

2.2 Trotz Passwort Zugriff auf Ihren PC – wie Hacker in wehrlose PCs eindringen!

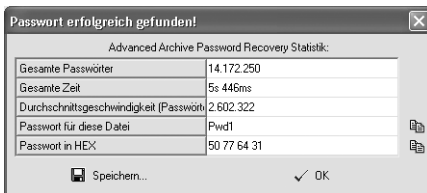
Passwörter gelten als die Sicherheitsfunktion schlechthin. Egal, ob es sich um ein echtes Passwort handelt, das Sie auf einer Webseite eingeben, um Ihre E-Mails zu lesen, es sich um die Benutzeranmeldung für Windows handelt oder Sie am Geldautomaten Ihre vierstellige Geheimzahl tippen – Sie glauben daran, dass die so geschützten Daten und Möglichkeiten keinem Fremden zugänglich sind und Sie sich auf der sicheren Seite befinden.

Dabei bieten die meisten Passwörter nur einen absolut rudimentären Schutz vor neugierigen Mitmenschen. Vor allem der Aufstellungsort und die Art der Zugangsmöglichkeiten machen aus Stand-alone-PCs ein Dorado für Angreifer. Die Geräte sind oft nur wenig geschützt und verfügen über zahlreiche Angriffsmöglichkeiten wie Tastatur, CD-ROM und das Gehäuse. Kann sich der Angreifer Zugang zum PC verschaffen, ist er auch schon so gut wie an Ihren Dateien. Wie dreist so ein Datendiebstahl abläuft, lesen Sie auf Seite 50.

Für die meisten Windows-Systeme gibt es kleine Programme, die den einfachen Passwortschutz, den die Systemanmeldung und der Bildschirmschoner bieten, einfach aushebeln. Dazu muss nur eine CD vorbereitet werden und schon kann der Hacker Gott auf Ihrem Rechner spielen, wie der Bericht ab Seite 66 zeigt.

Passwortschutz ade

Vielleicht gehören Sie aber auch zu den paranoiden Anwendern, die jede Datei verschlüsseln und mit einem Passwort gegen fremde Augen zu schützen versuchen. Kein Problem, denn für fast alle Passwortschutze gibt es das passende Tool, was in wenigen Sekunden den Code knackt und so den Vollzugriff auf Ihre Daten ermöglicht.



Nach nur fünf Sekunden ist das Passwort bekannt

Sogar Passwörter für Webseiten lassen sich ermitteln (s. Seite 93) – längst nachdem Sie den Arbeitsplatz im Internetcafé verlassen haben, verschafft

sich der Hacker dann Zugriff auf Ihr Onlinekonto und wirft einen Blick in Ihre Kontobewegungen.

Passwörter knacken mithilfe des Herstellers

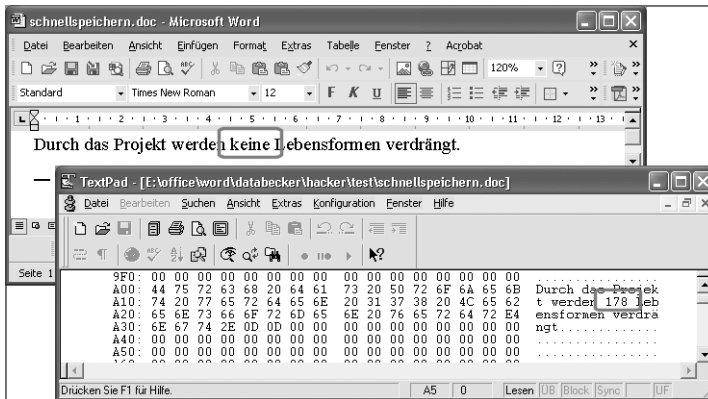
Und auch wenn Sie es nicht glauben wollen, auf Seite 49 erfahren Sie, wie sogar Ihr PC-Hersteller dem Hacker kräftig unter die Arme greift und ihm die nötigen Informationen dank des Internets frei Haus liefert, um sich an Ihrem PC zu schaffen zu machen – vorausgesetzt, Sie sind mal eben ein paar Minuten nicht im Raum, weil Sie Mittagspause machen oder der Servicetechniker vom Kundendienst um ein Glas Wasser gebeten hat.

2.3 Sensible Daten sind urplötzlich verändert – wie vertrauliche Dokumente für jeden sichtbar ins Internet geraten

MS-Word gehört mittlerweile in den allermeisten Firmen zur Standardsoftware für die Textverarbeitung. Egal, was geschrieben werden soll, man greift auf Word zurück und verschickt dann sogar Dokumente in E-Mails, um sich zwischen Kollegen abzustimmen oder an einem Projekt zu arbeiten. Dass dabei ganz leicht mal Firmengeheimnisse preisgegeben werden können oder der Chef mitbekommt, was Sie wirklich von ihm halten, ist oft nicht bekannt.

