Infobrief Datenschutz
Ausgabe 04 | 2011

agentia wirtschaftsdienst

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

gehören Sie auch zu den Personen, die gerne telefonieren, im Internet surfen und E-Mails schreiben? Dann sollten Sie sich diese Ausgabe ganz genau ansehen. Im Internet lauern neuartige Gefahren, die Ihren privaten oder dienstlichen Computer bereits bedrohen, wenn Sie sich auch nur eine Webseite ansehen. Damit nicht genug, werden die Methoden zum Knacken von Passwörtern immer besser. Können Ihre Passwörter dem noch widerstehen?

Wie ist es mit Ihnen selbst? Können Sie widerstehen, wenn Ihr Telefon einmal kurz klingelt, oder rufen Sie gleich zurück, um zu erfahren, was der Anrufer wollte? Und wissen Sie eigentlich, ob Sie Ihren dienstlichen E-Mail-Anschluss auch privat nutzen dürfen? Am besten schauen Sie sich dazu gleich den neuen Artikel hier in Ihrer Mitarbeiterzeitung an.

Für Rückfragen stehe ich Ihnen gerne zur Verfügung! Ihr *Udo Wenzel, Datenschutzbeauftragter*

So wird Ihr Passwort (hoffentlich nicht) geknackt

Wenn Ihr Passwort acht Stellen lang ist und nur aus Zahlen besteht, brauchen findige Hacker gerade einmal zehn Sekunden, um es zu knacken. In Zukunft wird es noch schneller gehen, wie die Methoden der Passwortdiebe zeigen.

Beliebt und nutzlos

Wenn es Hackern wieder einmal gelungen ist, eine Passwortdatenbank im Internet zu knacken und zu veröffentlichen, werden Einblicke in die Qualität der genutzten Passwörter möglich. So konnte zum Beispiel der Sicherheitsanbieter Symantec eine Hitparade der beliebtesten Passwörter aufstellen. Auf den ersten drei Plätzen landeten dabei "123456", "Password" und "12345678". Solche Passwörter sind zwar einfach zu merken, sie sind aber völlig nutzlos.

Passwortlänge allein reicht nicht

Wenn Sie nun beim 3. Platz gewisse Ähnlichkeiten zu Ihren Passwörtern feststellen, aber eine andere achtstellige Zahlenkombination gewählt haben, sollten Sie sich nicht in Sicherheit wiegen. Auch solche Passwörter helfen wenig. Denn geübte Hacker knacken sie in gerade einmal zehn Sekunden.

Nutzen Sie für Ihr Passwort Groß- oder Kleinbuchstaben, aber nur sechs Stellen, ist Ihr Zugang sogar nur drei Sekunden geschützt, wenn es zu einem Hackerangriff kommt.

Verwenden Sie dagegen insgesamt acht Groß- oder Kleinbuchstaben für Ihr Passwort, kommen Sie immerhin auf 35 Minuten, die sich ein Hacker bemühen muss.

Sichere Passwörter müssen komplex sein

Angriff mit roher Gewalt

Der einfachste Angriff auf die Passwortsicherheit basiert auf einer schier endlosen Versuchsreihe, bei der die Rechner der Datendiebe möglichst viele Zahlen- und Zeichenkombinationen ausprobieren. Je länger und komplexer das Passwort ist, desto länger braucht man für diese sogenannte Brute-Force-Attacke. Da die verfügbare Rechen-leistung immer höher wird, werden diese Angriffe mit der Zeit immer erfolgreicher werden. Passwortlängen, die heute noch als guter Standard gelten, werden dann nicht mehr ausreichen.

Keine Passwörter aus dem Wörterbuch!

Ein anderer Passwortangriff nutzt Inhalte aus Wörterbüchern. Dabei wird automatisch ein Eintrag nach dem anderen aus den Wörterbüchern ausprobiert, um Ihren Zugang zu Computer, Netzwerk oder Online-Dienst zu knacken. Wenn Sie also Ihr Passwort in einem Wörterbuch finden können, stellt es keinen Schutz dar. Die Rechner der Angreifer sind so schnell im Ausprobieren der Begriffe, dass es nicht lange dauert, bis Ihre scheinbar geschützten Daten offenliegen.

