

Datenschutz Now!

14

Der Datenschutz-Infobrief



Liebe Leserin, lieber Leser,

Facebook hat sich zum wichtigsten Angebot im Internet entwickelt und leider auch zu einem der gefährlichsten. Erfahren Sie in der heutigen Ausgabe, wie Sie sich als Nutzer dieses sozialen Netzwerks jetzt besser schützen können. Wissen sollten Sie aber auch, was Sie auf Facebook über Ihre Arbeitstätigkeit veröffentlichen dürfen und was nicht.

Was man unter dem Datengeheimnis versteht, verrät Ihnen der Beitrag auf der Rückseite dieser Ausgabe. Doch bevor Sie umblättern: Wissen Sie eigentlich, wo Ihr Handy im Moment ist und wie groß der Schaden durch verlorene Mobiltelefone sein kann? Den Beitrag zu Smartphones und den zugehörigen Selbsttest sollten Sie nicht verpassen!

Ich wünsche Ihnen viele wichtige Erkenntnisse mit dieser Ausgabe und stehe gerne für Rückfragen zur Verfügung! Ihr *Gilbert Staffler, Datenschutzbeauftragter*

Legen Sie Ihr Smartphone an die Kette!

Wo ist eigentlich mein Handy? Wenn Sie diese Frage nicht mehr beantworten können, droht Ihnen und Ihrem Arbeitgeber ein massiver Schaden. Nicht das Gerät an sich ist so wertvoll, sondern die Daten darauf.

Vergessen, verloren, gestohlen

Vier von zehn Unternehmen vermissen bereits Mobiltelefone und damit auch die Daten, die sich darauf befinden. Der Schaden, der dadurch entsteht, ist schier unglaublich: Wie das Sicherheitsunternehmen McAfee herausfand, beträgt der durchschnittliche Schaden pro verlorenes Smartphone rund 30.000 Euro! Sie haben richtig gelesen.

Der Grund für den großen Schaden: Fast jedes zweite in Deutschland verkaufte Handy ist ein Smartphone, also ein Mini-Computer, mit dem man auch telefonieren kann. Was allerdings darüber hinaus möglich ist, ist die Speicherung riesiger Datenmengen.

Smartphone weg, Daten weg

Geht nun ein Smartphone verloren oder wird es gestohlen, sind alle darauf gespeicherten Kontaktdaten, E-Mails, SMS und Geschäftsdokumente ebenfalls weg, ohne vorherige Datensicherung sogar für immer. Doch der Datenverlust ist nicht alles. Denn wer ein Smartphone stiehlt, hat es nicht nur auf das einige Hundert Euro teure Gerät abgesehen.

Fette Beute für Datendiebe

Die Daten auf einem Smartphone sind für Diebe äußerst interessant, speichern doch viele ihre Passwörter auf dem mobilen Begleiter. Besonders riskant ist der Verlust eines Smartphones, da nur 38 Prozent der Smartphone-Nutzer laut einer Umfrage von Steria Mummert eine Verschlüsselung für notwendig erachten.

Schützen Sie Daten und Gerät

Damit das Verschwinden Ihres Handys oder Smartphones nicht auch zur Datenpanne ausartet, sollten Sie in Absprache mit Ihrer Systemadministration das vom Unternehmen gestellte Mobiltelefon verschlüsseln und die Daten regelmäßig sichern. Das empfiehlt sich übrigens auch für Ihr privates Handy!

Wie wäre es mit einer unsichtbaren Kette?

Sie können aber auch den Gerätediebstahl oder das peinliche Vergessen des Smartphones selbst verhindern. Die Sicherheitschlösser und Ketten für Notebooks kennen Sie vielleicht. Für Ihr Handy brauchen Sie aber

keine Kette, wie zum Beispiel bei einem Taschenmesser. Es gibt unsichtbare Ketten!

Bitte dicht zusammen bleiben!