Aus Bequemlichkeit ist nämlich oft die Schnellspeichern-Funktion aktiviert und die hat es in sich: Alle Änderungen, die Sie an einem Dokument durchführen, werden protokolliert und lassen sich mit wenig Aufwand wieder sichtbar machen (s. Seite 108). Wenn Sie also den vertraulichen Bericht über das letzte Geschäftsjahr benutzen, um durch Löschen einzelner (negativer) Textpassagen den Bilanzbericht für den neuen Geschäftspartner zu erstellen, der Ihre Firma retten soll, dann kann dieser mit einem einfachen Text-Editor nachprüfen, was Sie gelöscht haben und wie es wirklich um Ihre Firma steht. Noch schlimmer, wenn Sie sogar Word-Dokumente auf Ihrer Webseite im Internet als Pressemitteilung o. Ä. veröffentlichen: Jetzt liefern Sie die vertraulichen Informationen jedem neugierigen Anwender frei Haus. Und nicht genug damit: Wenn Sie Pech haben, machen Sie sich vielleicht sogar strafbar durch die Weitergabe eines Office-Dokuments: Enthält dieses nämlich vertrauliche Informationen, die zwar eigentlich nicht sichtbar, aber dennoch enthalten sind, können Sie unter Umständen haftbar für den Verstoß gegen Datenschutzbestimmungen gemacht werden, wenn Sie beispielsweise

so die ärztliche Schweigepflicht brechen oder als Anwalt Parteienverrat begehen.



Mit geeignetem Werkzeug ist es für den Hacker ganz einfach, Textänderungen sichtbar zu machen

Verstecken Sie geheime Daten unauffällig

Wollen Sie Ihre Daten wirklich schützen? Dann kann Steganografie ein Weg sein: Anstatt jeden Hacker gleich mit der Nase auf Ihre verschlüsselten Daten aufmerksam zu machen, verstecken Sie die geheime Botschaft in einer Bilddatei. Auf den ersten Blick schicken Sie dann ein harmloses Bild zu Ihrem Bekannten, dieser weiß aber um die wahre Bedeutung der Bilddatei und kann dann zusammen mit dem entsprechenden Passwort das Dokument, das zwischen den Bildpunkten versteckt wurde, auslesen.

2.4 Total einfach: wie tödliche Viren ganze Firmenexistenzen in den Ruin treiben können

Nicht jeder Virus muss es gleich auf Ihre Festplatte abgesehen haben. Auch wenn die meisten Viren noch immer als Hauptaufgabe die Zerstörung von Dateien einprogrammiert haben, bieten sich in Zeiten des Cyberwars für Viren ganz neue Möglichkeiten.

Da sich Viren heutzutage im Internet in wenigen Stunden über den ganzen Globus ausbreiten, muss ein Programmierer nicht mehr monatelang darauf warten, bis die Virendatei über Disketten und andere Datenträger genügend Verbreitung gefunden hat. Auch Sie als ganz normaler Anwender, der eigent-

lich nur seine E-Mails lesen will, kann dazu beitragen, dass sich ein gefährlicher Virus verbreitet.

Ausgehend von dem Umstand, dass ein Großteil der Anwender mit Windows arbeitet und gern Microsoft-Produkte einsetzt, kann ein Virenbastler sich ganz auf wenige, eng abgegrenzte Produkte konzentrieren. Kein Wunder also, dass 1999 Melissa gewaltige Wellen schlug. Der Virus war so konzipiert, dass er, wenn die Mail mit dem Virus in Outlook geöffnet wurde, sofort an alle Einträge im Adressbuch des Betrachters eine E-Mail mit einer Kopie von sich selbst verschickte. Traf der Virus auf ein gut gefülltes Adressbuch einer größeren Firma, verschickte er sich an so viele Anwender, dass die Server der Firma keine Chance mehr hatten. Denn vor allem in Firmen ist die Gefahr groß, dass der Virus wiederholt an die gleichen Adressen verteilt wird, da ja der Empfänger einer E-Mail auch oft alle anderen Kollegen in seinem Adressbuch führt (ebenso wie der Absender). In Minuten entsteht so ein gewaltiges Datenaufkommen, das nicht nur die alltägliche Arbeit ausbremst, sondern auch enorme Kosten für die genutzten Datenleitungen und die Schadensbehebung verursachen kann. Ein Virens Scanner kann deshalb nur helfen, wenn er auch regelmäßig aktualisiert wird.

