



Herzlich willkommen...

Risikofaktor Mitarbeiter – Unwissenheit schützt nicht

mIT Sicherheit ein guter Partner

IT-ON.NET 

The logo for IT-ON.NET features the text "IT-ON.NET" in a bold, blue, sans-serif font. To the right of the text is a stylized icon of a person, composed of a blue circle for the head and a grey vertical bar for the body, with horizontal bars for arms and legs.

Vorstellung der heutigen Themen



17.30 Uhr

Begrüßung

Tobias Fritzsche, IT-On.NET Süd GmbH

17.35 Uhr

Einleitung

Tobias Fritzsche, IT-On.NET Süd GmbH

17.40 Uhr

Unwissenheit schützt nicht

Daniel Renoth/Tobias Fritzsche, IT-On.NET Süd GmbH

18.20 Uhr

Fragen und Antworten



IT-On.NET Süd GmbH

Tobias Fritzsche

mIT Sicherheit ein guter Partner

IT-ON.NET 

The logo icon consists of a blue circle above a vertical blue bar, which is flanked by two grey vertical bars, forming a stylized 'i' or 'IT' shape.



- **Gründung: 2006 mit 2 Mitarbeitern**
- **Firmenentwicklung: jährliches zweistelliges Wachstum**
- **9 Mitarbeiter, davon 5 Systemtechniker**
 - Wir sind auf der Suche! Kennen Sie jemanden?
- **Spezialisten für Serverinfrastrukturen, IT-Sicherheit und deren modulare und pauschale Betreuung**
- **Kunden: Helios Ventilatoren GmbH, Teubert Maschinenbau GmbH, VHW Metallpresswerk GmbH, Föhrenbach GmbH, Storz Schokolade GmbH & Co. KG, PAPST LICENSING GmbH & Co. KG, ...**



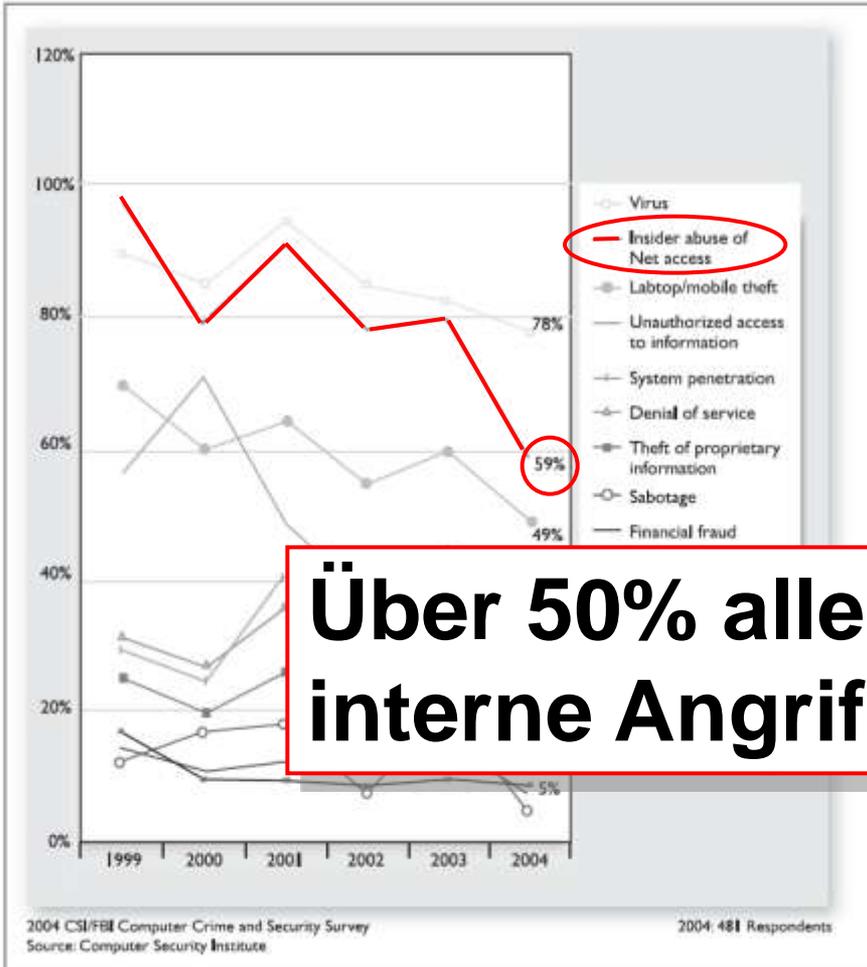
Einleitung „Unwissenheit schützt nicht“

Tobias Fritzsche

mIT Sicherheit ein guter Partner

IT-ON.NET 

Wie groß ist die Gefahr von innen?



