BRENNPUNKT MOBILE DATENSICHERHEIT

Wie Sie Sicherheitslücken wirksam schließen

Die aktuellen Medienberichte über unerlaubte Zugriffe auf mobile Kommunikationswege haben das Problembewusstsein zum Thema Datensicherheit gestärkt. Gerade mittelständische Unternehmen haben oft massive Sicherheitslücken und fragen sich, ob und wie sich diese schließen lassen. Denn Datenverlust kann wirtschaftliche Existenzen gefährden.

1 Welche Bedeutung hat Industriespionage in Deutschland?

Durch Spionage entsteht deutschen Unternehmen ein jährlicher Gesamtschaden von 20 Milliarden Euro.[1] Gerade der Mittelstand steht im Visier, deckt eine aktuelle Studie zur Industriespionage auf und stellt fest, dass 2012 mindestens 21,4% der befragten Unternehmen betroffen waren. Rechnet man Verdachtsfälle dazu, sind es sogar mehr als 50% – wobei es noch eine große Dunkelziffer gibt.[2]

2 Warum sollte es gerade uns treffen?

Denken Sie z.B. an Ihre Innovationen, Ausschreibungen, Angebote, Kundendaten – alles begehrte Informationen für Wettbewerber. Auch Bankdaten, Passwörter etc. sind interessant für Cyberkriminelle. Wer sich nicht als gefährdet einstuft, wird leicht zum Angriffsziel, weil sein IT-System vielfache Sicherheitslücken hat. Angefangen bei Remote-Access-Zugängen über Web-Portale, CRM-Systeme, unklare Zugriffsverwaltung und zu einfache Passwörter bis hin zu mobilen Endgeräten, Cloud Computing und Mitarbeitern, die nach der Studie an rund 70% aller Informationsabflüsse beteiligt sind.[2] Oft unbeabsichtigt durch die Nutzung eines einzigen, unzureichend abgesicherten Smartphones für Geschäftliches und Privates.

3 Wie kann ich unsere Sicherheitslücken schließen?

Es geht um die gesamten Kommunikationswege. Also muss Ihr IT-Sicherheitskonzept die Verschlüsselung aller wichtigen Daten sowie den gesicherten Zugriff auf Soft- und Hardware inklusive aller mobilen Endgeräte wie Tablets und Smartphones umfassen, auch die mitarbeitereigenen. Der Übergriff privater Smartphone-Apps auf geschäftliche Daten muss ebenso verhindert werden wie die Möglichkeit, Sicherheitseinstellungen zu umgehen. All das lässt sich heute mit dem BlackBerry® 10 Betriebssystem und dem BlackBerry® Enterprise Service 10 (BES 10) realisieren.

4 Ist so ein Sicherheitskonzept für uns nicht sehr kompliziert und teuer?

Es gibt viele Lösungsbausteine am Markt, auch kostenlose, mit denen Sie Ihre IT-Sicherheit verbessern können. Aber das kann zu komplizierten, inhomogenen Systemen führen, die immer noch Lücken lassen. Für die komplexen Anforderungen – gerade in Bezug auf Mobile Device Management (MDM) – bietet die BlackBerry Lösung klare Vorteile, da mobile Endgeräte, Software und MDM transparent ineinander übergreifen, die Administration vereinfacht und Risiken durch fehlerhafte Konfiguration minimiert werden. Und: Zwischen BlackBerry® 10 Smartphones und BES 10 ist die Kommunikation standardmäßig verschlüsselt!

1 Bayerisches Landesamt für Verfassungsschutz
2 *Industriespionage 2012,* Corporate Trust Business Risk & Crisis Management GmbH München

BlackBerry®

5 Was ist mit den iOS und Android Smartphones meiner Mitarbeiter?

Kein Problem. Mit BlackBerry Enterprise Service 10 lassen sich alle mobilen Endgeräte vollständig integrieren und über eine einzige Administrationskonsole verwalten. Diese erste und einzige plattformübergreifende MDM-Lösung setzt weltweit höchste Ende-zu-Ende Sicherheitsstandards. Mit dem Modul Secure Workspace ist der bisher BlackBerry exklusive, mit AES256 verschlüsselte Datenkanal, auch für iPhone und Android™ verfügbar.

