Fast Facts:

- Im Durchschnitt sind rund ein Drittel der Mitarbeiter in Unternehmen regelmäßig auf Dienstreise unterwegs.
- Doch nur eines von drei Unternehmen ist durch Security-Richtlinien und andere Maßnahmen darauf vorbereitet.
- Der Artikel erklärt, wie man Smartphones schützt und worauf man bei Security-Lösungen für mobile Geräte achten sollte.
- **Zeichen: 8.738 inkl. Leerzeichen**

Gut ein Drittel der Mitarbeiter sitzt nicht nur in den Firmenzentralen, sondern reist zu Kunden und Partnern. Doch vor allem die Smartphones dieser mobilen Mitarbeiter sind oft außerhalb des Unternehmens schutzlos. Der Artikel zeigt, wie man Smartphones schützt und was mobile Security-Lösungen können müssen.

IT-Sicherheit auf Dienstreise

Gut ein Drittel der Belegschaft ist im Durchschnitt auch unterwegs im Dienst. Für Unternehmen wird es deshalb Zeit, die Sicherheitsstrategie konsequent auf mobile Nutzer auszudehnen. Der Artikel verrät, was man dafür braucht.

Egal, ob IT-Sicherheitsexperten selbst viel reisen oder nicht, ihre Kundschaft tut es in vielen Fällen und das ist gerade eine der größten Sicherheitsherausforderungen in der IT. Nach einer Umfrage von Kaspersky unter 1.300 IT-Entscheidern in 11 Ländern ist gut ein Drittel der Mitarbeiter in Unternehmen regelmäßig auf Dienstreise [1]. Doch mit Stift und Papier reist hier niemand mehr durchs Land. Zur Grundausstattung gehören Notebook und Smartphone. Viele Sicherheitsstrategien in Unternehmen umfassen aber nur Computer und Netzwerke in der Niederlassung, außerhalb sind die Nutzer oft auf sich allein gestellt. Denn nach den Studienergebnissen von Kaspersky sind zwei von drei Unternehmen nicht mit einer fertigen Security-Strategie für Remote-Arbeiter ausgestattet. Nur 30 Prozent der Unternehmen haben ihre Richtlinien für mobile Geräte angepasst und 27 Prozent verschlüsseln die Inhalte der beruflich genutzten Smartphones [2]. Trotzdem findet zumindest ein Umdenken statt, denn 55 Prozent der

befragten Unternehmen geben an, dass sie heute viel besorgter über mobile Gefahren sind als noch vor einem Jahr. Doch das Bewusstsein schärfen allein reicht nicht, hier sind Tipps für die Praxis.

Mobile Schutzstrategie ist nötig

Warum sollte man als Unternehmen Smartphones in der Security-Strategie berücksichtigen? Einfache Antwort: Weil Smartphones eine Menge Funktionen haben? Die häufigste Aufgabe, die Smartphones in Unternehmen erledigen, ist der Zugriff auf Kommunikationssysteme, allen voran natürlich Anrufe und E-Mail, aber auch zunehmend andere Messaging-Systeme samt Verwaltung von Terminen und umfangreichen Zugriff auf Kontaktdatenbanken. Hier muss die Vertraulichkeit sensibler Firmendaten gewahrt werden. So sollten Dritte keinen Einblick in Geschäfts-E-Mails bekommen und natürlich auch keinen Zugriff auf Kunden- oder Lieferantendaten haben.

Einen Schritt weiter geht der komplette Zugriff aufs Firmennetz: Hier wählen sich Mitarbeiter meist über eine VPN-Verbindung ins Unternehmensnetzwerk ein und können dann auf Dateien und Business-Applikationen zugreifen, etwa ERP-Systeme. Klar ist, dass man als Unternehmen hier verhindern muss, dass Unberechtigte auf Firmeninterna zugreifen, Daten abzweigen oder vorhandene Anwendungen manipulieren.

