ZUR SOFORTIGEN VERÖFFENTLICHUNG

DEVICELOCK-UMFRAGE ZUM iPHONE-SICHERHEITSKONZEPT: MANGELNDE VORBEREITUNG IN UNTERNEHMEN

Moskau, Russland – 25. März 2010 – Device Lock Inc., ein weltweit führendes Unternehmen für Endpoint Data Leak Prevention-Softwarelösungen, gibt heute die Ergebnisse seiner Umfrage zum Sicherheitskonzept für iPhones in Unternehmen bekannt. Es stellt sich heraus, dass nur wenige der befragten Unternehmen Maßnahmen zur Bekämpfung der Risiken ergreifen, die durch die verstärkte Nutzung von iPhones am Arbeitsplatz entstehen. Sieben Monate lang wurden mehr als 1000 Antworten auf die Frage erfasst: „Haben Sie Maßnahmen ergriffen, um Ihr Unternehmen gegen die Sicherheitsbedrohung durch iPhones zu schützen?“ Wie vorauszusehen war, entsprach die Beteiligung der geografischen Verteilung der weltweiten Kundenbasis von DeviceLock: etwa zwei Drittel der Antworten kamen aus Nordamerika und Westeuropa, das restliche Drittel aus Osteuropa, dem Mittleren Osten und Südostasien. Weniger als 40 Prozent der Unternehmen bejahten die Frage nach konkreten Sicherheitsmaßnahmen für iPhones. Insbesondere Unternehmen aus der westlichen Welt, beispielsweise Nordamerika und Westeuropa, erklärten, dass das Sicherheitsrisiko durch das iPhone ein Thema ist, das immer wieder zurückgestellt wird. So beantworteten auch nur etwa 25 Prozent der befragten Unternehmen der westlichen Welt die Frage nach konkreten Sicherheitsmaßnahmen mit „Ja“. Diese Tendenz ist bei den Unternehmen aus Osteuropa, im Mittleren Osten und Südostasien nicht erkennbar. Insgesamt wurde die Frage nach konkreten Sicherheitsmaßnahmen in Osteuropa, im Mittleren Osten und Südostasien zu fast 60 Prozent bejaht.

„Obwohl diese Umfrage, die über eine Website erfolgte, von sich aus schon Beschränkungen unterliegt, legen die Ergebnisse die Vermutung nahe, dass das Risiko des iPhones für die Datensicherheit in Unternehmen generell unterschätzt wird,” erklärt Ashot Oganesyan, Chief Technology Officer und Gründer von DeviceLock. „Da die iPhone-Plattform bei den Verbrauchern sehr populär ist und immer weiterentwickelt wird, ist der Einsatz am Arbeitsplatz in Zukunft jedoch unvermeidlich.“

„Der Grund für die unterschiedliche Einschätzung des iPhone-Risikos in den gut entwickelten IT-Märkten im Westen im Vergleich zu den aufstrebenden IT-Märkten im Osten kann darin liegen, dass sich die IT-Verantwortlichen in den westlichen Unternehmen auf fest verwurzelte Lieferanten, wie RIM und Microsoft, stützen, die ihnen Rückendeckung geben und Smartphones nicht ohne die erforderlichen Sicherheitsfunktionen für Policy Enforcement und Verschlüsselung einführen,“ vermutet Ashot Oganesyan. „Die Apple iPhone-Entwicklergemeinschaft hat jedoch weniger zu verlieren und könnte eher das Ziel erreichen. In der Zwischenzeit sind die IT-Verantwortlichen in den Entwicklungsländern aufgrund wirtschaftlicher Notwendigkeiten und geringerer Erwartungen bereits näher an dem „Konvergenztraum“, all das tun zu können, was sie sonst mit einem Laptop und Telefon tun können. Sie haben daher einfach schneller erkannt, wie stark das iPhone als „Konkurrent“ im Unternehmen ist. Wir unterstützen DeviceLock-Kunden und Interessenten weltweit darin, Vorsichtsmaßnahmen für iPhones am Arbeitsplatz zu ergreifen,“ erklärt er.

Ebenso wie andere komfortable Geräte, die den Arbeitsplatz erobert haben – von CD-ROMS über lokale Drucker bis hin zu Thumb Drives – bietet das iPhone mehr Flexibilität und Produktivität und birgt gleichzeitig ein größeres Risiko für gefährliche Datenlecks über die Endpunkt-PCs der Unternehmen. Die Vergangenheit hat gezeigt, dass IT-Abteilungen in Unternehmen am besten fahren, wenn sie klare Richtlinien für neue Geräte erstellen und sich die entsprechende Ausrüstung beschaffen, um diese Richtlinien auch umzusetzen. Das besondere Risiko mit mobilen Kommunikationsgeräten wie dem iPhone besteht darin, dass ein Mitarbeiter durch eine lokale Datensynchronisation alle netzwerkbasierten Sicherheitslösungen komplett umgehen kann. Mit DeviceLock können Sicherheitsverantwortliche eine Richtlinie für Mobilgeräte einführen, die den Datenaustausch nur für bestimmte iPhones und nur für die Datentypen erlaubt, die der Mitarbeiter für die Erledigung seiner Aufgaben benötigt.

