

Datenschutz und Sicherheit in der IT

Aktuelle Praxistipps und Informationen



Liebe Leserin, lieber Leser,

wer von einer Datenschutz-Panne hört, denkt zuerst an Kundendaten, die versehentlich im Internet veröffentlicht wurden, oder an Festplatten, die ohne sichere Datenlöschung weiterverkauft wurden. Doch Datenschutz fängt bereits bei der Entsorgung von Altpapier an!

Natürlich drohen personenbezogenen Daten aber auch im Internet Gefahren. Millionen von Computern werden bereits als PC-Zombies zu kriminellen Zwecken missbraucht. Wie Sie sich bzw. Ihren privaten oder geschäftlichen PC davor schützen, erfahren Sie ebenfalls in dieser Ausgabe. Immer mehr Unternehmen und Privatpersonen müssen erkennen, wie raffiniert Datenspione arbeiten. Lesen Sie deshalb, wie die Wirtschaftsspionage um sich greift und wie winzige Programme versuchen, Ihr Handy auszuspionieren.

Für Ihre Rückfragen zu diesen wichtigen Themen stehe ich Ihnen gerne zur Verfügung!
Herzlichst Ihr **Thomas Jundel, Datenschutzbeauftragter**

Altes Papier - gewaltiger Ärger

Sie gehören zu denen, die nur noch am PC arbeiten und auch nie eine Mail ausdrucken? Herzlichen Glückwunsch! Dann sollten Sie sich eine kleine Pause gönnen, statt diesen Artikel zu lesen! Oder haben Sie eher den Eindruck, dass bei Ihnen das Papier immer mehr wird? Dann lesen Sie mal lieber weiter, bevor Sie die erste Abmahnung in Händen halten!

Ein typischer Fall - echt so passiert!

Ein öffentlicher Altpapiercontainer quillt über. Zufällig kommt am Sonntag ein Spaziergänger vorbei. Da ihm langweilig ist, schaut er sich das Ganze etwas näher an und findet es hochinteressant. Was da nicht alles zu entdecken ist: Alte Personalakten, Bewerbermappen aus der letzten Zeit mit Lebensläufen und Fotografien, auch ein paar Lohnsteuerunterlagen sind dabei.

Der Spaziergänger ruft die Polizei. Die nimmt die Sache sehr ernst und beschlagnahmt erst einmal den ganzen Container. Am Montag spricht sie bei der Firmenleitung vor und möchte wissen, wie so etwas vorkommen kann. Jetzt bricht Hektik aus, und plötzlich ist das alte Zeug Chefsache.

Schauen Sie sich einmal in Ihrem Büro um!

Wo werfen denn Sie das ganze Papier hin, das Sie loswerden wollen? Also die Telefon-Notizzettel, die Mailausdrucke von letzter Woche, die Liste mit den Urlaubsvertretungen und was sich sonst so alles ansammelt?

Da stehen zwei Papierkörbe, der eine gelb, der andere grün, oder was die Farbkombination in Ihrem Büro gerade ist? Moment, was unter den Datenschutz fällt, gehört in den grünen Eimer, alles andere in den gelben? Oder war es nicht umgekehrt? Fragen Sie doch mal die Kollegin gegenüber! Sie ist sich auch nicht sicher?

Sie selbst sind gefordert!

Schon sehen Sie das Dilemma! Dieses System funktioniert nur, wenn sich jeder selbst um die Trennung des Papiers kümmert. Sie sagen sich vielleicht: Könnte man denn nicht einfach das gesamte Papier datenschutzgerecht schreddern und sich so das Trennen sparen? Das sagt sich leicht, es ist aber auch eine Kostenfrage. Technisch geht bei der Entsorgung alles, aber das Zerkleinern ist teurer als das Pressen von Altpapier.

Also: Informieren Sie sich, was wohin gehört, und achten Sie darauf, dass alles in den richtigen Abfalleimer kommt.

