02/2003

Februar April Juni August Oktober Dezember

IT-SICHERHEIT
Technik • Organisation • Recht

IT-SICHERHEIT

Technik • Organisation • Recht

Vorwärts, Trojaner!

Spionagesoftware - Angriff und Abwehr

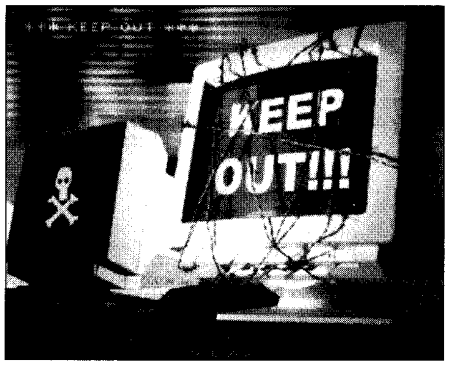
Schwerpunkt-thema: Kommunikations-sicherheit

CeBIT 2003: Innovative Sicherheitslösungen

Datenschutz-Management: Vorabkontrolle und Risikoanalyse

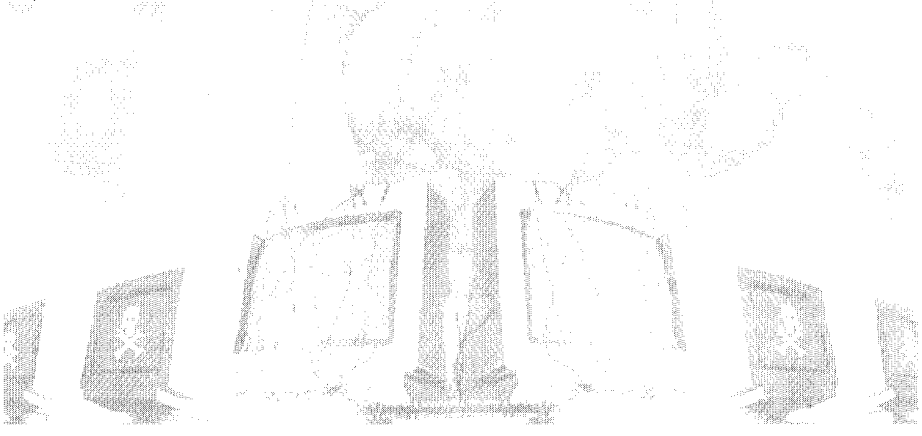
www.it-sicherheit-fachzeitschrift.de

INHALT



Die Trojaner von heute kämpfen nicht mit offenem Visier. Wer sich nicht zur Wehr setzt, bleibt auf der Strecke.

„Die Schaffung und Verbreitung eines Sicherheitsbewusstseins im Mittelstand betrachten wir als eine essentielle Anfgabe"
(Harald Summa, eco-Initiator)



Vorwärts, **Trojaner!**

Wer seinen Feind kennt, kann ihn besser abwehren; dies gilt besonders für Spiongesoftware.

RALF SCHMIDT, MÖHLAU*

Bereits vor dreitausend Jahren benutzten die Griechen der Sage nach ein hölzernes Pferd, um ihre Krieger in das von den alten Göttern als unbezwingbar bezeichnete Troja hinein zu schmuggeln. Pikant und zur damaligen Zeit einmalig war die Tatsache, dass trotz der Warnungen Kassandras die einfachen Bürger von Troja das Pferd mit seinem unheilvollen Inhalt in die Stadt brachten und damit ihren Untergang besiegelten.

Waren es in der Antike Städte, gegen die Krieg geführt wurde, so sind es heute Unternehmen und unternehmenskritische Daten, welche das Ziel sind. Hölzerne Pferde vor den Unternehmenszentralen aufzustellen ist in unserer computerisierten Zeit nicht mehr nötig. Spezielle Computerprogramme sind wesentlich effektiver und bleiben oft unbemerkt.