Gefahr durch Übersetzungstabellen

Selbst verschlüsselt gespeicherte Passwörter lassen sich knacken, wenn sie nicht komplex genug ausgewählt wurden. Dazu suchen die Datendiebe nach den verschlüsselten Passwörtern im Netzwerk oder auf dem Rechner ihrer Opfer. Die entsprechenden Verschlüsselungswerte, Hashwerte genannt, versuchen sie dann in das ursprüngliche Passwort zu übersetzen. Die Übersetzungstabellen, die zu den unverschlüsselten Passwörtern führen können, werden auch Regenbogen-Tabellen genannt. Diese Methode des Passwortangriffs ist zwar aufwendig, kann aber leider bei zu einfachen Passwörtern recht erfolgreich sein.

Bevor Sie sich nun neue Passwörter überlegen, sollten Sie sich das **Quiz "Gute Passwörter, schlechte Passwörter" auf Seite 4** anschauen!

Privat gemailt - und tschüss?

Es soll immer wieder vorkommen: Einem Mitarbeiter in einem Unternehmen wird gekündigt, weil er während der Arbeitszeit privat gemailt hat. Gibt es das? Darf der Arbeitgeber überhaupt nachprüfen, ob eine Mail privat ist?

Ihr Problem wird es kaum sein

Solche Sorgen möchte ich einmal haben, sagen Sie sich jetzt vielleicht: Privat mailen während der Arbeitszeit? Ich habe so viel zu tun, dass das schon rein zeitlich gar nicht geht. Verständlich! Aber Sie wissen ja: Andere haben schon einmal etwas Luft, und dann kann die Frage schnell aktuell werden.

Manche sind völlig schmerzfrei

Über das, was in einer niedersächsischen Gemeindeverwaltung möglich war, kann man sich nur wundern. Der stellvertretende Leiter des Bauamtes war wohl wenig ausgelastet. Hemmungslos mailte er in Netzwerken, die der Partnersuche dienen, und das alles natürlich während der regulären Arbeitszeit. 140 bis 150 Mails am Tag waren für ihn der übliche Schnitt. Besonders toll trieb er es an drei bestimmten Tagen.

Es gibt seit Langem eindeutige Spielregeln der Gerichte

Die Spielregeln für privates Mailen am Arbeitsplatz (und für die private Nutzung des Internets insgesamt) sind in der Rechtsprechung seit Langem festgelegt:

- Sofern die private Nutzung des Internets nicht gestattet worden ist, verletzt der Arbeitnehmer durch privates Mailen grundsätzlich seine Pflicht zur Arbeit.

- Aber auch sonst darf eine private Nutzung des Internets die Erbringung der Arbeitsleistung nicht wesentlich beeinträchtigen.

- Die Pflichtverletzung wiegt umso schwerer, je mehr der Arbeitnehmer wegen der privaten Internetnutzung seine Arbeitspflicht zeitlich und inhaltlich vernachlässigt.

Das hat das Bundesarbeitsgericht schon vor mehreren Jahren entschieden.

Ist das private Mailen verboten, kommt das Fernmeldegeheimnis erst gar nicht ins Spiel

Wenn man davon ausgeht, dass er für das Lesen und Bearbeiten jeder Mail, die er von außen bekam, auch nur drei Minuten brauchte, war seine Arbeitszeit an diesen Tagen schon allein damit voll ausgefüllt.

In diesem Fall kam trotz 32 Arbeitsjahren die Quittung

Als die Gemeinde das bemerkte, zog sie natürlich die Konsequenzen. Sie kündigte ihm fristlos. Dass er schon seit 32 Jahren bei der Gemeinde tätig war, half ihm nichts. Es führte lediglich dazu, dass ihm die Gemeinde eine "Auslauffrist" gewährte. Sie hielt also die Frist für ordentliche Kündigungen ein, obwohl es sich um eine fristlose Kündigung handelte.