Nichts gelernt und wieder Opfer geworden

Dass die meisten Anwender nichts aus ihren Fehlern lernen, zeigte sich ein Jahr nach Melissa, als I-Love-You zuschlug und eine ähnliche Verbreitungsroutine nutzte. In Skandinavien und Großbritannien waren neben Privatfirmen auch die Parlamente betroffen. In Belgien wurden nach Medienberichten fast die Hälfte aller Computer vom Virus heimgesucht. In Spanien erwischte es etwa eine halbe Million Computer – darunter 80 % der Rechner der wichtigsten Firmen sowie mehrere Zeitungen und Fernsehsender. In Italien hatten vor allem kleinere Firmen zu kämpfen. In den USA schlich sich der Wurm in die Netzwerke des Kongresses, des Verteidigungsministeriums, der Zentralbank, der Küstenwache und vieler weiterer Behörden ein. 60 bis 80 % aller Unternehmen waren ebenfalls betroffen.

Ein derartiger Virus kann also nicht nur Firmenexistenzen bedrohen, sondern auch Ihr privates Internetaufkommen so weit steigern, dass Sie nicht mehr Surfen können, weil Ihr PC permanent E-Mails verschicken will. Aber auch zur Spionage oder Sabotage ließe sich ein Virus einsetzen, wenn man ihn gezielt darauf programmiert, bestimmte Firmen zu infiltrieren.

2.5 Nix ging mehr: Mailbomben und übergelaufene Postfächer

Wer heute einen PC hat, der nutzt vermutlich auch immer E-Mail, denn die elektronische Post ist schnell, bequem und billig. Was liegt also näher für einen Hacker, als sich perfide Attacken für diesen Dienst auszudenken? Spam ist da sicherlich noch das kleinste Übel. Auch wenn das Postfach täglich mit Dutzenden von überflüssigen Angeboten für Brustvergrößerungscremes, Potenzmittel, Webdomains und Krediten überläuft: Bis auf Ärger verursachen diese Mails keinen erheblichen Schaden. Natürlich kostet es Sie Zeit und damit Geld, die Mails vom Server abzuholen und zu sortieren, aber mit ein paar Tricks, wie sie ab Seite 367 beschrieben werden, können Sie sich das Leben leichter machen.

E-Mails bedrohen Ihren Posteingang

Anders sieht die Sache dann aus, wenn Sie Ihre normalen E-Mails nicht einmal mehr lesen können. Hat es Ihr böser Nachbar auf Sie abgesehen, dann schickt er Ihnen vielleicht einfach mal eine Mailbombe. In wenigen Minuten hat er sich das passende Programm (s. Seite 369) heruntergeladen und deckt Sie mit Hunderten von Mails so zu, dass Ihr Postfach vollgestopft ist und wirklich wichtige Nachrichten abgewiesen werden und zurück an den Absender gehen, der sich dann wundert. Je nachdem, wie Sie ins Internet gehen, dauert es dann ewig, bis Sie alle Nachrichten heruntergeladen haben, damit wieder Platz frei wird.

Ein Hacker könnte Ihnen aber auch eine E-Mail schicken, die ganz genau auf Ihr E-Mail-Programm zugeschnitten ist. Da Sie ziemlich viel über sich selbst preisgeben, wenn Sie im Internet unterwegs sind oder E-Mails verschicken, weiß der Angreifer, dass Sie vielleicht Outlook Express nutzen, und bastelt so eine Nachricht, die Ihren E-Mail-Client jedes Mal zum Abstürzen bringt, wenn Sie Nachrichten abrufen wollen. Da der Absturz genau dann erfolgt, wenn die Nachricht übertragen wird, bleibt die E-Mail immer auf dem Server und Sie kommen im Zweifelsfall nie wieder an Ihre E-Mails.

Eine harmlosere Alternative wäre eine Mailbombe mit Hunderten von Nachrichten, die Sie dann alle einzeln löschen müssen, aber bei jedem Versuch erst einmal Outlook abstürzen lassen, sodass Sie sehr viel Zeit vertrödeln (mehr dazu auf Seite 177).

Sie haben auch die Faxen dicke und wollen sich nicht länger von Spammern belästigen lassen? Lesen Sie, wie eine Gruppe von Leuten diese Spammer

mit ihren eigenen Waffen schlägt. Vor allem, wenn es darum geht, miese Abzocker, die Sie um Ihr Geld betrügen wollen, an den Pranger zu stellen, ist die Nigeria Connection ein Betätigungsfeld der sog. Scambaiter (dt. etwa Betrüger-Hetzer). Statt Geld zu verlieren in der Hoffnung, Millionen zu gewinnen, lesen Sie, wie die Betrüger ab Seite 353 selbst aufs Korn genommen werden.