Manchmal fragt man sich schon, wie es denn dazu kommen kann, dass plötzlich brisante

Unterlagen im öffentlichen Papiercontainer landen. Das kann bei uns doch nicht passieren? Was tun Sie eigentlich, wenn ein größerer Berg Altpapier entsorgt werden soll, etwa damit volle Schränke wieder frei werden?

So sollte es ablaufen: Sie planen das Ganze einige Tage vorher. Dann fordern Sie die nötigen Metallboxen an, in die das Altpapier hineingepackt wird. Die Boxen werden verschlossen und bis zur Abholung an der vorgeschriebenen Stelle zwischengelagert.

Die Realität sieht oft leider anders aus:

Der Entschluss zum großen Entrümpeln fällt spontan am Freitagmorgen. Ein paar alte Kartons sind rasch gefunden. Da wird dann alles hineingepackt. Dann raus mit dem alten Zeug in die Flurecke, da steht es vorläufig gut. Und jetzt muss bloß noch ein blöder Zufall dazu kommen, etwa ein offenes Fenster und ein etwas heftiger Wind - und schon liegen ein paar Blätter draußen auf der Straße. Nicht so schlimm? Wehe, wenn es die falschen Blätter sind und ein Passant nichts Besseres zu tun hat, als die Zeitung anzurufen!

In einem solchen Fall hilft es nichts, dass wir genaue Regeln für die Entsorgung von Altpapier haben, die Sie im Prinzip sicher kennen. Viel wichtiger ist, dass Sie im richtigen Augenblick daran denken. Und darum bitte ich Sie als Ihr Datenschutzbeauftragter. Wenn es Fragen dazu gibt, rufen Sie mich doch kurz an!

Handy-Spion: Vorsicht, die Konkurrenz liest mit!

Sind Sie immer per Handy erreichbar und lesen jede SMS-Nachricht gleich nach dem Eintreffen? Das machen viele Handynutzer, da sind Sie in guter Gesellschaft. Aber vielleicht sind Sie auch in schlechter Gesellschaft: Ein Wettbewerber oder ein neugieriger Bekannter könnte jede SMS, die Sie erhalten oder verschicken, automatisch als Kopie bekommen. Wie ist das möglich? Ein Fehler des Mobilfunkbetreibers?

Eine kurze Unaufmerksamkeit reicht

Solche unerlaubten Zugriffe auf Ihre SMS-Nachrichten könnten schnell Realität werden, wenn Sie Ihr Handy einmal unbeobachtet liegen lassen.

Bleibt Ihr Handy versehentlich in der Mittagspause auf dem Schreibtisch liegen, liegt es unbewacht auf dem Besprechungstisch am Messestand, oder vergessen Sie es im Zug, wenn Sie kurz einmal den Waschraum aufsuchen, bieten sich genug Gelegenheiten, Ihr Handy zu durchstöbern.

Ganz ohne PIN-Eingabe ...

Ist das Mobiltelefon wie gewöhnlich eingeschaltet, ermöglichen Sie es einem Dritten, auf Ihre Handy-Daten zuzugreifen, ganz ohne PIN-Eingabe. Ein Datendieb hat dann nicht nur die Chance, Ihr Telefonbuch, Ihre Anrufliste und die gespeicherten SMS und E-Mails auf dem Handy zu lesen. Er kann sich auch einen dauerhaften Zugriff auf Ihre SMS-Nachrichten verschaffen.

Handy-Spionage in weniger als einer Minute

Dazu muss er nur ein kleines Programm auf Ihrem Handy installieren, einen Handy-Spion, den es sogar als kostenlosen Download im Internet gibt. Die Installation selbst dauert keine Minute und hinterlässt keine Spuren, die ein Anwender sehen könnte.

Perfekte Tarnung

Sie finden solch ein Handy-Spionageprogramm weder als Symbol auf dem Handy-Display noch in der Liste der installierten Handy-Programme. Der Handy-Spion tarnt sich perfekt.

Das Aufspielen der Spionage-Software auf Ihr Handy muss nicht über einen PC und ein USB-Kabel erfolgen, wie dies in einem verlassenem Büro in der Mittagspause ohne Weiteres möglich ist. Der Handy-Spion kann auch über Bluetooth kommen, kabellos per Funk in



Unbewachte Handys machen es Spionen leicht, ihre Spionagesoftware unbemerkt aufzuspielen

weniger als 45 Sekunden.