Das Arbeitsgericht bestätigte die Kündigung. Jedem Arbeitnehmer sei klar, dass exzessives privates Mailen, bei dem für das reguläre Arbeiten keine Zeit mehr bleibt, schlicht und einfach nicht erlaubt sein kann. Das Gericht meinte, dass sei jedem klar - auch ohne vorherige Abmahnung!

Das Fernmeldegeheimnis wird überschätzt

Wie sieht es eigentlich aus, wenn die Frage auftaucht, ob jemand privat gemailt hat, obwohl es nicht erlaubt war? Darf der Arbeitgeber dann nachprüfen, was gemailt wurde? Oder greift hier das Fernmeldegeheimnis ein? Diese Frage wird dann akut, wenn der Arbeitgeber den Verdacht hat, dass Missbrauch getrieben wird und er Unterlagen zusammenstellen möchte, mit denen er eine Kündigung begründen kann.

Falls das private Mailen generell verboten ist, spielt das Fernmeldegeheimnis überhaupt keine Rolle! Es gilt dann nämlich schlicht nicht. Das Fernmeldegeheimnis ist von vornherein nur von Bedeutung, wenn der Arbeitgeber das private Mailen erlaubt hat. Ansonsten kann es ja nur dienstliche Mails geben. Deshalb kann der Arbeitgeber auch verlangen, dass ihm diese Mails vorgelegt werden.

Das Fernmeldegeheimnis gilt nur während des Transports

Im Ergebnis sieht es fast genauso aus, wenn das private Mailen nicht ausdrücklich verboten ist und geduldet wird. Dann sind Mails zwar während der Übermittlung vom Fernmeldegeheimnis geschützt. Aber eben nur während der Übermittlung. Sobald sie auf dem Rechner des Empfängers liegen (egal, ob auf einem zentralen Server des Arbeitgebers oder auf dem PC des einzelnen Mitarbeiters), spielt das Fernmeldegeheimnis wieder keine Rolle mehr.

Listen und Ausdrucke von Mails für das Gericht sind erlaubt

Dann gilt nur noch das generelle "allgemeine Persönlichkeitsrecht". Es ist rechtlich deutlich schwächer als das Fernmeldegeheimnis. Es gilt nämlich nicht absolut, sondern nur nach einer Abwägung der Interessen von Arbeitgeber und Arbeitnehmer. Deshalb hindert es den Arbeitgeber nicht daran, in einem Kündigungsschutzprozess Beweise dafür vorzulegen, dass über jedes vernünftige Maß hinaus privat gemailt wurde. Im Klartext: Listen mit der Dauer von Verbindungen und im Bedarfsfall sogar Ausdrucke von Mails dürfen erstellt und dem Gericht vorgelegt werden.

Alles Theorie?

Aber wie schon gesagt: Für die meisten bleibt das alles Theorie. Denn wer hat heute überhaupt noch die Zeit, private Mails am Arbeitsplatz zu schreiben?

Impressum

Redaktion:
Udo Wenzel
Datenschutzbeauftragter

Anschrift:
agentia wirtschaftsdienst
Dipl.-Inform. Udo Wenzel
10787 Berlin
Telefon: 030 / 2196 4390
E-Mail: udo.wenzel@agentia.de

Angriff aus dem Browser: Kein Klick genügt!

Inzwischen reicht bereits der Besuch einer Webseite, um sich einen Trojaner einzufangen. Sie müssen noch nicht einmal mehr einen verseuchten Link anklicken. Bisherige Vorsichtsmaßnahmen reichen daher nicht mehr aus.

Datendiebe sind flexibel

Erinnern Sie sich noch an die Zeiten, in denen davor gewarnt wurde, den Anhang einer E-Mail zu öffnen, wenn es sich um die Dateiendung .exe handelt? Diese Dateien waren häufig keine praktischen, kostenlosen Programme, die ein netter Unbekannter verschenken wollte, sondern Schadsoftware.