2.6 Wie von Geisterhand fährt der PC plötzlich herunter

Nicht nur über das Internet ist Ihr PC Gefahren ausgesetzt – auch in Firmennetzen lauert der Feind und wartet darauf, seinen nächsten Schritt zu machen. Intranets sind zwar praktisch, um mit Kollegen oder Mitgliedern einer WG Daten auszutauschen, Netzwerkgames zu spielen und sich gegenseitig zu helfen, doch ebenso bieten sie zahlreiche Angriffspunkte, da oft zu wenig auf die Sicherheit geachtet wird.

Wer will schon glauben, dass der Kollege drei Büros weiter sich über die eigene MP3-Sammlung hermacht oder Ihre Arbeit der letzten Tage einfach löscht. Wenn Sie wissen wollen, wie Sie Ihre Laufwerkfreigaben sicherer machen, dann lesen Sie ab Seite 410 weiter.

Wissen, was andere sich per E-Mail schreiben

Je nachdem, wie viel Aufwand man als Hacker betreiben möchte und kann, ist sogar Ihr privater E-Mail-Verkehr gefährdet. Mithilfe eines Netzwerk-Sniffers (s. Seite 437) kann man nämlich genau protokollieren, was Sie so den ganzen Tag treiben und auf welchen Webseiten Sie sich aufgehalten haben. Im Intranet findet man dann auch gleich passend dazu die Passwörter, die Sie auf den Webseiten benutzt haben, um sich bei irgendeinem Dienst anzumelden.

So mit Webadresse und Zugangsdaten ausgestattet, kann sich der Hacker still und heimlich am Mobbing gegen Sie beteiligen, indem er beispielsweise eine indiskrete Mail über Ihren Chef unter Ihrem Namen verbreitet.

Manchmal kann man als Hacker den Eindruck gewinnen, Microsoft unternimmt alles, um es diesen Menschen so einfach wie möglich zu machen. Warum sonst wurde in Windows XP eine Funktion integriert, die es einem Anwender ermöglicht, Ihren PC über ein beliebiges Netzwerk fernzusteuern? Wenn Sie Pech haben, sitzen Sie dann vor Ihrem Bildschirm und müssen zur

Tatenlosigkeit verdammt mit ansehen, wie erst alle Ihre Daten geklaut werden und dann die ganze Festplatte gelöscht und als krönender Abschluss der Rechner einfach ausgeschaltet wird.

Wenn Sie die dafür verantwortlichen Gast- und Wartungszugänge nicht brauchen, sollten Sie sich ab Seite 461 darüber informieren, was dagegen hilft.

2.7 Surfen ohne Firewall – und Sie haben nix gemerkt

Sie haben eine Firewall als Schutz gegen ungewollte Kommunikation Ihres PCs mit dem Internet installiert? Sehr gut, denn damit haben Sie schon den ersten Schritt gegen Hacker unternommen. Aber wussten Sie auch, dass Ihre Firewall bereits unterminiert wurde und Sie vielleicht gar nicht mehr geschützt sind?



Symbol von ZoneAlarm im Traybar

Wenn Sie ZoneAlarm benutzen, dann bewegen Sie doch mal die Maus über das Symbol im Traybar. Wenn das Symbol daraufhin verschwindet, hatten Sie die ganze Zeit ungeschützten Verkehr.

Eine Firewall gehört zu den wichtigsten Schutzmechanismen, um sich vor externen Angreifern aus dem Internet zu schützen. Aber auch ungewollte Kommunikation von installierter Software mit dem Hersteller (so genannte Phonehomes) oder mit einem Hacker unterbindet die Software zuverlässig. Kein Wunder, dass die meisten Hacker was gegen Firewalls haben. Selbst Microsoft ist in dieser Beziehung nicht zu trauen, denn die bei Windows XP integrierte Firewall bietet nicht einmal rudimentären Schutz.

Will ein Hacker also die Macht über Ihr System übernehmen, muss er erst einmal an der Firewall vorbei. Da trifft es sich gut, dass ein paar Zeilen Quellcode, wie Sie ab Seite 457 vorgestellt werden, die beliebte Software ZoneAlarm einfach beenden, ohne dass Sie das mitbekommen, da das Symbol im Traybar so lange sichtbar bleibt, bis Sie (zufällig) mit der Maus darüber streichen.

Und während Sie sich noch auf der sicheren Seite wähnen, nimmt der Hacker im Hintergrund Anlauf für seinen Angriff.