

Informationstag "IT-Sicherheit in der Marktforschung"

Gemeinsame Veranstaltung von TeleTrust und ADM

Berlin, 16.10.2013

Begrüßung und Einführung

Hartmut Scheffler,

Geschäftsführer TNS Infratest

Vorstandsvorsitzender ADM

Mehr Daten

Klassische
Marktforschungs-
daten

Neue Tools und
neue Daten

Kundendaten

Big Data

Social Media

Mehr Gefahren



Hacker, Viren
und Vieles
mehr



Mehr Angriffs-
möglichkeiten



Cloud
(Un)Sicherheit

IT-Sicherheit: Warum?

Das beiden Verbänden gemeinsame Verständnis von IT-Sicherheit als technische Ausprägung von Datenschutz ist eine unabdingbare Voraussetzung für die Vertrauenswürdigkeit der angewandten Erhebungs- und Auswertungsmethoden.

- * Informationssicherheit umfasst neben Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht-elektronisch verarbeiteten Informationen (Handnotizen etc.)

IT-Sicherheit: Ziele

Datenschutz

Datensicherheit
(Vertraulichkeit,
Integrität, Verfügbarkeit)

IT-Sicherheit:
Sicherheit von
technischen und
logischen Systemen der
Informations- und
Kommunikations-
technologie

IT-Sicherheit: Bedrohungen

- Technischer Systemausfall
- Systemmissbrauch (illegitime Ressourcennutzung, Veränderung von Inhalten etc.)
- Sabotage
- Spionage
- Betrug und Diebstahl

IT-Sicherheit: Ursachen

- Höhere Gewalt (Blitz, Feuer etc.)
- Fehlbedienung
- Computerviren, Trojaner, Würmer
- Phishing
- Physischer Einbruch
- Social Engineering etc.

IT-Sicherheit: Maßnahmenbeispiele

- Eingeschränkte Benutzerkonten
- Restriktive Konfiguration
- Software aktuell halten, veraltete Software deinstallieren
- Sicherungskopien erstellen
- Antiviren-Software verwenden
- Software-Diversifikationen
- Firewalls
- Deaktivieren aktiver Inhalte
- Verschlüsselung sensibler Daten
- Protokollierung
- Sensibilisierung und Training der Mitarbeiter
- Überprüfungen, Audits
- EDV-Maßnahmen: Nachweis von Eingriffen, Installation von Frühwarnsystemen, interne Kontrollsysteme

Das Beispiel Teletrust





Bundesverband IT-Sicherheit e.V.

Startseite

- Arbeitsgruppen
- Projekte
- EBCA
- T.I.S.P.
- T.E.S.S.
- IT-Sicherheit in der Hotellerie
- IT Security made in Germany
- Veranstaltungen
- Innovationspreis
- Publikationen
- Jahresbericht
- Presse
- Über TeleTrust

TeleTrust-Video



TeleTrust-Kooperationen



TeleTrust-Kurzinfos auf Twitter: @TeleTrust_Info

Kontakt Impressum



Sie sind hier: Startseite

Aktuelle Fachinformationen

TeleTrust kooperiert mit dem Fachinformationsdienst "All about security":
www.all-about-security.de



TeleTrust-Termine

Termine 1 bis 5 von 12 | << Erste < zurück Seite 1 vor > Letzte >> » Archiv

- IT Security-Messe 'it-sa' 08.10.13 10.10.13
- TeleTrust-Informationstag "IT-Sicherheit in der Ma 16.10.13
- ISSE-Konferenz 22.10.13 23.10.13
- TeleTrust-AG "Recht" 29.10.13
- T.I.S.P. Community Meeting 2013 04.11.13 05.11.13

» alle Termine

TeleTrust-Informationen

News 1 bis 5 von 136 | << Erste < zurück Seite 1 vor > Letzte >>

- TeleTrust-Information: Mitglieder und Aktivitäten Montag, den 30.09.13
- Verbandsnachrichten 2013/12 » weiterlesen
- TeleTrust-Information: Mitglieder und Aktivitäten Freitag, den 23.08.13
- Verbandsnachrichten 2013/11 » weiterlesen
- TeleTrust-Info: Hinweise auf bevorstehende Veransta Dienstag, den 08.08.13
- Verbandsnachrichten 2013/10 » weiterlesen
- TeleTrust-Information: Mitglieder und Aktivitäten Donnerstag, den 11.07.13
- Verbandsnachrichten 2013/09 » weiterlesen

suchen »

TeleTrust engagiert sich



TeleTrust-Mitgliedschaft

- 10 gute Gründe
- Mitglied werden

TeleTrust-Kalender

Oktober - 2013						
Mo	Di	Mi	Do	Fr	Sa	So
	01	02	03	04	05	06
07	08	09	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

» alle Termine

Service: securityNews

securityNews

Aktuelle Sicherheitsupdates

Update

07.10.2013
Google: Chrome 30 schließt 50 Sicherheitslücken ...

Update

27.09.2013
Apple: Sicherheitspatch 7.0.2 schließt Lücke im Lockscreen ...

Update

19.09.2013
Apple: Neue iTunes-Version 11.1 schließt Sicherheitslücke ...

» Alle Meldungen anzeigen

» Neueste Meldungen abonnieren

Aktuelle IT-Sicherheitslage



Bundesverband IT-Sicherheit e.V.