Spionage-Kommandos kommen per SMS

Ist der Handy-Spion erst einmal installiert, muss der Datendieb nur noch Ihre Mobilfunknummer kennen. Alle Befehle an den Handy-Spion kommen als SMS. Für den Handybesitzer bleiben diese SMS-Befehle unsichtbar. Im Gegenzug bekommt der Datendieb dann alle SMS, die Sie von nun an erhalten oder verschicken.

Auf der SMS-Liste, die Ihr Handy speichert, finden Sie diese SMS-Kopien aber nicht. Auch der eigentliche Versand der SMS-Kopien erfolgt ohne jeden Hinweis.

Sperrern Sie die Handy-Spione aus!

Um diese heimtückische SMS-Spionage zu verhindern, sollten Sie

1. Ihr Handy nie unbeobachtet liegen lassen,
2. wenn möglich einen zusätzlichen Passwortschutz einrichten, der nach Aktivierung aus dem Ruhezustand eine Kennwortabfrage startet, und

3. die Bluetooth-Schnittstelle Ihres Handys nur dann aktivieren, wenn Sie sie wirklich brauchen, und sie danach wieder abschalten.

Wie sich Handy-Spione enttarnen lassen

Ob bereits ein Handy-Spion auf Ihrem Mobiltelefon aktiv ist, können Sie auf zwei Wegen feststellen:

1. Zum einen erkennen spezielle Anti-Viren-Programme für Handys und Smartphones diese listigen, kleinen SMS-Spione und vernichten sie.
2. Zum anderen finden Sie die als Kopie an den Datendieb gesendeten SMS-Nachrichten auf Ihrem Einzelverbindungsanweis (EVN), vorausgesetzt, Sie haben keine SMS-Flatrate, bei der es keinen EVN gibt.

Achten Sie immer auf die Zielnummern

Achten Sie deshalb bei der Kontrolle Ihres Einzelverbindungsanweises nicht nur auf die Kosten, sondern auch auf die Zielnummern der SMS-Verbindungen. Bei Firmen-Handys, bei denen die Privatnutzung nicht erlaubt ist, sehen Sie die Zielnummern der SMS ebenso wie bei der Abrechnung für Ihr privates Handy, vorausgesetzt, es wurde kein verkürzter EVN beauftragt.

Wenden Sie sich bei Verdachtsfällen einfach an Ihren Datenschutzbeauftragten!

Sollten Sie den Verdacht haben, dass von Ihrem Handy SMS an eine Ihnen unbekannte Mobilfunknummer geschickt werden, sprechen Sie Ihren Datenschutzbeauftragten an. Er kann Ihr Handy unter Beachtung Ihrer Privatsphäre mit einem Anti-Viren-Programm auf Spionagesoftware hin untersuchen.

Impressum

Thomas Jundel

Anschrift:
mc-Technik
Marienthaler Str. 24
24340 Eckernförde

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

Firmenspionage am Telefon: Wer fragt, kriegt oft auch Antworten

Wir sind freundlich - aber bitte nicht dumm. Das sollte die Leitlinie sein, wenn telefonische Anfragen kommen, die jedenfalls beim zweiten Nachdenken merkwürdig wirken. Wenn Sie die folgenden Beispiele lesen, fragen Sie sich doch bitte einmal, ob Sie auch schon solch merkwürdige Erlebnisse hatten.

Direkten Fragen entkommen Sie leicht

Wie würden Sie reagieren, wenn Sie jemand direkt nach dem Passwort für Ihren PC fragt? Natürlich würden Sie ihm das Passwort niemals sagen, klar. Aber wie reagieren Sie, wenn das Ganze abläuft wie in der folgenden Geschichte?

