CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Securing Mobile Devices aka BYOD

Key Message: Ensuring the security of personal mobile devices that have access to enterprise networks requires action from employers and users.

Executive Summary

Users want to use their own personal devices (often referred to as BYOD – Bring Your Own Device) to perform work, to connect to organizational networks and applications, and to access organizational data. This is particularly true for professionals who have grown up using these devices as a way of life. Enabling BYOD enhances productivity (user response), improves response time, and may provide for greater organizational control of the devices that connect to their networks. That said, the increased use of personal devices has provided a new target for attackers. The implementation of comprehensive policies and practices is essential to mitigate new risks that come with supporting the use of these devices.

In this podcast, Joe Mayes, a member of CERT's Workforce Development team, discusses some of the critical actions that organizations should take to help secure users' personal mobile devices.

PART 1: MOTIVATION FOR BYOD; POLICY AND PRACTICES

Motivation

BYOD (Bring Your Own Device) is the concept of users being permitted to use their own personal devices to connect to organizational networks and use these devices to perform work.

In the military, key leaders were the first to ask for this capability. President Obama made it clear that he was going to use his Blackberry.

People only want to have one device to perform their work-related and personal transactions. They don't want to be burdened with multiple devices to do the same things.

Policy Questions

Key questions to address in policy include:

- First of all, do you permit BYOD in the work place?
- If the answer is yes, what do you allow users to connect to/access? Email? Internal websites? Data on corporate servers?
- Can users run search queries on corporate databases? Can they operate and run servers? Can they operate and run applications?
- What can users do with the access they have?
    - With respect to data, read only? Read-write?
    - Can users change and delete documents?
    - Can they download and store external documents?
    - Is data downloaded to their devices or can they only access it virtually?

The answers to each of these questions result in a wide range of security issues and controls to consider.

Critical Security Practices

Employer practices include:

- a decision on what devices are permitted, for example, iPhones and Androids. The more devices you permit, the more security procedures you will require. Some organizations limit the types of devices.
- two considerations for encryption
    - between the mobile device and the home office (to protect data in transit)
    - any data (including passwords) on the device, in case the device is compromised or lost
- training
- implementation of security controls with proper enforcement

Vendor products for mobile device management across the enterprise are available.

User practices include:

- exercising caution in connecting to public networks
- protecting passwords that are required for authentication (using encryption if these are stored on the device)
- being aware of and complying with corporate policies

Users are often unaware of their responsibilities until something bad happens such as having their phone compromised or lost or having their identity stolen.

PART 2: DEPLOYMENT CHALLENGES; DEALING WITH BREACHES

Challenges

The challenge in putting BYOD policies in place is similar to other policies that don't get followed. Users think of their devices as their devices, and they often are not willing to have someone else tell them what they can and can't do.

Even when an organization has control of a computing asset (servers, desktop, laptops, etc.), the assets still get compromised and data is still stolen. Mobile devices only exacerbate the situation.

Given that you really can't protect the device, protecting the data is critical. Many approaches to protecting data are automated and work in the background, which is a better security solution.

Such approaches often have a means for automatically wiping a device based on defined triggers such as:

- an excessive number of days since the device last connected
- invalid connection attempts
- report of a lost device

It is often challenging to obtain logs from mobile devices. There has to be a proactive action to send logs from devices to a centralized location where they can be analyzed. Some device vendors have unique solutions; some treat mobile devices in the same fashion as they treat desktops and laptops.

The ability to access logs may affect an organization's decision as to which devices to support.

Breaches

Mobile devices have capabilities that haven't been considered for more traditional devices including:

- phones
- ability to record
- video
- cameras

All of these methods can be used to move information and thus can be used by attackers. For example, an incident at the Jackson Health System in Florida resulted when a former hospital volunteer used his cell phone to take pictures of more than 1,000 patient records. He was then able to walk out of the facility with this information.

Even though the data was secured on the computer where it was stored and accessed, there was no means to prevent someone taking a picture of the screen. Jackson Health's solution was to ban the use of cell phones by hospital volunteers.

The lesson here is that you can put a policy in place and then modify it based on experience.

PART 3: GETTING STARTED – FIRST STEPS

Useful Ways to Get Started

Start with a risk assessment, which includes:

- understanding which worst case scenarios you are willing to tolerate
- understanding which risks need to be proactively mitigated and which ones you are willing to accept

Start with a pilot project. A few alternatives include:

- selecting those in the organization who have the greatest need. Often this includes the IT department or corporate executives.
- selecting a sample of individuals in various roles across the organization to see how the use of mobile devices works for different use cases
- starting with a particular device such as an iPhone or an iPad and then add devices once lessons learned have been addressed
- determining which applications should be accessed first such as email or those in the field being able to send information to corporate applications

Make adjustments to policies and future roll outs based on pilot project results.

Resources

[Chen 2012] Chen, Lily; Franklin, Joshua; Regenscheid, Andrew. *Guidelines on Hardware-Rooted Security in Mobile Devices, NIST Special Publication 800-164*. National Institute of Standards and Technology, 2012.

[Souppaya 2012] Souppaya, Murugiah & Scarfone, Karen. *Guidelines for Managing and Securing Mobile Devices in the Enterprise, NIST Special Publication 800-124 Revision 1*. National Institute of Standards and Technology, 2012.

NIST Telecommuting and Mobile Computer Security Policy (NIST draft).

CTIA Stolen Smartphones Quarterly Status Update The Wireless Association® ("CTIA"), in coordination with the Federal Communications Commission and the Major City Police Chiefs, announced a voluntary commitment by CTIA and participating wireless companies to take certain actions to help law enforcement deter smartphone theft and protect personal data.

US Department of Defense Mobile Device Strategy, June 2012.

US Department of Defense Commercial Mobile Device Implementation Plan, 15 February 2013.

US National Security Agency Information Assurance Directorate. *Mobility Capability Package Version 2.1*, 15 December 2012.

U.S. Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) Security Technical Implementation Guides (STIGS) and Supporting Documents, specifically Mobility Policy Version 2 Release 1 STIG, March 8, 2013.

CERT Podcast: Mobile Device Security: Threats, Risks, and Actions to Take, 31 August 2010.