[Startseite](#)

[Arbeitsgruppen](#)

[Biometrie](#)

[Gruppenleitung](#)

[Termine](#)

[Inhalte und Ziele](#)

[Themen+Referenten](#)

[Dokumente](#)

[Projekt BioTrust](#)

[Biometrie-Übersicht](#)

[Cloud Security](#)

[Mobile Security](#)

[ISM](#)

[Recht](#)

[Smart Grids/Industrial Security](#)

[SOA Security](#)

[SICCT](#)

[EBCA-Technik](#)

[Projekte](#)

[EBCA](#)

[T.I.S.P.](#)

[T.E.S.S.](#)

[IT-Sicherheit in der Hotellerie](#)

[IT Security made in Germany](#)

[Veranstaltungen](#)

[Innovationspreis](#)

[Publikationen](#)

[Jahresbericht](#)

[Presse](#)

[Über TeleTrust](#)

TeleTrust-Kurzinfos auf Twitter: @TeleTrust_Info

[Kontakt](#) | [Impressum](#) |



Sie sind hier: [Arbeitsgruppen](#) » [Biometrie](#)

■ Arbeitsgruppe "Biometrie"

Prof. Dr. Christoph Busch, Fraunhofer-Institut IGD

Ziel:

- Ziel dieser Arbeitsgruppe ist, Rahmenbedingungen und Akzeptanz für den Einsatz von biometrischen Verfahren zu schaffen und zu fördern.

Schwerpunkte:

- Regelmäßiger Informations- und Erfahrungsaustausch
- Bearbeitung von aktuellen Anforderungen
- Entwicklung von Positionspapieren
- Organisation des interdisziplinären Dialogs zwischen an Entwicklung und dem Betrieb von biometrischen Systemen beteiligten Akteuren

Kommunikationsstruktur:

- Arbeitstreffen (üblicherweise drei Mal im Jahr)
- Unterarbeitsgruppen zu Schwerpunktthemen
- Ad-hoc Initiativen via E-Mail
- E-Mail-Informationsverteiler für informellen Datenaustausch
- Dokumenten-Archiv im TeleTrust-Datenraum

Informationsangebot:

- Kriterienkatalog zur Vergleichbarkeit biometrischer Verfahren
- Orientierungshilfe für Betriebsvereinbarungen
- White Paper zum Datenschutz in der Biometrie
- Positionspapier "Körperscanner"
- Pressemitteilungen via TeleTrust
- Projektbericht BioTrust

suchen »

■ TeleTrust engagiert sich



■ TeleTrust-Mitgliedschaft

- » 10 gute Gründe
- » Mitglied werden

■ TeleTrust-Kalender

Oktober - 2013						
Mo	Di	Mi	Do	Fr	Sa	So
	01	02	03	04	05	06
07	08	09	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

[» alle Termine](#)

■ Service: securityNews

securityNews

Aktuelle Sicherheitsupdates

Update 07.10.2013   
Google: Chrome 30 schließt
50 Sicherheitslücken ...

Update 27.09.2013   
Apple: Sicherheitspatch
7.0.2 schließt Lücke im
Lockscreen ...

Update 19.09.2013   
Apple: Neue iTunes-Version
11.1 schließt
Sicherheitslücke ...

[» Alle Meldungen anzeigen](#)
[» Neueste Meldungen abonnieren](#)

Aktuelle IT-Sicherheitslage

Beispiel: Cloud Security

Vertragsstrafen

Persönliche
Geschäftsführer-
Haftung

Vertragsinhalte



Bundesverband IT-Sicherheit e.V.

[Startseite](#)

[Arbeitsgruppen](#)

[Projekte](#)

NEG

[Wireless LAN Sicherheit](#)

[Elektronische Signatur](#)

[PKI Referenzprojekt](#)

[SICCT](#)

[OID](#)

[BioTrust](#)

[Kartenterminal](#)

[EBCA](#)

[T.I.S.P.](#)

[T.E.S.S.](#)

[IT-Sicherheit in der Hotellerie](#)

[IT Security made in Germany](#)

[Veranstaltungen](#)

[Innovationspreis](#)

[Publikationen](#)

[Jahresbericht](#)

[Presse](#)

[Über TeleTrust](#)

[TeleTrust-Video](#)



TeleTrust-Kurzinfos auf Twitter: @TeleTrust_Info

[Kontakt](#) | [Impressum](#) |

■ TeleTrust engagiert sich



■ TeleTrust-Mitgliedschaft

» 10 gute Gründe

» Mitglied werden

■ TeleTrust-Kalender

Oktober - 2013						
Mo	Di	Mi	Do	Fr	Sa	So
	01	02	03	04	05	06
07	08	09	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

[» alle Termine](#)

■ Service: securityNews

securityNews

Aktuelle Sicherheitsupdates

Update 07.10.2013
Google: Chrome 30 schließt
50 Sicherheitslücken ...

Update 27.09.2013
Apple: Sicherheitspatch
7.0.2 schließt Lücke im
Lockscreen ...

Update 19.09.2013
Apple: Neue iTunes-Version
11.1 schließt
Sicherheitslücke ...

