

Firewalls

Contentfilter

VPN-Router

Appliances

Security Service

OEM Development



Sicherheit in Behördennetzen

***Security-Aspekte bei der Einführung
moderner Lösungen in der Verwaltungs-
kommunikation***

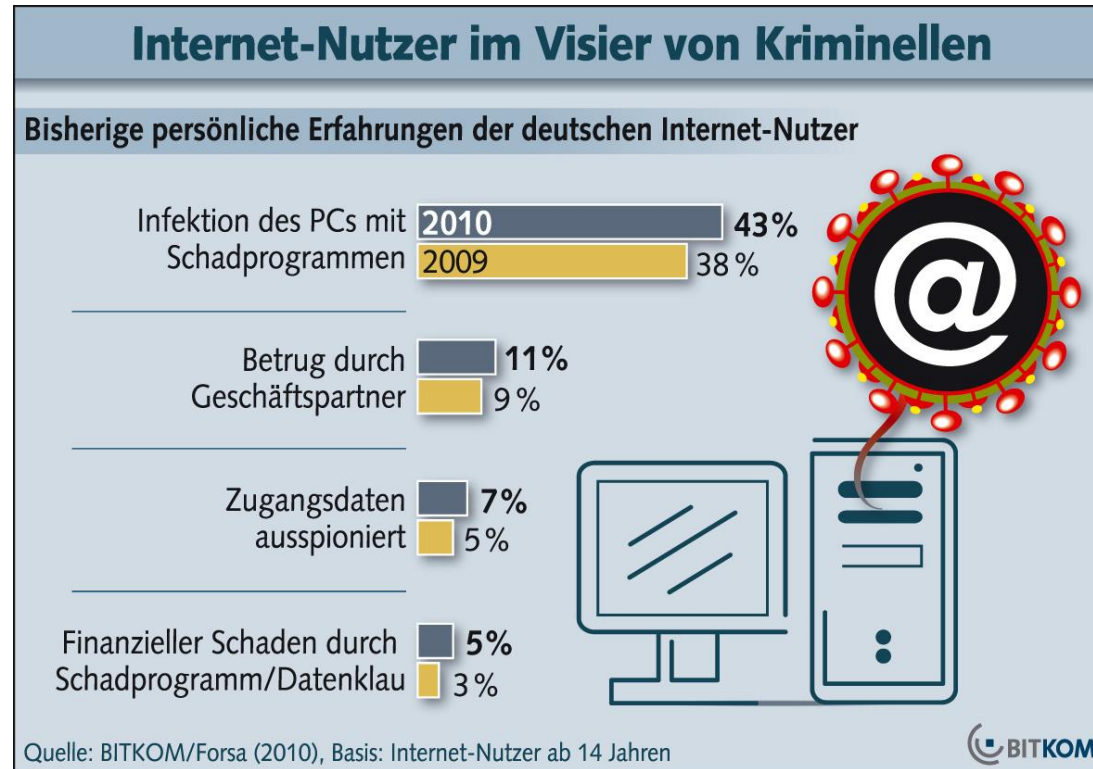
Dipl.-Ing. Gerd Lochter

| IT-SECURITY | | | |
|---|------------|---|--|
| Entwicklung | Produktion | Consulting | Training |
| Firewall-Systeme VPN-Systeme Intrusion Prevention Systeme Application Level Gateways Proxy-Systeme Datensicherungs-Systeme Embedded-Systeme | | Sicherheitsanalyse Sicherheitskonzeption | Produkttraining Sicherheitstraining |
| Managed Security Service | | | |

Grundsätzliches

Trend zur Mobilität ->

- Netzwerk-Perimeter schwinden
- “**extern**“ und “**intern**“ verlieren an Bedeutung
(früher : intern = gut und extern = böse)
- Nutzer + Betriebssysteme sind mobil
- Bedrohungen überall !