Da hilft es auch nicht, wenn IT-Verantwortliche die fast täglichen Schreckensmeldungen über neue Programme, sogenannte Viren, welche sich selbst im Unternehmensnetzwerk verbreiten und wichtige Daten zerstören, ernst nehmen und sofort Gegenmaßnahmen einleiten. Gegen die so genannten Würmer, welche nur das Ziel haben sich zu verbreiten und damit die Leistungsfähigkeit eines Unternehmensnetzwerkes beeinträchtigen, sind IT-Verantwortliche auf Grund der Warnungen professioneller Antivirenfirmen relativ sicher.

Computerviren und -würmer haben jedoch den „Vorteil", dass sie schnell, oft innerhalb weniger Stunden, von spezialisierten Firmen erkannt werden und ein Schutz durch die Verwendung aktueller Anti-Virenprogramme relativ einfach ist. Effektive IT-Sicherheitskonzepte können darüber hinaus unternehmenseigene Computer und Computernetze durch die Verwendung spezieller Server- und Firewallsoftware so schützen, dass ein Angriff auf firmeninterne Ressourcen von außen praktisch ausgeschlossen werden kann. Trojaner können jedoch diese Barrieren überwinden und unter Umständen jahrelang unentdeckt in ihrem „Wirtssystem" schlummern.

Angriffsziele erkennen

Wie die antiken Trojer, deren Stadtmauern absoluten Schutz vor feindlichen Angriffen boten, können Führungskräfte heute in der Regel darauf vertrauen, dass mit einem effektiven IT-Sicherheitskonzept unternehmensinterne Daten sicher wären, wenn es in der Computerwelt nicht die Programme geben würde, welche sich an dem antiken Vorbild orientieren.

Ähnlich den Griechen im trojanischen Krieg mit dem hölzernen Pferd versucht heutzutage sogenannte Spy- und Spionagesoftware, auch Trojaner genannt, ein Computersystem von innen her auszuspionieren. Trojaner sind dabei so programmiert, dass sie unbemerkt vom Benutzer und installierter Sicherheitssoftware Daten sammeln, versenden und/oder den unbefugten Fern- (Remote-) zugriff auf den infizierten Rechner ermöglichen. Dabei verfolgen Trojaner folgende Ziele:

- ▷ das Sammeln z.B. von Passwörtern und Kreditkartennummern bis hin zu kompletten Eingaben über die Tastatur,
- ▷ das Versenden von ausspionierten Daten über das Netzwerk des PC (Intranet und Internet),
- ▷ das Kopieren und das Versenden kompletter, sicherheitsrelevanter Dateien,
- ▷ die Übernahme der kompletten Steuerung des PC über das Netzwerk (Remotezugriff) durch Unbefugte.

Im Gegensatz zu Viren und Würmer sind Trojaner so programmiert, dass deren Wirken auf dem infizierten Rechner über Jahre hinweg unbemerkt bleibt. So werden z.B. Texteingaben (Pass- und Kennwörter) mitprotokolliert und zu einem günstigen Zeitpunkt über das Netzwerk unbemerkt an Dritte weitergeleitet – und wenn dieser Dritte die Daten diskret behandelt, so ist es relativ sicher, dass der Trojaner nie erkannt wird. Allein verlorene Ausschreibungen, geplatzte Verträge oder Wettbewerber, welche „zufällig" gleichartige Produkte zur gleichen Zeit anbieten, können ein Hinweis auf das Wirken von Trojaner sein und sollten Alarm auslösen.

Die vielfach von IT-Spezialisten vorgetragene Argumentation, dass jeder Computernutzer selbst dafür verantwortlich sei, welche Programme auf seinem Computer installiert sind, hat nur begrenzt Gültigkeit. Auch Spezialisten sind nicht vor ungebetener Software sicher wie die Berichte über Viren und Würmer beweisen. Problematisch ist vor allem, dass sich Trojaner ähnlich

INHALT:

* Ralf Schmidt ist aktuell als Freelancer in den Bereichen Perfomance Montoring / Netzwerksicherheit und Netzwerküberwachung tätig. Aus seinen früheren Tätigkeiten verfügt er über Erfahrungen als Projektleiter für Linux- / Windows-Netzwerke.

wie die berühmt berüchtigten 0190-Dialer völlig unbemerkt mit zwei Mausklicks im Internet-Browser auf einem Computersystem installieren und ihre Tätigkeit aufnehmen.

