



How to Keep Jailbroken iPhones Off Corporate Networks

3 August 2010

Now that **jailbreaking** the iPhone and iPad is **legal**, corporate enterprises have even more to worry about.

Until 26 July 2010, corporate IT and security managers only had to worry about keeping rogue iPhones and their associated security and compliance holes in check. With the latest government ruling, however, jailbroken iPhones and iPads present even greater threats to the privacy and security of corporate networks.

Winn Schwartau, Chairman of **M.A.D. Partners, LLC**, the **smartphone security company** said, "iPhone users can now download apps from anywhere they choose, not just the iTunes store. This signifies a far greater risk to companies who are trying to leverage the unique capabilities of the Apple platform. But Mobile Active Defense provides a strong, workable and automatic solution that solves the jailbreaking problem on corporate networks."

To maintain high levels of security, privacy and compliance across the enterprise, IT administrators must have complete control over devices that connect to the company network, use company resources and store or process sensitive data. They must meet HIPAA, GLBA, PCI, SOX and myriad other compliance guidelines, especially in the mobile arena.

With M.A.D.'s powerful **Mobile Enterprise Compliance and Security (MECS) Server**, says Schwartau, "we can detect jailbreaking within one minute. That's pretty cool. Once this clear violation of security policy is discovered, the MECS managed firewall issues immediate remediation options to the administrator."

With Mobile Active Defense, the iPhone stays in communication with the MECS Server. If any company-defined 'out of compliance' or 'out of policy' conditions are detected on any of the organization's iPhones, an immediate alert is generated.

According to M.A.D. Partners' CTO, Rob Smith, "The administrator configures the MECS Server to inspect the security state of the iPhone. How do we do it? That's our secret sauce. How quickly the administrator responds to a remediation request from the MECS Server is what is really important. We give him all the tools he needs."

The remediation response taken by the company is policy driven and enforced through the MECS Server. The administrator can choose to isolate the offending iPhone/iPad from connecting to anything, pending further investigation. Or s/he can choose to wipe the entire device with no notification to the user. Lastly, the administrator can choose to be notified by email, SMS or MECS Server console popup, allowing him to individually choose the remediation response.

The M.A.D. Mobile Enterprise Compliance and Security (MECS) Server supports the U.S. Government's NIST 800-53 critical guidance for mobile device access control and media storage, as well as those for ISO 27001 that map directly to HIPAA, GLBA, PCI and SOX.

Adding MECS Servers to any enterprise does not require any changes to existing security or IT infrastructures and can be up and running within one day.

Contact/ Jackie Baumann jbaumann@MobileActiveDefense.com or 1.941.266.3819

Phone/ 1.877.HALOM.A.D. www.MobileActiveDefense.Com