Source: CSI / FBI Computer Crime and Security Survey, by Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson

Über 50% aller Angriffe sind interne Angriffe !

Figure 13. Types of Attacks or Misuse Detected in the Last 12 Months (by percent)

Welche Mitarbeitertypen gibt es?



Der Sicherheits-Softie

Jeder fünfte Angestellte lässt Familienmitglieder oder Freunde mit dem Firmen-Notebook oder –PC im Internet surfen.

Der Gadget-Freak

Mehr als die Hälfte der Umfrageteilnehmer schließen ihre eigenen mobile Geräte wie USB-Sticks, Digitalkameras und Mobiltelefone an den Firmen-PC an.

Der Illegale

Rund 60 Prozent geben an, dass sie persönlichen Content auf ihrem Arbeitscomputer ablegen. Jeder Zehnte in Europa lädt unerlaubte Contents herunter.

Der Saboteur

Fünf Prozent dringen in Bereiche des IT-Systems ein , für die sie keine Berechtigung haben.

Wieso ist diese Zahl hauptsächlich so hoch?



„Jeder dritte Mitarbeiter wurde am Arbeitsplatz nicht in IT-Sicherheit geschult. Dennoch fühlen sich die meisten ausreichend informiert – ein Trugschluss, meint Clearswift.“

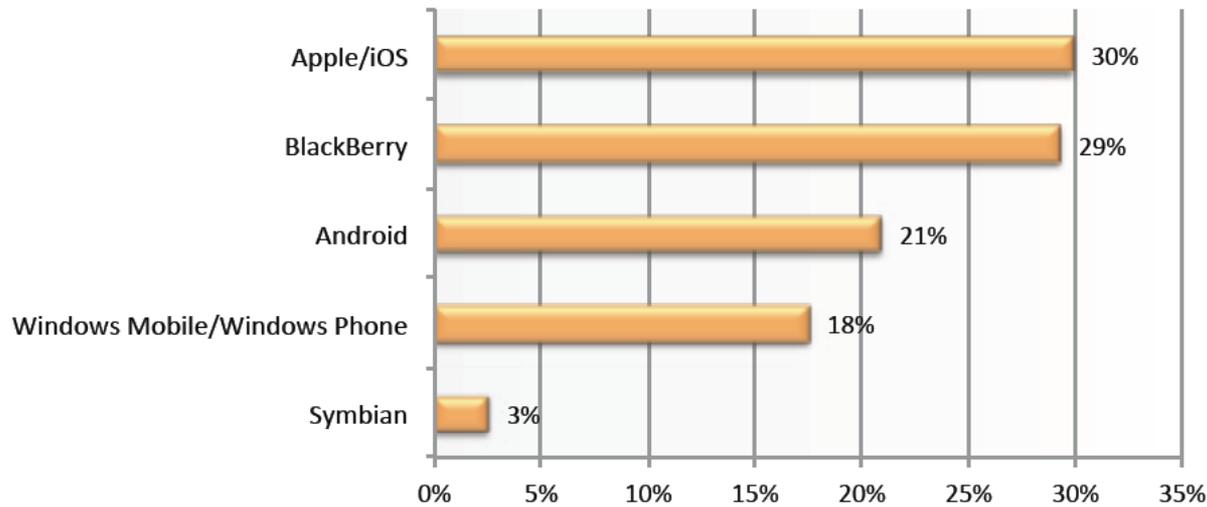
Thomas Pelkmann, Computerwoche, 22.09.2011



Was ist die größte Herausforderung?



