audatis.INFO
Newsletter für Datenschutz + Datensicherheit in kleinen und mittleren Unternehmen

Ausgabe 3 / 2012
bundesweit

Hardware-Rückgabe mit besonderen Tücken

Sie freuen sich über Ihr neues Smartphone? Dann freut sich vielleicht ein Datendieb gerade über Ihr altes. Viele Geräte, die entsorgt oder zurückgegeben werden, enthalten noch vertrauliche Daten. Kennen Sie schon alle Datenverstecke?

83 Millionen Mobiltelefone wurden 2011 als Altgeräte abgestempelt und werden nicht mehr genutzt. Zehn Millionen neue Smartphones, drei Millionen neue Business-Notebooks und zwei Millionen neue Tablets wurden in nur einem Jahr gekauft - diese Zahlen des Hightech-Verbands BITKOM sind ein deutliches Zeichen für die kurze Nutzungsdauer bei IT-Geräten.

Wegwerfen verboten

Wenn ein IT-Gerät, das Sie betrieblich nutzen, aus dem Verkehr gezogen wird, geben Sie es in der Regel an die Administration zurück. Auch privat dürfen die Smartphones, Handys und Notebooks nicht etwa in den Müll. Für die Rückgabe von Elektronikgeräten gibt es klare Spielregeln. Leider wird dabei oftmals nicht an die Daten auf den Geräten gedacht.

Aber der Speicher war doch leer?!

Volle zwölf Prozent aller Datenverluste lassen sich laut der Unternehmensberatung KPMG International auf die unsachgemäße Entsorgung von IT-Geräten zurückführen.

"Bei mir passiert das nicht!", denken Sie jetzt vielleicht. "Wenn ich ein Gerät zurückgebe oder dem Recycling zuführe, dann lösche ich immer meine Daten." Aber löschen Sie wirklich alle Daten?

Nicht nur „richtig“ löschen, sondern auch „komplett“ löschen ist angesagt

Mit dem Löschen personenbezogener, vertraulicher Daten ist das so eine Sache. Zum einen muss man mehr tun, als über das Betriebssystem zu löschen. Man braucht eine Lösung zur sicheren Datenlöschung, einen Daten-Schredder. Damit nicht genug, reicht es auch nicht, einfach den Speicher des Smartphones oder Notebooks zu löschen. ...

(*Fortsetzung auf Seite 3*)

Schwerpunkt dieser Ausgabe:

Sichere Entsorgung von Smartphones und anderer IT-Hardware!

IN DIESEM NEWSLETTER

IM NÄCHSTEN NEWSLETTER

Veranstaltungen 2013 /1
Aktuelle Themen
Sicherheit + Cloud Computing

audatis
Datenschutz und Informationssicherheit | NEWSLETTER

Falscher Viren-Alarm - trotzdem echtes Risiko

Eigentlich soll die Anti-Viren-Software ja Ihre Daten und Ihren Rechner schützen. Doch Sicherheitssoftware kann schnell selbst zum Risiko werden, wenn sie Freund und Feind nicht mehr richtig unterscheidet. Dann sind Sie gefragt!

Nichts geht mehr

Stellen Sie sich vor, Sie sitzen am Computer und öffnen eine Textdatei. Plötzlich erscheint eine Warnung Ihrer Anti-Viren-Software: Eine Spyware wurde gefunden, die heimlich Ihre Daten stehlen wollte. Nichts wie weg damit, sagen Sie sich, und geben die Spyware zum Abschuss frei. Sofort wird die Anti-Viren-Software aktiv und löscht die entsprechenden Dateien. Doch nun funktioniert Ihr Office-Programm nicht mehr, schlimmer noch, beim versuchten Neustart will selbst das Betriebssystem nicht. Was ist geschehen?

Nicht zu spät gelöscht, sondern das Falsche

Nun denken Sie vielleicht, dass Ihre Anti-Viren-Software leider zu spät reagiert hat und die Schadsoftware bereits Unheil über Ihren Computer gebracht hat. Doch das Gegenteil ist vielleicht der Fall: Ihre Anti-Viren-Software hat das Office-Programm und das Betriebssystem beschädigt, eine Spyware gab es überhaupt nicht!