Um die Ecke fragen führt meist zum Erfolg

Das Telefon klingelt, am Apparat eine junge Frau, vom Typ kommunikative Kollegin. Sie sagt, sie arbeite beim Forschungsinstitut Sonstnochwas, und da mache man gerade eine große Studie zum Thema Passwortsicherheit. Die Presse würde ja laufend darüber berichten, und Sie hätten von der Studie sicher auch schon gehört.

Das haben Sie zwar nicht, aber weil die Frau so nett ist und engagiert wirkt, hören Sie ihr trotzdem weiter zu. Sie stellt allerhand Fragen dazu, was aus Ihrer Sicht bei der Passwortsicherheit wichtig ist und was Sie persönlich dabei beachten. Nach sechs oder sieben Fragen sagt sie schließlich: Jetzt würde ich gern mal sehen, wie Sie das alles praktisch angewandt haben. Ihr Passwort heißt also?

Ob Sie es glauben oder nicht: Die Erfolgsquote ist bei dieser Fragetechnik hoch!

Der freundliche Urlaubstrick ist ein Klassiker

Würden Sie Ihr Passwort herausgeben, könnten Sie es natürlich gleich danach ändern, insofern wäre wahrscheinlich nicht viel passiert. Anders sieht es aus, wenn ein Anrufer vertrauliche Daten aus Ihnen herausgekitzelt hat, die beispielsweise die Konkurrenz nicht wissen soll. Das sind manchmal Dinge, die zunächst wenig spektakulär wirken. Dazu ein Beispiel:

Ein Anrufer sagt, er sei Kunde. Dass Sie ihn nicht kennen, überspielt er mit dem Hinweis, zuständig für ihn sei sonst Ihr Kollege Müller, der aber wohl gerade in Urlaub sei. Das stimmt. Deshalb schöpfen Sie auch keinen Verdacht,

als der Anrufer weiter fragt, ob Ihr Kollege am X-Projekt arbeite. Sie wissen, dass das so ist, und antworten mit ja. Nun kommen inhaltliche Fragen. Um die beantworten zu können, holen Sie sogar Unterlagen her, man will ja nicht unhöflich sein. Erst später stellt sich heraus, dass hier wohl die Konkurrenz recherchiert hat.

Frechheit siegt oft genauso

Während der Anrufer in diesem Beispiel den Einstieg über banale Fragen gewählt hat, arbeitet der nächste Anrufer mit Einschüchterung:

Das Telefon klingelt. Am anderen Ende eine hektische Stimme: "Hier Müller vom Vertrieb. Sie haben doch Zugriff auf die X-Konstruktionspläne." Sie bejahen. Die Antwort: Gott sei Dank, sonst hätten wir jetzt die Katastrophe. Ohne dass Sie zum Nachfragen kommen, fährt der Anrufer fort: "Schicken Sie mir die gleich. Der Kunde tobt, er kündigt uns den Auftrag, wenn er die nicht sofort kriegt, das muss Ihr Kollege verbummelt haben."

Erst jetzt fällt Ihnen auf, dass Sie von einem Herrn Müller im Vertrieb noch nie gehört haben. Sie sagen ihm das. Jetzt rastet er fast aus: "Sie können das ja später Ihrem Gruppenleiter erklären, warum Sie mich nicht kennen. Ich jedenfalls kenne Sie jetzt. Wenn Ihr Getue uns den Auftrag kostet, dann haben Sie einiges zu erklären."

Einige Tipps zur emotionalen Abwehr:

Sie bleiben standhaft? Hoffen wir es! Die drei Beispiele zeigen, dass Anrufer über die emotionale Ebene am leichtesten weiterkommen. Und damit ist auch klar, wie Sie gegensteuern können:

1. Machen Sie sich bewusst, dass das so ist und dass wir alle emotional ansprechbar sind.
2. Ziehen Sie das Gespräch bei unbekanntem Anrufer immer erst auf die Sachebene und geben Sie nicht nach, bis der Anrufer sicher identifiziert ist.
3. Überlegen Sie sich Strategien dafür, wie Sie reagieren, wenn der Anrufer die Oberhand gewinnt. Bestehen Sie etwa darauf, dass Sie zurückrufen werden, und verlangen Sie dazu die Telefonnummer Ihres Gegenübers. Wenn er hier ausweicht, stimmt etwas nicht.
4. Bereden Sie einmal mit Kolleginnen und Kollegen, was schon alles an merkwürdigen Anrufen vorgekommen ist und wie die anderen damit umgegangen sind.

