Check-up Mobile Security

Wissen Sie, ob Ihr Notebook, Handy oder PDA wirklich alle Daten sicher verwaltet?
Mit den nachfolgenden kurzen Checklisten können Sie prüfen, ob Sie in Ihrem Unternehmen die wichtigsten Punkte bedacht haben, um mobile Systeme sicher zu machen.

Fordern Sie außerdem gratis ein Exemplar des <kes>-Specials Mobile Security mit 60 Seiten Grundlagen-Informationen sowie Marktübersichten zu Device-Management und Personal Firewalls an.
Inhaltsverzeichnis, ausgewählte Beiträge und Marktübersicht Personal Firewalls finden Sie unter www.kes.info/mobilesecurity

Check-up Notebook, Handy und PDA

— Haben Sie Ihr Notebook/Handy/PDA immer im Blick? Gehen Sie Tagesroutinen in Gedanken durch und achten Sie darauf, dass Sie jederzeit wissen, wo sich die technischen Geräte befinden, die Sie unterwegs benötigen.
— Auch Handy und PDA können von Viren befallen werden. Haben Sie Schutzsoftware installiert und achten Sie auf regelmäßige Aktualisierung?
— Eine Anmeldung am System sollte nur mit sicherer Authentifizierung möglich sein.
Haben Sie ein individuelles Passwort, melden Sie sich mithilfe eines Security Tokens oder per Biometrie an?
— Verfügen Ihre mobil genutzten Geräte als zweite Hürde für den Verlustfall über eine Verschlüsselung gespeicherter Daten?
— Sind eine VPN-Funktion oder E-Mail-Verschlüsselung zum abhörsicheren Datenaustausch eingerichtet?
— Deaktivieren Sie Bluetooth- und WLAN-Funktion sowie Infrarotschnittstellen, wenn diese nicht gebraucht werden?
Nutzen Sie diese nur in sicheren Umgebungen.
— Sind Sie sicher, dass Sie beim Datenabgleich mit Ihren mobilen Geräten nichts Unerwünschtes ins Firmennetz einschleppen?
Auch mobile Geräte sollten in das Gesamtschutzkonzept des Firmennetzwerks integriert sein.

Check-up USB-Stick, MP3-Player und iPod, Digitalkamera

— Sind alle USB-Sticks oder andere tragbare Speicher erfasst, die in Ihrem Unternehmen genutzt werden?
— Existiert eine Firmen-Policy, welche die Verwendung von USB-Devices regelt?
— Gibt es einen festen/sicheren Platz zur Aufbewahrung der Datenspeicher?
— Ist ein Passwort-Schutz eingerichtet?
— Besteht die Möglichkeit zur Verschlüsselung der aufgespielten Daten?
— Werden Datenspeicher so transportiert, dass sie nicht beschädigt werden können? Kann man einen Schreibschutz aktivieren?
— Dürfen private Daten (z. B. Musik, Videos, Bilder) auf Firmen-Datenträger aufgepielt und von dort ins Firmennetz übertragen werden?

Die Zeitschrift für Informations-Sicherheit

Wir danken den Mitherausgebern für die freundliche Unterstützung des <kes> Specials Mobile Security

Bundesamt für Sicherheit in der Informationstechnik

CenterTools Software GmbH

itWatch GmbH

KOBIL secure your identity

NCP SECURE COMMUNICATIONS

PGP

SafeBoot MOBILE DATA SECURITY

SYSTEMS IT.Media.Communications 23-26 Oktober 2007

utimaco safeware

SecuMedia Verlags-GmbH, Lise-Meitner-Str. 4, 55435 Gau-Algesheim, Tel.: +49 6725 9304-0, Fax: +49 6725 5994, E-Mail: probeheft@kes.de, www.kes.info

