

Link: <https://www.computerwoche.de/a/diebstahl-und-vergesslichkeit,2488195>

Probleme der Consumerization

Diebstahl und Vergesslichkeit

Datum: 15.06.2011

Die private und geschäftliche Nutzung eines Geräts ist normal geworden. Mit der Consumerization vermischen sich zunehmend auch Privat- und Firmendaten. Leider lassen die Anwender ihre mobilen Geräte gern in Taxis oder am Flughafen liegen. Nicht Viren, sondern Diebstahl und Vergesslichkeit sind daher also die größten Gefahren.



Das größere Risiko für mobile Geräte: "nicht Viren, sondern Diebstahl und Vergesslichkeit", meint Olaf Mischkovsky, Sicherheitsexperte bei Symantec.

Foto: Symantec

Mehr als die Hälfte der deutschen Arbeitnehmer greifen im Urlaub per Notebook oder Smartphone auf geschäftliche E-Mails zu, heißt es in einer repräsentativen Umfrage des Marktforschungsunternehmens **Emnid**¹. Ähnlich klingt eine aktuelle Erhebung der **Enterprise Strategy Group**² unter 174 Firmen. Dort erklärten rund 40 Prozent der Unternehmen, dass ihre Mitarbeiter vertrauliche Firmendaten wie Kundeninformationen auf ihren Mobilgeräten speichern. Ein Trend zur "Consumerization der IT", der auf die Sicherheitsstrategien in Unternehmen ein neues Licht wirft.

MMS-Nachrichten als Spam-Schleuder

Im Gegensatz zu PC-Arbeitsplätzen hinkt der Einsatz von **Sicherheitssoftware**³ auf mobilen Geräten wie Smartphones und Notebooks noch hinterher. Nur ein relativ kleiner Anteil dieser Devices ist bereits mit einer adäquaten Sicherheitssoftware geschützt. Häufig fehlt bei IT-Verantwortlichen sogar die Erkenntnis darüber, dass Sicherheitsrisiken mittlerweile auch im mobilen Umfeld existieren. Andere wiederum gehen davon aus, dass die Verantwortung zum Schutz der Verbindungen und Endgeräte im Zusammenhang mit Smartphones ausschließlich bei den jeweiligen Service Providern liegt.

Wie relevant ein entsprechender Schutz auch für mobile Informations- und Kommunikationstechnologien ist, zeigte beispielsweise "Sexy Space", der erste SMS-Wurm für Symbian-Telefone. Er verschickte automatisch SMS an alle Adressen des Telefons. Ein anderer Schadcode nutzte den SMS-Dienst, um Nachrichten gezielt an teure Premium-Nummern zu versenden.

Nach Informationen von Netz Providern sind bis zu 12 Prozent der MMS-Nachrichten bereits mit solchen **Handy-Viren**⁴ infiziert. Ebenso erhöht sich das Risiko, sensible Daten durch ein Fehlverhalten der eigenen Mitarbeiter zu verlieren. Der Flughafen Frankfurt etwa zählte im vergangenen Jahr von insgesamt rund 17.000 registrierten Fundgegenständen 1800 Laptops und etwa 1000 Mobiltelefone.

Schutz für Smartphones

In Folge dieser Entwicklung sehen sich Organisationen damit konfrontiert, ihr Sicherheitskonzept zu überdenken, um auch mobile Endgeräte in eine unternehmensweite Sicherheitsstrategie einzubeziehen. Unerlässlich bei der Verwendung von Mobiltelefonen sind für die gesamte Firma geltende Passwort-Richtlinien sowie ein stets aktueller Überblick über den derzeitigen Gerätebestand.

Zu den obligatorischen Maßnahmen gehören darüber hinaus Authentifizierungsmechanismen und Funktionen, mit denen sich die Informationen auf mobilen Geräten verschlüsseln lassen. Und für den Fall der Fälle äußerst hilfreich: eine Remote-Wipe-Funktion und eine Anti-Theft-Strategie zur Absicherung gegen Diebstahl. Damit sind IT-Verantwortliche in der Lage, Daten von Mobiltelefonen per Fernzugriff zu löschen oder Geräte komplett zu deaktivieren. Zum Teil lassen sich Sicherheitsrichtlinien heute je nach Bedarf sogar über das GSM-Netz an die jeweiligen Smartphones übermitteln.

Schlechte Noten für Online-Shops und Carrier

Mit der anhaltenden Attraktivität mobiler Rechner wie Notebooks, Laptops und Tablet PCs gilt vor allem die Festplattenverschlüsselung auch in Zukunft als zentrales Sicherheitsthema. Denn: wenn tragbare Geräte entwendet werden oder versehentlich abhanden kommen, bedeutet das in der Regel auch den Verlust vertraulicher und teils geschäftskritischer Informationen. Mithilfe verschlüsselter Partitionen für sensible Daten oder der Chiffrierung der gesamten Festplatte lassen sich diese Informationen nicht auslesen, sollte das Gerät Unbefugten in die Hände fallen.

Wie wichtig solche Maßnahmen - etwa zum Schutz von Kundendaten - sind, beweist auch eine Umfrage von Emnid: Demnach stehen Deutsche dem Schutz ihrer persönlichen Informationen in Unternehmen immer skeptischer gegenüber. Vor allem Online-Shops (Schulnote 4,4), Telekommunikationsanbieter und Internet Service Provider (4,2) sowie der Einzelhandel (3,7) schnitten dabei schlecht ab.

Im Rahmen eines umfassenden und unternehmensweiten Sicherheitskonzepts sollten deshalb Strategien greifen, die den Anwender sowie den gesamten Lebenszyklus von Daten und Geräten einbezieht. Technologien wie Symantec Data Loss Prevention, Endpoint Encryption oder Device Control regeln beispielsweise, wie und wo der Benutzer welche portablen Speichergeräte und Medien an welchen Anschlüssen verwenden darf. Die Software überwacht darüber hinaus, welche Dateien da tatsächlich auf die Speichermedien transferiert werden. Solche Konzepte können schließlich verhindern, dass sensible Daten unautorisiert kopiert werden. Ebenso ist es im Rahmen solch einer Data Loss Prevention-Strategie möglich, automatische Verschlüsselungen für die kopierten oder verschobenen Daten einzurichten.

Gefahrenherd Social Media

Zur Vorsicht raten Sicherheitsexperten künftig auch beim Einsatz von **Social-Media-Plattformen**⁵: Eine Manipulation von persönlichen oder unternehmensspezifischen Informationen auf einer Social-Media-Seite kann es Angreifern leicht machen, die Reputation von Personen und Unternehmen nachhaltig und empfindlich zu schädigen. Im schlimmsten Fall lassen sich so sogar Aktienkurse und Börsenticker manipulieren und für kriminelle Zwecke missbrauchen. Dass das kein Hirngespinnst ist, zeigt eine Studie von Symantec: Bei etwa 90 bis 95 Prozent aller Angriffe im Netz handelt es sich inzwischen um ganz gezielte Attacken gegen Einzelpersonen. So reicht es aus, nur einen kleinen Umstand aus dem Leben inklusive der dazugehörigen E-Mail-Adresse zu kennen, um den Ruf von Menschen und Unternehmen erheblich in Gefahr zu bringen. Für die kriminellen Drahtzieher ist dieses Vorgehen deutlich effektiver als beispielsweise der Versand von Spam-Mails: Verschickten Angreifer früher 200 Millionen Nachrichten und erzielten so eine Rücklaufquote von 0,5 Prozent, reichen heute 2000 zielgerichtete Nachrichten für eine Quote von zehn Prozent.

Pflicht und Kür

Bei allen Anstrengungen für die Sicherheit mit mobilen Devices und Social-Media-Plattformen dürfen die klassischen Vorkehrungen jedoch nicht in den Hintergrund geraten. Neben der Verwendung von Firewalls, VPN, Sicherheits-Updates für Software und WLAN-Verschlüsselungen gehört selbstverständlich ein aktueller Schutz vor Malware zum Gesamtpaket. Allein im Jahr 2009 hat Symantec 240 Millionen einzigartige Varianten von Schadcode entdeckt. Jeder der Codes wurde im Schnitt auf weniger als 20 Computern weltweit nachgewiesen. Der rapide Wandel der Malware setzt das traditionelle Schutzprozedere der Sicherheitsindustrie unter Druck.

Links im Artikel:

¹ <http://www.tns-emnid.com/>

² <http://www.enterprisestrategygroup.com/>

³ <https://www.channelpartner.de/channelcenter/security/>

⁴ <https://www.channelpartner.de/channelcenter/security/295715/>

⁵ <https://www.channelpartner.de/channelcenter/security/2383308/index.html>