Es passiert immer wieder

Ihre Anti-Viren-Software hat sich leider geirrt und harmlose Dateien für gefährlich gehalten. Ein solcher Falschalarm passiert in der Abwehr von Schadprogrammen immer wieder: So stufte zum Beispiel im Mai 2012 eine bekannte kostenlose Anti-Viren-Software den Windows Explorer, Microsoft Office und den Opera-Browser als schädlich ein. Die Computer der betroffenen Nutzer wurden lahmgelegt.

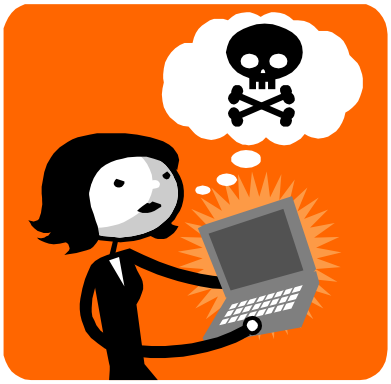
So reagieren Sie richtig bei falschem Alarm

Damit so etwas nicht passiert, ist natürlich zuerst die Qualitätssicherung der Sicherheitsanbieter gefragt. Doch ganz ohne Fehler werden auch die Anti-Viren-Programme der Zukunft nicht sein. Deshalb müssen Sie als Anwender auf solche Situationen vorbereitet sein. Daher: Keine Panik bei Virenalarm! So gehen Sie am besten vor:

1. Stellen Sie in Ihrer Anti-Viren-Software als Standardverhalten ein, dass verdächtige Dateien in die Quarantäne kommen und nicht etwa gleich gelöscht werden.
2. Wenn Sie sich nicht sicher sind, welche Option bei Ihrer Anti-Viren-Software die richtige ist, fragen Sie lieber Ihren Administrator.
3. Auch im Fall einer konkreten Viren-Warnung sollten Sie sich an das Standardvorgehen halten: Quarantäne ja, sofort löschen nein.
4. Fallen Sie nicht auf Virenwarnungen Dritter herein, die per E-Mail eintreffen. Das sind in der Regel selbst getarnte Angriffe.
5. Merken Sie sich, welche Anti-Viren-Software Sie nutzen. Wenn ein Programmdialog eines Ihnen unbekannten Sicherheitsprogramms erscheint, folgen Sie nicht den Anweisungen, sondern melden Sie dies sofort Ihrem Administrator.

Falsche Virenwarnung als getarnter Angriff

Nicht nur Ihre eigene Sicherheitssoftware kann also eine falsche Virenwarnung ausgeben. Sie können auch eine E-Mail bekommen, die behauptet, Ihr Rechner sei verseucht. Folgen Sie nicht den Anweisungen in der E-Mail und klicken Sie auf keinen Link in der E-Mail, der angeblich die Viren löschen soll. Melden Sie die E-Mail umgehend Ihrem Administrator, denn dahinter steckt in der Regel selbst ein Angriff.



"Wenn die Anti-Virensoftware nicht zuverlässig funktioniert, können auch nicht infizierte Systeme und Programme verdächtigt werden."

Wissen Sie, wie Ihr Anti-Viren-Programm heißt und aussieht?

Das Gleiche gilt, wenn plötzlich im Browser ein kleines Programmfenster aufgeht, das behauptet, Ihr Computer sei verseucht. Merken Sie sich, wie Ihr Anti-Viren-Programm heißt und aussieht. Ein Sicherheitsprogramm, das offiziell nicht bei Ihnen läuft, wird sich kaum mit einer echten Warnung melden. Vielmehr ist dies meist ein Versuch, Ihnen durch den Klick auf die Warnung erst Viren zu übertragen.

