BRING YOUR OWN DEVICE?

CapaSystems
...because time matters

BRING YOUR OWN DEVICE SORGT FÜR SCHLAFLOSE NÄCHTE

Der Mix aus privaten und geschäftlichen Anwendungen auf ein und demselben IT-Gerät sorgt in IT-Abteilungen für Unruhe

Wir alle tun es – wir verwenden dasselbe IT-Gerät für die Arbeit und für private Zwecke. Das gilt für Smartphones, Tablets, Laptops usw. Zweifellos eine flexible Lösung, die den Benutzern wie auch den Arbeitgebern hilft, Kosten zu senken. Aber wie ist es in diesem Universum privater und geschäftlicher Apps, das die BYOD-Kultur erschaffen hat, um die Sicherheit Ihres Unternehmens bestellt?

Benutzer wechseln ständig zwischen Geschäftlichem und Privatvergnügen hin und her. Die Möglichkeit, dies innerhalb von Sekundenbruchteilen tun zu können, steigert die Zufriedenheit und Produktivität der Endbenutzer. Außerdem können Sie durch BYOD Ihren Kosten- und Zeitaufwand für die Konfiguration von Geräten und den Benutzer-Support senken. Doch mit einer Herausforderung hat die BYOD-Kultur zu kämpfen: Sicherheit. Besonders die eher vergnügungsorientierten Apps sind lukrative Ziele für Hacker —wodurch auch den Unternehmensdaten Infektionen mit Malware und andere böse Überraschungen drohen.

Untersuchungen zeigen, dass Dänen im Schnitt 33 verschiedene Apps auf ihren Smartphones haben. Und rechnen wir Deutschland, Schweden und das Vereinigte Königreich mit ein, sprechen wir laut Mobile Planet von durchschnittlich 32,2 Apps pro Gerät. Außerdem bewegen wir uns häufig in Social Media-Kanälen der privateren Natur (wie Facebook, Twitter oder Instagram). Was Onlineeinkäufe über Mobilgeräte angeht, zeigen sich die Benutzer aus diesen Ländern zwar noch eher zurückhaltend—nur 33,6 % kaufen online über ihre Smartphones ein, was die Gefahr von Attacken auf diese Geräte und ihre Daten jedoch nicht weniger real macht! Und nutzen wir die VPN-Verbindung unseres Unternehmens auf unseren IT-Geräten, dann stehen die Tore zu den Geschäftsdaten sperrangelweit offen.

Malware bahnt sich ihren Weg durch Apps hinein und beginnt damit, die Unternehmensbandbreite zu fressen, was zu verringerten Netzwerkgeschwindigkeiten und eingeschränkter Produktivität führt. Betrachten wir die oben genannten Länder, in denen die Gehälter hoch sind, könnten Unternehmen dadurch in Zukunft durchaus ihre Wettbewerbsfähigkeit einbüßen.

Deshalb ist es interessant zu untersuchen, wie die mit BYOD verbundenen Sicherheitslücken geschlossen werden können, ohne die Produktivität und Flexibilität der Endbenutzer zu opfern.

Viele Unternehmen haben dies erfolglos versucht, weil Maßnahmen wie die Verschlüsselung, Sicherheitsüberprüfungen und IT-Richtlinien für die mobile Sicherheit in der Praxis kaum umgesetzt werden.

Eine andere Möglichkeit, die Sicherheit zu gewährleisten, wäre ein Downloadverbot für bestimmte Apps. Doch dies führt üblicherweise nur zu Frust bei den Benutzern—weshalb sollen sie plötzlich ihr Lieblingsspiel löschen? Und außerdem werden die Benutzer ohnehin immer Mittel und Wege finden, um ihre Lieblingsspiele zu behalten. Denn die Unternehmenssicherheit spielt für sie nur eine untergeordnete Rolle. Komfort und Vergnügen sind ihnen wichtiger.

Unternehmen können allerdings beschließen, die Apps ihrer Benutzer mithilfe von Mobile Device Management-Software, die ihnen die zentrale Kontrolle über die Bereitstellung von Software und Konfigurationsänderungen auf allen Geräten liefert, zu verwalten und kontrollieren. Etliche dieser Lösungen ermöglichen ein einfaches und schnelles Rollout simpler wie auch komplexer Software ohne Beeinträchtigung der Endbenutzer. Und IT-Abteilungen können Unternehmensanwendungen aus dem Apple App Store und Google Play Store auf iOS- und Android-Geräten bereitstellen.