Most used mobile platform connecting to corporate networks



© Heise Zeitschriften Verlag

- ***Ponemon Institute, 2010:***
„330 Firmen,
84.500 verlorene mobile Geräte,
nur 4.000 wurden wieder gefunden,
25 % wurden gestohlen!“
- ***„Bei der Bundesregierung sind 515 Computer mit teils***
geheimen Informationen verschwunden“, Bild 18.04.2008



**„Unwissenheit schützt nicht“
oder worauf Sie achten sollten!**

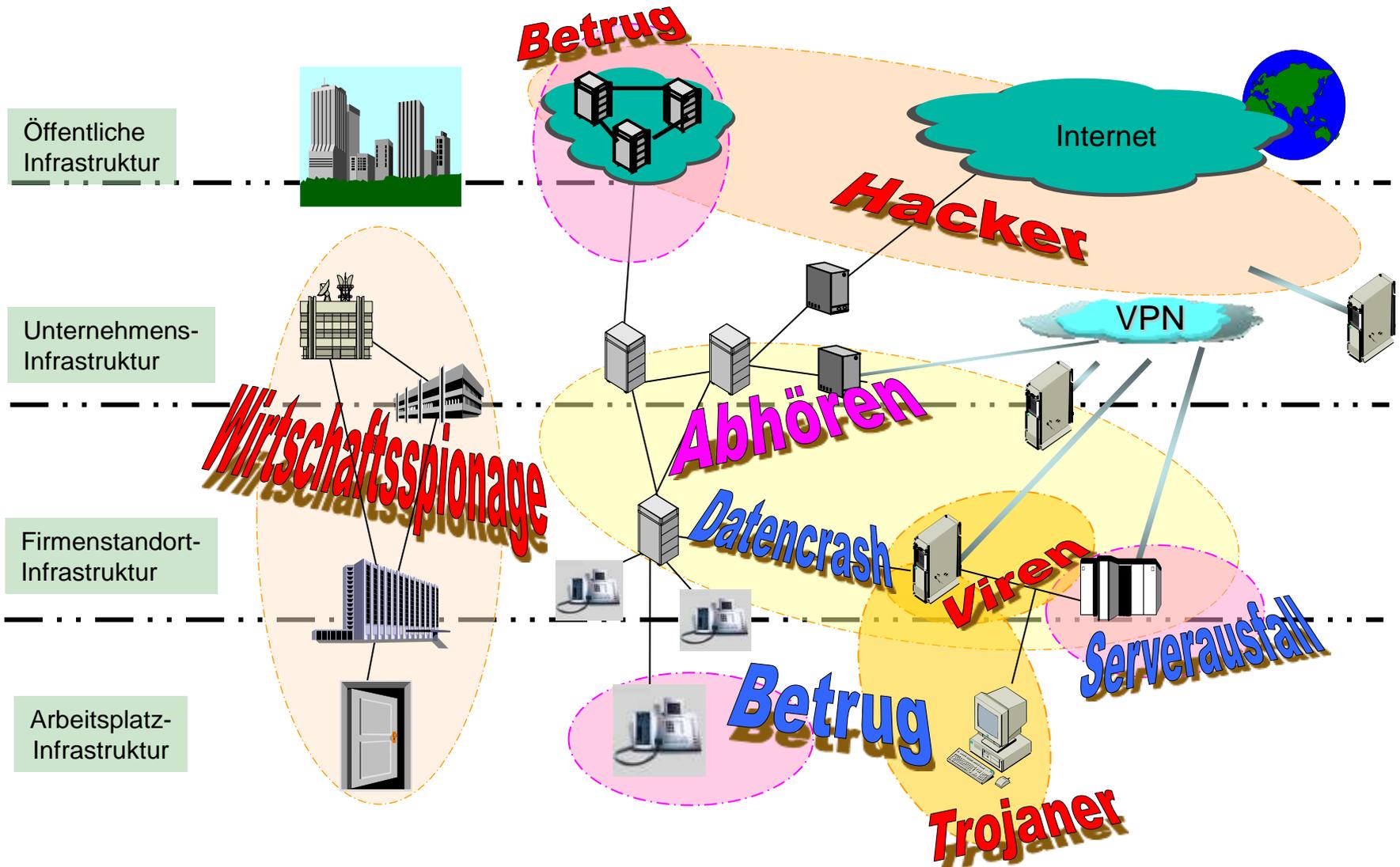
Daniel Renoth – Tobias Fritzsche

mIT Sicherheit ein guter Partner

IT-ON.NET 

The logo for IT-ON.NET features the text "IT-ON.NET" in a bold, blue, sans-serif font. To the right of the text is a stylized icon of a person, composed of a blue circle for the head and a grey vertical bar for the body, with horizontal lines extending from the top and bottom of the body to represent arms.

Wo kann denn überhaupt was passieren?



26.03.2012

Wen lassen Sie in Ihr Haus rein?