Denken Sie daran: Anti-Viren-Software ist sehr wichtig, aber nicht unfehlbar! Reagieren Sie nicht vorschnell bei einer angeblichen Virenwarnung, sondern bleiben Sie besonnen. Dateien, die Sie in die Quarantäne schicken, können Sie bei Falschalarm schnell wieder aktivieren. Das Löschen von Dateien kann jedoch den Rechner erst einmal lahmlegen. (WN)

Hier finden Sie aktuelle Testergebnisse für Anti-Viren-Software:

http://ds-its.eu/avtest

Fortsetzung von Seite 1

Hardware-Rückgabe mit besonderen Tücken

Das Risiko mit der Speicherkarte

Bei einem Smartphone zum Beispiel lassen sich Daten auf der SIM-Karte speichern. Die meisten Geräte haben zusätzlich einen internen Speicher, interner Flash-Speicher genannt. Um den internen Speicher zu erweitern, können noch Speicherkarten in das Gerät eingesetzt werden. Die microSD-Karten zum Beispiel sind so klein und oftmals so gut innerhalb des Geräts versteckt, dass sie schnell vergessen werden könnten - und mit ihnen gegebenenfalls einige Gigabyte Daten.

Wissen Sie, wo die Speicherkarte aus Ihrem alten Smartphone ist? Haben Sie diese ebenfalls gelöscht, wenn sie im Gerät verblieben sein sollte?

Kameras, Kopierer, Router, Speicher

Zudem haben weitaus mehr Geräte einen internen Speicher, als man glauben möchte. So könnten sich zum Beispiel auf alten Beamern, Anrufbeantwortern, Kopierern, Digitalkameras, Druckern, E-Book-Readern oder MP3-Playern noch Kopien von Daten befinden, ungelöscht und ungeschützt!

Selbst der heimische WLAN-Hotspot hat heute in der Regel einen internen Speicher, eigentlich dafür, dass jeder Nutzer über WLAN von einem zentralen Speicher Gebrauch machen kann. Wird der WLAN-Router aber entsorgt und der Speicher nicht gelöscht, haben bald andere Zugriff darauf.

Auch hier könnten noch Daten versteckt sein:

- PCs und Notebooks: zusätzliche Festplatte, eingesteckte Speicherkarten, noch angeschlossene USB-Sticks, CDs oder DVDs im Laufwerk
- Beamer, Kopierer, Drucker, E-Book-Reader, WLAN-Router: ggf. interner Speicher, eingesteckte Speicherkarten, noch angeschlossene USB-Sticks
- Digitalkameras, Anrufbeantworter, MP3-Player: interner Speicher, eingesteckte Speicherkarten
- Telefone, Faxgeräte, Scanner: interner Speicher
- Smartphones, Handys: SIM-Karten, interner Speicher, Speicherkarten

Auch im Lager besteht Gefahr!

Die Restdaten auf alten IT-Geräten müssen also gesucht und richtig gelöscht werden, bevor die Geräte entsorgt, dem Recycling zugeführt oder an Dritte weitergegeben werden.

Doch viele Nutzer behalten ihr Altgerät auch in der Schublade, zur Sicherheit, wenn das neue vielleicht einmal kaputtgeht. Diese scheinbare Sicherheitsmaßnahme ist in Wirklichkeit ein großes Risiko: Denn meist ist das alte Gerät bei dieser Einlagerung in der Schublade oder im Schrank völlig ungeschützt vor dem Zugriff Unbefugter.

Menschen vergessen, IT-Geräte nicht

Zudem besteht die Gefahr, dass Sie, eine Kollegin oder ein Kollege eines Tages auf diesen IT-Schrott vergangener Tage stoßen. Dann weiß kein Mensch mehr, dass auf dem Gerät noch Daten gespeichert sein könnten, die bei der Entsorgung in Gefahr geraten!

IT-Geräte sind in der Regel nicht so vergesslich wie wir Menschen, die Daten werden also auch nach längerer Zeit noch vorhanden und damit möglicherweise bedroht sein!