Für alle Mobiltelefone, die über Bluetooth verfügen, lässt sich eine kleine Alarmanlage einsetzen, um den Verlust oder Diebstahl sofort zu bemerken. Bluetooth ist eine mögliche Funkverbindung zwischen Ihrem Smartphone und einem anderen Gerät, das Bluetooth unterstützt. Dies kann etwa ein Bluetooth-fähiges Armband sein, das Teil einer speziellen Alarmanlage ist. Wird die Bluetooth-Verbindung zwischen Armband und Handy unterbrochen, weil das Mobiltelefon zu weit entfernt ist, schlägt das Armband Alarm.

Aufmerksamkeit und Verschlüsselung sind immer noch am besten

Selbst wenn Sie solch eine Bluetooth-Alarmanlage für Ihr Smartphone haben sollten, sind die Verschlüsselung der Daten und Ihre Aufmerksamkeit immer noch der beste Schutz. Sie müssen dann an Ihrem Smartphone Bluetooth nicht immer aktiv haben. Bluetooth kann zwar für eine Mini-Alarmanlage genutzt werden, Datendiebe nutzen Bluetooth-Verbindungen aber auch als Angriffsweg.

Der beste Schutz ist eben immer noch der aufmerksame Nutzer. Werden Sie also selbst zur Kette für Ihr Smartphone!

So wird Facebook endlich sicherer!

Neue Funktionen am laufenden Band - das macht Facebook interessanter, aber auch gefährlicher. Mit kostenlosen Zusatztools können Sie einiges dafür tun, dass Ihre Teilnahme an Facebook oder anderen sozialen Netzwerken gefahrloser wird.

Schon wieder alles anders

Gehören Sie zu den 50 Prozent der 900 Millionen Nutzer, die täglich einen Blick in Facebook werfen? Dann sollte man meinen, dass Sie Facebook gut kennen. Doch gleichgültig, wie oft man Facebook nutzt, dauernd stößt man auf neue Funktionen und Möglichkeiten. Das ist spannend und riskant zugleich.

Wo ist das Handbuch?

Wenn Sie Ihre Einstellungen bei Facebook ändern möchten, um zum Beispiel Ihren Selbstschutz zu verbessern, werden Sie feststellen, dass sich die Abläufe und Optionen häufig ändern. Da reicht auch ein dickes Facebook-Handbuch nicht. Denn die Empfehlungen für eine datenschutzfreundliche, sichere Nutzung haben bei Facebook ein sehr begrenztes Haltbarkeitsdatum.



Soziale Netzwerke wie Facebook machen es ihren Nutzern oft nicht leicht, sich zurechtzufinden

Neue Freunde, neue Funktionen, neue Gefahren

Dabei haben Datendiebe und Spammer das führende soziale Netzwerk ganz besonders im Fokus. Kaum eine Woche vergeht, ohne dass ein neuer Facebook-Trojaner oder eine neue Facebook-Spam-Welle bekannt wird.

Das Sicherheitsunternehmen Kaspersky hat in einer Studie veröffentlicht, dass jedes dritte Unternehmen mit Viren-Angriffen rechnen muss, die Mitarbeiter durch ihre Teilnahme an Netzwerken wie Facebook ermöglichen. Beispiele für die gesteigerte Viren-Gefahr sind:

- gefälschte Facebook-Mails zu neuen Nachrichten und Statusänderungen von Kontakten mit verseuchten Links

- interne Nachrichten oder Einträge auf der Pinnwand mit verseuchtem Link, zu Themen wie interessante Fotos und Videos, wer angeblich das eigene Profil besucht hat, Einladung zu vermeintlichen Events, angebliche Nachrichten zu Stars und bekannten Personen oder angebliche Sicherheitswarnungen

- bösartige Facebook-Anwendungen mit Spyware-Funktionen, die sich z.B. als Spiel tarnen

- Meldungen innerhalb von Facebook, dass für das Betrachten eines Videos ein neuer Media-Player nötig ist, wobei der angebliche Link zur Player-Installation verseucht ist

- die Verwendung gekürzter Links in sozialen Netzwerken, wobei der Nutzer nicht ohne Weiteres erkennen kann, wohin sie führen

Wie soll man sich da nur schützen? Ganz einfach: Machen Sie es wie Facebook, und bringen Sie neue Funktionen ins Spiel!