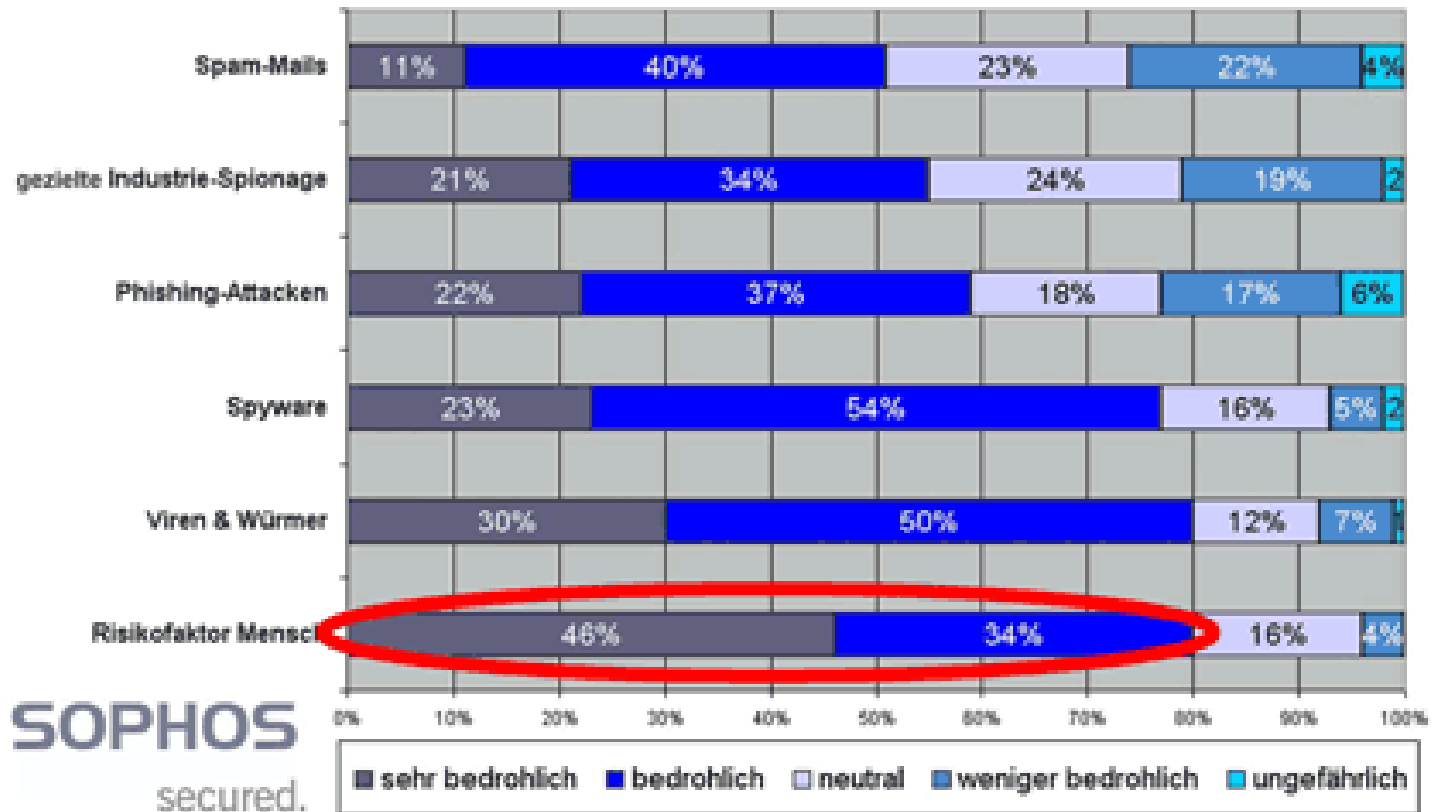


Prominente Warnung: BKA-Präsident Ziercke: Online-Banking wird immer unsicherer. Er selbst wickelt seine Bankgeschäfte nicht am Computer ab.

Quelle: Bundespressekonferenz 01.09.2010

Was sind die Bedrohungen?

Was ist für Sie die größte Bedrohung der IT-Sicherheit in Unternehmen?



Microsoft Patch Teil 1

Microsoft stopft 34 heikle Sicherheits-Löcher

11.08.2010, 10:12 Uhr | Jörg Hofmann



Update-Alarm: Microsoft veröffentlicht neue Sicherheitsupdates für Windows.

Patch-Rekord bei **Microsoft**: Satte 34 Lecks in 14 Flickern müssen von Nutzern in allen Versionen von Windows, aber auch von Office und dem **Internet Explorer**, mit neuen Patches geschlossen werden. Mindestens neun Updates entfallen auf Windows XP, elf auf Vista und zehn Updates auf Windows 7. Microsoft Office schlägt mit zwei weiteren Updates zu Buche – wir haben für Sie alle aktuellen Sicherheitsupdates zum Download zusammengestellt.