Akten- und Datenträgervernichtung reichen deshalb nicht. Auch die Daten auf den Altgeräten müssen sauber entsorgt werden! (WN)

Datenschutz-schulung für Ihre Mitarbeiter

Datenschutz kann als Wettbewerbs- und Marketingvorteil genutzt werden, um das Vertrauen von Kunden und Geschäftspartnern zu gewinnen. Vorausgesetzt es beteiligen sich alle Mitarbeiter und Führungskräfte.

Für viele Datenschutzbeauftragte ist die Motivierung der Mitarbeiter zur Umsetzung der Datenschutzvorschriften eine Sisyphos-Aufgabe und wird als Arbeitsbehinderung, etc. abgetan. Noch schlimmer ist die Situation, wenn sogar die Führungskräfte nicht von der Notwendigkeit des Datenschutzes und der entsprechenden Einhaltung im Unternehmen überzeugt sind dann fehlt den Mitarbeitern das Vorbild und sie werden sich erst recht nicht an die Datenschutzanforderungen halten.

audatis Training hat die Probleme der Datenschutzbeauftragten, aber auch die Argumente der Mitarbeiter und Manager, analysiert und daraus ein Datenschutz-Schulungskonzept zur Sensibilisierung von Mitarbeitern im Unternehmen entwickelt (Datenschutz-Awareness). Dieses enthält:

- Abstimmung der Inhalte mit dem betrieblichen DSB
- Auswahl der Zielgruppen
- Erstellung der Schulungsunterlagen (PDF + PPT)
- Schulung durch unsere Referenten bei Ihnen vor Ort (pro Gruppe ca. 1,5 Std.)
- Integration von Live-Hackings und Beispielen aus Betrieb und Privatleben

Bei Interesse oder Fragen: training@audatis.de

Veranstaltungen und Seminare zu Datenschutz und Datensicherheit von September 2012 bis Dezember 2012

Im **Bereich Datenschutz** finden folgende Veranstaltungen zwischen **September und Dezember 2012** statt:

10.09. **Seminar: Datenschutz für IT-Leiter und IT-Experten (W)**
09:00 - 17:00 in Berlin [**dsitl**]

02.10. **Seminar: Erstellen und Pflegen des Verfahrensverzeichnisses (W)** 09:00 - 17:00 in Köln [**dsvztuv**]

15.10. - 16.10. **IDACON 2012: 12. Fachkongress für Datenschutzbeauftragte (F)**
10:00 - 18:00 in Würzburg [**idacon**]

15.10. **Seminar: Datenschutz für IT-Leiter und IT-Experten (W)**
09:00 - 17:00 in München [**dsitl**]

21.11. - 22.11. **Seminar: Datenschutzassistent mit TÜV-Zertifikat (W)**
09:00 - 17:00 in Berlin [**dsastuv**]

29.11. **Seminar: Datenschutz für IT-Leiter und IT-Experten (W)**
09:00 - 17:00 in Hannover [**dsitl**]

Für die Sparte **Datensicherheit** konnten wir folgende Veranstaltungen für Sie zwischen **September und Dezember 2012** finden:

15.10. - 19.10. **Seminar: IT-Security-Beauftragter mit TÜV-Zertifikat (W)**
09:00 - 17:00 in Berlin-Spandau [**isbtuv**]

17.10. - 18.10. **Seminar: IT-Sicherheit für Datenschutzbeauftragte (W)**
09:00 - 17:00 in Nürnberg während der it-sa [**isitsds**]

06.11. **Seminar: Professioneller Umgang mit Datenpannen (W)**
09:00 - 17:00 in Hamburg [**isdptuv**]

14.11. - 15.11. **Seminar: IT-Sicherheit für Datenschutzbeauftragte (W)**
09:00 - 17:00 in Berlin [**isitsds**]

19.11. - 23.11. **Seminar: IT-Security-Beauftragter mit TÜV-Zertifikat (W)**
09:00 - 17:00 in Berlin-Spandau [**isbtuv**]

(F) = Fachtagung / Forum
(O) = Online / Webinar
(W) = Weiterbildung / Seminar

Sie finden **weitere Informationen** zu den Veranstaltungen und die Veranstalter über folgenden Shortlink: **http://ds-its.eu/CODE** dabei ersetzen Sie den CODE durch den entsprechenden Wert in [eckigen Klammern], welcher unter jedem Veranstaltungshinweis steht.