Vorsicht, aber bitte kein Verfolgungswahn

Wenn Sie das beachten, wird Schaden für das Unternehmen vermieden. Mit der Zeit gewinnen Sie dann die nötige Sicherheit, mit solchen Anrufen umzugehen. Dabei sollte man auch bedenken: Nicht hinter jedem etwas merkwürdigen Anruf stecken finstere Machenschaften. Mancher Anrufer verhält sich auch einfach einmal ungeschickt, ohne Böses zu wollen.

Bot-Netze: Hilfe, die PC-Zombies kommen

Sind Sie Spammer oder haben Sie illegale Downloads auf Ihrem Rechner? Nein! Sind Sie wirklich sicher, dass das nicht so ist? Vielleicht sind Sie bereits Teil dunkler Machenschaften im Internet, ohne es zu wissen.

Verseuchung statt Nachrichten

Schon der Besuch einer renommierten Nachrichtenseite im Internet kann ausreichen, um sich einen Computer-Virus einzufangen. Immer mehr Werbebanner auf den Internetseiten sind verseucht und nutzen

Schwachstellen Ihres Webbrowsers aus, um Ihren Computer zu infizieren. Dazu müssen Sie die Online-Anzeigen nicht einmal anklicken.

Es reicht, wenn diese im Browser normal angezeigt werden, und schon könnte sich ein kleines Programm, Bot genannt, installieren.

Fernsteuerung für Ihren Computer

Der Name Bot stammt von der englischen Bezeichnung für Roboter (Robot) und deutet bereits an, was dieses Schadprogramm aus Ihrem Rechner machen möchte: einen ferngesteuerten Computer, einen PC-Zombie. Der Computer gehorcht dann nicht nur Ihnen, sondern auch seinem Meister, der ihm über das Internet Befehle erteilen kann.

Jeder vierte PC betroffen

Dieses Schicksal teilen zahllose Computer. Man schätzt, dass mindestens jeder vierte PC schon mit einem Bot verseucht wurde. Die befallenen Computer bilden sogar ein Netzwerk untereinander, ein sogenanntes Bot-Netz, zu dem mehrere Tausend Rechner gehören können. Diese große Rechnerzahl gehorcht dann gemeinsam dem Bot-Meister, einem Internetkriminellen, der das gekaperte Computernetzwerk zu seinen Zwecken missbraucht. Die Namen der bekanntesten Bot-Netze, Pushdo/Cutwail, Bredolab, Zeus, Waledac und Conficker, klingen wie griechische Götter oder schrille Musikbands, und doch gehören sie zu den größten Bedrohungen im Internet.

Deutschland ist Bot-Europameister

In Deutschland gibt es europaweit die meisten Bot-Netze. Mitunter vermieten Internetkriminelle sogar die von ihnen kontrollierten Bot-Netze. Im Internet kursieren bereits Angebote, ein Bot-Netz für 55 Euro pro Tag für eigene kriminelle Zwecke zu nutzen. Die ferngesteuerten Computer verschicken dann im Auftrag Spam-Mails, laden illegale Software herunter und speichern diese für ihren Meister, sie greifen gemeinsam andere Rechner an und blockieren Webserver mit ihren zahllosen Anfragen, ganz wie es ihr Bot-Meister will.

Verdacht fällt auf die Opfer

Wenn nun die Absender der Spam-Mails identifiziert werden oder nach Raubkopien auf Computern gesucht wird, dann könnten auch Sie in Verdacht geraten, an solchen Internetverbrechen beteiligt zu sein, wenn ein Bot bei Ihnen installiert ist. Sie aber haben keine Ahnung, was Ihr Rechner ohne Ihr Wissen alles angestellt hat.