Microsoft Patch Teil 2

Falscher Windows-Patch installiert Trojaner

13.08.2010, 17:14 Uhr | t-online.de



Spam-Mail versendet Schädlinge

Mit einem Schlag 34 Sicherheits-Lücken in **Windows** beheben – das verspricht eine vermeintliche **Microsoft**-Mail. Doch anstelle auf die wichtigen Patches verweisen die enthaltenen Links auf einen gefährlichen **Trojaner**. Mit diesem können Online-Kriminelle einer Warnung des Sicherheits-Dienstleisters BitDefender zufolge den befallenen PC kontrollieren und zum Spam-Versand missbrauchen. Clevererweise verstecken sich die Gangster hinter dem aufsehenerregenden **Microsoft Rekord-Patchday** von dieser Woche.

Passwortsicherheit – ein alter Hut?

- Gibt es eine Richtlinie?
- Länge / Ablaufzeit

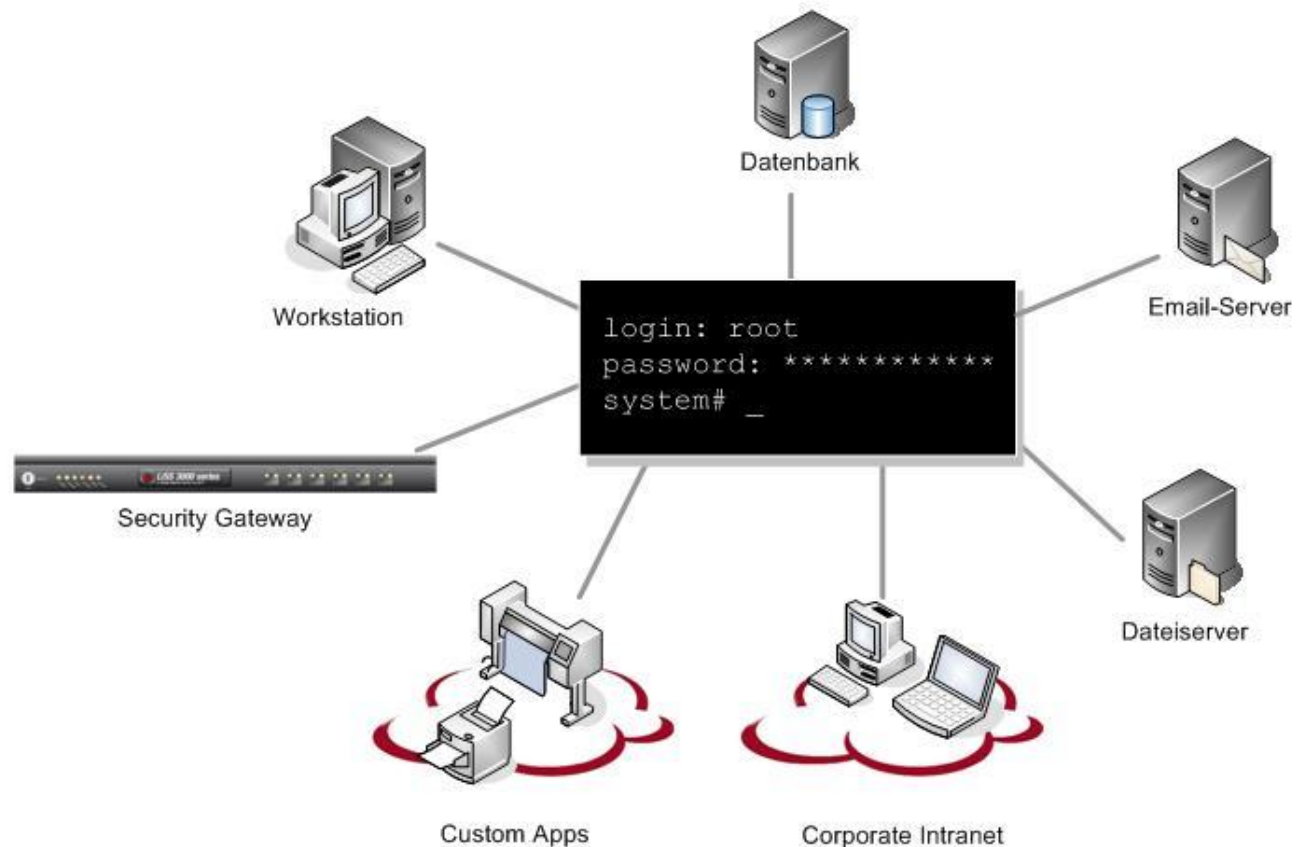
Viele Passwörter hoffnungslos veraltet

16.08.2010, 8:51 Uhr | Andreas Lerg



Unzählige private Daten sind gefährdet, weil zu viele Nutzer zu kurze **Passwörter** verwenden. Forscher des Georgia Tech Research Institutes haben nun belegt, dass sogar eine handelsübliche **Grafikkarte** genügend Rechenleistung bietet, um Passwörter mit sieben oder weniger Stellen in kürzester Zeit zu knacken.