Kostet nichts, bringt viel

Neben den Sicherheitseinstellungen bei Facebook selbst gibt es Zusatztools, die Sie längerfristig vor zahlreichen Facebook-Gefahren schützen können. Verschiedene Sicherheitsunternehmen bieten ergänzende Sicherheitsfunktionen an, häufig im Rahmen einer Partnerschaft mit Facebook.

Beispiele sind die Dienste Defensio 2.0 von Websense, ShareSafe von F-Secure, BitDefender Safego, Norton Safe Web for Facebook, WOT (Web of Trust) und das Zscaler Likejacking Prevention-Tool.

Wenn die Verschlüsselung fehlt

Besonders kritisch ist es, wenn Sie Facebook oder ein anderes soziales Netzwerk ohne Verschlüsselung nutzen. Bei Facebook können Sie die SSL-Verschlüsselung aktivieren, bei manchen Netzwerken geht dies dagegen gar nicht. Um immer die SSL-Verschlüsselung im Browser einzusetzen, können Sie bei Facebook & Co. auf das Zusatztool HTTPS Everywhere (www.eff.org/https-everywhere) setzen, das es für den Firefox-Browser gibt.

Die besten kostenlosen Tools

Defensio 2.0 (www.defensio.com) prüft Facebook-Nachrichten auf Spam-Charakter und analysiert das Risiko, das von Links in Facebook-Nachrichten ausgeht, bevor Sie die Links anklicken.

WOT (www.mywot.com) führt Prüfungen von Hyperlinks in Facebook-Nachrichten durch. Basis ist die Bewertung der Hyperlinks durch die sogenannte WOT-Community. Wurde also ein Link in den Facebook-Nachrichten als gefährlich eingestuft, werden die anderen WOT-Nutzer entsprechend gewarnt.

ShareSafe von F-Secure (apps.facebook.com/sharesafe) prüft die auf Facebook angezeigten Links, ob sich dahinter Malware versteckt. Dadurch sehen Sie eine mögliche Gefahr, noch bevor Sie den Link in Facebook anklicken.

BitDefender Safego (apps.facebook.com/bd-safego) prüft Nachrichten und Inhalte in Facebook auf Spam- und Malware-Verdacht.

Norton Safe Web for Facebook (apps.facebook.com/nortonsafeweb) untersucht Links in Facebook auf mögliche Schadsoftware.

Zscaler Likejacking Prevention-Tool (www.zscaler.com/zscaler_likejacking.html) prüft Facebook-Like-Buttons auf Webseiten, ob sich dahinter ein Angriffsversuch oder Betrug versteckt.

Dieses Tool erzwingt die SSL-Verschlüsselung, wo immer dies möglich ist. Das ist etwa dann besonders wichtig, wenn Sie ein soziales Netzwerk über einen öffentlichen WLAN-Hotspot nutzen, zum Beispiel im Hotel oder am Bahnhof.

Sie sehen also: Immer neue Funktionen bei Facebook stiften zwar Verwirrung und machen die Sicherheitseinstellungen komplizierter. Aber mit den richtigen Zusatzfunktionen lassen sich Gefahren wie gefälschte, verseuchte Links und Viren-Angriffe schneller erkennen. Nutzen Sie diesen Vorsprung gegenüber den listigen Datendieben!

Facebook & Co.: Statusmeldungen aus der Arbeit

Sie sind selbst in Facebook? Oder zumindest haben Sie ziemlich viele Bekannte, die Facebook nutzen oder auch ein anderes soziales Netzwerk wie XING? Dann haben Sie sicher schon von dem Problem gehört: Darf man denn eigentlich aus der Arbeit posten? Und auf was ist dabei zu achten?

