Managing Mobile Device Security Essential

Jordan Shropshire
Managing mobile device security essential

Mobile, hand-held devices will become the leading source of internet traffic within the next 3 to 5 years, eclipsing more traditional devices such as laptops and desktop computers.

Indeed, organizations of all sizes are increasingly outfitting their workers with mobile phones instead of laptops.

Providing mobile devices over PCs makes sense. They are relatively less expensive, require less user training, provide a wide array of features and call for smaller initial investments over wireless computer networks.

Some businesses require their employees to pay part of the monthly connectivity fee, further reducing costs.

In summary, there are significant benefits in adopting the smart phone. As a result, individuals are more beholden to their hand-held devices than ever. Despite the increased reliance, most smartphone users are in the dark when it comes to securing their mobile devices.

This article outlines practical suggestions for improving mobile device security within the enterprise.

The single best way to improve mobile device security is to increase threat awareness among users. Mobile phones are, in reality, miniatures. They can install third-party software and remain online indefinitely. These are the prerequisites for malware attacks.

Just as viruses grew when personal computers became more mainstream and sophisticated, viruses, worms and Trojan horse attacks are becoming increasingly common for mobile phones.

Therefore, smart phone users should apply the same precautions to their smart phones that they would for ordinary laptops or desktops.

Mobile devices are equally susceptible to attacks originating from browsers, e-mail messages or attachments, downloads and text messages.

Organizations should devise strategies for implementing smart phone security. These policies should answer basic questions, such as who will provide the device and who is responsible for charges and damaged or missing devices.

ACTION ITEMS

- Improve security threat vigilance.
- Create and convey policies for acceptable use.
- Acquire antivirus software for mobile devices.
- Activate device authentication software.
- Prepare for missing/damaged hand-helds.
- Routinely back up important data.

If employees are expected to supply their own mobile devices, the organization will have less control over device security. If the organization provides hand-helds, there should be a clear understanding regarding responsibility for replacement costs, should devices become lost or damaged.

Furthermore, there should be a system for reporting missing or stolen devices. Large organizations lose thousands of devices each year. When a device is lost, it is necessary to account for the data the device held, the authentication/access privileges stored in the phone and to warn individuals who may be included in contact lists.

In addition, organizations should determine which mobile device functions will be incorporated into the business.

For instance, it seems obvious that employees will use smart phones for calls and text messages, but should they also use them for sending and receiving potentially sensitive e-mail messages?

Smart phones also contain Web browsers. Should employees be allowed to use smart phones to connect to corporate intranets? Should certain websites or Web applications remain off-limits to mobile phones?

As a starting point, security plans for mobile devices should take up from security controls for laptop computers.

Another recommendation involves user authentication. Unattended or lost mobile devices may end up in the hands of strangers. Their intentions may range from benevolent to sinister.

It is therefore recommended that users enable the password authentication system built into the operating systems of their devices. All major mobile device manufacturers incorporate software that allows users to set passwords which must be entered in order to grant access to the device. Unless the user correctly enters the password, he or she will not be able to interact with the software.

Finally, users should offload and back up important data from their mobile devices. All too often, hand-helds are lost, broken or misplaced. Their software may fail or a device battery may die.

Ultimately, it is necessary retain access to documents, communications and other data stored on smart phones. Therefore, it is recommended that a regular schedule of backups be conducted on devices.

In some cases, it is possible to automatically sync devices when connected to a computer via USB docking station. By considering these recommendations and enacting a sensible plan, businesses and individuals can cover significant ground toward improved mobile device security.

Jordan Shropshire is an assistant professor of information technology at Georgia Southern University and be reached at jshropshire@georgiasouthern.edu.

Development and Renewal Authority hosts ribbon-cutting for La' Berry Frozen Yogurt Café

At the event were shop owners Lori Long and Jack Largent as well as representatives from the City of Savannah, the SDRA, the Sanitation Outreach and Education Coordinator, the Savannah Entrepreneurial Center and the Downtown Business Association.

La' Berry Frozen Yogurt Café, which opened between Barnard and Jefferson streets July 2, boasts yogurt that is "healthy, delicious and good for your digestive tract," according to Long and Largent.

The frozen yogurt shop offers a self-service “weigh and pay” concept. It features eight yogurt flavors that change regularly as well as more than 30 topping options.

La' Berry Frozen Yogurt Café is open 11 a.m. to midnight daily.

Business in Savannah | businessinsavannah.com | 912-652-0300