Schützen Sie sich und Ihre Daten

Wer sich gegen Bot-Infektionen schützt, schützt damit nicht nur die Daten auf seinem

Datenschutz-Quiz: Wie schütze ich mich vor Bot-Netzen?

1. Computer, die Teil eines Bot-Netzes sind, werden ohne Wissen des rechtmäßigen Benutzers für illegale Zwecke genutzt. Wie können Sie einen Bot-Befall erkennen?

- a. Rechner in Bot-Netzen sind immer besonders langsam.
- b. Die Internetverbindung wird stark belastet und verliert an Geschwindigkeit.
- c. Rechner, die von einem Bot befallen sind, verhalten sich meistens unauffällig.

Antwort c ist richtig: Durch die hohe Rechenleistung moderner Computer und die hohe Bandbreite der Internetverbindungen lassen sich Bot-Netze durch den Computernutzer nicht einfach an einer geringen Leistung erkennen. Sollte Ihr Computer besonders langsam sein, sprechen Sie aber trotzdem mit dem Systemadministrator, der durch Netzwerk- und PC-Analysen die Ursache finden kann.

2. Bevor ein PC gekapert werden kann, muss ein Bot installiert werden. Wie passiert diese Infektion?

- a. Bot-Programme kommen per E-Mail, als Dateianhang oder über einen E-Mail-Link, der angeklickt wird.
- b. Bot-Infektionen sind möglich, wenn an den PC ein USB-Stick angeschlossen wird.
- c. Auf verseuchten Webseiten lauern Trojaner, die einen Bot installieren können.

Antworten a, b und c sind richtig. Bot-Infektionen drohen immer dann, wenn Ihr Computer Kontakt mit dem Internet hat oder mit anderen Geräten oder Speichermedien in Verbindung kommt.

3. Bot-Netze gehören zu den größten Datenrisiken im Internet. Jeder Internetnutzer sollte Gegenmaßnahmen ergreifen. Was gehört dazu?

- a. Schützen Sie Ihren PC vor unerlaubten Zugriffen (Passwortschutz).
- b. Alle Dateien, die auf Ihren Rechner gelangen sollen, müssen mit einem aktuellen und professionellen Anti-Viren-Programm und Anti-Spyware-Programm überprüft werden. Das gilt nicht nur für Anwendungsprogramme (.exe), sondern unter anderem auch für Word-, Excel- und PDF-Dateien.
- c. Eine aktive Firewall reicht aus, um einen externen Zugriff zu verhindern.
- d. Die JavaScript-Funktion im Browser sollte deaktiviert werden.

Antworten a, b und d sind richtig. Eine Firewall (Antwort c) ist auch wichtig, reicht allein aber nicht aus.

Computer, die ebenfalls von dem Bot-Meister ohne Schwierigkeiten gestohlen werden könnten. Sie schützen sich auch davor, in den Verdacht zu geraten, Schadsoftware oder gestohlene Daten auf Ihrem Rechner vorzuhalten oder Spam-Mails zu verschicken.

Leider kann nicht jede Anti-Virus-Software die Bot-Angriffe erkennen und abwehren, auch ein Grund dafür, dass es bereits so viele befallene Rechner weltweit gibt. Insbesondere Ihr privater PC könnte unzureichend geschützt sein, wenn Sie keine professionelle Schutzsoftware einsetzen. Es gibt aber kostenlose Programme wie Spybot Search & Destroy, die Ihnen am heimischen Computer wichtige Unterstützung bei der Suche nach

den kleinen Bot-Programmen leisten. Für Ihren geschäftlichen Computer sind kommerzielle Spezialprogramme verfügbar, die meist das Wort "Anti-Bot" im Namen tragen.

Werden Sie zum Bot-Kenner, nicht zum Bot-Opfer

Zusätzlich sollten Sie jedoch besondere Vorsichtsmaßnahmen ergreifen, um das Einschleusen der Bots zu verhindern und Ihren Computer davor zu bewahren, ein Zombie-PC zu werden.

Machen Sie dazu den oben abgedruckten Wissenstest zur Abwehr von Bot-Netzen und erfahren Sie mehr über die gefährlichen Bots.