[» Alle Meldungen anzeigen](#)

[» Neueste Meldungen abonnieren](#)

Aktuelle IT-Sicherheitslage

■ NEG

TeleTrust-Begleitprojekt zum Netzwerk Elektronischer Geschäftsverkehr (NEG)

Noch immer ist das Know-how bei kleinen und mittelständischen Unternehmen (KMU) in puncto Informationssicherheit eher unterdurchschnittlich ausgeprägt.

Konkrete Hilfestellung bot in diesem Zusammenhang 2009 bis 2011 eine Veranstaltungsreihe im Rahmen des Begleitprojektes zum "Netzwerk Elektronischer Geschäftsverkehr" unter Beteiligung von TeleTrust. Unter der Überschrift "Unternehmer lernen von Unternehmern" wurde eine Reihe regionaler "Stammtische" bundesweit etabliert.



Netzwerk Elektronischer
Geschäftsverkehr

Aus dem Feedback der Stammtisch-Teilnehmer wurden Themenstellungen sichtbar, die als Grundlage für Flyer und Checklisten dienen. Damit konnten die Erkenntnisse aus dem Netzwerk transferiert werden. Die Flyer können digital und über die TeleTrust-Geschäftsstelle bezogen werden. Weitere Informationen finden Sie außerdem auf kmu-sicherheit.de.

Download der Checklisten "Aus der Praxis für die Praxis"

[NEG Checkliste Faktor Mensch.pdf](#)

[NEG Checkliste Netzwerke.pdf](#)

[NEG Checkliste Risikoanalyse.pdf](#)

[NEG Checkliste Schutzkonzept.pdf](#)

Download der Flyer "Aus der Praxis für die Praxis"

[NEG Flyer Datensicherung.pdf](#)

[NEG Flyer E-Mail-Sicherheit.pdf](#)

[NEG Flyer Netzwerkverwaltung.pdf](#)



Risiken

Checkliste: Wie gehe ich mit IT-Risiken um?

Der richtige Umgang mit IT-Risiken ist für Unternehmen eine Überlebensfrage. Um so wichtiger ist eine Risikoanalyse, mit der Sie die Risiken erkennen, den Schutzbedarf ermitteln und so möglichen Schäden vorbeugen können. Auch rechtliche Auflagen gilt es zu erfüllen und Haftungstragen zu klären. Die Checkliste hilft Ihnen dabei.

Risiken erkennen

- Kennen Sie die rechtlichen Anforderungen im Zusammenhang mit Ihrer IT? Z.B.
 - Anforderungen des Datenschutzes (z.B. auch Bestellung eines Datenschutzbeauftragten)
 - Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
 - Branchenspezifische Regelungen (z.B. im sozialen Bereich)
 - Vertragliche Regelungen (z.B. Vertraulichkeitsvereinbarungen, IT-Outsourcing)
- Haben Sie Rat von Dritten eingeholt (Expertise, Sicht eines Betriebsfremden)?
- Haben Sie für Ihre wichtigen IT-Anwendungen identifiziert,
 - welche IT-Systeme dafür notwendig sind?
 - welche Daten in diesen Anwendungen verarbeitet werden?
 - wo und wie die Hardware für diese Systeme aufgestellt ist?

Risiken bewerten

- Haben Sie überprüft, was für Schäden eintreten können?
 - Schäden, die durch Nichtverfügbarkeit von Daten und Systemen entstehen (z.B. wenn Daten „verschwinden“ sind, die Kommunikation wie z.B. E-Mail nicht funktioniert)
 - Schäden, die durch fehlerhafte (manipulierte) Daten entstehen können (z.B. durch frustrierte Mitarbeiter oder durch Schadsoftware)
 - Schäden, die durch Verletzung von Betriebsgeheimnissen entstehen können (z.B. Entwürfe, Angebote oder Prozessbeschreibungen)

Unternehmen
risiken erken
Auch rech
tlich Ihnen

erungen in
hutzen (z.B.

ansparenz
ingen (z.B.
.B. Vertrau
lt (Expert
wendung
tzwendig si
wendungen
ür diese Sy

den eintre
rfügbarkeit
unden“ sin

aft (manip
rbeiter ode
ung von Be
der Prozes

- Haben Sie sich einen Überblick über mögliche Schadenshöhen verschafft?
 - Schadenshöhen bei Ausfall der Hardware oder Software
 - Schadenshöhen bei Datenverlust
 - Schadenshöhen durch „Datenlebstahl“ (z.B. unbefugte Einsichtnahme, Kopieren)
- Haben Sie Schadenskategorien festgelegt, wie etwa „Schaden darf nicht eintreten“, „hoher Schaden“, „niedriger Schaden“ oder auch nach „Schulnoten“?
- Haben Sie eine Liste der potenziellen Schäden erstellt und diese den Kategorien zugeordnet?
- Haben Sie für jeden dieser möglichen Schäden eine Eintrittswahrscheinlichkeit festgelegt?
- Haben Sie die Schwachstellen Ihrer IT identifiziert?
- Haben Sie geprüft, ob Ihre vorhandenen Schutzmaßnahmen ausreichen?

Sicherheitsmaßnahmen

- Haben Sie sich über notwendige Sicherheitsmaßnahmen informiert und auch z.B. „best practices“ berücksichtigt?
- Haben Sie geprüft, ob eine Änderung der Arbeitsabläufe das Risiko minimieren kann?
- Haben Sie geprüft, ob Sie Versicherungen gegen etwaige Risiken abschließen können?
- Haben Sie geprüft, ob Sie risikobehaftete Prozesse an externe Dienstleister auslagern können?