Herausforderung – Passwortkonsistenz



Single Sign On

Social Media

- geringe Kosten
- unkomplizierte Produktionsprozesse
- einfache Zugänglichkeit
- globale Verbreitung
- Aktualität



Malware



Erneute Spam-Attacke durch Sicherheitslücke in Facebook

Beim Hochladen von Fotos versäumte Facebook die korrekte Überprüfung, ob das Bild für das Ziel-Profil zugelassen

ist.

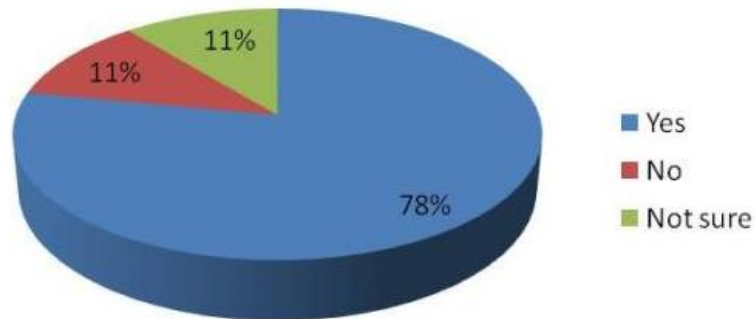
Von Sabine Friedrich (06.09.2010)

06.09.2010

The Macwelt logo, featuring the word "Macwelt" in white, bold, sans-serif font on a red rectangular background.

SPAM - die neuen Tricks auf Facebook

Is spam a problem on Facebook?



Source: F-Secure survey of Facebook users, October and November 2010. n=363

- Unmengen gefälschter Nutzerprofile
- "Dislike Button" 12%
- Anzeige der Besucher des Profils 20%

Bei Aktivieren derartiger Spam-Anwendungen werden sie mit allen **Freunden** geteilt und verbreiten sich rasend schnell.

Instant Messaging

YAHOO! MESSENGER

- Nachrichtenübermittlung (chatten)
- Push-Verfahren
- Dateitransfer möglich
- keine Installation



Sonderfall



- Läuft hinter Firewall und NAT
- hebt Sicherheitsmechanismen aus
- Kontrollverlust über ext. Kommunikation



Sicherheitsmaßnahmen (organisatorisch)

- Sicherheitsrichtlinien / Sicherheitspolitik
- Aktualität der verwendeten Software
- verschiedene Virens Scanner
- Nutzung von Terminalservern
- Internetnutzung mit Inhaltsfilter
- Passwörter
- Nutzerverhalten
- Zugriffsrechte

Sicherheitsmaßnahmen (technisch)

- Kontrolle der Umsetzung der Sicherheitspolitik
- verstärkter Einsatz universaler Sicherheitssysteme
- sinnvolle Kombination von :
 - Authentifizierung
 - Datenverschlüsselung
 - Schutz vor schädlicher Software
 - Ferngesteuertes Sperren

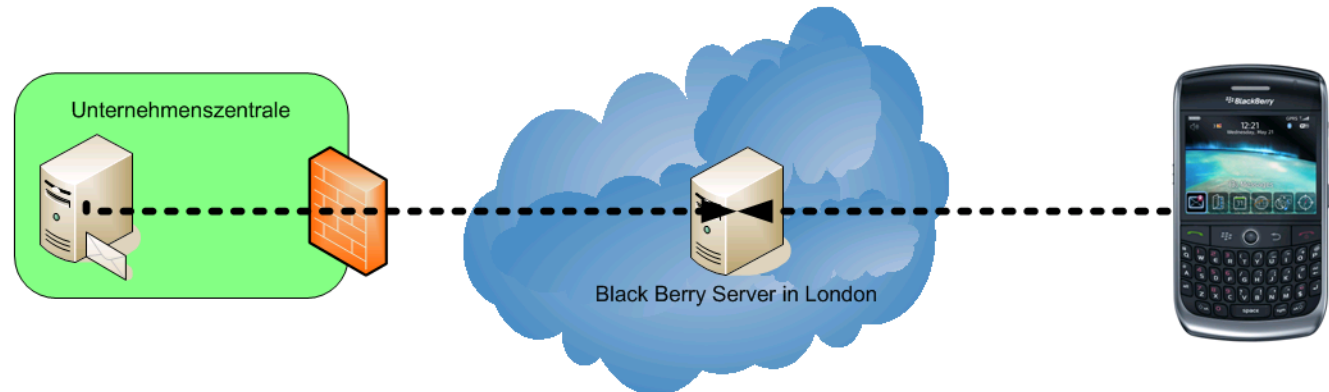
BlackBerry, iPhone und Co.

