Cybersecurity and Mobile Devices

Instructor: While mobile devices continue to evolve and are prevalent in today's business environments, organizations have to carefully balance the ability to effortlessly and efficiently conduct on-demand business functions while protecting data. The attack surface for mobile devices continues to grow; with new functionality and new applications come new vulnerabilities. The risk of a device being stolen or compromised and exposing sensitive information is a growing concern.

A significant part of mobile device security is awareness training to educate users on physically securing their device and following best practices for restricting access to the underlying applications and data. From a business perspective, Mobile Device Management, MDM, is a wholistic approach for managing mobile devices through policies, configurations, and infrastructure. MDM software suites allow organizations to adopt an in-house self-managed deployment method.

There's also cloud-based deployments where MDM is a software-as-service; configurations, updates and maintenance are handled by a third party. Which model employed for end-to-end device, data, and communications security depends upon a business's internal resources and objectives.

The organization's device deployment model is also a consideration for mobile management. BYOD, Bring Your Own Device, allows employees to use personal devices for work functions. Employees must adhere to the organization's mobile device security policy before connecting to the internal network. Security can be more difficult when more responsibility is put on the user. With a COPE model, devices are corporate-owned but personally-enabled. The organization purchases devices and issues them to users for both work and personal use. The security controls and configurations are managed by the organization similar to an issued desktop or laptop.

Choose you own device is similar to COPE with the difference being the organization allows their users to select the type of mobile device they wish to use. Commonly, it will require company security configurations. Corporate-owned is the strictest model in terms of security. The organization purchases and configures the device and prohibits any personal use.

A mobile device architecture model designed to secure data and communications with devices is Virtual Desktop Infrastructure. With VDI all applications and data are stored on a remote server with traffic encrypted between the server and the device. This centralized model makes managing applications, data, and updates in a single location more

efficient than having to deploy to many devices and different operating systems.

Discussing mobile communications would be amiss if Internet of Things was not included. IoT describes the growing network of devices that connect to the Internet and collect, process and exchange data. The mundane has become 'smart' with real-time data to better inform actions. Sensors gather and report data that is then analyzed into usable information like the precise location of postal packages or luggage at airports to more complex activities like HVAC controls and weather patterns that drive agricultural decisions.

IoT devices are vulnerable to compromise. A survey by digital security company Thales Group reported that 48% of businesses are not able to detect if an IoT device suffers a breach. With estimates of close to 30 billion devices connected to the IoT ecosystem, it's concerning. Potential attacks include IoT devices participating in a bot for denial-of-service attacks, a complete takeover where the attacker controls the data sent by a sensor, or communication jamming that prevents a sensor from transmitting. Functionality and convenience have been the priority for IoT; security is an after-thought.

While there are IoT-specific frameworks and guidance such as from the IoT Security Foundation, standards are not established.

IoT and mobile device use will continue to expand. Not just for conveniences: email on-the-go, purchases with a swipe, or remote control of home amenities. Devices are also relied upon in many industries and for security functions like multi-factor authentication. They're an important facet of everyday living. Managing risks associated with mobile devices is a critical concern.

Addressing threats to mobile computing is a multi-level approach: The physical device - operating system vulnerabilities or operating characteristics. Applications - third-party applications that may expose data, or unpatched applications. Communications - wireless or cellular networks. Users - physical security of a device and honoring acceptable use policies.

There are resources to help enterprises understand mobile computing threats and managing those risks.

For instance, the Open Web Application Security Project, OWASP, mobile security project is a source that includes top 10 mobile security issues, an application verifications standard, and mobile security checklist.

Staying current on mobile threat trends and ensuring user awareness are important components for information security. Normal activities that are part of typical

device usage may be vulnerabilities: An innocuous application could pilfer data; a link on a social media site may contain malware; wireless access at the public library could be capturing traffic; using a USB charger is not just charging the device battery, but potentially transmitting data; Yes, 'Juice jacked' when simply intending to recharge a device. The list goes on.

Mobile business functions allow for high efficiency and convenience. It is only going to expand as technology gets faster, cheaper, and easier to use. Mitigating mobile security risks to protect sensitive and proprietary information requires a strong defense strategy. Best practices include user education and awareness and a mobile device management solution that includes frequent trend and threat information updates.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM18-0098