

Datenschutz und Sicherheit in der IT

Aktuelle Praxistipps und Informationen



Liebe Leserin, lieber Leser,

reich werden wollen wohl alle Diebe, auch die Datendiebe. Inzwischen werden Regierungen bereits gestohlene Bankdaten angeboten, und eine Krankenkasse wurde mit illegal kopierten Patientendaten erpresst. Doch Datendiebstahl bringt keinen Geldregen, sondern ist strafbar. Lesen Sie in dieser Ausgabe, womit die Datendiebe, die auf Millionen hoffen, wirklich rechnen können.

Auch soziale Online-Netzwerke wie XING & Co. klingen erst einmal vielversprechend. Neue Kontakte, wiedergefundene alte Freunde und eine Gruppe von Gleichgesinnten, all das können soziale Netzwerke im Internet ermöglichen. Doch machen sie oft mehr möglich, als den Teilnehmern lieb sein dürfte: Identitätsdiebstahl und die Offenlegung vertraulicher Geschäftsbeziehungen. Diese Ausgabe zeigt Ihnen deshalb, wie Sie von XING & Co profitieren, ohne Ihre vertraulichen Daten zu gefährden.

Herzlichst Ihr **Thomas Jundel, Datenschutzbeauftragter**

Streng geheim?

Was Sie schon immer über Marine One, den Hubschrauber des US-Präsidenten Barack Obama, wissen wollten

Fast jede Woche sieht man Marine One, den Hubschrauber des US-Präsidenten, in den Nachrichten. Doch Details über diesen Hubschrauber werden aus Sicherheitsgründen nicht verraten.

Stimmt leider nicht!

Ausführliche Informationen über das Navigationssystem, die Kommunikationseinrichtungen und andere sicherheitskritische Daten waren im Internet für jedermann zu finden.



Marine One: Verzeichnis mit geheimen Bauplänen versehentlich unter Windows "freigegeben"

Möglich wurde dies durch eine Nachlässigkeit in einem amerikanischen Rüstungsunternehmen. Dort wurden Programme eingesetzt, mit denen sich Dateien über das Internet austauschen

lassen. Dazu gibt man in der Theorie gezielt Teilbereiche seiner Festplatte frei. In der Realität aber werden oftmals nicht nur die Dateien freigegeben, die ein anderer über das Internet einsehen darf, sondern gleich die ganze Festplatte.

Wie die Federal Trade Commission (FTC) festgestellt hat, war Marine One leider kein Einzelfall. Bei Stichproben wurden rund hundert Unternehmen entdeckt, die ebenfalls ungewollt weit mehr Daten im Internet preisgeben, als ihnen bewusst ist.

Haben auch Sie vertrauliche Dateien ungewollt freigegeben? Das kann schnell geschehen, wenn Sie Programme zur Datenübermittlung ins Internet einsetzen, einen Ordner auf Ihrer Festplatte über das Netzwerk freigegeben haben oder Drucker über das Netzwerk verwenden. Sind Sie unsicher, ob bei Ihnen alle Freigaben stimmen? Sind alle vertraulichen Dateien verschlüsselt und getrennt von den freigegebenen Verzeichnissen?

Holen Sie sich Rat von Ihrem Datenschutzbeauftragten und dem Systemadministrator, damit Ihre Festplatte nicht zum Lesesaal im Internet wird!

Woher wissen Sie das?

Der Kunde nervt wegen seiner Daten. Was sollen Sie ihm sagen?

Vor allem wenn ein Kunde nicht kriegt, was er will, fallen ihm als letzter Kritikpunkt Fragen ein wie: Woher wissen Sie denn eigentlich schon, dass ich kürzlich umgezogen bin? Oder: Liegt das alles vielleicht nur an den falschen Behauptungen in meiner SCHUFA-Auskunft?

Bevor Sie ihn bloß abwimmeln, bitte Vorsicht:

Ab **1.4.2010** gibt das Bundesdatenschutzgesetz dem Kunden erweiterte Auskunftsrechte über seine Daten! Die vielen Skandale der letzten Jahre haben dazu geführt, dass der Gesetzgeber die Nase voll hatte und die Rechte der Betroffenen deutlich erweitert hat.

Dank einer **gesetzlichen Neuregelung zum 1.4.2010** kann ein Kunde jederzeit Auskunft über die folgenden vier Fragen verlangen:

- Welche Daten sind über mich bei Ihnen vorhanden?
- Woher stammen sie?
- An welche Empfänger werden sie weitergegeben?
- Wozu sind die Daten denn bei Ihnen gespeichert?