- Anbindung von Smartphones
- E-Mail Kommunikation immer und überall
- Kalender / Kontakte immer dabei

- verschiedene Varianten

BlackBerry

- Verschlüsselte Verbindung vom Smartphone zum Server
- Daten werden komprimiert übertragen (Kosten)
- Komplette Kommunikation läuft über Server in London



BlackBerry

Verschlüsselte Smartphones

Artikel-Services

Saudi-Arabien sperrt „Blackberry“-Dienste

Im Streit um die verschlüsselte Übertragung von Daten über Smartphones der kanadischen Marke „Blackberry“ hat der Golf-Staat seine Ankündigung wahr gemacht und als erstes Land der Welt Dienste des Telefons abgeschaltet.

Von Matthias Rüb, Washington

06.08.2010

Franfurter Allgemeine
FAZ.NET

BLACKBERRY

RIM lässt Saudi-Arabien in Kundendaten spähen

Saudi-Arabien sagt, Blackberrys werden künftig überwacht. Der Hersteller RIM installiere einen Server dort. Es wäre ein Präzedenzfall. Der Konzern selbst schweigt dazu.

07.08.2010

ZEIT  ONLINE

BlackBerry

Indien setzt BlackBerry-Hersteller unter Druck

Die indische Regierung will Zugriff auf die Datenkommunikation von BlackBerry-Handys. Sollte Hersteller Research in Motion das nicht bis Ende August ermöglichen, sollen die BlackBerry-Dienste auf dem Subkontinent deaktiviert werden.

12.08.2010

SPIEGEL ONLINE

Indien kann bald BlackBerry-Kurznachrichten lesen

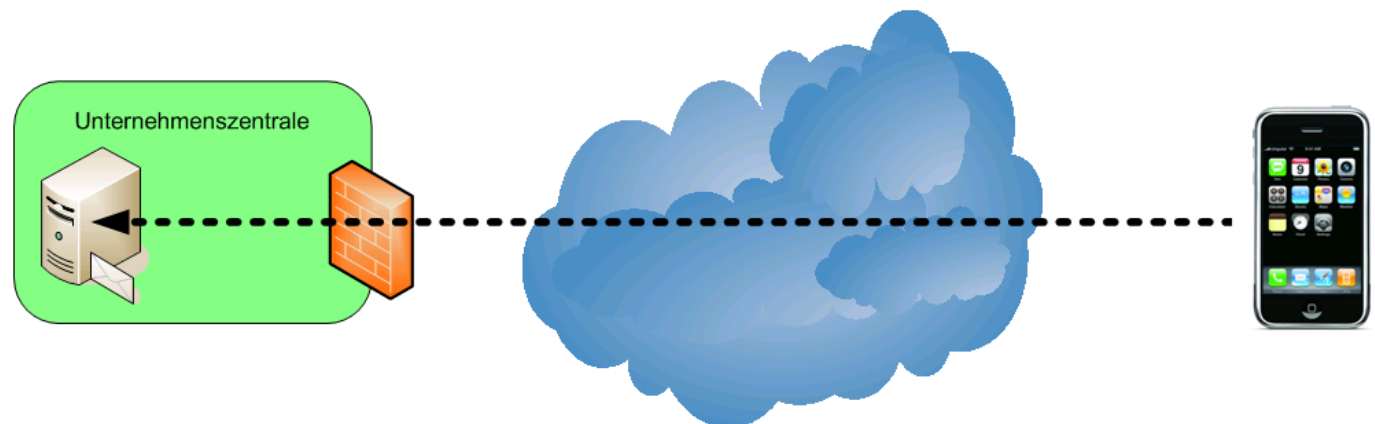
Der BlackBerry-Hersteller Research in Motion geht auf Forderungen der indischen Regierung ein. Das Unternehmen will den Behörden des Landes ermöglichen, künftig Kurznachrichten mitzulesen, die verschlüsselt zwischen Blackberrys ausgetauscht werden. Doch die Regierung will noch mehr.

