

Bring Your Own Device – Ein Risiko für die Daten Ihres Arbeitgebers

29.08.2012, 17:35 | IT, New Media & Software

Pressemitteilung von: *Kensington*

Presseagentur: *OnPR GmbH*



Eine neue Umfrage verdeutlicht die Einstellung vieler geschäftlicher Benutzer mobiler Lösungen, dass Datenverlust ein Problem des Unternehmens sei, selbst wenn die Daten sich auf dem eigenen Laptop befinden

Schorndorf – 29. August 2012 – Eine heute von Kensington Computer Products Group, dem weltweit führenden Anbieter von physischen Sicherheitslösungen für mobile Geräte, veröffentlichte neue Studie bestätigt, dass zwar zahlreiche Büroangestellte den Gedanken begrüßen, im Büro die eigenen Geräte zu verwenden (Bring Your Own Device – BYOD), dass die meisten Arbeitgeber aber noch nicht über geeignete Sicherheitsrichtlinien zum Schutz vor Datenverlust verfügen.

Ergebnisse einer unter Büroangestellten in Großbritannien, Frankreich und Deutschland durchgeführten Studie zeigen, dass 67 Prozent der Unternehmen ihren Angestellten erlauben, persönliche Geräte mit zur Arbeit zu bringen, statt Unternehmensgeräte bereitzustellen. Der wachsende BYOD-Trend führt dazu, dass Arbeitnehmer ihre eigenen Notebooks, Tablets, iPads und Smartphones an das Unternehmensnetzwerk anschließen, um die täglichen Aufgaben wie E-Mail-Korrespondenz etc. zu erledigen.

Die Studie von Kensington bringt aber auch schlechte Nachrichten für Arbeitgeber ans Licht: Die Achtsamkeit der Angestellten, was mögliche Schäden durch den Verlust von vertraulichen oder geschäftskritischen Unternehmensdaten angeht, ist geringer, als ihre Sorge um den unbefugten Zugriff auf eigene persönliche Inhalte oder Social Media-Kanäle. Weniger als die Hälfte der Befragten, nämlich 40 Prozent, machten sich Gedanken um mögliche Schäden für ihren Arbeitgeber im Falle eines Geräteverlusts oder -diebstahls.

Viele Arbeitgeber ignorieren das Problem – erschreckende 44 Prozent der Unternehmen geben zu, dass sie über keine Sicherheitsrichtlinien oder -hinweise für Benutzer verfügen, die ihre eigenen Geräte mit zur Arbeit bringen.

„Die Umfrageergebnisse enthüllen, dass die meisten Arbeitnehmer ein zwiegespaltenes Verhältnis zum Risiko haben, das mit dem Speichern von Unternehmensdaten auf eigenen Geräten verbunden ist“, erklärt Stephen Hoare bei Kensington. „Sie erwarten, dass das Unternehmen den Datenschutz sicherstellt – durch Verschlüsselung und andere Sicherheitsmethoden.“

Hoare fügt hinzu: „Zwar gibt es eine deutliche Akzeptanz des BYOD-Trends am Arbeitsplatz, die meisten Arbeitnehmer sind aber nicht bereit, die damit verbundene eigene Verantwortung zu tragen. Arbeitgeber sollten sich nicht nur dieser Tatsache bewusst sein, sie sollten auch proaktiv handeln und den Schutz ihrer eigenen Daten sicherstellen.“

Nicht alle Unternehmen und Angestellten nehmen das Problem ernst, obwohl die EU-Datenschutzgesetze empfindliche Strafen für Verstöße gegen den Datenschutz vorsehen, die im schlimmsten Fall mehr als 500.000 € betragen können. Diese Strafen können sogar noch höher ausfallen, wenn die EU-Datenschutzgesetze in naher Zukunft überarbeitet werden. Zudem kann sich kaum ein Unternehmen die Negativwerbung leisten, die ein Datenschutzverstoß mit sich bringt. Um sich vor diesen Konsequenzen zu schützen, sollten Firmen über eine individuell zugeschnittene BYOD-Richtlinie verfügen, die die erlaubte Verwendung definiert, einschließlich Verschlüsselungstechniken, starker Kennwortmethoden, Diebstahlabwehr, Frühwarnsystem für Geräteverluste und Löschfunktion per Fernzugriff.

Sperren oder Verlieren

Ein klarer erster Schritt beim Schutz von Unternehmensdaten auf Laptops der Angestellten besteht laut Kensington darin, Unternehmensrichtlinien zu formulieren, damit die Mitarbeiter sich der Tatsache bewusst werden, dass sie für ihre Computer die Verantwortung tragen.