Die Bedrohung, die von BYOD ausgeht, ist sehr real und bereitet vielen CIOs aufgrund der katastrophalen Folgen, die die Verletzung der Datensicherheit nach sich zieht, verständlicherweise Kopfzerbrechen.

Stellen Sie sich einfach vor, Ihr Unternehmen stünde kurz vor einem revolutionären Durchbruch, und dann würden Sie zum Opfer eines Hacker-Angriffs. Dadurch könnte die Arbeit vieler Jahre vernichtet werden und die finanziellen Konsequenzen könnten verheerend sein.

Dieses Sicherheitsproblem ist keinesfalls ein neues Phänomen, aber es ist höchst relevant, es regelmäßig neu zu beleuchten, weil sich die Gefährdungslage durch Erfindungen und immer kreativere Hacker ständig verändert. BYOD einfach zu ignorieren ist keine Option.

MaaS360 präsentiert: "DIE ZEHN GEBOTE VON BYOD"

– 10 Ratschläge über Bring Your Own Device:

1. Erstellen Sie vor dem Erwerb neuer Technologien entsprechende Sicherheitsrichtlinien
2. Verschaffen Sie sich einen Überblick über die Anzahl der Geräte Ihrer Belegschaft und benachrichtigen Sie ihre Nutzer, bevor Sie etwas unternehmen
3. Der Rollout muss einfach und sicher sein und die Möglichkeit zur Konfiguration von Geräten beinhalten
4. Der Rollout und die Konfiguration von Geräten muss schnell und einfach und ohne Beeinträchtigung der Benutzer vonstattengehen
5. Bieten Sie den Benutzern eine reibungslos arbeitende Selbstbedienungsplattform
6. Schützen Sie persönliche Daten und erklären Sie den Benutzern die Datenschutzrichtlinien Ihres Unternehmens
7. Trennen Sie Unternehmensdaten von privaten Daten
8. Verwalten Sie Ihre Datennutzung—erstellen Sie Regeln, um Benutzern zu helfen
9. Sorgen Sie für eine konstante Überwachung der im Unternehmen verwendeten Geräte, um sicherzustellen, dass die Sicherheitsrichtlinien eingehalten werden
10. Behalten Sie den Einfluss von BYOD auf den ROI Ihres Unternehmens im Blick

CAPAINSTALLER

CapaInstaller ist eine Software, die Ihnen hilft, Installations- und Updateprozesse zu automatisieren, in Kontrolle zu bleiben und Ihre Zeit effektiv zu nutzen. Dank der zentralisierten Verteilfunktion von CapaInstaller müssen Sie Software nie mehr manuell auf einzelnen Computern installieren—nie wieder Pendeln zwischen unterschiedlichen Standorten. Dadurch gewinnen Sie mehr Zeit für wirklich wichtige Aufgaben und können Nutzeranfragen schneller beantworten. Schnelle Antworten steigern die Effizienz und Zufriedenheit der Benutzer—Kriterien, an denen die Leistung jeder IT-Abteilung gemessen wird.

PERFORMANCEGUARD

PerformanceGuard hilft Ihnen, IT-Probleme zu identifizieren, wo und wann immer sie auftreten, egal aus welchem Grund und egal, welcher Endbenutzer davon betroffen ist. Dies geschieht durch die Überwachung der tatsächlichen Qualität sowie Quantität von IT-Dienstleistungen aus Sicht der Endbenutzer. Mit PerformanceGuard können Sie Ausfallzeiten identifizieren, das Benutzererlebnis überwachen, definierte KPIs messen und Vieles mehr.

CapaSystems
...because time matters

Buchen Sie ein Treffen

Rufen Sie uns an und vereinbaren Sie einen Termin zur Präsentation unserer Produkte, die Ihnen und Ihrem Unternehmen wertvolle Zeit einsparen können.

Webinar

Nehmen Sie an einem unserer monatlichen Demo-Webinare teil und erhalten Sie eine 30-minütige Einführung in die Welt unserer Produkte.

CapaInstaller webinare finden immer am letzten Donners eines jeden Monats von 10:00-10:30 Uhr Mez statt.

PerformanceGuard-Webinare finden immer am letzten Montag eines jeden Monats von 11:00-11:30 Uhr MEZ statt.

CapaSystems A/S
Roskildevej 342C • DK-2630 Taastrup
Godthåbsvej 33 • DK-8660 Skanderborg
Tel. (+45) 70 10 70 55

www.capasystems.com