16.08.2010

SPIEGEL ONLINE

iPhone

- Zugriff aus dem Internet muss freigeschaltet werden
- Direkte Kommunikation (ohne Zwischenstationen)



Sicherheitsleck gefährdet iPhone und iPad

04.08.2010, 9:04 Uhr | t-online.de

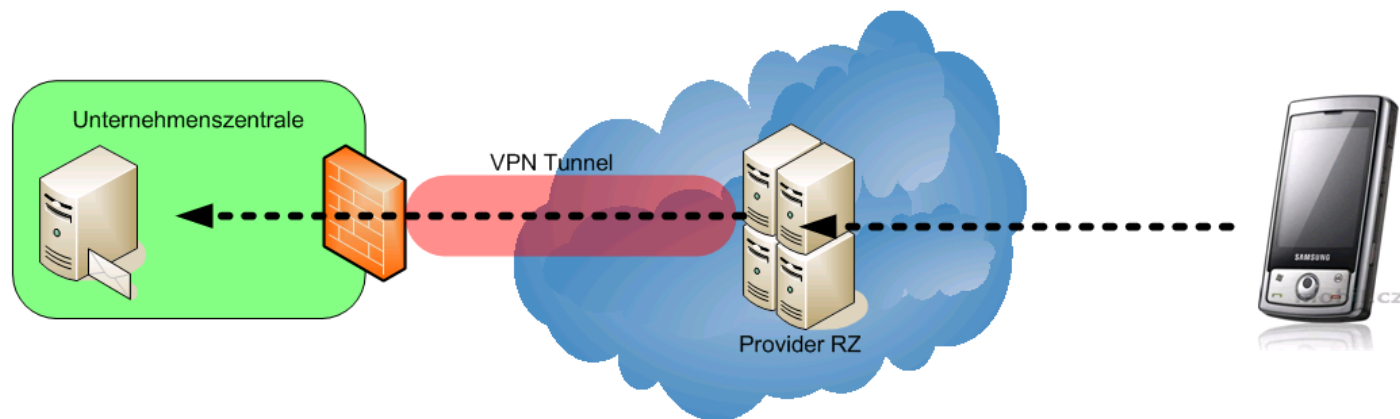


Gleich drei Sicherheitsfirmen warnen vor einer Lücke im Betriebssystem von iPad und iPhone (Foto: dpa).

Eine Sicherheitslücke im Betriebssystem von **Apple iPad** und **iPhone** erlaubt es **Online-Kriminellen**, sich Zugang zu den Geräten zu verschaffen. Das melden gleich drei auf Computer- und Softwaresicherheit spezialisierte Unternehmen. Die Schwachstelle steckt in Apples mobilem Betriebssystem, das auch auf dem Medienplayer iPod Touch läuft. **Hacker** könnten über eingeschleuste und manipulierte PDF-Dateien die Kontrolle über die Geräte übernehmen und private Informationen stehlen. Auch der heimliche Anruf bei teuren Bezahlnummern oder Online-Einkäufe auf Kosten der Opfer sind denkbar. **Apple** soll bereits Untersuchungen eingeleitet haben.

Anbindung über Provider

- Traffic wird über Rechenzentrum geschickt
- Zugriff für Provider auf internen Server



Hackingtools für Jedermann

Verwandeln Sie Ihr Handy in ein Geheimschon

Haben Sie gewusst, dass man ein kleines Tool auf das gewöhnliche Handy installieren kann, um aus dem Telefon einen intelligenten Spion zu machen? Refog Mobile Spy wird versteckt auf dem Mobiltelefon installiert und läuft unbemerktbar und unentdecktbar für den Inhaber. Nach der Installation wird Refog Mobile Spy versteckt ausgeführt und nimmt alles auf, was auf oder um den Telefon herum passiert; Sie werden darüber per sicheres Online-Konto informiert. Auf dieses können Sie vom beliebigen PC mit Internetanschluss oder Mobiltelefon zugreifen.

Was genau leistet Refog Mobile Spy? Sie werden es nicht glauben, wie viel Information durch das gewöhnliche Mobiltelefon aufgezeichnet werden kann!



Hackingtools für Jedermann

Nutzt die Personal-Überwachung Ihrer Firma was?

Nutzen all Ihre Mitarbeiter die PCs und Internet ausschließlich für Geschäftszwecke? Arbeiten sie gleich fleißig, egal, ob Sie über ihre Schulter schauen oder außerhalb des Büros sind? In anderen Wörtern – zweifeln Sie manchmal deren Produktivität an? Sie sollten daran denken, ein Überwachungssystem zu installieren, um sich mit dem Problem zu befassen.