Was sind denn "sensible Daten"?

Der Begriff „besonders sensible Daten“ ist weit verbreitet. In den Datenschutzgesetzen findet er sich aber nicht. Dort ist die Rede von "besonderen Arten personenbezogener Daten". Und für solche Daten gelten besonders strenge Vorschriften. Unter anderem ist eine "Vorabkontrolle" vorgesehen. Aber um welche Daten geht es eigentlich? Und was soll eine Vorabkontrolle?

Welche Daten über eine Person als besonders sensibel anzusehen sind, hängt sehr von den Umständen und stark vom persönlichen Empfinden ab.

Dazu ein Beispiel: Der eine möchte auf keinen Fall, dass jemand erfährt, in welcher Gewerkschaft er ist. Der andere erwähnt das bewusst überall und versucht beständig aktiv, neue Gewerkschaftsmitglieder zu gewinnen.

Das Gesetz muss von genauen Begriffen ausgehen

Weil die Auffassungen so unterschiedlich sind, kann das Gesetz es nicht vom Einzelfall abhängig machen, welche Daten es als besonders sensibel bewertet. Maßstab kann vielmehr nur sein, welche Daten von den meisten Menschen als besonders heikel angesehen werden.

Diesen Weg geht das Bundesdatenschutz-gesetz in § 3 Absatz 9. Der Absatz lautet: "Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben."

Das Gesetz bewertet nur bestimmte Daten als besonders sensibel

Für das Beispiel der Mitgliedschaft in einer Gewerkschaft gilt somit: Diese Angabe wird vom Gesetz als besonders sensibel bewertet, mögen die Meinungen darüber auch geteilt sein. Dasselbe gilt für die Mitgliedschaft in einer Partei, denn sie berührt "politische Meinungen".

Nicht besonders sensibel wäre dagegen die Angabe der Nationalität, also etwa die Angabe "Herr A besitzt die italienische Staatsangehörigkeit." Anders sieht es aus, wenn gesagt wird: "Herr A ist ein dunkelhäutiger Afrikaner." Das weist nämlich auf seine rassische oder ethnische Herkunft hin.

Dass Angaben über die Gesundheit besonders sensibel sind, dürfte jedem klar sein. Und das Sexualleben geht natürlich erst recht niemand anderen etwas an.

Bei sensiblen Daten ist eine Vorabkontrolle nötig

Schön und gut, sagen Sie sich nun vielleicht. Aber welche praktische Bedeutung hat es denn etwa im Unternehmen, wenn mit "besonderen Arten personenbezogener Daten" umgegangen wird? Zunächst einmal hat dies formale Folgen, auf die zu achten ist. Wenn beispielsweise irgendein EDV-Verfahren solche Daten enthält, muss der Datenschutzbeauftragte des Unternehmens eine Vorabkontrolle durchführen.

Die Vorabkontrolle soll die Beachtung schwieriger Datenschutzvorschriften sicherstellen

Wie der Begriff schon sagt, muss diese Überprüfung stattfinden, bevor das Verfahren eingesetzt wird, also nicht erst dann, wenn es etwa zu Beschwerden kommt.

Das hat seinen guten Grund: Für die Daten, die das Gesetz als besonders sensibel ansieht, gelten nämlich in vielfacher Hinsicht besondere Vorschriften. Sie sind im Einzelnen recht kompliziert, und deshalb muss der Datenschutzbeauftragte schon im Vorfeld ganz besonders darauf achten, dass sie beachtet werden.