Bloß eine gute Nachricht, ...

Das Bild war völlig harmlos. Man sah darauf ein paar Weißwürste und daneben ein Glas mit Hefeweizen. Der Mitarbeiter eines Unternehmens, das - Sie ahnen es - seinen Sitz in Bayern hat, hatte es in Facebook eingestellt. Bildunterschrift: "So haben wir heute den Abschluss unseres Projekts gefeiert."

Was er nicht bedacht hatte: Die Konkurrenz war ausgesprochen daran interessiert, wie es um dieses interne Projekt stand. Sie konnte sich jetzt ausrechnen, wann in etwa das Unternehmen mit dem neuen Produkt an den Markt gehen würde, und konnte ihre eigenen Planungen entsprechend gestalten.

... aber eigentlich ein Geschäftsgeheimnis

Dieses nicht erfundene Beispiel zeigt, dass sich Geschäftsgeheimnisse auch dann ausplaudern lassen, wenn man über sie eigentlich gar nicht redet. Oder besser gesagt: Wenn man irrtümlich meint, gar nicht darüber geredet zu haben, andere aber ihre Rückschlüsse ziehen können.

Bilder - oft eine heikle Sache

Vielen ist es nicht ganz wohl, wenn sie ein Bild von sich in Facebook stellen, und Frauen sind hier oft noch sensibler als Männer. Bloß Getue? So einfach ist es nicht! Aus rechtlicher Sicht besteht durchaus Anlass zur Vorsicht.

Wenn ein Bild in Facebook (oder auch in einem anderen sozialen Netzwerk) so präsentiert wird, dass jeder darauf zugreifen kann, der den Account aufruft - und beispielsweise nicht nur wenige echte Freunde, denen man diesen Zugriff individuell erlaubt -, kann es nämlich schnell fatal werden: Aus der freien Zugriffsmöglichkeit ziehen die Gerichte nämlich den Schluss, dass auch wirklich jeder zugreifen darf.

Ärger für eine Pilotin

Was das bedeuten kann, musste eine junge Pilotin sehr unangenehm erfahren. Sie hatte ein Passagierflugzeug gesteuert, das beim

Landen über die Landebahn hinausrutschte. Die "Zeitungen mit den großen Buchstaben" griffen den Vorfall natürlich gleich auf. Und zwar mit einem Bild der Pilotin!

Das Bild stammte aus einem sozialen Netzwerk. Die Pilotin hatte es selbst hineingestellt und den Zugriff in keiner Weise begrenzt. Deshalb konnte sie auch nichts dagegen unternehmen, dass sich eine Zeitung daran bediente. Später stellte sich übrigens heraus, dass sie bei der Landung nichts falsch gemacht hatte. Es lag vielmehr ein technischer Fehler vor. Aber da war sie in der Öffentlichkeit schon bloßgestellt.



Bilder in sozialen Netzwerken sagen oft mehr aus als ursprünglich beabsichtigt, wie der "Weißwurst-Fall" beweist

Noch heikler: Bilder von anderen Leuten

Sie vermuten es sicher, aber vielleicht haben Sie sogar schon davon gelesen: Wer das Bild einer anderen Person ins Netz stellen will, braucht die Einwilligung dieser Person. "Einwilligung" bedeutet dabei, dass man vorher fragen muss. Es darf also nicht so sein, dass erst das Bild eingestellt wird und später irgendwann einmal die Frage kommt: "Du hast da doch bestimmt nichts dagegen?"

Denken Sie also bitte darüber nach, bevor Sie Bilder von einer gemeinsamen Feier ins Netz

stellen - und zwar auch dann, wenn es sich um völlig seriöse Bilder handelt. Denn auch hier gelten dieselben Regeln, also nicht nur in den Fällen, in denen sich jemand auf einem Bild blamiert!

