DAS bhv TASCHENBUCH

Windows 7 Sicherheit

Das Anti-Scareware-Buch

von
Andreas Winterer

1. Auflage

Thematische Gliederung:

Computersicherheit

mitp/bhv 2011

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 8266 7547 8

Inhaltsverzeichnis: Windows 7 Sicherheit – Winterer

Windows 7 Sicherheit

Dieses Buch richtet sich an Einsteiger und Fortgeschrittene, die die Sicherheitsrisiken an ihrem Rechner kennen lernen wollen oder bereits konkrete Befürchtungen haben und die daran interessiert sind, mit möglichst wenig Aufwand und Kosten möglichst viel dagegen zu tun.
Das Buch versteht sich als nachvollziehbare Anleitung für Windows 7 und seine Sicherheitsfunktionen. Es bemüht sich darum, genau aufzuzeigen, was der Leser tun kann, um die Sicherheit seines Rechners zu erhöhen. Der Autor schlägt nur Werkzeuge vor, die er selbst mehrfach verwendet hat und die allgemeines, gewachsenes Vertrauen genießen.

EINFÜHRUNG
Gefährliche Zeiten am PC, Relevanz von Sicherheitsproblemen, alltägliche Horrorszenarien, eine neue Art von Sicherheit

DIE ANGREIFER, DIE BEDROHUNG
Bedrohung durch Hacker, moderne Hacker, typische Hacks, WLAN Hacking, Suchmaschinen-Hacking, Social Engineering, Online-Betrug, gefährliche Fehler: Exploits, Viren, Würmer, Trojanische Pferde, Keylogger, Scareware, Botnetze

WINDOWS 7 SICHERHEIT
Sichere Benutzerkonten, sichere Windows-Netze, Sicherheit im LAN, Sicherheit im WLAN, Windows-7-Firewall, eingebauter Windows-7-Virenschutz, Verschlüsselung, Backup, automatische Updates, weitere Sicherheitsfunktionen

GRATIS-UPGRADE SICHERHEIT
Kaufberatung Virenscanner, MSE: Microsoft Securtiy Essentials, avast! Free Antivirus, Virenscanner mit Echtzeitschutz, Virenscanner ohne Echtzeitschutz, spezielle Schutztools, Trial-Versionen kommerzieller Antiviren-Produkte, sichere Anwendungen

ANTI-CRASH-UPGRADE: BACKUP
Verschiedene Backup-Typen, Alternativen zum Windows-Backup, Backup Service Home, Image-Alternative: Paragon Backup & Recovery Free, Online-Backup, Online-Backup vs. Festplatte, Backup-Strategie

PASSWORTSICHERHEIT
Unsichere Passwörter vermeiden, sichere Kennwörter wählen, Online-Passwort-Generatoren, kleine Tricks für höhere Komplexität, Passwörter sicher verwenden

VERSCHLÜSSELUNG
TrueCrypt, Anti-Diebstahlprogramme, Verschlüsselungstipps für Office, Web, Mail

SICHERES LÖSCHEN
Dateien und Festplatten sicher löschen, Gebrauchsspuren entfernen, spurenfrei surfen

ANONYMITÄT
Anonymisierende Web-Proxys, Open Proxy, Tor: The Onion Router, Cyberghost, Erfolg der Anonymisierung prüfen

Probekapitel & Infos
erhalten Sie unter:
info@bhv-buch.de
www.bhv-buch.de

Regalsystematik:
Betriebssysteme, Sicherheit
ISBN 978-3-8266-7547-8

(D) € 19,95

Windows 7 Sicherheit

bhv Das bhv Taschenbuch

Andreas Winterer

Windows 7 Sicherheit

Über 700 Seiten
€ 19,95 (D)

7547

KAPITEL

1

Einführung: Sicherheit auf Ihrem PC

Sicherheit ist mehr als nur ein installiertes Antivirenprogramm. Das wird spätestens dann klar, wenn man einen genaueren Blick auf die vielfältigen Möglichkeiten wirft, durch die man seine Daten komplett verlieren oder in die Hände Unbefugter geben kann.

Einführung: Sicherheit

Dieses Buch richtet sich an Einsteiger und Fortgeschrittene, die Sicherheitsrisiken zumindest erahnen oder konkrete Befürchtungen haben und die daher daran interessiert sind, mit möglichst wenig Aufwand möglichst viel dagegen zu tun.