Weitere Informationen zum Thema IT-Risikoanalyse finden Sie in unserem Flyer:
„IT-Risiken erkennen und vermeiden - 10 Prodstipps für kleine und mittlere Unternehmen und das Handwerk“



Checkliste: Faktor Mensch

Technische Lösungen wie etwa Firewalls oder Virensensoren reichen alleine nicht aus, um Unternehmen vor den Gefahren aus dem Internet, vor Datenverlust und unbefugtem Zugriff zu schützen. Wenn Mitarbeiter sorglos und nachlässig mit Daten, Programmen und Rechnern umgehen, helfen auch die besten technischen Schutzmaßnahmen nichts. Erforderlich ist ein grundlegendes Verständnis für die Bedeutung von IT-Sicherheit. Informieren Sie Ihre Mitarbeiter über mögliche Gefahrenquellen, damit sie lernen, sich richtig zu verhalten. Die Checkliste kann Ihnen dabei helfen.

Vorbereitung

Bevor Sie Ihre Mitarbeiter über mögliche Gefahrenquellen und den richtigen Umgang mit Daten informieren, sollten Sie sich in einem ersten Schritt selbst einen Überblick verschaffen, wo Risiken für Ihre IT stecken, und Richtlinien für ein „sicheres“ Verhalten der Mitarbeiter formulieren. Diese Richtlinien sind Anweisungen, die beschreiben, wie ein Mitarbeiter sich im Umgang mit der IT im Unternehmen verhalten soll. Halten Sie diese sehr knapp (manchmal genügt ein Satz) und verzichten Sie auf Fachkaudenwelsch.

- Haben Sie Ihre schutzbedürftigen Daten identifiziert, z.B. Personaldaten (Verpflichtung aus Datenschutzvorschriften), Kundendaten, kaufmännische Daten (z.B. Angebote, Rechnungen, Einkaufsdaten) und technologische Daten (z.B. Konstruktionsdaten, Fertigungsdaten)?
- Haben Sie festgelegt, wer auf welche Daten Zugriff hat und haben muss bzw. soll (Lbte)?
- Haben Sie festgelegt, wer für welche Anwendungen autorisiert sein muss bzw. soll (Lbte)?
- Haben Sie (einfache) Benutzerrichtlinien erstellt?
 - Passwortrichtlinie (regelt z.B. Art, Erzeugung, Geheimhaltung und Erneuerung von Passwörtern)
 - Internetrichtlinie (regelt z.B. ob und wie das Internet genutzt wird, Browser-Einstellungen, Hoch- und Herunterladen von Daten und Software)
 - E-Mail-Richtlinie (regelt z.B. den Umgang mit bekannten und unbekannten Absendern, mit Anhängen und den Einsatz von Signaturen und Verschlüsselung)
 - Datenträgerrichtlinie (regelt z.B. den Einsatz, Art, Aufbewahrung, Verschlüsselung, Weitergabe und Löschung bzw. Vernichtung von Datenträgern)
 - Installationsrichtlinie für Hard- und Software (regelt, ob und wie Hardware und Software installiert werden)

der Viren Internet, v d nachlässi zhen Schut ung von IT : sie lerner

Befahrenq m ersten S nien für ei ungen, die ilten soll. i chkauderv Daten ideo schriften), aufsdanten en)?

che Daten

he Anwen

tlinien erst .B. Art, Er

3. ob und v erunterlad . den Umg ind den Eir t z.B. den ung bzw. ' ard- und Sc)

- Zutrittsrichtlinie (regelt den Zutritt zu Betriebsgelände und Räumen für Personal und Betriebsfremde)
- Arbeitsplatzrichtlinie (regelt z.B. die Sperrung des PCs, den Verbleib von Unterlagen auf dem Schreibtisch auch bei kurzer Abwesenheit)
- Richtlinie für mobile Geräte (regelt z.B. die Nutzung, Aufsicht und Aufbewahrung, Anbindung an das Unternehmensnetz, Verschlüsselung und Wartung bzw. Updates mobiler Geräte)
- Richtlinie für externe Zugriffe (regeln z.B. den Zugriff auf das Firmennetzwerk von zu Hause oder unterwegs)
- Weitere
 - Haben Sie konkrete Verantwortlichkeiten für die Umsetzung der Richtlinien vergeben?

Kommunikation - Mitarbeiter richtig ansprechen

Am besten lernt der, der es aus eigenem Interesse und mit Freude tut. Gefragt sind daher praktische, anschauliche Beispiele, die die Risiken im Unternehmen aufzeigen und Lösungen anbieten. Motivieren Sie Ihre Mitarbeiter, indem Sie sie aktiv beteiligen, einbinden und Verantwortlichkeiten vergeben.