Es ist nicht nötig, dass der Kunde diese Fragen schriftlich stellt. Er kann vielmehr auch mündlich Auskunft verlangen. Erhält er keine Auskunft, kann es letztlich sogar bis zu einer Klage gegen das Unternehmen kommen!

Die erste Empfehlung an Sie lautet aber gerade deswegen: Fangen Sie jetzt nicht einfach an, dem Kunden alles Mögliche zu erzählen, womöglich auch noch Dinge,

die Sie bloß zu wissen glauben!

Wenn klar ist, dass der Kunde wirklich auf Auskunft besteht, notieren Sie das zunächst einmal und bitten Sie um Verständnis, dass Sie für so etwas nicht die richtige Adresse sind.

Die zweite Empfehlung lautet: Geben Sie die Nachricht an den zuständigen Vorgesetzten oder die zuständige

Vorgesetzte weiter. Er oder sie werden sich darum kümmern.

Sowohl für Sie als auch für Ihre Vorgesetzten gibt der Datenschutzbeauftragte gerne Hinweise, was dann bei der Auskunft zu beachten ist. Auch dazu, was als Geschäftsgeheimnis zählt und deshalb von der Auskunft ausgenommen ist. Denn bei solchen Auskünften müssen auch die Interessen der Firma bedacht werden!

Wer wird Datenklau-Millionär?

Wenn man den Medien glaubt, ist es ganz einfach: Als Mitarbeiter einer Bank kopiert man ein paar Daten von Kunden, die vielleicht Steuern hinterzogen haben, bietet das auf einer CD den staatlichen Stellen an, und dann geht es nur noch darum, ob man dafür eine, zwei oder sogar mehr Millionen Euro bekommt. Die Realität sieht wie so oft anders aus.

Wer so vorgeht, hat in der Regel den Staatsanwalt am Hals und ist seinen Job los. Das gilt sogar dann, wenn er wirklich Übeltäter erwischt haben sollte. Und das ist oft genug gar nicht der Fall. So gibt es beispielsweise mehrere hunderttausend Deutsche, die zwar ein Konto in der Schweiz haben, von ihrer dortigen Bank aber Kontrollmitteilungen über die Zinsen an den deutsche Fiskus schicken lassen, damit erst gar kein falscher Verdacht entsteht.

Aber einmal unterstellt, man ist sich sicher, dass bestimmte Kunden keine saubere Weste haben. Gegen welche Strafvorschriften verstößt man, wenn man solche Daten kopiert? Die häufigste Antwort lautet: Das ist dann Datendiebstahl!

Die Daten selbst können nicht gestohlen werden

So einfach ist es allerdings nicht. Gestohlen werden können lediglich bewegliche Sachen. So heißt es in der entsprechenden Vorschrift des § 242 Strafgesetzbuch (StGB), die den Diebstahl unter Strafe stellt. Und eine bewegliche Sache ist nur etwas, das man anfassen kann, oder, wie es Juristen ausdrücken, ein "körperlicher Gegenstand".

Daten selbst kann man nicht anfassen, höchstens die CD, auf denen sich die Daten befinden. Und diese CD bringt ein kluger Täter selbst mit, statt sie zu klauen, denn sonst fällt am Ende noch auf, dass eine CD fehlt. Ergebnis: Datendiebstahl wörtlich genommen gibt es nicht!

Das Ausspähen von Daten erfasst besonders geschützte Daten

Das, was der Volksmund Datendiebstahl

nennt, ist häufig als Ausspähen von Daten anzusehen. Dazu heißt es in § 202a StGB: "Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten

besonders gegen den Zugriff gesichert, weil für den Zugriff ein fremdes Passwort nötig war. Dass K durch den Klebezettel diese Sicherung letztlich aufgehoben hat, ändert daran nichts, denn das hatte der Arbeitgeber nicht erlaubt.

Vorsicht mit Passwörtern!

Angenommen, ein Täter kann Kundendaten kopieren, weil Sie Ihr Passwort unter der Tastatur kleben hatten. Fällt Ihnen sofort eine gute Erklärung dafür ein, dass Sie mit dem Täter nicht unter einer Decke stecken? Nein?

Dann sollten Sie den Zettel gleich jetzt sicher entsorgen!

Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft."

Wesentlich sind dabei zwei Punkte, die beide erfüllt sein müssen:

- Die Daten dürfen nicht für den Täter bestimmt sein.
- Sie müssen besonders gegen unberechtigten Zugang gesichert sein.

Dazu ein Beispiel: Der klauende Mitarbeiter M kopiert Daten, auf die eigentlich nur sein Kollege K zugreifen dürfte, weil nur der für diese Kunden zuständig ist. Dabei verwendet A das Passwort von K, das der auf einem gelben Zettel unter seiner Tastatur kleben hat.

Hier sind alle Voraussetzungen für ein strafbares Ausspähen erfüllt: Die Daten waren nicht für M bestimmt, und sie waren

Eigene Daten kann man nicht ausspähen

Anders sieht es natürlich aus, wenn ein Mitarbeiter Daten klaut, auf die er mit dem Willen seines Arbeitgebers zugreifen darf. Auch dazu ein Beispiel:

Der klauende Mitarbeiter kopiert Daten der Kunden, die er zu betreuen hat. Die Merkmale eines strafbaren Ausspähens sind nicht erfüllt! Erstens waren die Daten für den Mitarbeiter bestimmt, und zweitens musste er keine Zugangssicherung überwinden, denn er sollte ja Zugang zu den Daten haben. Dass er sie für einen anderen Zweck missbraucht hat, ist zwar verwerflich, aber nach dieser Vorschrift nicht strafbar.

Das UWG bestraft den Verrat von Kundendaten

Da sieht man es, wird mancher Leser und manche Leserin sagen: Also kommt so einer doch straffrei davon! Das stimmt jedoch nicht. Denn eine wenig bekannte Vorschrift im Gesetz gegen unlauteren Wettbewerb (UWG) stellt gerade solche Verhaltensweisen unter Strafe. In § 17 Absatz 1 UWG heißt es:

"Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des

Geltungsdauer des Dienstverhältnisses unbefugt an jemand in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft".

Das gilt auch beim Verrat gegenüber Behörden

Kundendaten sind in aller Regel als Geschäftsgeheimnisse anzusehen. Und wer solche Daten an Steuerbehörden weitergibt, wird im Normalfall dem eigenen Unternehmen schaden wollen wozu tut er es denn sonst? Wichtig dabei: Obwohl die

Vorschrift im UWG steht, sind auch Fälle erfasst, in denen Kundendaten nicht an die Konkurrenz, sondern an staatliche Stellen verraten werden!

Die fristlose Kündigung droht außerdem

In allen Fällen, die oben dargestellt sind, reicht das Verhalten des Täters für eine fristlose Kündigung durch den Arbeitgeber aus. Denn wenn ein Mitarbeiter Kundendaten hinter dem Rücken des Arbeitgebers außer Haus schafft, um Strafverfahren einzuleiten, ist das Vertrauensverhältnis zwischen beiden ruiniert.

Soziale Netzwerke: Profitieren statt Kontrolle verlieren!

Soziale Netzwerke im Internet liegen voll im Trend, privat wie beruflich. Leider sind nicht nur mögliche Geschäftspartner und alte Freunde an Ihren Daten interessiert. Auch Wettbewerber, Industriespione und Datendiebe werfen bei XING, Facebook & Co. ihre Netze aus.

Bekanntschaften wollen gepflegt werden

Gehören auch Sie zu den mehr als 26 Millionen aktiven Nutzern sozialer Netzwerke in Deutschland? Dann haben Sie wahrscheinlich ein Profil bei Facebook, MySpace oder wer-kennt-wen.de. Solche Netzwerke sind aber nicht nur privat interessant, um alte Schulbekanntschaften aufzufrischen, neue Freunde nach einem Umzug zu finden oder Gleichgesinnten seine Meinung über den neuesten Kinofilm mitzuteilen.

Auch für den Beruf lassen sich soziale Netzwerke wie XING oder LinkedIn vorteilhaft einsetzen. So können Sie dort Ihre beruflichen Qualitäten präsentieren und sich für weitere Projekte oder neue Kunden empfehlen. Das hilft auch dem Unternehmen, für das Sie tätig sind.