Dabei möchte ich eine Handvoll Dinge unter einen Hut bekommen:

- **Keine Panikmache, kein Bullshit:** Natürlich muss man auf dem Fischmarkt etwas lauter werden, wenn man seine Ware an den Mann bringen will. Klappern gehört zum Handwerk, daher ist es Tradition, die Gefahren am Computer zu überzeichnen. Dieses Buch versucht, darauf zu verzichten. Das fällt leicht, denn der Medienhype gilt meist nur den spektakulären Sicherheitsproblemen. Doch im völlig unspektakulären Raum eines Privatmenschen oder Selbstständigen steckt noch genug Gefahrenpotenzial, um auf den Hype verzichten zu können. Nehmen Sie es mir trotzdem nicht übel, wenn ab und zu von „Killer-Programmen“ die Rede ist – korrekte Begriffe wie „Maliziöser Code auf mobilen Endgeräten“ sind oft etwas sperrig.
- **Konkret und praktisch:** Das Buch versteht sich als nachvollziehbare Anleitung für Windows 7 und seine Sicherheitsfunktionen. Es bemüht sich um eindeutig benannte Tools, die Sie nutzen können, um die Sicherheit weiter zu erhöhen. Ich schlage nur Werkzeuge vor, die ich auch selbst mehrfach verwendet habe und die allgemeines, gewachsenes Vertrauen genießen.
- **Kostenlos:** Die meisten der Features, Erweiterungen, Lösungen und Tools in diesem Buch sind in irgendeiner Form „kostenlos“ zu haben. Ich halte das für wichtig, denn nicht jeder – Schüler, Studenten, rein nichtkommerzielle Benutzer – hat das Geld für Sicherheitssoftware. Ich appelliere aber an alle, die ihren PC beruflich nutzen und damit Geld verdie-

nen, jeweils den Kauf der kommerziellen Vollversionen der Programme in Erwägung zu ziehen, denn auch der Kampf gegen digitale Probleme ist aufwendig und hat viele Mäuler zu stopfen.

Abgesehen von dem Kapitel, das sich speziell mit den Sicherheitsfeatures von Windows 7 beschäftigt, funktionieren fast alle erwähnten Tools und Methoden meist auch mit Windows Vista oder XP.

Dieses Buch soll etwas Licht ins Dunkle der Windows-7-Sicherheit bringen. Sie werden erfahren, welche Gefahren derzeit wirklich akut sind und welche nicht. Das Buch gibt Tipps und leistet Hilfe zur Selbsthilfe. Ich nenne die Schutzprogramme nicht nur, ich erkläre auch, wie sie funktionieren – und warum sie es manchmal nicht tun oder möglicherweise überhaupt nicht sinnvoll sind.

Folgen Sie mir also auf dem Weg ins Reich der Viren, Würmer, Trojanischen Pferde, Botnetze und Zombie-PCs und erfahren Sie (fast) alles über die Möglichkeiten, sich gegen Hacker, Spione und Online-Kriminelle zur Wehr zu setzen.

Gefährliche Zeiten am PC

Seitdem wir mit unseren PCs und Notebooks über den Informations-Superhighway surfen, ist in Sachen Sicherheit die Hölle los: Noch bevor Sie diese Seite zu Ende gelesen haben, werden Tausende von Rechnern infiziert – und andernorts auch wieder von digitalen Schädlingen aller Art befreit. Tausende von Spam-Mails werden verschickt, um über die darin enthaltenen Links Benutzer auf gefälschte Websites zu locken, um Tausende von Zugangsdaten abzugreifen oder die Rechner en gros mit Malware zu infizieren.

Malware ist heute der Überbegriff für alles, was als Software daherkommt (*ware*) und dabei „schädlich“ (*malicious*) ist: Viren, Würmer und Trojaner ebenso wie Spionageprogramme. Mehr über die verschiedenen Malwares erfahren Sie im nächsten Kapitel

Allerdings ist die Zeit vorbei, in der vor allem Computerviren und Computerwürmer Schlagzeilen machten, indem sie in kürzester Zeit Millionen von Rechnern infizierten. Das passiert heute nur noch selten.

Die Bedrohungslage hat sich geändert und ist noch vielfältiger geworden. Noch immer sind Schadprogramme in Massen unterwegs. Doch immer öfter dienen sie vor allem als Grundlage für neue Probleme des digitalen Zeitalters, vor allem Online-Betrug, Online-Bankraub und Identitätsdiebstahl.