Dann kam die Zeit, in der auch andere Dateiformate wie Word, PDF, Excel und MP3 nicht immer die erhofften Informationen oder Musikstücke enthielten, sondern Schadprogramme.

Dateianhänge wirkten bald nicht mehr wie von den Datendieben gewünscht

Langsam, aber sicher kamen die Dateianhänge in Verruf. Die Empfänger wollten sie nicht mehr so einfach öffnen, die Anti-Viren-Programme entdeckten vielfach den gefährlichen Dateiinhalt. Also ließen sich die Datendiebe etwas Neues einfallen.

Schauen Sie lieber genau hin, bevor Sie einen Link in einer E-Mail anklicken

Bitte klicken Sie hier (nicht)

Statt die Schadprogramme als E-Mail-Anhang zu verschicken, fügten die Internetkriminellen angeblichen Gewinnmitteilungen oder Bestellbestätigungen einen Link bei, auf den man klicken sollte.

Natürlich führte der Link in der Mail nicht zur genannten Webseite, sondern auf eine manipulierte, verseuchte Webadresse. Statt der Bestellbestätigung kam ein Trojaner auf den Computer. Sicherheitsexperten warnten deshalb davor, Links einfach anzuklicken. Doch inzwischen reicht selbst diese Warnung nicht mehr aus!

Ein Blick genügt

Heute kann es schon der erste Blick und nicht erst der erste Klick sein, der zu einer Viren-Infektion des Rechners führt. Man spricht auch von einem "Angriff im Vorbeigehen", einer Drive-by-Attacke. Wenn der Webbrowser die gewünschte Webseite öffnet, lädt er dabei automatisch und ohne Ihr Zutun Zusatzinformationen neben den Texten und Bildern, die Sie als Nutzer sehen möchten.

Gefährliches Design

Unter anderem lädt der Browser Befehle, wie das Layout der Webseite aussehen soll. In diesen Layout-Befehlen kann bereits die Datenfalle stecken. Statt eine Design-Vorlage für die Darstellung der Internetseite zu laden, holt sich der Browser ein Spionageprogramm auf die Festplatte des Rechners.

Erkennt der Anti-Viren-Schutz diese Attacke nicht, werden ab sofort Ihre Passworteingaben und andere vertrauliche Daten mitgeschrieben und an einen Datendieb übertragen.

Besonders gefährlich: seriöse Webseiten

Nun werden Sie sicherlich sagen, dass Sie solch zwielichtige Webseiten, die derart verseucht sind, mit Ihrem Browser gar nicht erst öffnen.

Das ist leider ein Irrtum! Nicht nur die unseriösen Webangebote werden präpariert, sondern insbesondere die scheinbar vertrauenswürdigen. Die Betreiber der Webseiten ahnen oftmals gar nicht, dass ihre Internetseiten verseucht wurden und nun die Besucher angreifen. So erging es kürzlich der berühmten britischen Rundfunkanstalt BBC, die zugeben musste, dass es Hackern gelungen war, einige ihrer Webseiten zu manipulieren. Bereits das Öffnen der BBC-Seiten reichte aus, um den Angriff zu starten.

Studie: 5,5 Millionen infizierte Webseiten in 12 Monaten

Dabei ist BBC nur ein Beispiel: Innerhalb eines Jahres wurden laut Georgia Institute of Technology ganze 5,5 Millionen Webseiten zu Angriffswerkzeugen umfunktioniert, meist ohne Wissen der Betreiber.

Goldene Regeln gegen Drive-by-Attacken

1. Halten Sie Ihren Webbrowser aktuell, indem Sie automatisch nach Browser-Updates suchen lassen.

2. Denken Sie an mögliche Sicherheitslücken in den Browsererweiterungen (Plug-ins) wie Flash-Player oder PDF-Reader, die ebenfalls regelmäßig aktualisiert werden müssen.