- **Geeignete Zutrittskontrolle?**
- **Video-/Fotoaufnahmen?**
- **Wie wird mit Besuchern/ Delegationen umgegangen?**
- **Wie viel Einsicht erhalten Praktikanten?**
- **Stehen Ordner einfach nur rum?**
- **„Honigfallen“?**



Margot Kessler / pixelio.de

Ist der PC auch ein Arbeitsmittel/Werkzeug?



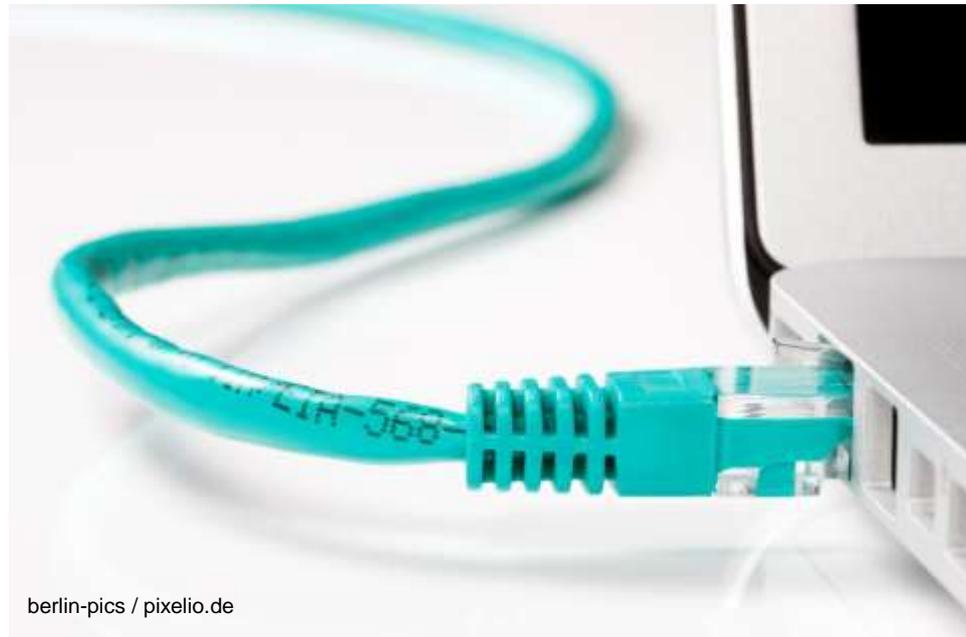
- **PC Wartung und Pflege?**
- **Jedes Arbeitsgerät in der Produktion wird gewartet, gepflegt, geputzt, ...**
- **Jedes Auto muss in die Inspektion, wird gewaschen, gehegt und gepflegt**



Was darf ich installieren?



- **Anwendungssteuerung**
- **„Datenflusskontrolle“**
- **Aufklärung der Benutzer/-innen**



Was interessieren mich die Daten anderer?



- **Rechtestruktur**
- **Bildschirmschoner**
- **Kennwortschutz**
- **Bürozugang/Zutrittsgenehmigungen**
- **Persönliche Gründe**

The image shows a close-up of a German tax slip (Lohnsteuerbescheinigung) with the following data:

Verdienstbescheinigung	
Gesamt-Brutto	3.86903
Lohnsteuer	
SoZ	
SV-Brutto	3.86903
KV-Beitrag	29018
AV-Beitrag	12576
Rest	

Other visible text includes 'KUG-Akt' and 'Darlehen Rest'.

Claudia Hautumm / pixelio.de

„Das war doch ein netter Herr!“



- **Ausnutzung von menschlichen Schwachstellen**
- **Vortäuschung von Identitäten**
- **Ausnutzung von Verhaltensweisen**
- **„Social Engineering sei die bei weitem effektivste Methode, um an ein Passwort zu gelangen...“, Wortlaut Kevin Mitnick**

Das ist „Social Engineering“ oder auch „Social Hacking“!!!



Wikipedia.de – Kevin Mitnick 2008

Und was ist z. B. mit USB-Sticks?