Unter 18 - ein No-go

Wer wirklich viel Ärger will, stellt Bilder auf Facebook, bei denen manche der abgebildeten Person unter 18 Jahre alt sind. Das Gesetz ist hier nämlich eindeutig und klar: In solchen Fällen ist die Einwilligung der Erziehungsberechtigten notwendig.

Sie meinen, da hält sich ja doch niemand daran? Das mag mitunter so sein - und daraus erklärt sich dann manches Anwaltsschreiben und mancher Antrag bei Gericht. Diese Dinge sind sehr real.

Ist alles nur böse?

Wenn Sie dies lesen, gewinnen Sie vielleicht den Eindruck, außer Ärger könne man bei sozialen Netzwerken nichts erwarten. Nun, so schlimm ist es sicher nicht. Im Gegenteil: Soziale Netzwerke können ein sehr gutes Schaufenster sein, in dem sich ein Unternehmen gut darstellt und in dem auch dessen Mitarbeiter ein gutes Bild abgeben.

Abreden im Unternehmen sind nötig

Das sollte dann aber bitte im Unternehmen abgesprochen sein. Denn oft wird übersehen, dass es etwas anderes ist, wenn man privat in Facebook vertreten ist und nur über private Dinge berichtet, oder wenn man munter aus der Arbeit plaudert.

Was jemand rein privat tut, ist seine Sache. Wenn aber Interessen des Unternehmens ins Spiel kommen, muss man sich mehr Gedanken machen!

Impressum

Redaktion:
Gilbert Staffler
Datenschutzbeauftragter

Anschrift:
EHS-Datentechnik
Uhlendahlweg 24
45279 Essen
Telefon: 0201-530091
E-Mail: info@ehs-datentechnik.de

Das Datengeheimnis - überhaupt nichts Geheimnisvolles!

Irgendwann einmal haben Sie ein Merkblatt unterschrieben. Die Überschrift hieß "Verpflichtung auf das Datengeheimnis" oder so ähnlich. Wahrscheinlich liegt es noch in Ihren Unterlagen. Holen Sie es doch noch einmal heraus! Sein Inhalt ist nämlich wichtig.

Verpflichtung - ein gesetzliches Muss

Die Verpflichtung auf das Datengeheimnis schreibt das Bundesdatenschutzgesetz ausdrücklich vor. Warum eigentlich? Die Antwort lautet: Diese Verpflichtung soll Ihnen ganz persönlich bewusst machen, dass auch Sie Verantwortung für den Datenschutz in unserem Unternehmen tragen.

Machen Sie sich Gedanken!

Müssen Sie deshalb Datenschutzexperte werden? Nun, das sicher nicht. Aber Sie sollten sich ab und zu Gedanken über den Datenschutz machen. Etwa wenn es darum geht, wer alles auf einen Text zugreifen darf, den Sie in einer Projektgruppe gemeinsam bearbeiten. Dabei sollten Sie auch darüber nachdenken, ob das Dokument ausreichend dagegen geschützt ist, dass Unbefugte von außen darauf zugreifen.

Reden Sie mit anderen!

Alle Ihre Kolleginnen und Kollegen haben dieselbe Pflicht wie Sie: Jede und jeder muss in seinem Verantwortungsbereich darauf achten, dass der Datenschutz eingehalten wird. Deshalb ist es sinnvoll, miteinander darüber zu reden. Zum Beispiel einmal darüber, ob es eigentlich in Ordnung ist, wenn jemand im Home Office die eigenen USB-Sticks benutzt, und das auch noch, ohne den anderen etwas davon zu sagen.

Den Ärger mit Viren, die dann vielleicht eingeschleppt werden, hat nämlich die ganze Gruppe. Also reden Sie darüber, wie sich so etwas vermeiden lässt. Geht es vielleicht auch ohne USB-Sticks, und wenn ja, wie?

Fragen Sie den Datenschutzbeauftragten!