- Leben Sie als Chef das Thema IT-Sicherheit selber vor?
- Wissen Sie, wieviel Ihre Mitarbeiter über IT-Sicherheit wissen?
- Können Sie den Sinn der Richtlinien plausibel erläutern?
- Haben Sie Ansprechpartner benannt, die Rückfragen von Mitarbeitern beantworten können?
- Haben Sie Maßnahmen geplant oder getroffen, um die Richtlinien in Erinnerung zu rufen?
 - z.B. Plakate, wohl dosierte Erinnerungsmails, Kontrollen
- Haben Sie Maßnahmen geplant oder getroffen, um das IT-Sicherheitsbewusstsein zu vertiefen?
 - z.B. Schulungen, Hinweis auf Publikationen, Lernspiele

Weitere Informationen zum Thema Mitarbeitersensibilisierung finden Sie in unserem Flyer:

„IT-Sicherheit, Faktor Mensch - 10 Proxistips für kleine und mittlere Unternehmen und das Handwerk“

Datensicherung

Datensicherung hilft Unternehmen sichern

Daten, wie etwa Kunden- oder Lieferantendaten, zählen heute zu den wichtigsten Gütern im Unternehmen. Sie ausreichend zu schützen ist für Unternehmen eine Überlebensfrage.

Wertvolle Daten schützen

Nicht nur Viren, Würmer und andere Schadsoftware können unternehmenskritische Daten vernichten. Mindestens genauso hoch ist das Risiko des Datenverlustes durch Ausfälle von Hard- und Software oder durch Fehlbedienung wie etwa versehentliches Löschen. Wenn beispielsweise ein so genannter Festplatten-Crash die Daten zu Kunden, Aufträgen, Buchhaltung und Personal vernichtet, stehen kleine Unternehmen praktisch vor dem Aus.

Daten sind wichtige Unternehmenswerte

Das versehentliche Löschen eines elektronischen Dokuments kann die Arbeit von Tagen oder Wochen zunichte machen. Datenverluste können schnell entstehen: Wenn Sie versehentlich Ihre zentrale Adressdatenbank löschen. Oder ein Virus vernichtet alle Text-Dokumente.



Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr in 28 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk ist das einzige bundesweite Angebot seiner Art und verzeichnet jährlich rund 30.000 Besucher in Beratungen und Veranstaltungen. Es stellt Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.



Praxistipps

Aus der Praxis für die Praxis

Wie sichere ich meine Daten?

10 Praxistipps für kleine und mittlere Unternehmen und das Handwerk

Gefördert durch:



aufgrund eines Beschlusses des Deutschen Bundestages



TeleTrust

TeleTrust Deutschland e.V. ist Partner des Begleitprojektes „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerkes Elektronischer Geschäftsverkehr und veranstaltet bundesweit „Stammtische“ rund um das Thema Informationssicherheit.

TeleTrust ist mit mehr als 100 Mitgliedern aus Wirtschaft, Wissenschaft und Verwaltung ein führendes Kompetenznetzwerk in Fragen der IT-Sicherheit in Deutschland und Europa.



Impressum

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr in 29 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business-Lösungen.

Herausgeber:

TeleTrust Deutschland e.V., Chausseestraße 17, D-10115 Berlin

Konzeption und Redaktion:

Harald Kesberg Consulting, Hans-Joachim Bierschenk, Harald Kesberg

Grafik und Gestaltung:

Harald Kesberg Consulting, Karl-Heinz Kottenhahn

Druck:

Buersche Druckerei Neufang KG

Bildnachweis:

bildbox - Fotolia.com, ECC Handel, Stachelbaerle/Pixelio

Stand: 08/2010



Datensicherung

10 Tipps, die wirklich helfen

Was können Sie tun, um Ihre Unternehmensdaten zu schützen?

10 grundlegende Praxistipps helfen Ihnen, Ihre Unternehmensdaten zu sichern.

Die Tipps stammen alle aus der betrieblichen Praxis kleiner und mittlerer Unternehmen und dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet. Weiterführende Informationen und Tipps rund um das Thema Datensicherung und Datensicherheit finden Sie unter www.ec-net.de.

Bedienungsfehler können zu schwerwiegenden Datenverlusten führen – regelmäßige Datensicherung beugt vor.

Was sollten Sie sichern?

Sie sollten auf jeden Fall die Daten sichern, die Sie selbst erzeugt haben. Dazu zählen die Daten, die Sie durch Anwendungsprogramme (z.B. Textverarbeitung, Tabellenkalkulation, Präsentation, E-Mail, Rechnungswesen, Konstruktion, Lager und Finanzen) erstellt haben oder die Sie im Rahmen Ihrer Geschäftsbeziehungen mit Ihren Kunden (z.B. Artikeldaten, Preisangaben, Informationen zu den Angeboten und zum Auftrag) erhalten haben.

- Tipp 1:** Organisieren Sie die zu sichernden Daten auf Ihren Rechnern in möglichst wenigen Ordnern. Sichern Sie diese Ordner komplett und definieren Sie die Zugriffsrechte.

Wann sollten Sie sichern?

Wie oft Sie Ihre Daten sichern, hängt davon ab, welche Risiken Sie in „Kauf nehmen“ wollen. Wir empfehlen eine tägliche Sicherung.

- Tipp 2:** Bestimmen Sie in Ihrem Unternehmen einen Verantwortlichen für die Datensicherung. Wenn Sie nicht täglich sichern wollen, sondern z.B. wöchentlich, legen Sie am besten einen bestimmten Zeitpunkt für die Datensicherung fest, z.B. „jeden Freitag 16.00 Uhr“.