Die Angreifer sind längst nicht mehr die gleichen wie noch vor 10, 15 Jahren. Damals waren es vor allem verspielte Hacker, Cracker und Programmierer, die auf der Suche nach Ruhm, aus verantwortungsloser Freude an der Zerstörung oder auch nur aus purem Spaß daran, es zu können, zerstörerische Programme entwickelten. Heute stecken hinter Angriffen nur noch selten unprofessionelle „Skript-Kids“, also Möchtegern-Hacker mit geringen technischen Fähigkeiten, die sich mit Anleitungen (Tutorials) aus dem Internet und den von anderen entwickelten Fertig-Tools einen Spaß erlauben wollen.

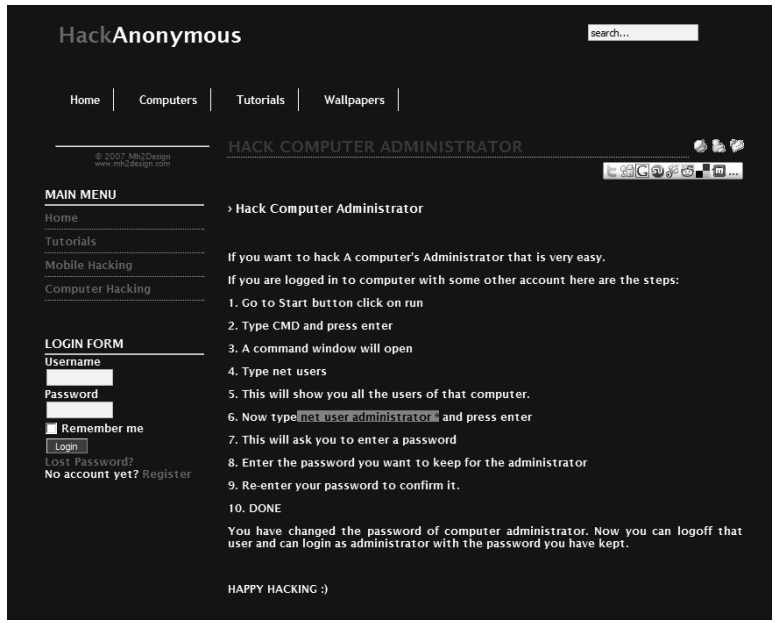

Abbildung 1.1: Typisches Hacker-Tutorial für „Skript-Kids“

Die weitaus größere Gefahr geht längst von einer neuen Art der professionellen und teils auch organisierten Kriminalität aus. Diese Leute haben sich ihr Know-how nicht selbst erarbeitet oder in Tutorials zusammengelesen, sondern sie kaufen es als Dienstleistung bei Hackern ein, die ihrerseits aus ihrer Leidenschaft einen gut bezahlten Beruf gemacht haben.

Früher legten *Hacker* sehr viel Wert darauf, sich selbst als nicht kriminell darzustellen. Inzwischen haben sich neue Begriffe etabliert: *White-Hat-Hacker* oder *Ethical Hacker* besitzen alle Fähigkeiten, die für den Einbruch in Datensysteme aller Art nötig sind, setzen sie aber nur zur Aufklärung ein (offiziell etwa der Chaos Computer Club) oder um im Auftrag eines Unternehmens Gegenmaßnahmen zu erarbeiten (IT-Sicherheitsberater). Ihnen gegenüber stehen die *Black-Hat-Hacker*, die nur Böses im Sinn haben, meist aus rein

kommerziellen Gründen, zunehmend auch aus politischen Motivationen (China, Al-Kaida etc.). Zwischen ihnen stehen technisch fortgeschrittene Menschen, die ihr Wissen sowohl für gute als auch für schlechte Ziele einsetzen und sich daher in einer Grauzone befinden: die *Gray-Hat-Hacker*. Wenn in diesem Buch nur von einem „Hacker" die Rede ist, dann eigentlich stets von einem Gray-Hat-Hacker.