Überlegen Sie nicht weiter! Refog Employee Monitor überwacht und zeichnet die Aktivitäten Ihres Personals auf und ermöglicht einen örtlichen und Fernzugriff auf die Personal-Logs und PC-Bildschirme in Echtzeit. Die Software-Lösung kann innerhalb der Minuten installiert werden und braucht keine andere Hardware, als einen normalen PC. Sie brauchen keine spezielle Überwachungs-Kenntnisse oder Sicherheits-Training, um Refog Employee Monitor erfolgreich zu konfigurieren und zu verwalten.

Hackingtools für Jedermann

Arbeitgeber



- Überwachen Sie die akzeptable Internetnutzung
- Überwachen Sie die Leistungsfähigkeit Ihrer Mitarbeiter
- Spüren Sie unerlaubte Zugriffsversuche auf
- Machen Sie die Text-Sicherheitskopie
- Erstellen Sie Statistiken für Computernutzung

Eltern



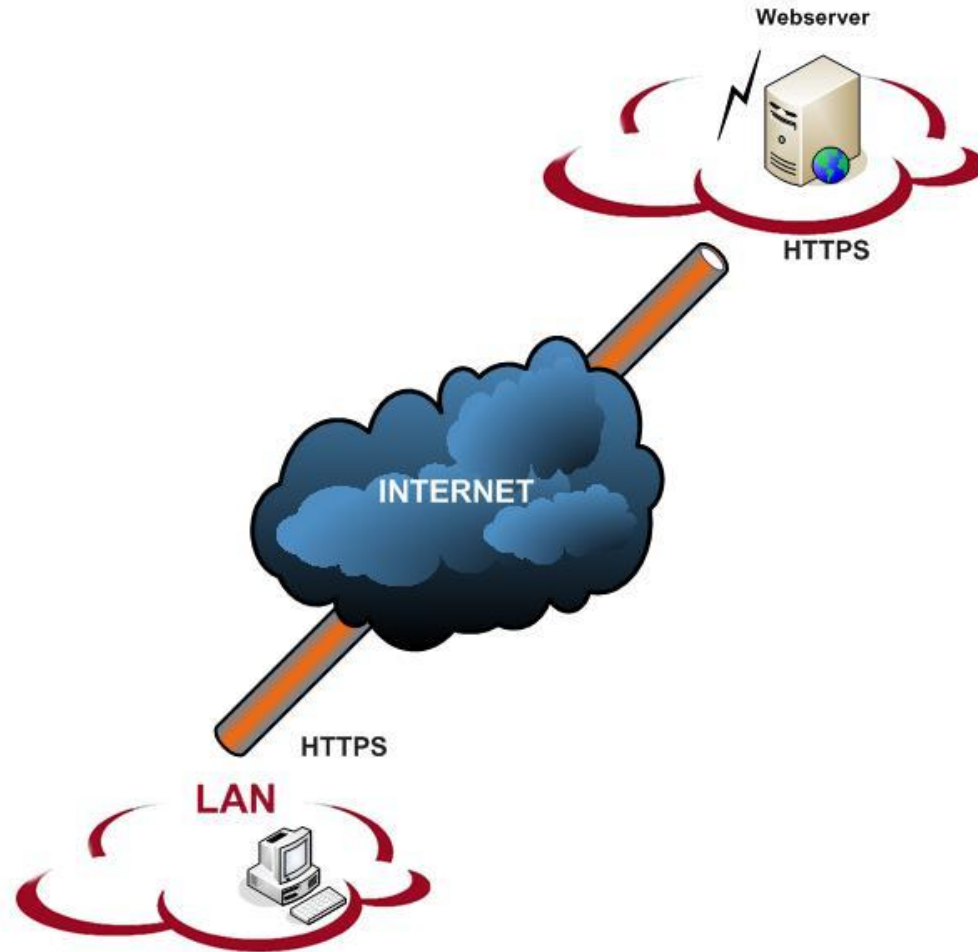
- Überwachen Sie die Computernutzung in der Familie
- Schützen Sie Ihr Kind vor den Internetgefahren und Online-Straftätern
- Überwachen Sie die Nutzung von WWW-Seiten, E-Mail und Chat
- Speichern Sie Dokumentkopien