6 Wie kann ich private Anwendungen sicher von geschäftlichen abgrenzen?

Private und geschäftliche Anwendungen lassen sich mit BlackBerry® Balance™ auf BlackBerry 10 Smartphones in zwei Bereichen sicher voneinander abschirmen, inklusive des Datenstroms. Der Arbeitsbereich ist vollständig verschlüsselt, vom Unternehmen verwaltet, gesichert und kommuniziert ausnahmslos mit dem Unternehmensnetz. Unerlaubte Zugriffe, z.B. durch Soziale Netzwerke, werden verhindert. Alle privaten Anwendungen laufen über den regulären Internetzugang. Mit dieser Trennung lässt sich auch der zunehmende Trend hin zu BYOD (Bring-Your-Own-Device) sicher umsetzen.

7 Was ist, wenn ein Mitarbeiter das Unternehmen verlässt, ich mein Smartphone verliere oder es gestohlen wird?

Umfassende Sicherheit muss auch das berücksichtigen. Ein weiterer Vorteil von BES 10 ist, dass der Administrator den dienstlichen Bereich auf dem Smartphone per Fernzugriff spurenfrei löschen und den Zugang zum Unternehmensnetz blockieren kann. Auf dem BlackBerry Smartphone selbst sind alle Daten zudem separat verschlüsselt und die Zugänge zu Gerät und Anwendungen lassen sich zusätzlich mit frei wählbaren Passwörtern absichern.

8 Macht all das mein Smartphone nicht langsam und kompliziert?

Kurz gesagt: Nein. Denn das gesamte BlackBerry 10 Sicherheitskonzept wurde unter der strikten Vorgabe hoher Benutzerfreundlichkeit entwickelt. Deshalb gibt es für den Administrator nur noch 50 Policies, was fehlerhaften Konfigurationen vorbeugt.

9 Mobile Device Management können angeblich viele – worauf muss ich achten?

Die Administration muss einfach, sicher und kostensparend sein. Das lässt sich mit nur einer Management-Plattform für alle Geräte sowie einem einzigen zu sichernden Kommunikationskanal erreichen, wie bei der BlackBerry 10 Infrastruktur. Alle Geräte[3] kommunizieren also nur mit einem Port hinter der Firewall, was deutlich sicherer ist, als multiple Ports für ActiveSync, Apple und Google zu öffnen.

10 Wie kann ich mein Smartphone auch privat sicherer nutzen?

Abhörsicheres Telefonieren in öffentlichen Mobilfinknetzen ist nur mit Kryptohandies möglich. Aber was andere Anwendungen und Daten betrifft, können Sie einiges tun: Keine Apps herunterladen, die ungefragt Daten sammeln bzw. auf Daten zugreifen. Messenger-Dienste meiden, die Daten abgreifen. Anti-Viren-Programme installieren. Öffentliches WLAN über VPN-Dienste nutzen. Passwörter häufiger wechseln.
Mehr Privatsphäre bieten der Messenger-Dienst BBM™ von BlackBerry, da er keine persönlichen Information wie z.B. Telefonnummern der Teilnehmer benötigt, und die BlackBerry 10 Smartphones allgemein – mit individuellen Benutzereinstellungen und Fernlöschen von Daten über BlackBerry® Protect bei Verlust des Smartphones.

BlackBerry 10 Zertifizierungen: NATO & Presseinformation, SecuSUITE for BlackBerry 10, FIPS Presseinformation

Weitere Fragen zum Thema Sicherheit beantworten wir Ihnen gern und umfassend: **sicherheit@blackberry.com**

BlackBerry®

3 BlackBerry 10 Smartphones oder Android und iPhones mit Secure Work Space Option