Im Gegensatz zu einem 0190Dialer, dessen Auswirkungen an Hand der Gebühren auf der nächsten Telefonrechnung schwarz auf weiß zu lesen sind, kann ein Trojaner Monate ja sogar Jahre auf einem Computersystem unbemerkt Daten sammeln und an Dritte weiterleiten. Selbst der Gesetzgeber hat im Rahmen des zweiten Gesetzentwurfes zur „Bekämpfung des Missbrauchs von 190er-/0900er-Mehrwertdiensterufnummern"[1] zumindest indirekt die Möglichkeit anerkannt, dass Software ohne Wissen und Wollen des Benutzers auf einem Computer installiert werden kann.

Dabei reicht es aus, wenn ein Unbefugter wenige Minuten unbemerkt an den auszuspionierenden Computer herankommt oder der Computernutzer einen E-Mail-Anhang mit dem Absender einer absolut vertrauenswürdigen Person öffnet. Man kann es Paranoia nennen, aber selbst internationale Unternehmen kaufen auch für sicherheitsrelevante Unternehmensbereiche Computer mit (vor-) installierter Software, ohne im Einzelnen nachzuprüfen, ob sich Trojaner oder andere unerwünschte Software darauf befindet. Selbst die Installation frei verfügbarer Anti-Virensoftware[2] kann dazu führen, dass der Computernutzer ohne seine Kenntnis illegale Software und Trojaner sozusagen als „Zugabe" mitinstalliert.

Sicherheitsbewusstsein erzeugen

Obwohl in den meisten Unternehmen mit Windows ein Betriebssystem eingesetzt wird, welches unter anderem durch seine Systemarchitektur Trojaner erst möglich macht, betrachten nach einer Studie der Zeitschrift KES und des Sicherheitsunternehmens Utimaco nur 22% der befragten Unternehmen Spionage als Problem[3]. Ursache des offensichtlich fehlenden Sicherheitsbewusstseins in Bezug auf Spionage ist auch damit zu erklären, dass ein gut programmierter Trojaner seine Tätigkeit effektiv tarnen kann und dass betreffende Unternehmen unter Umständen nie erfahren, dass sie ausspioniert werden. Dies ist auch der Grund, weshalb es international keine (veröffentlichten) Untersuchung über die Kosten bzw. den Schaden, welchen Trojaner und Spionage verursachen, existieren.

Ein erhöhtes Sicherheitsbewusstsein gegenüber Trojanern ist auch deshalb angebracht, da die bereits erwähnte Systemarchitektur des Betriebssystem Windows es ermöglicht, dass ohne Wissen des Benutzers im Hintergrund laufende Programme jede Tastatureingabe, auch Pass- und Kennwörter, unbemerkt mitlesen und aufzeichnen können. Selbst das gerade aktive Programm kann nicht erkennen, ob die Tastatureingaben (hier eine Passworteingabe in der Bankingsoftware Quicken) von einem Trojaner mitgelesen wird. Auch Passworteingabefenster mit der Anzeige von Sternchen anstelle des Passwortes sind vor Trojanern nicht sicher, wie Abbildung 1 verdeutlicht.

Das Risiko besteht hier vor allem in der Tatsache, dass komplette Zugangscodes für Online-Konten mitgelesen und illegal genutzt werden können und dass das Risiko derartiger Software trotz vorhandener Lösungen derzeit allein dem Computernutzer überlassen wird.

Der ideale Schutz von Computerdaten, die physische Trennung des Computers vom Computernetz, ist praktisch jedoch nicht realisierbar und in vielen Fällen noch nicht einmal wünschenswert. Aus diesem Grund gibt es, abhängig vom jeweiligen Sicherheitsbedürfnis, verschiedene Möglichkeiten, um auch Trojanern die Arbeit unmöglich zu machen oder ihnen die Arbeit zumindest erheblich zu erschweren.