- **Schnittstellenkontrolle**
- **Vermeidung von Datenverlust**
- **Sicherheit vor Malware & Co.**





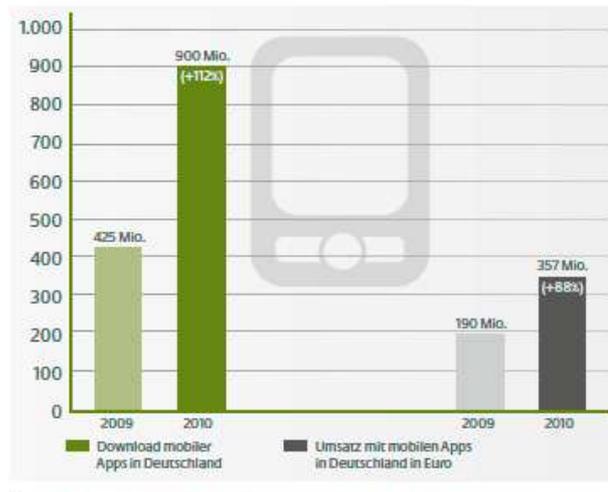
- **Mobile Geräte sind kleine PCs!**

- **Welche Geräte haben Sie?**

„Knapp jedes dritte verkaufte Handy war 2011 ein Smartphone. Insgesamt wurden 476,5 Millionen Computer-Handys abgesetzt. Das war im Jahresvergleich in Plus von 58 Prozent.“ dpa.de

- **Aktuelle Sicherheitspatches/Firmware**

Mobile Applikationen



Quelle: Bitkom

Abb. 12: Entwicklung von Download und Umsatz mobiler Applikationen für Smartphones in Deutschland [6]



- **Dringlichkeit zur Mobilität**
- **Hippe Technologien sind gefragt**
- **Virtualisierung von einzelnen „Anwendungen“**

- **„45 Prozent finden ihre eigene Hard- und Software nützlicher als die der Firma.“**
- **„Jeder Zweite nutzt sowieso seine eigenen Geräte für die Arbeit.“**
- **„Zwei Drittel – so das Ergebnis der Studie – kümmern sich nicht um die IT-Regeln ihrer Unternehmen. Da wird munter getwittert und bei Facebook gepostet.“**

Welt.de, Thomas Heuzeroth, 19.03.2012

Haben Sie noch nie etwas „verloren“?



- **Verschlüsselung**
- **Kennwortschutz**
- **Ortung und Komplettlöschung des Geräts**

Der Zustand der Befragten, als sie ihr Smartphone verloren:

	Gesamt	USA	England	Österreich	Neusee-land	Japan	Spanien	Italien	Deutsch-land	Frank-reich	Kanada
Konzentriert	15 %	16 %	19 %	18 %	18 %	7 %	10 %	20 %	8 %	20 %	20 %
In Eile	22 %	19 %	19 %	23 %	18 %	29 %	18 %	23 %	23 %	19 %	20 %
Beschäftigt/abgelenkt	35 %	43 %	28 %	31 %	39 %	25 %	44 %	29 %	45 %	40 %	20 %
Müde/schlafend	8 %	6 %	7 %	7 %	5 %	17 %	4 %	8 %	6 %	7 %	10 %
Mit Einkäufen beladen	7 %	5 %	8 %	5 %	5 %	7 %	10 %	10 %	4 %	5 %	17 %
Ängstlich/besorgt	6 %	6 %	6 %	4 %	4 %	8 %	8 %	8 %	5 %	7 %	10 %
betrunken	7 %	4 %	14 %	10 %	11 %	7 %	6 %	2 %	9 %	2 %	5 %

Ergebnis: Nur 15% der Smartphone-Besitzer waren konzentriert, als sie ihr Gerät verloren. Mehr als ein Drittel war beschäftigt oder abgelenkt – in Deutschland fast die Hälfte (45%). In England gab mehr als einer von acht Smartphone-Besitzern zu, während des Verlustes betrunken gewesen zu sein.

Haben Sie noch nie etwas „verloren“?



Villingen-Schwenningen

Henning Lichtes E-Mail-Daten geklaut

Von (st), aktualisiert am 21.03.2012 um 11:10



Bei Henning Lichte herrschte am Dienstag Mail- und Telefonterror, weil Unbekannte seinen E-Mail-Account geknackt hatten. Foto: Archiv

Villingen-Schwenningen - "Ich bin im Urlaub in Aberdeen, mir wurde der Geldbeutel und alles geklaut, bitte helft mir, ruft mich an oder schickt mir Geld über Western Union." Diese E-Mail hat den Freie Wähler-Stadtrat Henning Lichte gehörig ins Schwitzen gebracht. "Habe den schlimmsten Tag meines Lebens gehabt", zog er am Dienstagnachmittag Bilanz.