Wenn es an solche Fragen geht, dann merken Sie manchmal rasch: Manches ist nicht einfach. Es sind verschiedene Lösungen denkbar. Außerdem muss man stets darauf achten, dass die Abläufe weiterhin reibungslos funktionieren. In solchen Situationen bietet der Datenschutzbeauftragte unseres Unterneh-

mens gern seine Unterstützung an. Oft wurde nämlich ein Problem, das einer Abteilung zu schaffen macht, anderswo schon gelöst!

Und was ist dann das Geheimnis?

Jetzt fragen Sie sich vielleicht, was das alles mit dem Datengeheimnis zu tun hat. Geht es da nicht um Verbote? Um das, was man eben nicht tun darf?

Wenn man in den Wortlaut des Gesetzes schaut, könnte dieser Eindruck entstehen. Da heißt es nämlich unter dem Stichwort "Datengeheimnis" recht schroff: Es ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Aber natürlich lässt sich das auch positiv formulieren: Jeder muss sich ehrlich bemühen, personenbezogene Daten in rechtlich korrekter Weise zu erheben, zu verarbeiten und zu nutzen.



So formuliert, stellt sich das Ganze wesentlich freundlicher dar, und vor allem: Ihnen wird deutlich, dass hier nur das verlangt wird, was Sie ja ohnehin wollen. Denn das Letzte, was ein Unternehmen in der heutigen Zeit brauchen kann, ist ein Datenschutzskandal.

Werden Sie aktiv!

Besonders wenn Sie sehr viel mit personenbezogenen Daten zu tun haben, sollten Sie sich fragen, ob Ihr Wissen im Datenschutz ausreicht.

Googeln Sie doch einmal nach einer Datenschutzfrage, mit der Sie immer wieder zu tun haben. Sie finden dazu Antworten, die das bei Ihnen übliche Vorgehen bestätigen? Oder Sie merken, dass alle Welt das anders sieht? Oder Sie finden nur widersprüchliche Antworten? Egal wie: Diskutieren Sie im Kollegenkreis darüber und fragen Sie, wenn es schwierig wird, den Datenschutzbeauftragten. Denn dann haben Sie genau das getan, was der Sinn des Datengeheimnisses ist.

Ist Ihr Smartphone sicher? Machen Sie den Selbsttest!

Frage: Stellen Sie sich vor, Ihr Smartphone geht verloren, war aber zu diesem Zeitpunkt ausgeschaltet. Kann ein unehrlicher Finder an Ihre Daten kommen?

- a) Leider ja, wenn ich die Verschlüsselung vergessen habe.
- b) Nein, denn er bräuchte ja meine PIN, um das Smartphone anzuschalten.
- c) Wenn er die Speicherkarte aus dem Smartphone holt, kann er auch ohne PIN auf die Daten zugreifen.

Lösung: Antwort a) und c) sind richtig. Allein mit der PIN, die Zugang zum Mobilfunknetz gibt, können Sie Ihr Mobiltelefon nicht schützen. Denken Sie an die Verschlüsselung der Daten auf dem internen Speicher des Smartphones und auf der zusätzlichen Speicherkarte.

Frage: Ihr Kollege hat sein Mobiltelefon verloren, ist aber unbesorgt, denn er sichert auch die Daten auf dem Handy regelmäßig. Hat er Grund, sich nicht zu sorgen?

- a) Wenn er Backups seiner Daten vom Mobiltelefon hat, ist doch alles in Ordnung.
- b) Es kommt ganz darauf an, ob er die Daten auf dem Handy auch verschlüsselt hat.

Lösung: Antwort b) ist richtig. Allein die Datensicherung ist kein ausreichender Schutz. Der Datenverlust lässt sich so vermeiden, aber nicht der Datenmissbrauch durch einen Dieb oder unehrlichen Finder. Helfen könnte nur noch eine sogenannte Datenfernlöschung (Remote Wipe) für das Handy, aber nur, wenn dies vor dem Verlust bereits für den Fall der Fälle vorbereitet wurde. Besser ist in jedem Fall ein Backup in Verbindung mit einer Verschlüsselung.