Hoare erläutert: „Unsere Umfrage hat zutage gebracht, dass eine ernüchternde Zahl von Arbeitgebern immer noch nicht über Sicherheitsrichtlinien für Benutzer verfügen, die ihre eigenen Geräte mit zur Arbeit bringen. Das Problem zu ignorieren, ist so, also ob Sie den Autoschlüssel im Zündschloss Ihres Firmenwagens stecken lassen, oder das Bürofenster beim Verlassen des Gebäudes weit geöffnet lassen. Arbeitgeber müssen ihre Angestellten endlich beim Schutz der Unternehmensdaten unterstützen und sie in die Pflicht nehmen, und zwar, indem sie sicherstellen, dass die Mitarbeiter sich über die Konsequenzen im Klaren sind.“

Um Tablets, Smartphones und Laptops vor Datenverlust oder Diebstahl zu schützen, bietet Kensington eine Reihe von benutzerfreundlichen Sicherheitsgeräten an, beispielsweise die bequeme ClickSafe-Lock-Produktreihe, Sicherheit mit einem Klick dank eines Schlosses, das sich ganz einfach mit einer Hand wieder öffnen lässt.

Aufgrund der kontinuierlichen Entwicklung hin zu mobilen Geräten hat Kensington seine Auswahl an Sicherheitslösungen auch auf Tablets, wie das iPad und beliebte Android-Modelle, z. B. das Samsung Galaxy Tab, erweitert – mit SecureBack, einem verschließbaren Case für Tablets. Auch iPhone-Benutzer sind geschützt, mit dem innovativen BungeeAir Security Tether, einer „unsichtbaren Leine“, mit der das iPhone automatisch gesperrt wird, sobald es sich außerhalb des festgelegten Entfernungsbereichs befindet.

Die Ergebnisse stammen aus einer Umfrage, die von IDC im Juli 2012 unter Arbeitnehmern in Großbritannien, Frankreich und Deutschland durchgeführt wurde. Die Umfrage steht unter www.kensington.com zum Download bereit.

Ende/weiter

Die folgenden Kensington-Produkte sind in dieser News-Ausgabe enthalten:

- BungeeAir Security Cases für iPhone4 <http://www.kensington.com/kensington/de/de/s/1718/security-cases-for-iphone.aspx>
- SecureBack Security Cases für Tablets <http://www.kensington.com/kensington/de/de/s/1634/schutz-cases-fur-ipad.aspx>
- ClickSafe Laptop Locks <http://www.kensington.com/kensington/de/de/s/1636/clicksafe%C2%AE->

[sicherheitsverankerung.aspx](#)

Folgen Sie Kensington auf Twitter @KensingtonZone

Besuchen Sie den Kensington SafeZone-Blog: <http://blog.kensington.com/security/>

Weitere Informationen zu den Produkten finden Sie hier:

Video zu Kensington BungeeAir:

http://www.youtube.com/watch?v=sNMWRVHmKY4&list=UUPOXnw4z2DRRi0Vz_GAKifg&index=6&feature=plcp

Video zu Kensington SecureBack:

<http://www.youtube.com/watch?v=2xx4ysDuDmM>

Video zu Kensington ClickSafe:

http://www.youtube.com/watch?v=rxOM6kw3tDE&list=UUPOXnw4z2DRRi0Vz_GAKifg&index=9&feature=plcp

Download hochauflösender Produktbilder:

Kensington BungeeAir: <http://www.flickr.com/photos/48490242@N04/6142114368/in/photostream>

Kensington SecureBack mit Standfuß und ClickSafe für Galaxy Tab:

<http://www.flickr.com/photos/48490242@N04/6669860811/in/photostream>

Kensington SecureBack Sicherungsgehäuse mit 2-Wege-Standfuß & ClickSafe:

<http://www.flickr.com/photos/48490242@N04/6142116272/in/photostream>

Kensington ClickSafe Laptop Locks:

<http://www.flickr.com/photos/48490242@N04/7441708164/in/photostream>

Portrait

Info zu Kensington

smart, sicher, simpel (www.kensington.com)

Kensington ist ein weltweit führender Anbieter von smartem, sicherem und simplem Computerzubehör, dessen Produkte weltweit größtes Vertrauen genießen. Zu Kensingtons physischen Sicherheitslösungen gehören Schlösser für Laptops und andere mobile Geräte, die ein bisher nie erreichtes Maß an Geräteschutz bieten. Zudem umfasst Kensingtons Zubehörpalette Produkte von Netzadaptern und Ladegeräten, Mäusen, Tastaturen und Trackballs bis hin zu universellen Dockingstations, Desktopzubehör, Tragetaschen und iPad/iPhone/iPod-Zubehör. Kensington Computer Products Group, headquartered in Redwood Shores, California, is the technology division of ACCO Brands (NYSE: ABD), einem Marktführer für Markenbüroartikel, dessen Produkte in über 100 Ländern weltweit vermarktet werden. Weitere Informationen finden Sie unter www.kensington.com.

Kensington ist eine eingetragene Marke von ACCO Brands. smart.safe.simple, SecureBack und ClickSafe sind Marken von ACCO Brands. iPad 2 ist eine Marke von Apple Inc. Samsung Galaxy Tab, Motorola Xoom und any10" Android. Alle anderen eingetragenen und nicht eingetragenen Markenzeichen sind Eigentum der entsprechenden Inhaber.
© 2012 Kensington Computer Products Group, eine Abteilung von ACCO Brands. Alle Rechte vorbehalten.

News-ID: 659210 • Views: 201 (Stand: 30.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/659210/Bring-Your-Own-Device-Ein-Risiko-fuer-die-Daten-Ihres-Arbeitgebers.html>