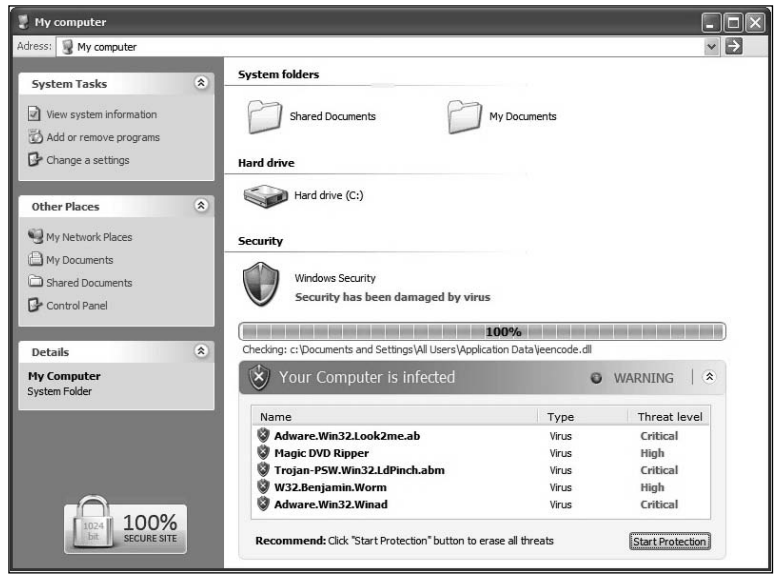

Abbildung 1.2: Geschäftsmodell Computerkriminalität: Scareware

Man muss sich vor Augen halten, dass man es hier mit einem Geschäftsmodell zu tun hat. Mit Sicherheit wird viel Geld verdient: Schätzungen der Studie „Die IT-Sicherheitsbranche in Deutschland" gehen von einem weltweiten Markt von jährlich etwa 33 Milliarden Euro aus. Doch auch mit Unsicherheit verdienen Organisationen mit mafiösen Strukturen Geld, zum Beispiel mit „gefälschten" Antivirenprogrammen, sogenannter *Scareware*, von der noch zu hören sein wird, oder bei Angriffen auf Online-Banking, wo zwar nicht die Bank überfallen, aber

eine große Zahl von Personen um ihr Geld gebracht wird. Gehackt werden große Unternehmen immer öfter nur deshalb, um an Datensätze heranzukommen – denn die Adressen lassen sich an Spammer verhökern und die Kreditkarten-Nummern an darauf spezialisierte Hehler verscherbeln. Die Möglichkeiten sind vielfältig.

Die Masse macht's: Auf eine Spam an Millionen von deutschen PC-Benutzern müssen nur wenige Promille reagieren, damit sich der Raubzug am Ende für die Online-Kriminellen lohnt. Und es kann jedem passieren, Profis ebenso wie Einsteigern. Die Banken kennen inzwischen das Problem (auch wenn sie nicht gerne darüber sprechen) und daher muss niemand fürchten, dass er plötzlich wie im Hollywood-Film eine negative Million auf seinem Konto „hat".

Doch erfahrungsgemäß ist der Ärger groß genug, wenn man sich die derzeit noch recht typischen 400 bis 4.000 Euro wiederholen muss. Und immer öfter ist auch das nicht mehr möglich: Bei der Betrugsmasche „Scareware" versucht man, Ihnen ein nicht funktionierendes Sicherheitsprogramm anzudrehen. Sie bezahlen es ganz legal für Preise um die 50 Euro, wie jede andere Software auch. Das lässt sich dann nicht mehr so einfach rückgängig machen. Und wer geht für 50 Euro zum Anwalt, wenn der Wohnsitz der Firme schwer zu finden ist (und sich dann als „irgendwo im Ostblock" herausstellt)?

Haben wir überhaupt Sicherheitsprobleme?

Fragt man einen durchschnittlichen Anwender, ob er das Ziel einer Computer-Attacke ist, lautet die Antwort meist „Nein, wozu auch?". Das gilt nicht nur bei Privatpersonen, sondern auch für Selbstständige und erstaunlicherweise für viele Unternehmen.

Man könnte sich nicht stärker irren. Denn jeder Anwender ist heute eine potenzielle Zielscheibe für vielfältige Attacken.

- Selbst wenn Sie nur in einem einzigen Shop mit Ihren Bankdaten eingekauft haben, ermöglicht das auch Hackern, prinzipiell mit Ihren Bankdaten zu arbeiten. Dazu muss man sich Ihre Bankdaten gar nicht bei Ihnen holen: Man holt sie sich einfach beim Shop. Denn der hat Tausende davon, und wie die Geschichte lehrt, geht er selten gut damit um.
- Wenn Sie „bloß" bei Facebook oder Twitter sind, dann sind Sie ebenfalls interessant, weil man über Ihr gehacktes Konto Links auf verseuchtes Material oder Phishing-Websites verschicken könnte – und dabei die besondere Vertrauensstellung ausnutzen kann, die mit Social-Media-Verbindungen einhergeht.
- Und wenn Sie ein Notebook, Netbook oder einen USB-Strick benutzen, dann bewahren Sie auf ihm Daten auf, die einen Teil Ihrer Privatsphäre darstellen. Fast immer sollen diese auf keinen Fall in die falschen Hände gelangen. Und doch passiert das ständig.