Das Interesse des Unternehmens

Bedenkt man, wie empfindlich die Öffentlichkeit inzwischen auf angebliche oder wirkliche "Datenschutzskandale" reagiert, dann ist ein solches Verfahren keine Förmlichkeit, die nur den Betrieb aufhält. Vielmehr sorgt es dafür, dass es erst gar nicht zu Pannen kommt. (WN)

Hier gibt es eine Videoerklärung zu personenbezogenen Daten:

http://ds-its.eu/pbdaten

“Wer mit besonders sensiblen Daten umgeht, muss sich an die gesetzlichen Vorgaben wie z.B. die Durchführung einer Vorabkontrolle halten.”

Bleiben Sie auf dem Laufenden mit unserem kostenlosen Newsletter!

http://ds-its.eu/info

Unsere Online-Services für Sie

Sie setzen ein **Webanalyse-Tool** auf Ihrer Webseite ein? Dann sollte es Sie interessieren, ob dieses auch datenschutzkonform genutzt wird bzw. werden kann. Testen Sie selbst:

http://ds-its.eu/wac

Wie ist es um das Datenschutzniveau in Ihrem Unternehmen bestellt? Halten Sie die wichtigsten Vorgaben ein? Oder gibt es noch wesentliche Baustellen? Der **Datenschutz-Schnelltest** für Unternehmen liefert die Antworten in wenigen Minuten online und als PDF zum Ausdrucken:

http://ds-its.eu/dst

Datenschutz-Studie 2012

Mit der **audatis Datenschutz-Studie 2012** möchten wir die größten Probleme im betrieblichen Datenschutz deutscher Unternehmen betrachten und die Ergebnisse zusammen mit den wichtigsten Datenschutz-Gesetzen als kostenloses e-Book veröffentlichen.

Ausgangslage für diese Studie

Datenschutz ist in vielen Unternehmen ein unbeliebtes Thema und wird aus unterschiedlichsten Gründen von einigen Unternehmen als "nicht so wichtig" angesehen.

Wir möchten in der "audatis Datenschutz-Studie 2012" die Probleme aus Sicht der Wirtschaft, die getroffenen Maßnahmen für die Umsetzung und die Verbesserungsvorschläge der Praktiker hinterfragen.

Diese Studie soll sodann jährlich durchgeführt werden, um eine Tendenz in der Entwicklung des Datenschutzes in deutschen Unternehmen zu repräsentieren.

Wir würden uns über eine rege Teilnahme an unserer Studie sehr freuen (Link siehe unten)!

Gefragt sind Teilnehmer (Mitarbeiter + leitende Angestellte / Inhaber) aus allen privatwirtschaftlichen Branchen.

Die Ergebnisse der Studie werden zusammen mit weiteren Hilfestellungen zur betrieblichen Umsetzung des Datenschutzes als kostenloses e-Book zum Download vermutlich gegen November 2012 bereitgestellt. (KH)

http://ds-its.eu/ads2012

Hat Ihnen unser Newsletter gefallen?

Dann empfehlen Sie diesen doch gerne weiter:

www.audatis.de/online/newsletter

Die nächste Ausgabe dürfen Sie in Q4 / 2012 erwarten.

Impressum

audatis - Datenschutz und Informationssicherheit
Consulting | Training | Services
Inh. Carsten Knoop

Hauptsitz / Büro Ostwestfalen:

Dreyener Str. 20
32130 Enger

Büro Rhein-Main-Neckar:

Wehrstr. 30
69488 Birkenau

Redaktion:

V.i.S.d.P. Carsten Knoop (CK)
Kerstin Hilß (KH)

Erscheinungsweise: 4 x jährlich

Kontaktmöglichkeiten

So können Sie uns zu allen Fragen oder Anregungen erreichen:

Telefon: (05224) 999 260 - 90
Telefax: (05224) 999 260 - 99

E-Mail: info@audatis.de (allgemein)
E-Mail: newsletter@audatis.de (Newsletter-Redaktion)

Internet: www.audatis.de
Facebook: www.facebook.com/audatis
Twitter: twitter.com/audatis