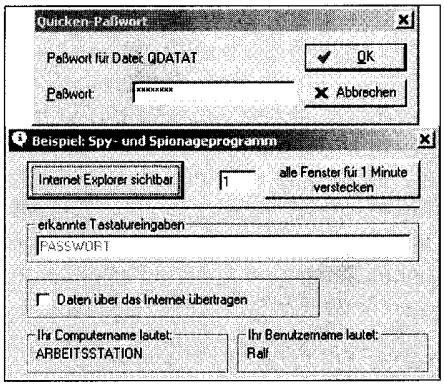


Abbildung 1: Passwort-Spionage

Schutzmaßnahmen ergreifen

Möglichkeiten des Schutzes vor Spionagesoftware und Trojanern sind:

- ▷ Verwendung alternativer Betriebssysteme wie Linux auf Servern und Arbeitsplatzcomputern,
- ▷ Deinstallation des Internet-Explorers und Verwendung alternativer Internet-Browser,
- ▷ Überwachung aller gestarteten Dienste und Programme,
- ▷ Verwendung alternativer Office-Programme wie z.B. Corel- oder StarOffice,
- ▷ Verwendung sicherer Pass- und Kennworteingabemasken vor allem bei Zugriffen über das Internet.

Verwendung alternativer Betriebssysteme

Die Argumentation von Microsoft, Viren und Trojaner sind nicht nur unter Windows bekannt sondern prinzipiell auch unter Linux oder anderen Betriebssystem möglich, ist so falsch nicht[4]. Da Windows jedoch das derzeit meist verbreitete Arbeitsplatzbetriebssystem in Unternehmen ist, richten sich schätzungsweise 70% aller Angriffe gegen Windows oder andere Microsoftprogramme. Hinzu kommt die Tatsache, dass viele Hacker Microsoft als eine Art ideologischen Gegner ansehen und direkt versuchen, Microsoftprodukte zu torpedieren. Schätzungsweise kann ein Unternehmen derzeit 70% aller Sicherheitsprobleme und

[1] http://www.heise.de/newsticker/data/hob-29.01.03-000/

[2] http://www.heise.de/newsticker/data/lab-03.01.02-000/

[3] http://www.heise.de/newsticker/data/pab-12.07.00-001/

[4] http://www.heise.de/newsticker/data/jes-07.11.02-000/

Angriffe allein durch die Verwendung alternativer Betriebssysteme wie Linux vermeiden und sich damit einen erheblichen Teil der Kosten für IT-Sicherheitsmaßnahmen sparen. Der Gewinn an Sicherheit gegenüber Viren und Trojanern, zumindest in sicherheitskritischen Unternehmensbereichen, ist unbezahlbar und reduziert gleichzeitig die Kosten für Soft- und Hardware.

Obwohl durch die Verwendung alternativer Betriebssysteme ein erheblicher Sicherheitsvorteil gewonnen werden kann und wie z.B. bei der Stadtverwaltung von Schwäbisch Hall auf Grund der Umstellung auf Linux mit einem erheblichen Einsparpotenzial[5] gerechnet wird, sollten auch nicht die Schwierigkeit[6] einer Betriebssystemumstellung und die Aufwendungen für die Aus- und Weiterbildung der Mitarbeiter vernachlässigt werden.

Speziell für Anwender, welche auf Microsoft Windows nicht verzichten wollen oder können, stellt das Betriebssystem Windows XP ein Sonderfall dar. Bereits in der Standardinstallation der Home- und der Professional Version sind sieben Funktionen aktiviert, welche unter die Rubrik „unbemerktes Daten sammeln" fallen. Viele Computernutzer fühlen sich unwohl, wenn ein Betriebssystem wie Windows XP ungefragt eine Internetverbindung aufbaut und Daten verschickt. Dies ist in etwa damit zu vergleichen, als würde ein Schreibtischhersteller ungefragt Mitarbeiter zu Ihnen ins Büro schicken und Ihren Schreibtisch durchsuchen. Würden Sie die Erklärung: „Er schaut nur nach eventuell defekten Schrauben" einfach so hinnehmen und ihn gewähren lassen?