Gefahren für Smartphones

Es gibt im Grunde drei Szenarien, vor denen Sie Smartphones schützen müssen. Am häufigsten dürfte aktuell Fall 1 eintreten, der Verlust oder Diebstahl eines Smartphones. Fall 2 ist ähnlich gelagert wie Fall 1, bei dem eine fremde Person kompletten Zugriff auf das mobile Gerät hat. Nur ist dieser Zugriff nicht permanent, sondern auf eine eher kurze Zeitspanne beschränkt. Beliebtes Beispiel: Ein Mitarbeiter lässt in der Mittagspause sein Smartphone am Schreibtisch liegen und eine andere Person kriegt das Gerät in die Finger. Auch hier droht Missbrauch von Firmeninformationen durch unerlaubten Zugriff. Fall 3 fasst dann alle weiteren Angriffsszenarien zusammen, etwa spezielle Malware für mobile Geräte, SMS-Angriffe oder gezielten Datendiebstahl über präparierte Mails oder Internetseiten. Die Besonderheit dabei: Die Angreifer haben das Gerät nicht wirklich "in der Hand".

Schutz bei Verlust oder Diebstahl

Geht das Smartphone verloren oder wird es gestohlen, dann hält eine dritte Person das Gerät in Händen. Handelt es sich nicht um einen ehrlichen Finder, dann hat diese Person jetzt alle Zeit der Welt, sich Zugang zu den gespeicherten Informationen auf dem Smartphone zu verschaffen. Zu den wertvollen Daten gehören aber nicht nur explizite Datensätze auf dem Mobilgerät, sondern auch Zugangsdaten zum Firmennetz oder den Kommunikationsdiensten. Sind VPN- und Mail-Server-Passwort bereits abgespeichert, dann reicht ein Fingertipp auf die passende App aus und schon hat ein Datendieb Zugriff. Schutzsoftware wie Kaspersky Endpoint Security 8 für Smartphones verhindert bei Verlust des Smartphones den Zugriff von Fremden durch eine spezielle Anti-Diebstahl-Funktion. Das Smartphone kann dann sogar nach dem Verlust noch aus der Ferne über eine Management-Software gesperrt werden. Zusätzlich können Geräte mit GPS-Empfänger, wie ihn die meisten Business-Smartphones ohnehin eingebaut haben, geortet werden. Alternativ können Sie auch zu noch härteren Mitteln greifen und über einen Löschbefehl das Gerät komplett in den Auslieferungszustand zurücksetzen. So hat man zwar den finanziellen Schaden des verlorenen Geräts zu tragen, das ist für die meisten Firmen aber vertretbar. Die sensiblen Firmendaten fallen aber nicht in die Hände von Dritten.

Ein professioneller Dieb wird schnellstmöglich einige Maßnahmen ergreifen, um nicht entlarvt zu werden. So dürfte der SIM-Kartentausch eine der ersten Aktionen sein. Doch auch dafür präsentiert Endpoint Security von Kaspersky eine passende Lösung: Die Funktion SIM-Watch hat auch dann das Gerät noch via Management-Software im Griff, wenn die SIM-Karte getauscht wurde. Sogar die neue Mobilfunknummer wird automatisch per SMS zum rechtmäßigen Besitzer geschickt. Doch was passiert, wenn man das Smartphone nicht mehr rechtzeitig sperren konnte? Für diesen Zweck hilft ein altbekanntes Mittel, das sich beim Schutz von Daten auf Notebooks schon seit Jahren bewährt hat, Verschlüsselung. Dateien, Ordner und Speicherkarten können mit Kaspersky Endpoint Security unknackbar verschlüsselt werden. Zugriff auf die Daten erhält man nur mit dem richtigen Passwort.