Wie sollten Sie sichern?

Da eine manuelle Sicherung schon mal fehleranfällig ist, sollte der Sicherungsvorgang idealerweise automatisiert werden. Für die Datensicherung gibt es professionelle Backup-Software, die teils auch als Freeware zur Verfügung steht.

- Tipp 3:** Meistens genügen die vom Betriebssystem bereitgestellten Backup-Routinen den Anforderungen in den meisten KMU und Handwerksbetrieben.



Wohin sollten Sie Ihre Daten sichern?

Grundsätzlich sind alle Medien geeignet, auf die sich Daten speichern lassen (z.B. CD/DVDs, Speicherbänder, externe Festplatten, USB-Sticks). Da Datenträger nur eine begrenzte Haltbarkeit haben, sollten Sie darauf achten, diese regelmäßig vor Ablauf der zugesicherten Haltbarkeit auszutauschen. Bei täglicher Sicherung empfehlen wir zudem, mehrere Medien (z.B. ein Speicherband für jeden Tag der Woche) zu verwenden.

- Tipp 4:** Da Datenträger nur eine begrenzte Haltbarkeit haben, sollten Sie darauf achten, ein Medium zu verwenden, auf das die komplette Datensicherung passt.
- Tipp 5:** Die Datensicherung kann auch über verschiedene Anbieter im Internet online durchgeführt werden. Lassen Sie sich hierbei ausführlich von Experten beraten.

Wo sollten Sie die Sicherungs-Medien aufbewahren?

Je nach Vertraulichkeit (z.B. personenbezogene Daten) und Wichtigkeit (z.B. für Betriebsprüfungen, PPS-Programme) der Daten sollten Sie die Medien in einem verschließbaren Schrank oder im Safe aufbewahren. Zum Schutz vor Feuer oder Wasserschäden sollte der Safe eine entsprechende Schutzklasse aufweisen.

- Tipp 6:** Bewahren Sie zusätzlich eine Sicherheitskopie (z.B. die vorletzte) an einem anderen sicheren Ort auf (z.B. zu Hause, Bankschließfach).

Worauf sollten Sie besonders achten?

Bei automatisierter Sicherung sollten Sie prüfen, ob die Datensicherung auch tatsächlich erfolgt ist und ob sie vollständig war. Ihre IT-Infrastruktur kann sich im Lauf der Zeit verändern (neue Software, neue Hardware), daher sollte das Prozedere für die Datensicherung entsprechend angepasst werden.

- Tipp 7:** Sicherungsprogramme erstellen in der Regel ein Protokoll, aus dem Sie ersehen können, wann und was gesichert wurde.
- Tipp 8:** Prüfen Sie gelegentlich, ob sich Ihre Daten auch zurücksichern lassen.
- Tipp 9:** Prüfen Sie bei Neuanschaffungen, ob die Datensicherung angepasst werden muss.

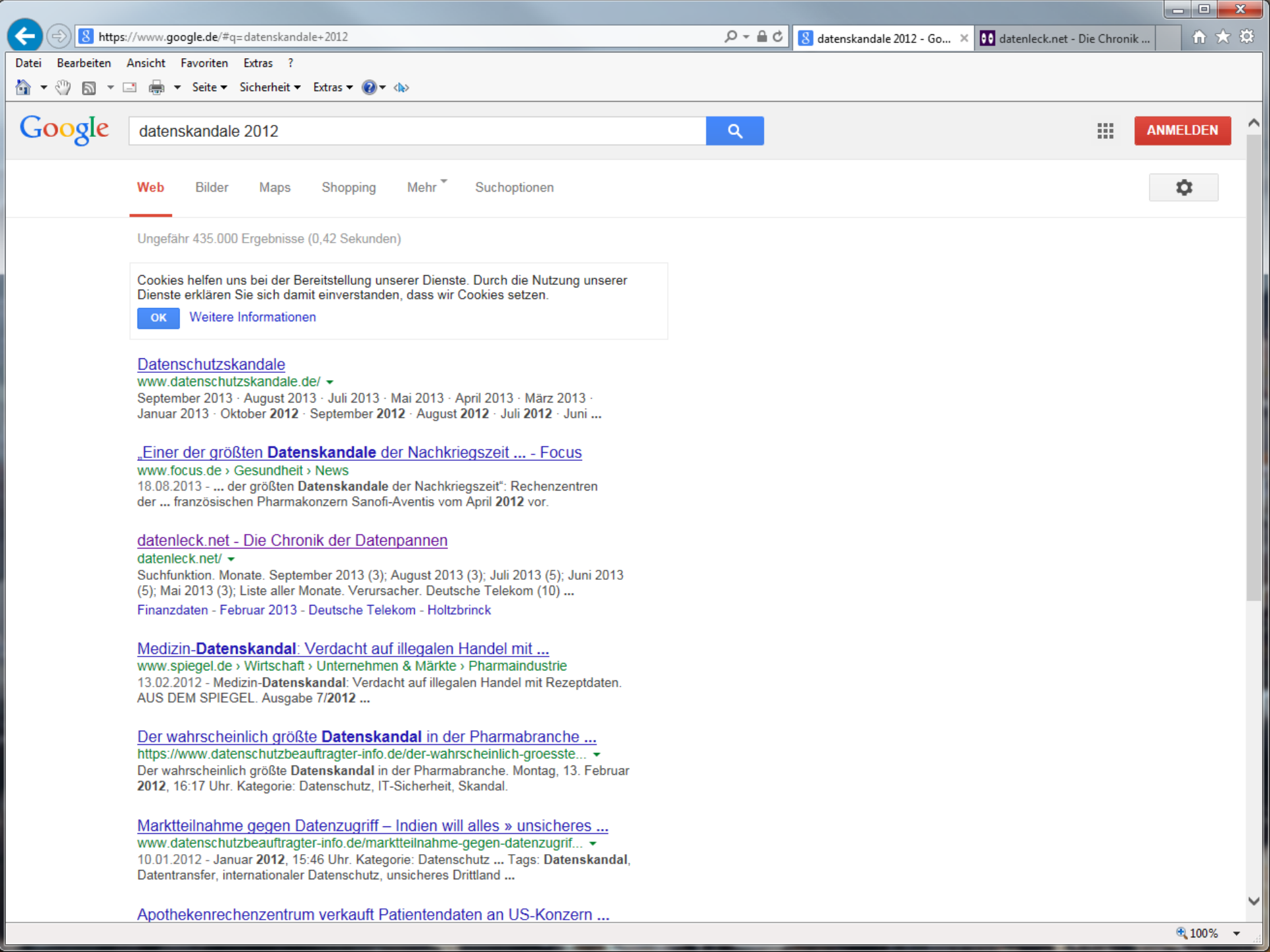
Was ist keine Datensicherung?