Aber auch ohne den Wechsel auf ein alternatives Betriebssystem wie Linux lässt sich bei der neuesten Betriebssystemvariante Windows XP die eigene Sicherheit durch das Abschalten von „neugierigen" Funktionen erhöhen. So aktiviert Windows XP bei der Installation standardmäßig folgende Programme bzw. Betriebssystemfunktionen, welche für die Arbeit des Betriebssystems Windows nicht notwendig sind aber (System-) Daten an Microsoft versenden. Funktionen dieser Kategorie, die ohne Nachteile für den Systembetrieb abgeschaltet werden können, sind unter anderem

Alexia – überwacht das gesamte Surfverhalten des Benutzers um die so genannten „VerwandtenLinks" zu finden. Dabei werden die IP-Adresse, Informationen über den Browser, die vollständigen Internetadressen der besuchten Seiten, der Zeitpunkt der Aufzeichnung und eine eindeutige Alexia-Cookie-Nummer an Microsoft übermittelt.

Uhrzeitsynchronisation – Jeder PC-Nutzer, jedes Unternehmen sollte selbst prüfen, ob Microsoft täglich über den Microsoft-Zeit-Server erfahren soll, wann er und seine Mitarbeiter mit der Arbeit beginnen. Wer diese Funktion als sinnvoll betrachtet fährt mit Sicherheit besser, einen eigenen Zeitserver im Intranet einzurichten.

Aktivierungstest – Mit Hilfe des Aktivierungstests wird überprüft, ob die Windows-XP-Installation bereits per Telefon/Online aktiviert ist oder nicht. Da während dieses Tests Daten an Microsoft übermittelt werden, sollte man dabei nicht online sein.

Automatisches WindowsUpdate – Das WindowsUpdate greift automatisch auf das Internet zu, prüft regelmäßig, ob neue Updates vorliegen. Welche Informationen an Microsoft übermittelt werden, ist nicht bekannt.

Deinstallation des Internet-Explorers und Nutzung alternativer Internet-Browser

Selbst Firewalls, Anti-Viren- oder Schutzprogramme wie z.B. ZoneAlarm sind zumindest unter dem Betriebssystem Windows und bei der Verwendung des Internet Explorers von Microsoft nicht in der Lage, die Aktivität von Trojanern in jedem Fall zu erkennen. So bietet der von Microsoft angebotene Internet Explorer die Möglichkeit der Fernsteuerung. Das heißt, ein Trojaner kann selbständig ein für den Benutzer unsichtbares Internet Explorerfenster öffnen und Daten versenden während der Benutzer nichts ahnend im Internet surft. Schutzsoftware wie ZoneAlarm und andere Firewalls können dabei nicht unterscheiden, ob die Daten vom Benutzer oder von einem Trojaner versendet werden.

Damit ist der Internet Explorer von Microsoft bezüglich der Sicherheit das schwächste Glied in allen Windows Betriebssystemversionen. Andere Browser verfügen standardmäßig nicht über die Möglichkeit der Ansteuerung durch andere Programme und können deshalb nicht zur unbemerkten Versendung von Daten genutzt werden. Der Umstieg auf alternative Browser ist dazumal kostenlos.

Überwachung aller gestarteten Dienste und Programme

Derzeitige Überwachungsprogramme wie z.B. ZoneAlarm überwachen sehr effektiv, wenn auch nicht vollständig, die Zugriffe des eigenen Computers auf das Netzwerk und erkennen zuverlässig, ob ein unbefugter Zugriff vom Netzwerk her versucht wird. Der Angriff auf einen Computer mittels Trojaner erfolgt jedoch nicht von außen sondern durch eine unbewusste oder unaufmerksame Aktion des Benutzers. Speziell unter Windows existieren Softwarelösungen mit der Möglichkeit der Überwachung aller auf einem Computer gestarteten Programme und Dienste und sind ein effektiver Schutz vor dem Start unerwünschter Software und Trojaner. Eine Warnmeldung evtl. direkt an den Systemadministrator, wenn ein unbekanntes Programm startet, ergänzt die Überwachungsfunktion. Leider ist diese Art der Überwachung noch nicht allgemein üblicher Standard.