Doch Vorsicht ist angesagt

Allerdings: Soziale Netzwerke wie XING, Facebook & Co sind auch eine wahre Fundgrube für Datendiebe und Industriespione. Mithilfe von Suchmaschinen und wenigen Klicks lassen sich die persönlichen Daten zahlloser Teilnehmer einsammeln. Teilweise werden richtige digitale Erntemaschinen auf soziale Netzwerke angesetzt, die die dort veröffentlichten Daten in den Teilnehmerprofilen einsammeln und auswerten. Reiche Datenbeute ist ihnen sicher.

Betriebsgeheimnisse in Gefahr!

Viele Teilnehmer an sozialen Netzwerken melden, wo sie wann was mit wem geplant haben. Das sind nicht nur Theater- oder Messebesuche, die da dem ganzen Internet angekündigt werden, sondern auch Statusmeldungen zu Unternehmensprojekten, die bislang kein Außenstehender kannte.

So wurde kürzlich der Fall eines Softwareentwicklers bekannt, der in einem sozialen Netzwerk ein wichtiges Sicherheitsdetail des noch unveröffentlichten Betriebssystems Windows 8 nannte. Wo früher ein Einbruch in die Entwicklungsabteilung notwendig war, reicht heute mitunter der Besuch eines sozialen Netzwerks. Denken Sie daran: Schon das Wissen über den Stand eines Projekts kann für die Konkurrenz bares Geld wert sein!

Identitäten werden gestohlen

Tatsächlich verraten viele Teilnehmer von sozialen Netzwerken nicht nur ungewollt vertrauliche Firmendaten, sondern veröffentlichen auch sehr private Informationen. Persönliche Details in sozialen Netzwerken laden geradezu dazu ein, die Daten und damit letztlich die Identität zu stehlen!

10 goldene Regeln für Soziale Netzwerke:

1. Überlegen Sie sich, was Sie mit der Teilnahme an dem sozialen Netzwerk erreichen wollen, und bestimmen Sie auf dieser Grundlage, was Sie in Ihrem Profil veröffentlichen und was nicht.
2. Denken Sie bei jeder Information in Ihrem Online-Profil daran, dass Einträge in sozialen Netzwerken kaum oder gar nicht mehr im Internet zu löschen sind.
3. Geben Sie keine Informationen über sich oder das Unternehmen weiter, die nicht auch am Schwarzen Brett oder in einer Pressemeldung stehen könnten.
4. Trennen Sie Ihr privates und Ihr berufliches Online-Profil und achten Sie auf die Unternehmensrichtlinie für die betriebliche Nutzung sozialer Netzwerke.
5. Akzeptieren Sie nicht jede Kontaktanfrage und reduzieren Sie die Datenfreigaben auch für Ihre Kontakte auf ein Minimum.
6. Verwenden Sie für jedes soziale Netzwerk ein eigenes und sicheres Passwort und speichern Sie dieses nicht.
7. Prüfen Sie die Datenschutzbestimmungen und die Standard-Datenschutzinstellungen des sozialen Netzwerks, bevor Sie dort Ihr Profil speichern.
8. Prüfen Sie Links und Dateien aus den sozialen Netzwerken auf Schadsoftware.
9. Geben Sie Ihre Zugangsdaten für Ihr Online-Profil immer nur auf der Startseite des sozialen Netzwerks ein, nicht aber in Webseiten, die Sie als Link per E-Mail geschickt bekommen.
10. Seien Sie kritisch gegenüber Zusatzprogrammen, die Ihr Online-Profil aus dem sozialen Netzwerk übernehmen wollen.

Nutzen Sie soziale Netzwerke, aber lassen Sie sich nicht ausnutzen

Viele Unternehmen erlauben inzwischen die betriebliche Nutzung sozialer Netzwerke, da sie Vorteile für Kundenberatung und Vertrieb sehen. Dennoch sollten Sie soziale Netzwerke nicht nur als Kontaktpflege, sondern auch als reale Bedrohung begreifen. Laut einer Studie des Sicherheitsunternehmens Sophos haben bereits 36 Prozent der Teilnehmer in sozialen Netzwerken Schadsoftware erhalten, 57 Prozent haben vermehrt Spam-Mails erhalten, da sie ihre E-Mail-Adresse veröffentlicht hatten.

Damit nicht auch Sie zu den Opfern gehören, sollten Sie die 10 goldenen Regeln für soziale Netzwerke beherzigen!

Schöne Grüße von falschen Freunden!

Sie nennen keine Betriebsinterna in Ihrem Online-Profil, und Ihre Tätigkeit erscheint Ihnen nicht so sicherheitsrelevant wie die des IT-Administrators?