Schutz vor Angriffen

Das Malware-Problem auf mobilen Plattformen wird oft belächelt, denn einem Vergleich mit der aktuellen Situation unter Windows hält es rein von den Bedrohungszahlen her

nicht stand. Es gibt zwar auch Schädlinge für diverse mobile Plattformen, etwa Trojaner, die SMS an Premium-Dienste schicken und so den Smartphone-Besitzer abzocken. Von großen Virenausbrüchen ist aber bisher nichts zu sehen. Doch Vorsicht: Mit steigender Verbreitung werden Smartphones und Tablets eine interessante Zielgruppe für Malware-Schreiber. Außerdem muss es auch nicht immer ein medienwirksamer Virenangriff sein. Sicherheitsexperten beobachten seit Jahren eine Professionalisierung der Malware-Szene. Qualität geht vor Quantität und wenn jemand an den Daten auf den Smartphones Ihrer Außendienstler interessiert ist, dann ist ein gezielter Angriff eine realistische Gefahr. Tipp: Sorgen Sie mit einem mobilen Virenschutz vor. Die Anforderungen: Der Virenscanner sollte mobile Geräte in Echtzeit überwachen und Geräte auch nach Zeitplan auf Malware prüfen können. Zusätzlich wichtig: Auch ein Anti-Spam-Modul sollte Teil der mobilen Schutzlösung sein. Die Funktion sollte sich aber nicht nur auf Mails beschränken, sondern auch SMS und Anrufe umfassen.

Zusätzliche Sicherungsmaßnahmen

Natürlich helfen eine Zugriffssperre und Verschlüsselung gegen neugierige Blicke von Kollegen, wenn das Smartphone mal kurz unbeaufsichtigt am Schreibtisch liegt. Clevere Schutz-Software hat aber hier auch noch andere Tricks zu bieten. So ist es etwa nützlich, wenn man durch zusätzliche Funktionen die Privatsphäre schützen kann. Beispielsweise kann man einzelne Details von Kontakten verbergen oder Anruflisten und SMS vor neugierigen Blicken verstecken.

Unternehmen sollten bei der Auswahl der Schutz-Software für mobile Geräte drei Punkte beachten:

Managementfunktion: Ein Smartphone lässt sich problemlos zu Fuß konfigurieren, bei 5 wird es nervig, ab 10 Geräten ist es nicht mehr wirtschaftlich ohne zentrale Management-Oberfläche zu arbeiten, die mobile Geräte jederzeit für Wartungszwecke zugänglich macht. Nur mit einer zentralen Verwaltung behalten die IT-Mitarbeiter jederzeit die volle Kontrolle über die Geräte, denn die Administration klappt auch aus der Ferne. So lassen sich gezielt und einfach Updates und neue Programme verteilen.

Richtlinien: Wer darf im Netzwerk was? Policies sind nicht nur aus Compliance-Gesichtspunkten aus Unternehmen nicht mehr wegzudenken. Deshalb ist das auch ein Muss für die nahtlose und sichere Einbindung von Smartphones. Kaspersky Endpoint Security erlaubt deshalb die Zuweisung von Richtlinien an verschiedene Benutzergruppen, natürlich auch "over-the-air". So können Administratoren bequem die Anti-Virus-Einstellungen anpassen und zum Beispiel festlegen, welche Dateitypen auf dem Smartphone nach Malware durchsucht werden sollen und welche nicht.

Support für alle eingesetzten Plattformen: Machen Sie bei der Smartphone-Sicherheit keine Kompromisse. Die eingesetzte Schutzsoftware muss alle vorhandenen Mobilplattformen in Ihrem Unternehmen unterstützen.

[1] Die Umfrage wurde in Kooperation mit dem globalen Marktforschungsinstitut B2B International durchgeführt. Insgesamt wurden 1.300 IT-Verantwortliche aus den folgenden elf Ländern befragt: Deutschland, USA, Brasilien, Großbritannien, Frankreich, Spanien, Italien, Russland, China, Japan und Indien. Alle Befragten haben Einfluss auf die IT-Sicherheitspolitik ihres Unternehmens und beschäftigen sich professionell mit IT-Sicherheitsbelangen sowie allgemeinen Geschäftsprozessen (zum Beispiel Finanzen und Human Resources). Die Umfrage ist nicht repräsentativ.

[2] www.kaspersky.com/images/kaspersky_global_it_security_risks_survey-10-100468.pdf