Die Zugangsberechtigung zu seinen E-Maildaten wurden geknackt und somit konnte diese Mail verschickt werden. Zudem sind alle seine rund 300 Mailadressen abhanden gekommen. Am Dienstag in den frühen Morgenstunden sind auf einmal 200 Antworten auf die vermeintlich hilfeschuchende Mail angekommen, dazu noch zwischen 50 und 60 Telefonanrufe.

Henning Lichte reagierte sofort, stoppte den Mail-Account und meldete den Vorfall der Polizei. Ganz offensichtlich seien bei Personen, die karitativ engagiert sind, derlei Dinge bei dem einen Anbieter schon öfter passiert, hatte Lichte erfahren. Das Ehepaar engagiert sich seit Jahren im Kifaz-Treff in Schwenningen.

Wissen Sie, welche Daten außer Haus sind?



- *Cloud*
- *Private, öffentliche, hybride Cloud*
- *Ihre Emails laufen IMMER über die Cloud!*
- *Welche Daten sind intern und welche extern?*



**„Unwissenheit schützt nicht“
oder was Sie tun können!**

Daniel Renoth – Tobias Fritzsche

mIT Sicherheit ein guter Partner

IT-ON.NET 



- **Einführung von geeigneten Schutzmaßnahmen in allen Bereichen, vor allem mobile Geräte**
- **Zentrale Plattformen für übergreifende Produkte**
- **Zentrales Patchmanagement**
- **Einsatz von aktuellen Software-Versionen**
- **Regelmäßige Backup-Möglichkeiten**
- **Geben Sie Ihrer IT in Abstimmung mit Ihnen (und evtl. Betriebsrat) das Ruder in die Hand!**



Gerd Altmann / pixelio.de



- **Internetvereinbarung**
- **Emailnutzungsvereinbarung**
- **Handhabung von Arbeitsmitteln/Technik**
- **Geheimhaltungserklärung**
- **Datenschutzvereinbarung**
- **Passwortrichtlinien**





- **Bestellung eines internen/externen Datenschutzbeauftragten**
- **Bestellung eines IT-Sicherheitsbeauftragten (bei dementsprechender Firmengröße)**
- **Nutzung externer unabhängiger Beratung**



Wieso ist die Zahl vom Anfang so hoch?



„Jeder dritte Mitarbeiter wurde am Arbeitsplatz nicht in IT-Sicherheit geschult. Dennoch fühlen sich die meisten ausreichend informiert – ein Trugschluss, meint Clearswift.“

Thomas Pelkmann, Computerwoche, 22.09.2011





**„Unwissenheit schützt nicht“
oder was Ihre Mitarbeiter wissen sollten!**

Daniel Renoth – Tobias Fritzsche

mIT Sicherheit ein guter Partner

IT-ON.NET 



- ***Was macht die IT überhaupt?***
- ***Auf was müssen Mitarbeiter achten?***
- ***Was bedeuten denn überhaupt Malware & Co.?***
- ***Generationenaustausch (Facebook-Generation)***





- **Geheimhaltung von Passwörtern, Kennzahlen, ... am Telefon, Email, SMS, ...**
- **Sichere Kennwörter verwenden!**
- **Vertrauenswürdigkeit *IMMER* prüfen, bei geringsten Zweifel „auflegen“**
- **Seien Sie bei Besuchern/Delegationen aufmerksam!**





- **Nutzung von vertrauenswürdigen Apps**
- **Sicherung und verantwortungsbewußte Nutzung des Bluetooth- und WLAN-Zugangs**
- **Nur eigene Nutzung, keine Weitergabe des Geräts!**
- **Vertrauliche Gespräche nur an vertraulichen Orten führen!**
- **Zugangsschutz**



Joachim Kirchner / pixelio.de

Wieso wird das alles überhaupt gemacht?



- **Vermeidung von hohen Folgekosten (Datenschutz, Finanzamt, fahrlässige Straftaten)**
- **Verminderung von Haftungsrisiken**
- **Erhöhung des Images**
- **Erhöhung der Kundenzufriedenheit**
- **Sicherung des technologischen Vorsprungs in bestimmten Bereichen vs. „gemeinschaftliche“ Entwicklung**
- **Organisatorische Vorteile**
- **Vorteile bei der Kreditvergabe (Basel II + zukünftig III)**





Vielen Dank! Und nun sind Sie dran!

Wir plädieren in diesem Vortrag nicht für Vollständigkeit! 😊

mIT Sicherheit ein guter Partner

IT-ON.NET 