Verwendung alternativer Office-Programme

Immer wieder wird in Warnungen vor Viren und Würmern darauf hingewiesen, dass diese Programme sich mit Hilfe von Microsoft-Software verbreiten. Sogenannte Makroviren, welche die VisualBasic Scriptsprache von MS Office verwenden, sind keine Seltenheit. Makroviren, welche z.B. die Script-Funktion von alternativen Office-Lösungen wie StarOffice benutzen, sind

[5] http://www.heise.de/newsticker/data/anw-26.11.02-000/

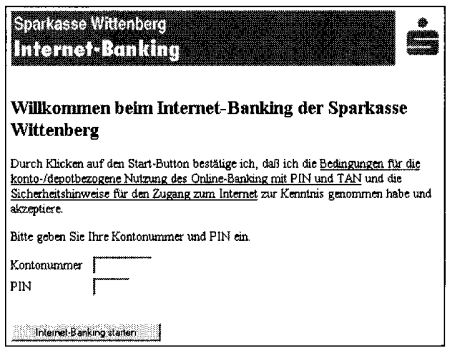
[6] http://www.heise.de/newsticker/data/odi-27.02.03-001/

zumindest dem Autor nicht bekannt. Aus diesem Grund bietet die Verwendung alternativer Office-Programme derzeit einen 100%igen Schutz vor Makroviren, welche sich z.B. auf die Script-Funktionen VBA von Outlook & Co. spezialisiert haben. Mit der Einbindung der VisualBasic Scriptsprache in das Betriebssystem Windows XP sind in Zukunft aber auch systemweit aktive Trojaner auf VB-Basis denkbar.

Verwendung sicherer Pass- und Kennworteingabemasken

Derzeitige Online-Banking-Angebote wie zum Beispiel von der HypoVereinsbank (Abbildung 2) oder den Sparkassen (Abbildung 3): nutzen noch immer ausschließlich die als sicherheitskritisch einzustufende Eingabe von Pass- und Kennwörtern per Tastatur und sind dadurch außerordentlich anfällig für Trojaner, welche Zugangsdaten für das Online-Banking sammeln und an unberechtigte Dritte weiterleiten. Dabei wäre es den Anbietern von Online-Banking-Angeboten bereits durch einfachste Änderungen am Seitenaufbau möglich, die Eingabe sicherheitsrelevanter Daten wie Pass- und Kennwörter vor dem Auslesen durch Trojaner zu schützen. Ein Programmieraufwand von 15 Minuten, und der Sicherheitsstandard des Online-Angebotes würde sich im Interesse der Bankkunden erheblich erhöhen.

Eine Möglichkeit besteht u.a. in der Verwendung der am 30.06.02 unter dem Aktenzeichen 202 10 080.4 beim



Deutschen Patent- und Markenamt eingereichten Lösung zur Eingabe sicherheitsrelevanter Daten. Diese Lösung verhindert außerordentlich effektiv, dass Eingaben von Zugangsdaten per Tastatur mitgelesen und über ein Netzwerk an Unbefugte versendet werden. Bereits in der einfachsten, mit HTML und Javascript programmierten Lösung wird verhindert, dass Trojaner die eingegebene Kreditkartennummer erkennen und an unbefugte Dritte senden können, was einen außerordentlich effektiven Schutz vor dem Missbrauch der Daten darstellt (Abbildung 4).