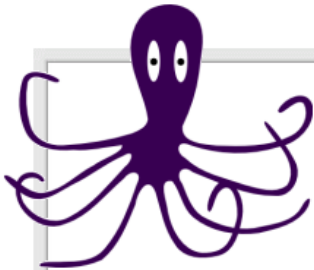
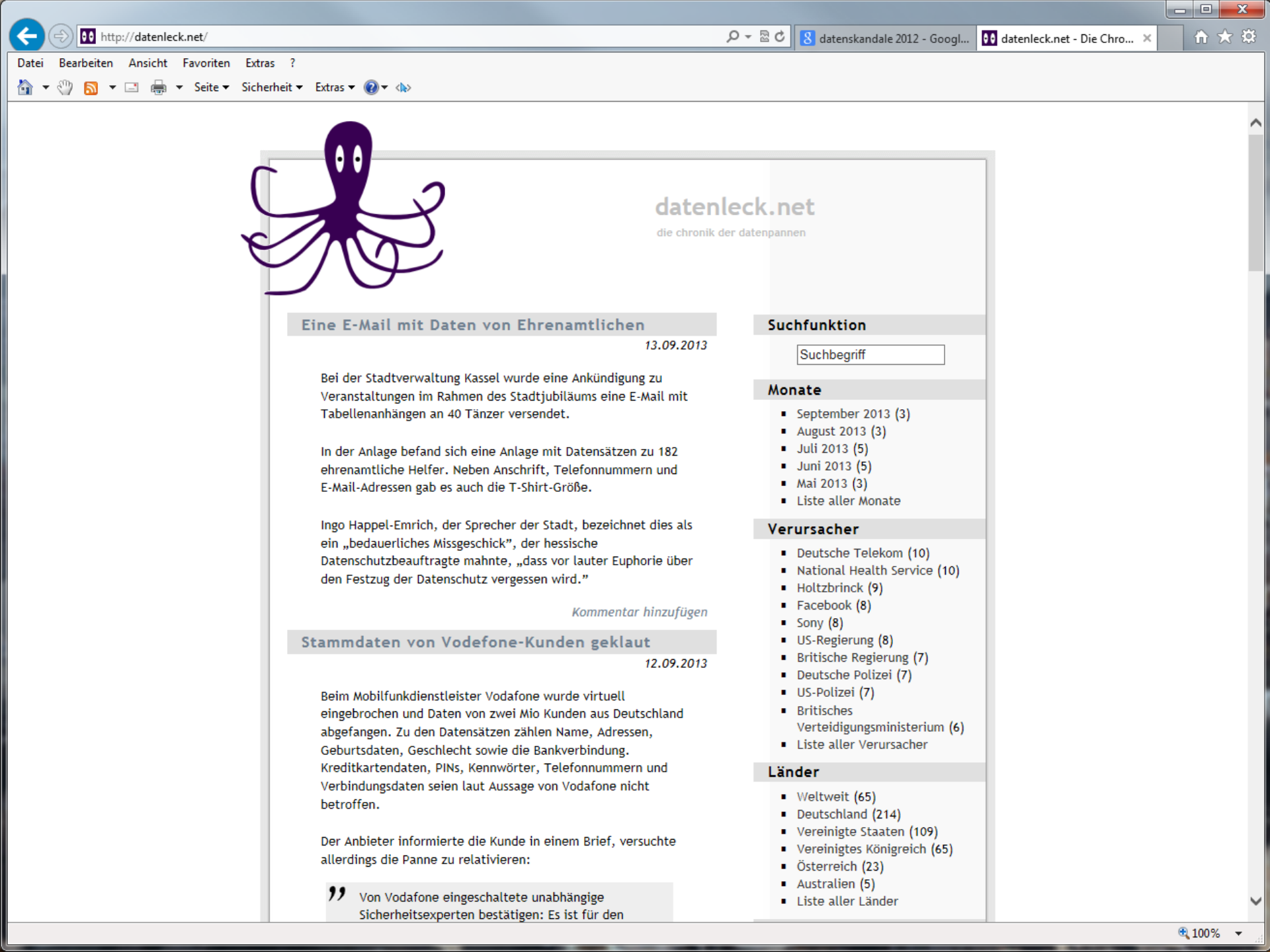
Die Daten sind nicht ausreichend gesichert, wenn Sie sie einfach nur auf dieselbe Festplatte in ein anderes Verzeichnis kopieren oder auf eine andere interne Platte. Ebenso wenig reicht das Speichern von Daten auf einem Server oder der Einsatz von gespiegelten Platten (z.B. RAID).

