider.

1

Mobile Device Loss

One of the biggest concerns for businesses is data stored on devices that could potentially get lost or stolen. Fingerprint scanners, passwords, and swipe patterns may keep small time burglars away, but more experienced hackers can bypass these measures.

Doug Herman, managing director of the eDiscovery and Digital Forensics Practice of UHY Advisors FLVS Inc., acknowledges that "settings certainly make a difference in how easy it is for a person with malicious intent to access data. Enabling the requirement for a password or fingerprint scan to access the phone goes a long way; however, for someone that really, really wants access to the phone, virtually no 'set' of settings will help."

According to Herman, some companies have implemented measures for that exact situation. He says, "An organization may require that a management application be installed on the phone, which forces the use of a strong password to access data. They may reserve the right to remotely 'wipe' the phone of all data (company and personal), should it be reported as lost or stolen"

2

Applications and Cloud Accounts

With dozens of applications with access to information, both personal and work related, gathered on your mobile device, users quickly lose sight of how much data is actually exposed.

“Storing unencrypted sensitive data on mobile devices is a significant cause for concern, but the often unsecured Web services commonly associated with mobile applications can pose an even bigger risk,” says Venkat.

A recently published survey on Web application security by Vanderbilt University suggests that 49 percent of applications online are unsafe. As a backup precaution, most remote device users automatically sync files to private cloud accounts like Dropbox or Google Drive. And according to Fortinet, 70 percent of employees worldwide use their personal cloud account for work purposes.

Peter Martini, cofounder and COO of network security solutions provider iboss Network Security, explains that issues with private cloud service accounts can easily arise through lack of sufficient knowledge. “A rising threat to businesses is the ‘shadow IT,’” he says. “This is an industry term for when users use an unapproved SaaS account to share files with customers. The employee does so without malice and unintentionally violates company policy. The company data is now stored in this rouge SaaS account, which can lead to a compliance violation or potential data loss.”

It is called the public cloud for a reason. When storing files online, users believe access to be restricted, which is not necessarily the case. If you want to share confidential information you need to make sure to encrypt your data, which isn’t a feature open services usually provide.

3

Network/Connectivity

When on business trips, free WiFi might seem like the perfect cost-saving alternative to paying scandalous roaming fees. It does, however, pose a threat.

“Public WiFi hotspots at places like coffee shops and airports are notoriously dangerous for mobile users,” says Sunday Yokubaitis, president of Golden Frog, an online services provider. “Any business that has employees who work remotely at these types of locations should install a personal VPN service on their employees’ mobile devices. A VPN will encrypt the Internet connection so business tasks like email communication, data transfers, and web browsing are kept private and secure.”

Peter Martini shares Yokubaitis’ concerns. “If accessing data remotely, businesses should ensure that employees are doing so through an encrypted VPN or through a company portal that is secured through SSL requiring a login where employees can access files,” he says. “Another alternative is utilizing SaaS services where companies can upload documents. This approach requires almost no investment into the business nfrastructure.”

4

Data Management

According to a recent survey by security technology solutions provider Lookout, 90 percent of businesses allow employees to bring their own devices to work (BYOD), "yet only half of these companies require employees to enroll in a security program as a prerequisite for BYOD use," reveals consumer safety advocate Jenny Roy.

Unless employees rigorously ensure that personal and businesses devices are kept separate, personal and business information will eventually blend. Doug Herman points out that on mobile devices, managing data works differently than on computers. "The functionality doesn't exist to segment information as easily," he says. "Take text messaging as an example – the mobile device likely only has one application that allows for the send/receipt of texts. If you're texting both friends/family as well as coworkers, those messages will be commingled together."

For Peter Martini, the most effective way to separate company from personal data is to use a Mobile Device Management (MDM) or Mobile Application Management solution. "These technologies allow businesses to create a 'lock box' app where employees can access business documents on a device. Essentially, it presents itself as an APP on the device and, when accessed, company documents are available. The same features are available for company email. The data is actually stored in the cloud and not on the device," he explains.

Sunday Yokubaitis suggests, "Use different applications for work and personal stuff. For example, Dropbox might be just fine for storing personal photos, but you might want to choose a completely different and more secure service for storing work-related files."

All facts considered, industry experts advise businesses to extend security measures beyond their own database and in-house network and consider the hazards posed by mobile devices. It is also important that businesses invest in training staff. A small investment in time and resources will help safeguard against potential data leaks and crises. Safe browsing and data handling is a skill that can be learned, and it will become increasingly vital that your employees have a hold on these skills.

About the Author

Philip Whitchelo is vice president of strategy at Intralinks, dealing in areas such as product development and business planning across Europe, the Middle East, and Pacific Asia. Connect with me on Facebook, Twitter and LinkedIn.