Mit einem zum Patent angemeldeten lokalen Synchronisierungsfilter gibt DeviceLock Sicherheitsadministratoren die zentrale Kontrolle darüber, welche Datentypen bestimmte Benutzer oder Benutzergruppen zwischen dem Unternehmensrechner und lokal angeschlossenen iPhones und iPods synchronisieren dürfen. DeviceLock kann ebenso zahlreiche Datenobjekttypen für iTunes®-Protokolle erkennen und filtern. So können Administratoren die Synchronisierung von Dateien, E-Mails, E-Mail-Anhängen und -Konten, Kontakten, Aufgaben, Notizen, Kalendereinträgen, Lesezeichen und sonstigen Datentypen wahlweise erlauben oder blockieren.

DeviceLock bietet ein skalierbares, zugleich jedoch leicht verständliches zentrales Management und eine Administration über ein speziell entwickeltes MMC-Snap-in, das komplett in den Gruppenrichtlinieneditor im Microsoft Active Directory (AD) integriert ist. Der DeviceLock-Agent kann vollständig aus einer bestehenden Microsoft AD-Domäne heraus verteilt, konfiguriert und verwaltet werden. Eine separate Komponente, der DeviceLock Enterprise Server (DLES), steht für die zentrale Protokollierung, Audits und die Spiegelung der Benutzeraktivitäten an geschützten Endpunkten zur Verfügung. Die granularen Ereignisprotokoll- und Dateispiegelungskonfigurationen machen eine Nachverfolgung, Beweissicherung und Analyse der Benutzeraktionen möglich und erlauben die von unternehmensinternen Sicherheitsrichtlinien geforderte Abbildung von Systemereignissen und Datentransfers. Zusätzlich kann der DLES den Status des DeviceLock-Agenten auf allen im Netzwerk vorhandenen Computern in Echtzeit auf Konsistenz und Integrität überprüfen und im Falle einer Abweichung eine zuvor definierte Master-Policy übertragen. Mit dieser Mischung aus konfigurierbaren Richtlinien-Parametern und Optionen erleichtert DeviceLock die Definition und Umsetzung einer unternehmensweiten Sicherheitspolitik gemäß dem “least privileges”-Prinzip. Systemadministratoren können anhand des Aufgabenbereichs der einzelnen Benutzer, Gruppen oder Abteilungen Profile definieren, indem die Benutzer so wenige Rechte wie nötig erhalten. Dadurch wird das Risiko von Datenlecks unternehmensweit reduziert. Mit DeviceLock können Unternehmen ihre Sicherheitsrichtlinien und Industrienormen optimal durchsetzen.

Über DeviceLock Inc.

Seit der Unternehmensgründung im Jahr 1996 entwickelt und vertreibt DeviceLock Inc. (anfangs unter der Firmierung SmartLine) Endpoint Device Control Softwarelösungen für kleine, mittelständische und Großunternehmen aller Branchen. Weltweit ist DeviceLock auf mehr als vier Millionen Rechnern in mehr als 60.000 Unternehmen und Behörden installiert und stellt sicher, dass alle Endpoint-Schnittstellen der Unternehmensnetzwerke geschützt sind. Zum breiten Kundenstamm von DeviceLock Inc. zählen unter anderem Finanz- und Kreditinstitute, Landes- und Bundesbehörden, militärische Einrichtungen, Anbieter aus dem Gesundheitswesen, Bildungseinrichtungen und Telekommunikationsunternehmen. DeviceLock Inc. ist ein internationales Softwareunternehmen mit Niederlassungen in San Ramon (Kalifornien, USA), London (Großbritannien), Ratingen (Deutschland), Moskau (Russland) und Mailand (Italien).

Weitere Informationen zu DeviceLock erhalten Sie unter www.devicelock.com bzw. www.devicelock.de

DeviceLock Europe GmbH
Mathias Knops
Halskestraße 21
40880 Ratingen
Tel.: +49 2102 89211-0
E-Mail: info@devicelock.de
Internet: http://www.devicelock.de

DEVICELOCK PRESSE KONTAKTE
Marina Baader/Franz-Rudolf Borsch
presse-seitig
St.-Cajetan-Str. 10
81669 München
+49 89 45207500
marina.baader@presse-seitig.de
rudolf.borsch@presse-seitig.de