Check-up Datensicherheit und Sicherheitsmanagement *

— Datenverschlüsselung: Sowohl die drahtlose Datenübertragung als auch die Speicherung der Daten auf mobilen Endgeräten sollte ausschließlich verschlüsselt erfolgen. Vorsicht: Der Verlust ungeschützter Daten kann unter Umständen die persönliche Haftung der Verantwortlichen und der Geschäftsführung nach sich ziehen.
— Direkte Verbindungen ins Internet sind zu vermeiden. Zu empfehlen ist der Zugang zum Firmennetz über einen VPN-Client.
— Für den Schutz des mobilen Clients gegen Gefahren aus dem Internet, sollten auf ihnen Personal Firewalls installiert sein, die je nach IT-Umgebung, nur gewünschte Kommunikations-Ports und Protokolle freigeben (siehe Marktübersicht „Personal Firewalls“ im <kes>-Special „Mobile Security“).
— Zugangskontrolle: Das mobile Endgerät ist mindestens mit einem Benutzernamen und einem Passwort abzusichern. Wesentlich besser ist ein Finger-Print-Sensor oder Smartcard-Leser, soweit dies der betriebliche Ablauf und das Endgerät zulassen.
— Sicherheits-Policy: Das betriebliche Regelwerk zur IT-Sicherheit sollte explizit das Thema „Mobile Security“ berücksichtigen. Insbesondere bei folgenden Punkten:
— Nutzungsregelung: Es empfiehlt sich, den betroffenen Mitarbeitern in schriftlicher Form klare Regeln für den Umgang mit mobilen Endgeräten an die Hand zu geben. Insbesondere ist dabei die Trennung zwischen beruflicher und privater Nutzung eindeutig zu regeln.
— Zentrales Management: Die Programme und Daten auf mobilen Endgeräten sollten der strikten Kontrolle der zentralen IT-Abteilung unterliegen. Das ist umso leichter durchzusetzen, je weniger Zugangsmöglichkeiten von außen die Geräte aufweisen.
— Device-Management: Welche externen Geräte (Devices) zugelassen sind, welche Daten auf ihnen gespeichert werden und wie man mit ihnen umgeht, sollte klar geregelt sein. Dies lässt sich etwa mit speziellen Software-Tools (siehe Marktübersicht „Device-Management“ im <kes>-Special „Mobile Security“) bewerkstelligen.

** Autor: Harald Duelli hat das <kes>-Special redaktionell betreut, er ist IT-Sicherheitsexperte und Gesellschafter von H.O.D-Consulting, München*

Möchten Sie ein Exemplar des <kes>-Specials oder eine Ausgabe der regulären Zeitschrift <kes> gratis erhalten?
Einfach mit unten stehendem Fax-Abschnitt oder formlos per E-Mail an probeheft@kes.de (solange Vorrat reicht) anfordern!

Glossar Mobile Security

AES – Advanced-Encryption-Standard
CA – Certificate Authority
COBIT – Control Objectives for Information and Technology
DoS – Denial-of-Service
GPRS – General Packet Radio Service
HIDS – Host-basiertes Intrusion Detection System
HIPS – Host-basiertes Intrusion Prevention System
Hotspot – Öffentlicher WLAN-Zugangspunkt
IDS – Intrusion Detection System
IPS – Intrusion Prevention System
IPSEC – Internet Protocol Security
KonTraG – Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
L2TP – Layer 2 Tunneling Protocol
MDM – Mobile-Device-Management
MMS – Multimedia Messaging Service
MTM – Mobile-Trusted-Module
NAC – Network-Admission-Control
NAP – Network-Access-Protection
NAT – Network-Address-Translation
NIDS – Netzwerk-basiertes Intrusion Detection System
OTA – Over-the-Air
OTP – One-Time-Passwort
PDA – Personal Digital Assistant
PIM – Personal Information Management
PPTP – Point-to-Point-Tunneling-Protocol
PKI – Public Key Infrastructure
SOXs – Sarbanes-Oxley-Acts
SSID – Service-Set-Identifier
SSL – Secure-Sockets-Layer
SSO – Single-Sign-On
Spyware – Programmcode mit Spionagefunktion
TC – Trusted Computing
TNC – Trusted-Network-Connect
TPM – Trusted-Platform-Module
UMTS – Universal Mobile Telecommunications System
VLAN – Virtual Local Area Network
VPN – Virtual Private Network
WAF – Web-Application-Firewall
WLAN – Wireless Local Area Network
ZeroDay Protection – Schutz vor unbekannten Attacken
802.1X – Standard zur Authentifizierung in Rechnernetzen

Tipp: *Auf der Website www.bsi-fuer-buerger.de gibt es leicht verständliche Basis-Informationen und Hinweise auf Schutzsoftware.*

PROBEHEFT-ANFORDERUNG

☐ **JA,** bitte schicken Sie mir gratis und unverbindlich ein Exemplar der <kes> - Die Zeitschrift für Informations-Sicherheit Ausgabe 2007#3 zum Probelesen zu.

☐ **JA,** bitte schicken Sie mir das <kes> Special zum Thema „Mobile Security“ gratis zu.

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.

Absender:

SecuMedia Verlags-GmbH, Lise-Meitner-Str. 4, 55435 Gau-Algesheim, Tel.: +49 6725 9304-0, Fax: +49 6725 5994, E-Mail: probeheft@kes.de, www.kes.info