- Tipp 10:** Das Medium, auf das die Daten gesichert werden, sollte physikalisch von der IT-Infrastruktur abgekoppelt werden (z.B. Speicherband herausnehmen, USB-Stick abziehen, CD aus dem Laufwerk nehmen, Verbindung zur externen Festplatte trennen).

Skandale

... was man so findet ...





datenleck.net

die chronik der datenpannen

Eine E-Mail mit Daten von Ehrenamtlichen

13.09.2013

Bei der Stadtverwaltung Kassel wurde eine Ankündigung zu Veranstaltungen im Rahmen des Stadtjubiläums eine E-Mail mit Tabellenanhängen an 40 Tänzer versendet.

In der Anlage befand sich eine Anlage mit Datensätzen zu 182 ehrenamtliche Helfer. Neben Anschrift, Telefonnummern und E-Mail-Adressen gab es auch die T-Shirt-Größe.

Ingo Happel-Emrich, der Sprecher der Stadt, bezeichnet dies als ein „bedauerliches Missgeschick“, der hessische Datenschutzbeauftragte mahnte, „dass vor lauter Euphorie über den Festzug der Datenschutz vergessen wird.“

[Kommentar hinzufügen](#)

Stammdaten von Vodafone-Kunden geklaut

12.09.2013

Beim Mobilfunkdienstleister Vodafone wurde virtuell eingebrochen und Daten von zwei Mio Kunden aus Deutschland abgefangen. Zu den Datensätzen zählen Name, Adressen, Geburtsdaten, Geschlecht sowie die Bankverbindung. Kreditkartendaten, PINs, Kennwörter, Telefonnummern und Verbindungsdaten seien laut Aussage von Vodafone nicht betroffen.

Der Anbieter informierte die Kunde in einem Brief, versuchte allerdings die Panne zu relativieren:

” Von Vodafone eingeschaltete unabhängige Sicherheitsexperten bestätigen: Es ist für den

Suchfunktion

Monate

- September 2013 (3)
- August 2013 (3)
- Juli 2013 (5)
- Juni 2013 (5)
- Mai 2013 (3)
- Liste aller Monate

Verursacher

- Deutsche Telekom (10)
- National Health Service (10)
- Holtzbrinck (9)
- Facebook (8)
- Sony (8)
- US-Regierung (8)
- Britische Regierung (7)
- Deutsche Polizei (7)
- US-Polizei (7)
- Britisches Verteidigungsministerium (6)
- Liste aller Verursacher

Länder

- Weltweit (65)
- Deutschland (214)
- Vereinigte Staaten (109)
- Vereinigtes Königreich (65)
- Österreich (23)
- Australien (5)
- Liste aller Länder

6 Beispiele für Datenschutzskandale

Ob Vodafone jetzt auch Anzeigenseiten kaufen muss ... Vodafone sind Kundendaten gestohlen worden	Datenpanne
Was lernt man nun aus der NSA-Affäre?	Datenschlüsselerei
Man soll nicht mit den Fingern essen, aber bezahlen	Fingerabdrücke
Zufällig in der Nähe eines Tatortes, SMS an die Freundin geschrieben und schwupps ist man in der Polizeiortung	Funkzellen-Abfrage
Wer braucht schon Detektive, wenn man Mülleimer hat?	Datensammelnde Mülleimer

Skandale

Stichwort „Datenschutzskandale“:
Eine unschöne Sammlung

- Archive
(von März 2008 – September 2013)
- Categories
(von Erpressung (1) bis
Kundendatenschutz (56))

Zertifizierung / Normreihe

Die internationale Norm ISO/ IEC 27001 ...
spezifiziert die Anforderungen für Herstellung,
Einführung, Betrieb, Überwachung, Wartung und
Verbesserung eines dokumentierten
Informationssicherheits-Managementsystems
unter Berücksichtigung der IT-Risiken innerhalb
der gesamten Organisation.

(Aus Wikipedia



)

Zertifizierung / Normreihe: Anwendung

Anwendungsbeispiele der ISO/ IEC 27001:

- Formulierung von Anforderungen und Zielsetzungen zur Informationssicherheit
- Kosteneffizientes Management von Sicherheitsrisiken
- Sicherstellung der Konformität mit Gesetzen und Regulatorien
- Prozessrahmen für die Implementierung und das Management etc.

Viele gute Gründe für den

Informationstag IT-Sicherheit in der Marktforschung

Was dürfen Sie erwarten?

Anregungen

Erkenntnisse

Gespräche

Kontakte