3. Installieren Sie nur die Browsererweiterungen, die Sie wirklich brauchen und die betrieblich erlaubt sind, denn Schwachstellen in den Plug-ins sind typische Hintertürchen für Drive-by-Attacken.

4. Nutzen Sie Ihren Rechner nicht mit lokalen Administratorrechten, wenn Sie sie nicht benötigen, insbesondere nicht für den Internetzugang.

5. Begegnen Sie auch Webseiten mit Vorsicht, die von einem seriösen Anbieter stammen.

6. Deaktivieren Sie aktive Inhalte in Ihren Browsereinstellungen, wenn Sie sie nicht zwingend für betriebliche Webanwendungen benötigen.

7. Nutzen Sie auch privat Anti-Viren-Programme mit Echtzeit-Schutz, die die Dateien schon vor dem Herunterladen auf die Festplatte prüfen.

8. Nutzen Sie Link-Scanner, die einen Link auf Schadsoftware prüfen können, bevor Sie ihn anklicken.

Solider Schutz statt Angriff im Vorbeigehen

Selbst wenn Sie vorsichtig sind und nicht einfach alle Links in E-Mails oder auf Webseiten anklicken, sollten Sie umgehend für einen erweiterten Schutz sorgen.

Frühzeitig fragen statt Probleme verschweigen

Beherzigen Sie die Goldenen Regeln gegen Drive-by-Attacken und fragen Sie Ihren Datenschutzbeauftragten/Ihre Datenschutzbeauftragte oder die Systemadministratoren, wenn Sie Probleme mit Ihren Browsereinstellungen haben!

Vorsicht - gefährlicher Rückruf!

Jeder kennt die Situation: Auf dem Handy steht die Nachricht, dass man einen Anruf verpasst hätte. Die Nummer des Anrufers sagt Ihnen nichts. War es ein wichtiger Anruf? Wer weiß, also lieber mal zurückrufen? Vorsicht! Oft nutzen Betrüger das aus!

Höflichkeit und Neugier helfen Betrügern

Wer einen Anruf versäumt hat, will manchmal einfach höflich sein. Manchmal ist er auch nur neugierig darauf, wer angerufen hat. Das Ergebnis ist in beiden Fällen dasselbe: Man ruft lieber einmal zurück! So sagen sich jedenfalls viele - und wundern sich dann, woher auf der Telefonrechnung die Nutzung einer "Mehrwertdienste-Nummer" kommt, bei der zum Beispiel eine Verbindung von wenigen Sekunden Dauer einen Euro kostet.

Betrüger missbrauchen Mehrwertdienste-Nummern

Dahinter steckt dann oft Folgendes: Betrüger besorgen sich einen "Telefoncomputer", mit dem man Tausende von Telefonnummern in kürzester Zeit automatisch anwählen kann. Dann lassen sie sich eine "Mehrwertdienste-Nummer" zuteilen. Bei solchen Nummern kostet jeder Anruf nicht nur die normale Telefongebühr, sondern es wird eine deutlich erhöhte Gebühr fällig.

Solche Nummern sind ein seriöses Mittel, um Gebühren zu verlangen, wenn damit eine echte Dienstleistung verbunden ist (etwa eine spezielle Wettervorhersage für Landwirte, die man so abrufen kann). Aber man kann sie natürlich auch zu einem Betrug missbrauchen. So war das in einem Fall, der schließlich vor die Gerichte kam.

Wer zurückruft, hört eine nutzlose Ansage

Die Betrüger sorgten dafür, dass das Telefon nur einmal klingelte, dabei jedoch in allen Fällen eine Mehrwertdienste-Nummer hinterlassen wurde. Rief jemand diese Nummer zurück, hörte er nur die völlig nutzlose Ansage: "Ihr Anruf wurde gezählt." Dafür wurden ihm dann mindestens 0,98 Euro auf der nächsten Telefonrechnung präsentiert. Wer meint, dass so etwas sicher nicht oft funktioniert, täuscht sich gewaltig!