Von dieser Lösung können alle Programme, welche die Eingabe von Pass- und Kennwörtern erfordern, profitieren, wobei weitere Schutzmaßnahmen z.B. vor Bildschirmfotos die vorgestellte Lösung ergänzen und in diese integriert werden können. Aus diesem Grund sollte bei der Anschaffung neuer oder bei einem Update vorhandener Software unbedingt geprüft

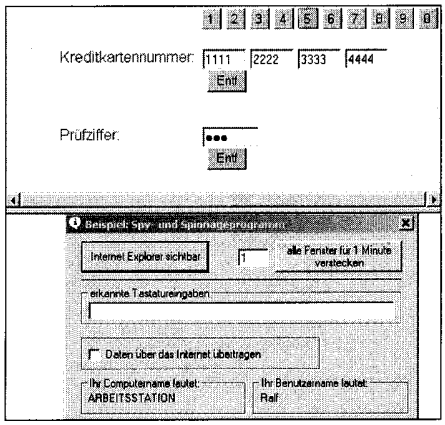
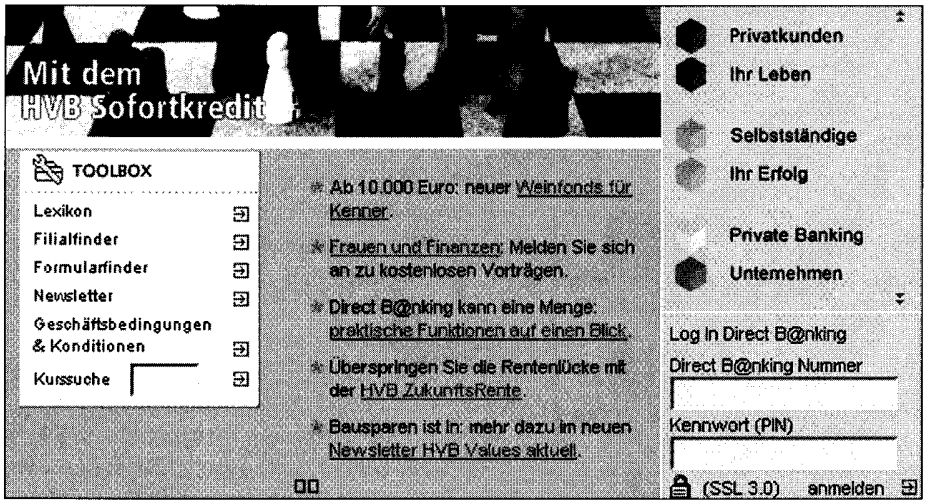


*Abbildung 4: Sichere **Eingabe** von Zugangsdaten*

werden, ob eine sichere Eingabe von Pass- und Kennwörtern möglich ist.

Zusammenfassung

Insgesamt kann festgestellt werden, dass es zum Ausspionieren von Daten und sicherheitsrelevanten Daten keines Angriffes von außen bedarf. Viele Unternehmen schützen ihr System außerordentlich effektiv gegen Angriffe von außen, sind aber gegen Spionage durch Trojaner von innen her relativ machtlos, zumal diese Spionage unter Umständen nie entdeckt wird. Gegen Angriffe von innen durch Trojaner schützt derzeit auch die beste Firewall nicht, vor allem dann nicht, wenn unternehmensintern der Internet Explorer verwendet wird. Auch der Hinweis vieler Unternehmen auf restriktive, interne Vorschriften in Bezug auf Softwareinstallation und ein eventuell geltendes generelles Verbot, fremde Software zu installieren, führt nur zu einer trügerischen Sicherheit. Selbst der deutsche Gesetzgeber hat mit der Telekommunikations-Verbraucherschutzverordnung vor allem im Zusammenhang mit den bereits erwähnten 0190-Dialern indirekt die Möglichkeit anerkannt, dass Software auch gegen den Willen und ohne Wissen des Benutzers auf einen Rechner installiert werden kann. Allein ein umfassendes Security-System im Unternehmen verbunden mit einer regelmäßigen Überprüfung der Computer zumindest in sicherheitsrelevanten Unternehmensbereichen bis hin zum Verzicht auf Risikosoftware kann die Sicherheit der Daten in Unternehmen gewährleisten. □



*Abbildungen 2 und 3 (oben): Online-Banking: **Zugangsdaten***