Ermittlungsbeamte



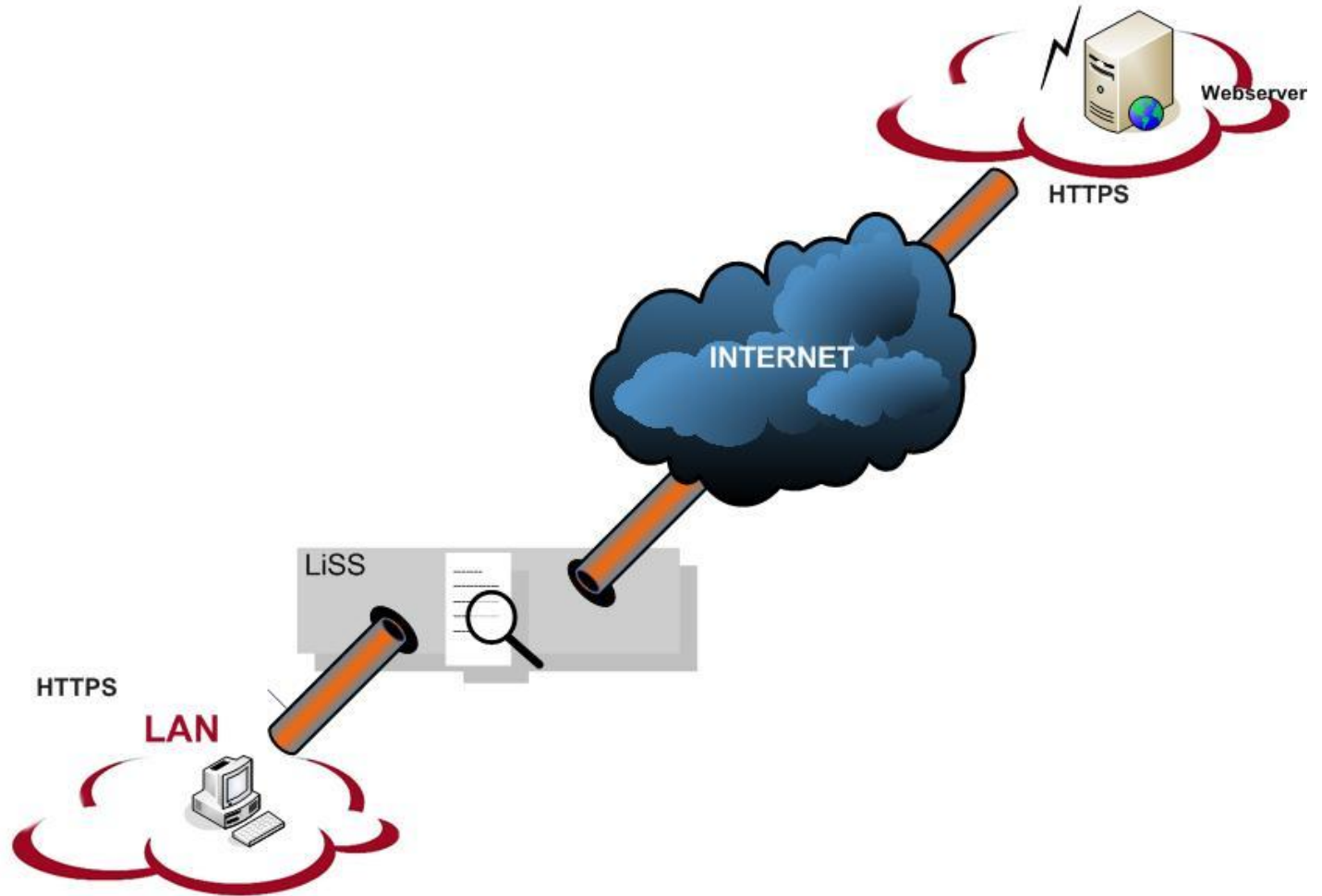
- Überwachen Sie Remote-Computer
- Stellen Ihre Passwörter wieder her, unabhängig vom Betriebssystem
- Sammeln Sie die mit dem Computer verbundene Evidenz
- Spüren Sie unerlaubte Zugriffsversuche zum Computerhardware auf

Verschlüsselung = Sicher ?



Surfen über HTTPS

Filterung im SSL-Tunnel



HTTPS-Proxy

Security - Motivation

- Haftungsrisiko
- Jugendschutz
- Produktivitätsverlust

Lösungsansätze

- Know-How
- Information / Beratung
- Partnerschaften



Firewalls

Contentfilter

VPN-Router

Appliances

Security Service

OEM Development



***Potsdamer Straße 18a
14513 Teltow***

Tel.: +49 (0) 3328 / 43 08 10

Fax: +49 (0) 3328 / 43 08 15

www.telco-tech.de

info@telco-tech.de