Die Masche geht zunächst auf

Wie die zuständige Staatsanwaltschaft ermitteln konnte, gingen mindestens 786.000 Rückrufe ein. Den Gewinn, auf den die Täter hofften, kann jeder leicht ausrechnen.

Aber: die zuständigen Behörden reagieren

Womit sie allerdings nicht gerechnet hatten, war die Aufmerksamkeit der Behörden. Obwohl die Täter die meisten Anrufe an den Weihnachtsfeiertagen starteten, reagierte die Bundesnetzagentur sehr rasch. Noch bevor sich die Täter das Geld sichern konnten, wurde der Anschluss der Täter gesperrt und dafür gesorgt, dass die Gebühren auf den Telefonrechnungen nicht auftauchten. Außerdem sorgte die Staatsanwaltschaft für eine Verhaftung der Täter.

Vorsicht ist geboten!

Gilt also: Ende gut, alles gut? Täuschen Sie sich nicht! Oft ist es so, dass auf einen Fall, in dem die Behörden rechtzeitig eingreifen, fünf Fälle kommen, in denen die Masche der Betrüger aufgeht. Seien Sie deshalb lieber vorsichtig, bevor Sie zurückrufen! Wenn Sie eine Nummer auf dem Handy nicht kennen, hat das vielleicht einen guten Grund. Vielleicht stammt sie gar nicht von jemandem, der Sie in einer wichtigen Angelegenheit erreichen wollte. Vielleicht wollte er Sie einfach nur betrügen!

Gute Passwörter, schlechte Passwörter: Machen Sie den Test!

Frage: Wenn niemand im Unternehmen den Namen Ihres Hundes kennt, haben Sie damit ein ideales Passwort, das Sie sich auch gut merken können. Stimmt das?

a) Natürlich, schließlich haben Sie den Namen Ihres Hundes bislang nie erwähnt.
b) Es kommt darauf an, wie ungewöhnlich der Name Ihres Hundes ist.
c) Nein, das stimmt nicht. Tiernamen sind ebenso unsicher wie Begriffe aus einem Wörterbuch.

Lösung: Richtig ist Antwort c). Wenn Sie nun glauben, das wäre jedem klar, irren Sie leider. Jeder Zehnte nutzt den Namen seines Haustiers als Passwort.

Frage: Passwörter müssen sehr lang sein. Welche Zeichen enthalten sind, ist dagegen gleichgültig. Glauben Sie das?

a) Nein, Passwörter sollen nicht nur lang, sondern auch komplex sein, also zum Beispiel aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen.
b) Ja, denn je länger ein Passwort ist, desto länger müssen die Rechner der Datendiebe versuchen, die Kombination zu erraten.

Lösung: Antwort a) stimmt. So brauchen Passwortdiebe für solch komplexe Passwörter bei nur sechs Stellen immerhin zwei Stunden, um sie zu knacken. Achtstellige Zahlenkombinationen dagegen schützen nur zehn Sekunden. Die Passwortlänge ist also wichtig, aber nicht alles.

Frage: Im Internet finden Sie ein Angebot, um die Stärke Ihres Passworts zu testen. Ist das ein guter Service, den man nutzen sollte?

a) Das ist eine tolle Sache; das probiere ich gleich aus und empfehle es den Kolleginnen und Kollegen.
b) Eigentlich keine schlechte Idee. Aber wer kann schon sagen, was der Anbieter des Passwort-Tests mit den Eingaben macht?
c) Interne Passwort-Tests sind sinnvoll, Angeboten aus dem Internet sollte man aber nicht einfach vertrauen.

Lösung: Die Antworten b) und c) sind korrekt. Wenn die Passwortstärke im eigenen Netzwerk bei der Anlage eines Benutzerkontos geprüft wird, ist dies eine wichtige Hilfe. Im Internet könnte dies jedoch auch ein Versuch sein, das Passwort zu stehlen. Besonders gefährlich wird es, wenn der Passwort-Test ohne Verschlüsselung arbeitet.