SPRING 2020 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we provide an overview of mobile device management and malware prevention. With the unprecedented increase of telecommuting resulting from the Coronavirus pandemic, secure data management by organizations is more critical than ever.

Mobile Device Management's Time to Shine

One of the upsides of the Coronavirus response measures the world is undertaking to slow the spread of the COVID-19 illness is that work functions formerly assumed to be essential in-house activities are being adapted for work-at-home situations. The necessity of reducing the contagion has become a catalyst to embrace technology innovation. However, the rapid pace at which employees had to transition from in-house to in-their-homes highlights the need for organizations to get ahead of the challenge of mobile devices in the modern, dispersed workplace. This is where Mobile Device Management, or MDM, fits nicely within the realm of IT department functions.

What is Mobile Device Management?

MDM is the administration of mobile devices in such a way that their functionality, mobility, and security is balanced with the need to protect the integrity and security of an organization's network(s) and data. MDM requires IT professionals to manage multiple elements including mobile service providers, mobile device operating systems, and an expanding array of mobile devices capable of connecting to a network or another networked device. MDM sits within the larger functions of Enterprise Mobility Management, the control of devices and applications that allow for mobile device connection to a network or networks, and Unified Endpoint Management, the management of all devices, mobile or not, that connect to a network or networks.

In administering MDM, IT professionals provide end-to-end security with an agent, which is a software solution specifically for MDM, and a server that can be either physically present or cloud-based. The basic functions of MDM include device inventory and tracking, distribution of whitelisted apps, prevention of restricted uploads and downloads, password management, and enforcement of data encryption rules. Once the device is configured in accordance with an MDM agent, many functions, including remote wiping of data, are done "over the air."

Increasing Device Security through MDM

Irrespective of device type or operating system, it is possible to increase device security by employing MDM. With MDM, IT professionals can monitor devices for potential security risks such as users sending data to personal, cloud-based storage which could create leaks of critical data. By adding Mobile Application Management, organizations can not only remotely install and update whitelisted apps, but also block blacklisted apps from being installed (at least on the work side of a partitioned device). One way in which this feature protects organizations is that if you are working from home and your child attempts to download a potentially malware infected app, MDM will prevent the installation of any unrecognized and unauthorized software. Some organizations have even created enterprise app stores which provide a variety of organization-approved apps for employees to download. By creating these app stores as part of their MDM activities, organizations can specify which mobile devices can download which apps, providing a higher level of security. Because MDM prevents users from changing settings and blocks downloading potentially dangerous apps while also enabling remote malware and security scans, cybersecurity mishaps are reduced. In the event a device is lost or stolen, many MDM administrators can perform remote locking, password changes, and device wiping to protect an organization's data. Additionally, MDM provides centralized control to reduce risk presented by less security-conscious employees. No solution is invincible, but employing MDM is a potential solution for dealing with employees who work via a satellite office, home office, or beyond the reach of the corporate office for other reasons.

Security can be increased even further by combining MDM with partitioning for smartphones and tablets. By isolating the personal data and work data that are often freely combined in a Bring-Your-Own-Device environment, employees can still retain their autonomy over their social media apps, email accounts, entertainment apps, photos, videos, music, and other personal data without sacrificing or exposing an organization's data to the prying eyes of cybercriminals. With the constant flow of phishing scams, Trojan malware, and other methods by which blackhat hackers attack, the double layer of protection afforded by MDM regulating activity on the work side of the partition can save an organization time, frustration, money, and potentially its reputation by preventing a data breach before it starts.

Finally, many MDM programs, and some smart-device operating systems, offer the advantage of remote enrollment for mobile devices including laptops and tablets, as well as accessories such as smart watches. Remote enrollment allows administrators to create identities and set permissions for devices without ever having to handle them in house. This ability makes onboarding remote workers easier, and, in the event of an emergency where new devices need to be added rapidly to the organization's network, is a boon for IT departments.

If your organization is relying increasingly on mobile devices, as most entities are, it's essential that MDM become part of your organization's best practices. Mobile devices are fantastic for keeping us connected irrespective of distance, but we need to be smart and careful about protecting the data on them and the larger networks to which they connect.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com. In the short term, she is available for webinars and remote e-conferences.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: