INTARGIA
IDEE.IT.ZIEL

Whitepaper: Mobile IT-Sicherheit

Wie sicher sind Ihre Daten unterwegs?

Kontaktdaten:

IT-RISIKO-
MANAGEMENT

Dr. Thomas Jurisch, Steffen Weber
Telefon: +49 (0)6103 350860
E-Mail: it-risikomanagement@intargia.com
Webseite: http://www.intargia.com

Mobile IT-Sicherheit – Wie sicher sind Ihre Daten unterwegs?

In vielen Unternehmen gibt es bereits Richtlinien zum Umgang mit sensiblen Unternehmensdaten. Doch wie sieht es mit der Sicherheit dieser Daten aus, wenn mobile Endgeräte genutzt werden? Laut einer Studie des Ponemon-Instituts entsteht durch Totalverlust eines Notebooks samt Daten ein finanzieller Schaden von durchschnittlich 50.000 US Dollar. In diesem Whitepaper möchten wir Ihnen daher die größten Gefahren im Bereich Mobile Business vorstellen und Lösungsansätze aufzeigen, um Ihre Daten auch dann zu schützen, wenn Sie mobil sein müssen.

1 Ausgangssituation

Um den Anforderungen einer zunehmend internationalen und immer stärker virtuellen Arbeitswelt gerecht zu werden, setzen Unternehmen in immer größerem Umfang mobile Endgeräte wie z.B. Mobiltelefone, Smartphones, PDAs und Laptops sowie drahtlose Kommunikationsverfahren, wie GSM, UMTS, Bluetooth und WLAN, ein

2 Risikobetrachtung

Welche Risiken bestehen im Umgang mit mobilen Endgeräten?

- Die wohl bekannteste Gefahr ist der physische Verlust von mobilen Endgeräten durch Diebstahl oder Nachlässigkeit womit natürlich auch der Datenträger verloren ist.
  Es gibt darüber hinaus viele andere Möglichkeiten, kritische Daten (z.B. Firmenwissen oder vertrauliche interne Informationen) zu verlieren bzw. unfreiwillig an Dritte herauszugeben. Laut einer aktuellen Studie der Zeitschrift <kes> mit dem Titel „Lagebericht zur Informations-Sicherheit“ steht an 1. Stelle der Gefahrenbereiche in einem Unternehmen *´Malware´*, direkt gefolgt von *´Irrtum´ und ´Nachlässigkeit eigener Mitarbeiter´*. Den 4. Platz belegt *´unbefugte Kenntnisnahme´, ´Informationsdiebstahl, Wirtschaftsspionage´*. Als „Hindernisse für bessere Informations-Sicherheit“ wird an erster Stelle mit 69% das fehlende Bewusstsein der Mitarbeiter genannt. Nicht umgesetzte Systeme liegen mit 27% an Platz 9.

	Vorhersage 2006		Bedeutung heute		akt. Prognose		Schäden	
	Rang	Priorität	Rang	Priorität	Rang	Priorität	Rang	ja, bei
Malware (Viren, Würmer, Troj. Pferde, ...)	1	1,51	1	1,12	1	1,29	4	21%
Irrtum und Nachlässigkeit eigener Mitarbeiter	2	1,17	2	0,93	2	0,79	1	36%
Hacking (Vandalismus, Probing, Missbrauch, ...)	4	0,59	3	0,58	3	0,77	8	11%
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	3	0,63	4	0,55	4	0,71	7	12%
Software-Mängel/-Defekte	5	0,58	5	0,54	5	0,49	3	26%
Hardware-Mängel/-Defekte	6	0,34	6	0,45	9	0,28	2	34%
Mängel der Dokumentation	9	0,27	7	0,40	10	0,27	6	15%
unbeabsichtigte Fehler von Externen	7	0,32	8	0,36	8	0,34	5	16%
Sabotage (inkl. DoS)	10	0,22	9	0,36	6	0,46	10	6%
Manipulation zum Zweck der Bereicherung	8	0,29	10	0,34	7	0,38	9	8%
höhere Gewalt (Feuer, Wasser, ...)	11	0,03	11	0,25	11	0,15	11	4%
Sonstiges	12	0	12	0,06	12	0,01	12	2%

Basis: 144 Antworten (Bedeutung), Ø 141 (Prognose), Ø 138 (Schäden), Ø 130 (Vorhersage 2006)

Tabelle: Bedeutung der verschiedenen Gefahrenbereiche, Quelle: <kes>, Ausgabe 4/2008

- Mobiltelefone/ Handhelds/ PDAs/ Smartphones:
  Vertrauliche Emails, Dokumente, Netzwerkzugangsdaten, Kundenkontakte, Lieferantendaten etc. werden oft ungeschützt gespeichert. Zusätzlich sind häufig WLAN oder Bluetooth- Verbindungen nicht deaktiviert und ermöglichen so anderen Personen den Zugang zu den sensiblen Daten. Die Arglosigkeit oder Unwissenheit des Benutzers paart sich hier mit dem Fehlen präventiver Maßnahmen, die mit den Möglichkeiten des mobilen Gerätes implementiert werden können.

- Mobile Speichergeräte:
  Das „Verlegen" von mobilen Speichergeräten, also ein Verlust von kurzer Dauer, kann bereits Identitätsdiebstahl, Einschleusung von Viren oder Datenverlust bedeuten. Oft wird diese Gefahr jedoch nicht beachtet, da das Speichergerät nicht endgültig verloren ging.
  Ein weiteres Problem ist die Benutzung von MP3-Playern und ähnlichen Entertainment-Devices als Speichergerät. Diese werden oft nicht nur vom Mitarbeiter allein sondern z.B. auch von anderen Familienmitgliedern benutzt, was eine Gefährdung der Daten bedeuten kann.

- Wireless LAN:
  Die vorhandenen Verschlüsselungsformen (z.B. WEP) von drahtlosen Netzwerkverbindungen reichen oft nicht aus, um sensible Daten ausreichend vor fremdem Zugriff zu schützen. Kann ein Angreifer das Passwort entschlüsseln ist es ihm möglich, alle Daten bzw. den gesamten Datenverkehr des mobilen Endgerätes mitzulesen oder zu manipulieren.

- Bluetooth:
  Die bequeme, kabellose Kommunikation zwischen Geräten mit kurzer Reichweite weist riskante Schwachstellen auf. So können zum Beispiel sensible Daten wie Telefonnummern, Adressen, Unternehmensdaten oder Kontonummern mittels Tools von Dritten eingesehen werden, was in Angriffsszenarien bestätigt wurde.

- Voice over IP:
  Aufgrund standardmäßig noch unverschlüsselter Daten kann es zur Ausspähung, Aufzeichnung oder Manipulation von Dateninhalten kommen. Auch kostenlose Kommunikation oder das Vortäuschen einer anderen Identität werden durch die Erschleichung von Authentifizierungsdaten ermöglicht.

- „Der Zug als Büro" – beispielhaft für Arbeiten unterwegs
  Ein für alle öffentlich zugänglicher Bereich eignet sich nicht für den Umgang mit sensiblen Unternehmensdaten. Leider wird dieser Aspekt von vielen Mitarbeitern nicht beachtet und führt somit zu folgenden Gefahren:
  - Integrierte Webcams in Laptops oder Kameras in Handys o.ä. von anderen „Mitreisenden" können zum Filmen oder Fotografieren sensibler Daten verwendet werden. Dies ist auch möglich, wenn der Benutzer gar nicht mit am (Nachbar-)Tisch sitzt, sondern gerade sein Gerät kurz allein lässt. Auch Telefonate lassen sich so abhören oder aufzeichnen.
  - Personen, die in der Nähe eines Laptop-Benutzers sitzen, z.B. hinter ihm, können meistens den gesamten Datenaustausch mitlesen und so an sensiblen Informationen teilhaben.
  - Von einem kurzfristig unbeaufsichtigten Laptop lassen sich in sekundenschnelle mobile Datenträger wie USB-Sicks oder CD-Roms / DVDs entfernen.

- Auch das Kopieren von Daten auf einen manipulierten USB-Stick ist für geübte Betrüger eine leichte Aufgabe und in kürzester Zeit durchzuführen.

3 Risikominderung und -vermeidung

Wie können die genannten Risiken vermieden werden?

Das Stichwort hier lautet: **Mobile Security Awareness**
Hierunter zählen nicht nur die bereits erwähnten vergessenen oder gestohlenen mobilen Endgeräte, sondern auch der sensible Umgang mit Informationen in der Öffentlichkeit, z.B. bei Telefonaten in Anwesenheit Dritter. Das Sicherheitsbewusstsein der Mitarbeiter muss erhöht werden, in dem Sie über die vorhandenen Gefahrenquellen informiert und in Abwehrmaßnahmen geschult werden. Zusätzlich sollte jedes Unternehmen Richtlinien für den Umgang mit sensiblen Daten „off premises“ festlegen.

- Physischer Diebstahl kann bei einem Laptop z.B. durch ein Kensingtonschloss deutlich erschwert werden. Doch auch für den Fall eines Diebstahls oder Verlusts sollte man vorsorgen: Die Verschlüsselung kompletter Geräte inkl. Betriebssystem oder Teilen der Festplatte sowie mobiler Datenträger wie USB-Sticks ist mit ausgereiften Tools mit geringem Aufwand kostengünstig zu bewerkstelligen.

- Mobiltelefone/ Handhelds/ PDAs/ Smartphones lassen sich durch die Einrichtung von Firewalls oder verschlüsselten VPN- Verbindungen zum Unternehmensnetz gezielt absichern. Weiterhin sollten für Benutzer von Firmen-Hardware keine Administratorenrechte auf den Geräten eingeräumt werden. So können weder bewusst noch unbewusst Sicherheitseinstellungen außer Kraft gesetzt werden.

- Mobile Speichergeräte sollten verschlüsselt sein und über sichere Passwörter verfügen. (Zu Verschlüsselungen siehe „Physischer Diebstahl“).

- Drahtlose Verbindungen sollten mit Passwörtern gesichert sein, die aus mindestens 32 Zeichen bestehen und Groß- und Kleinschreibung, Zahlen und Sonderzeichen beinhalten. Der Sicherheitsstandard 802.11i (WPA / WPA2) gilt derzeit als entschlüsselungssicher.

- Bluetooth sollte deaktiviert werden, sobald die Verbindung nicht genutzt wird. Zugriffe sollten nur von bekannten Geräten erlaubt werden. Auch dann sollte gründlich geprüft werden, ob die andere Seite wirklich ist, was sie zu sein scheint.

- Voice over IP sollte nur genutzt werden, wenn zuvor die Sicherheit des Netzes geprüft wurde. Zusätzlich sollten Verschlüsselungen vorgenommen werden, da diese meist kein Standard sind.

- „Der Zug als Büro“ – als Beispiel für das Arbeiten unterwegs
  Auf Reisen sollten alle Datenfreigaben sämtlicher mobilen Geräte deaktiviert werden. Spezielle Polarisationsfilter-Folien für Laptops verhindern eine unbefugte Einsichtnahme sensibler Daten durch Sitznachbarn oder Mitreisende.

Das allgemeine Bewusstsein für mögliche Gefahren und die Einrichtung und Implementierung von Sicherheitsrichtlinien für mobile Geräte bieten eine gute Basis für die Vermeidung von Da-

tenverlust und der Verbreitung sensibler Unternehmensdaten außerhalb des eigenen Unternehmens.

Sind Sie sich unsicher hinsichtlich der Wirksamkeit Ihrer Sicherheitsmaßnahmen für mobile Endgeräte? Möchten Sie besser auf aktuelle und zukünftige Bedrohungen vorbereitet sein? Wir unterstützen Sie gerne darin, in der Zeit des Ubiquitous Computing auf der sicheren Seite zu stehen.

Kontaktieren Sie uns unter
it-risikomanagement@intargia.com