ZUR SOFORTIGEN VERÖFFENTLICHUNG

DeviceLock 7.1 – Schutz gegen Cyber-Spionage

Ratingen, 12. Juli 2011: Mobilgeräte sind aus der Arbeitswelt nicht mehr wegzudenken: Sie sind Träger sensibler Firmendaten und Einfallstor für hochprofessionelle Cyber-Spione ins Firmennetz. Sicherheitsverantwortliche sind also gefordert, schnellstmöglich geeignete Abwehrmaßnahmen zu ergreifen. Worauf es dabei ankommt, erklärt Pascal Kurschildgen, Forensics Experte und externer Datenschutzbeauftragter. „Endpoint DLP-Lösungen müssen heute den Abfluss geschäftskritischer Daten verhindern, ohne jedoch Benutzern die Vorzüge mobiler Kommunikationswerkzeuge zu nehmen. DeviceLock 7.1 blockiert daher nicht einfach Schnittstellen, sondern setzt patentierte Kontext-Content-basierte Filtertechniken auf allen Arbeitsrechnern im Unternehmensnetz ein, die den Transfer sensibler Inhalte und die Ausführung kritischer Applikationen zuverlässig verhindern. So sind Unternehmen und ihre Mitarbeiter vor Datenverlust und Datenkorrumption besser geschützt. Moderne Endpoint Data Leak Prevention-Lösungen wie DeviceLock sollten zur Grundausstattung eines jeden Unternehmens zählen."

Tatwaffe Mobilgerät – Crime Zone, do not cross

Für Unternehmen bedeutet die zunehmende hochprofessionelle Cyber-Kriminalität einhergehend mit der rasant steigenden geschäftlichen Nutzung von Mobilgeräten ein essentielles Sicherheitsrisiko. Denn durch das Installieren von Schadsoftware oder das Surfen im Internet können sich Smartphone-Besitzer jederzeit einen Trojaner einfangen, der darauf befindliche Daten ausspäht und an den Hacker sendet. Besonders sicherheitskritisch: Mitarbeiter können mit ihren privaten mobilen Endgeräten bei der nächsten Datensynchronisation das Unternehmensnetzwerk infiltrieren. Kundendaten, Entwicklungsunterlagen und andere vertrauliche Geschäftsunterlagen werden auf diesem Weg ausspioniert oder Daten kompromittiert. Die DeviceLock DLP Suite schließt dieses Datenleck. Sie erkennt mobile Geräte absolut zuverlässig – ganz gleich, über welche Schnittstelle diese am Unternehmens-Client angeschlossen sind. In der zentralen Administrationskonsole des MMC Snap-ins geben Systemadministratoren jetzt die sicheren Nutzungsrichtlinien für die lokale Datenkommunikation von mobilen iOS-Geräten und anderen Smartphones unternehmensweit vor. Gemäß Unternehmensrichtlinien können sie beispielsweise die Synchronisation von Dateien, E-Mails, E-Mail-Anhängen, E-Mail-Konten, Kontakten, Aufgaben, Notizen, Kalendereinträgen, Lesezeichen und verschiedenen Speichermedien für Benutzer ohne per Firmenprofil geschütztem Smartphone komplett blockieren oder selektiv einzelne Datentypen zulassen. Über die Content Aware Rules können Administratoren Benutzern von iOS-Geräten jederzeit beispielsweise die Synchronisationsrechte für offene Dokumententypen nehmen, um Malware vom IT-Netzwerk fern zu halten. Aus diesem Grund kann man auch die Installation und Ausführung von mobilen Applikationen auf Windows Mobile-basierten PDAs oder Smartphones zentral blockieren. Denn raffinierte Angreifer verstecken zunehmend Trojaner in scheinbar harmlosen mobilen Applikationen, um damit unverschlüsselte Geschäfts- und Unternehmensdaten im IT-Netzwerk auszuspionieren.

Tatort Unternehmen – Der Spion in den eigenen Reihen

Auch Wechselspeicher wie USB-Sticks können in den Händen unzufriedener Mitarbeiter oder kriminalisierter Werkstudenten zur Spionage genutzt werden. Sicherheitsverantwortliche sollten daher die Verwendung von CDs, DVDs, USB-Laufwerken und anderen Wechselmedien an den Endpoints der Entwicklungsabteilung im Unternehmensnetz generell mit DeviceLock blockieren. Um den Arbeitsprozess der Mitarbeiter nicht zu behindern, genügen diese Kontext-basierten Kontrollen der lokalen Datenkanäle und der Übertragungsprotokolle für Web-Applikationen wie Twitter und Facebook alleine nicht. Schließlich ist unsere Arbeitswelt mobil, d. h. ein Key Accounter muss seine Vertriebsunterlagen auf dem Laptop immer zur Hand haben und der CEO den aktuellen Geschäftsplan. Daher verknüpft DeviceLock Kontext mit Content, und stellt Sicherheitsverantwortlichen das Modul ContentLock zur Verfügung. Damit können sie alle Dokumente und Dateien nach sensitiven Schlüsselwörtern, Dateitypen, Dokumenteneigenschaften, Datenmustern und anderen vorgegebenen Kriterien filtern und den Datenzugriff selektiv für einzelne Mitarbeiter oder Teams zulassen. Ein Pharmakonzern kann so beispielsweise zentral sicherstellen, dass nur die Gruppe der Chefchemiker Dateien, die eine geheime Formel enthalten, einsehen und bearbeiten

können – und das Kopieren dieser Dateien nur zwei Teammitgliedern erlaubt ist. Je nach Sicherheitslevel kann die DLP-Suite auch die Erstellung von Screenshots über die Windows-Zwischenablage durch nicht-autorisierte Benutzer an den Entwicklungsrechnern verhindern. Für die zuverlässige Umsetzung der vorgegebenen Unternehmensrichtlinien sorgt die patentierte Local Sync Control-Filtertechnik. Sie überwacht zuverlässig den lokalen Datenaustausch zwischen mobilen Endgeräten und DeviceLock-geschützten Computern im Unternehmensnetzwerk.

Die DeviceLock 7.1 Endpoint DLP Suite erhöht das Sicherheitslevel gegen Datenspionage von Außen und Innen. Unternehmen und Behörden können kritische Daten wirksam schützen, ohne ihre Mitarbeiter in ihrer Produktivität einzuschränken.

Über DeviceLock

Seit der Gründung im Jahr 1996 entwickelt und vertreibt DeviceLock Inc. Endpoint Device Control und Data Leak Prevention-Softwarelösungen für kleine, mittelständische und Großunternehmen aller Branchen. Weltweit ist DeviceLock auf mehr als vier Millionen Computern in mehr als 60.000 Unternehmen und Behörden installiert und stellt sicher, dass alle Endpoint-Schnittstellen geschützt sind. Zum breiten Kundenstamm von DeviceLock Inc. zählen unter anderem Finanz- und Kreditinstitute, Landes- und Bundesbehörden, militärische Einrichtungen, Unternehmen des Gesundheitswesens, Bildungseinrichtungen und Telekommunikationsfirmen. DeviceLock Inc. ist ein internationales Unternehmen mit Niederlassungen in San Ramon (Kalifornien, USA), London (Großbritannien), Ratingen (Deutschland) und Mailand (Italien).

Mehr Informationen zu DeviceLock erhalten Sie unter www.devicelock.com und 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 Pressekontakt
Marina Baader / Jürgen Höfling
presse-seitig
St.-Cajetan-Str. 10
81669 München
+49 89 45207500
marina.baader@presse-seitig.de
juergen.hoefling@presse-seitig.de