Wenn Sie nun glauben, Ihnen drohe keine Gefahr durch soziale Netzwerke, irren Sie sich leider.

Jeder Teilnehmer eines solchen Netzwerks ist bedroht. Wenn Sie in Ihrem Online-Profil Ihre Kontakte und Ihre E-Mail-Adresse anzeigen lassen, kann es schnell passieren, dass Sie neue Urlaubsbilder eines Bekannten per Mail bekommen.

Nur kommt die E-Mail nicht von der genannten Person, und die Fotos enthalten Schadsoftware, die sich im Firmennetzwerk ausbreiten kann.

Alle Zutaten für diesen Angriff per E-Mail geben Sie selbst in Ihrem Online-Profil!

Machen Sie bei XING das richtige Kreuz!

Mehr als acht Millionen Teilnehmer zählt das Business-Netzwerk XING bereits.

Wenn auch Sie XING zur Kontaktpflege und Präsentation Ihrer beruflichen Tätigkeiten nutzen, sollten Sie prüfen, ob Sie mit den Standard-Einstellungen zum Schutz Ihrer Daten einverstanden sind oder nicht.

Änderungen sind bei www.xing.com nach der Anmeldung unter dem Menüpunkt "Start - Einstellungen - Meine Privatsphäre" möglich.

Impressum:

mc-Technik
Thomas Jundel
Marienthaler Str. 24
24340 Eckernförde

Telefon: 04351-7321-0
E-Mail: datenschutz@mc-Technik.de

www.datenschutz.mc-technik.de

Machen Sie jetzt den Selbsttest!

Wissen Sie, was Google durch XING so alles über Sie weiß?

Suchmaschinen werten auch Online-Profile in sozialen Netzwerken wie XING aus, wenn man sie nicht daran hindert. Findet Google auch Ihr XING-Profil?

1. Öffnen Sie die Google-Startseite www.google.de in Ihrem Webbrowser und tragen Sie Ihren eigenen Namen in Anführungsstrichen (Beispiel Karl Müller) in das Google-Suchfeld ein.

2. Starten Sie die Suche und sehen Sie selbst, was das Internet bereits alles über Sie (oder Ihren Namensvetter) gespeichert hat.

3. Suchmaschinen wie www.yasni.de oder www.123people.com sind sogar darauf spezialisiert, Personen im Internet zu finden. Suchen Sie einmal Ihren eigenen Namen bei diesen Personen-Suchmaschinen. Oftmals entdecken diese Suchmaschinen sogar Fotos oder Videos von Ihnen und geben Ihre E-Mail-Adresse und Telefonnummer an. Dazu sammeln diese Suchmaschinen personenbezogene Daten von zahlreichen Internetseiten, darunter auch von den Wunschlisten bei Amazon.de oder Einträge in Firmenverzeichnissen.

4. Sprechen Sie mit Ihrem Datenschutzbeauftragten, wenn Sie personenbezogene Daten von sich vorfinden, die nicht öffentlich sein sollten!

Prüfen Sie Ihre Einstellungen bei XING:

Wollen Sie, dass Ihre E-Mail-Adresse, Ihre geschäftliche Telefonnummer und Ihr Geburtstag für alle Ihre XING-Kontakte sichtbar sind?

Haben Sie freiwillige Angaben (wie Hobbys, frühere Arbeitgeber, Privatadresse) gemacht, die Sie lieber wieder entfernen möchten?

Soll die Liste Ihrer Kontakte für alle anderen XING-Mitglieder sichtbar sein?

Wollen Sie Ihren Aktivitätsindex (also die Nutzungsintensität bei XING) anzeigen oder nicht?

Möchten Sie, dass alle XING-Nutzer in Ihr Gästebuch schreiben dürfen?

Akzeptieren Sie private Nachrichten von allen XING-Mitgliedern, nur von Ihren Kontakten oder überhaupt nicht?

Wollen Sie zulassen, dass auch Suchmaschinen Ihr Profil bei XING und Ihre Beiträge in den XING-Gruppen lesen und auswerten können?

Ist Ihnen bewusst, dass nach Anmeldung in XING jeder Besuch eines anderen Profils registriert und für eine Woche gespeichert wird?

Ist Ihnen klar, dass alle XING-Applikationen (auch die von Dritten) Ihre geschäftlichen Profildaten und Ihre Kontaktliste auslesen und nutzen können?