Das bedeutet natürlich nicht, dass die Hacker schon in Ihrem Keller sitzen.

Es bedeutet nur: Bloß weil Sie nicht James Bond sind, heißt das nicht, dass niemand die Geheimnisse auf Ihrem USB-Stick klauen will. Auch ganz normale Bürger und brave Familienväter haben etwas zu verbergen und eine Privatsphäre zu wahren, Selbstständige sind oft sogar abhängig von den auf dem PC gespeicherten Daten.

Ich führe daher in diesem Buch drei archetypische Personen ein, um das Gefährdungspotenzial etwas einfacher darzustellen.

Der Familienvater

Der Familienvater ist der einfache Anwender ohne größeres Know-how. Er kauft ab und zu etwas im Web ein, hat hier und da ein Benutzerkonto und hat letztlich bei einer Datenpanne nicht viel zu verlieren, zumindest auf den ersten Blick. Auf den zweiten sind es dann doch zum Beispiel digitale Erinnerungen,

die er verlieren kann, und ganz allgemein kann seine „digitale Identität“ das Ziel eines Angriffs sein.

Wichtig ist für diesen Nutzertyp vor allem, seine Privatsphäre zu wahren und nicht Opfer typischer Angriffe von Online-Kriminellen zu werden.

Der Selbstständige

Der Selbstständige ist in hohem Maße von seinem Computer abhängig. Er hat zahlreiche Benutzerkonten bei Kommunikationsdiensten und Business-Netzwerken und speichert auf seinem (meist mobilen) PC alle Materialien, die die Grundlage seiner Arbeit und seiner Kundenbeziehungen sind.

Das Know-how kann dabei ganz unterschiedlich ausfallen. Ein technischer Ingenieur mit fortgeschrittenen Kenntnissen speichert auf dem PC seine Baupläne. Ein Handwerker ohne besonderes IT-Know-how schreibt seine Rechnungen damit und hat die Buchhaltung darauf.

Letztlich verdient der Selbstständige sein Geld mit Leistungen, die direkt oder indirekt mit seinem Computer verknüpft sind. Wie wichtig der Computer bei ihrer Arbeit ist, merken diese Nutzer oft erst, wenn er verschwindet oder kaputtgeht. Oft werden dann Freunde um Rat gefragt, die viele Stunden ihrer Lebenszeit investieren, um (meist erfolglos) Probleme zu lösen, die sich mit (steuerlich absetzbaren!) Lösungen für wenige Hundert Euro gar nicht erst ergeben hätten.

Wichtig ist auch für diesen Nutzertyp, seine Privatsphäre zu wahren. Doch diese erstreckt sich bei Selbstständigen mit Kundendaten auch auf die Privatsphäre ihrer Kunden. Erhöhtes Augenmerk gilt natürlich der Abwehr einfacher Spionage-Angriffe von Konkurrenten, die man keinesfalls unterschätzen sollte. Besonders wichtig ist hier aber auch, nach einem wie auch immer gearteten Crash schnell wieder den reibungslosen Betrieb aufnehmen zu können, als wäre nichts geschehen.

Der Angestellte

Der Angestellte nutzt seinen PC im Büro, möglicherweise auch ein Notebook, um Arbeit nach Hause mitzunehmen oder weil er im Außendienst tätig ist.

Er ist zwar in hohem Maße von seinem Gerät abhängig, doch das Unternehmen hat dafür ja eine IT-Abteilung, auf die er sich in der Regel verlässt. Und das prinzipiell zu Recht, denn dafür ist diese ja da.

Allerdings stellt sich die Lage aus Sicht der IT-Leute ganz anders dar. Für sie ist der Angestellte prinzipiell eine Bedrohung, eben weil er die Verantwortlichkeit komplett abgegeben hat. Ihm zu erlauben, eigene Software zu installieren, stellt ein Risiko dar. USB-Stick – ein Risiko. Die Nutzung von Webdiensten – ein Risiko.

Obwohl dies kein Buch für Unternehmens-ITler ist, versuche ich, auch diesen Typ und seine besondere Gefährdungssituation zu berücksichtigen.

Der Geheimagent

Der Geheimagent ist jemand, der staatstragende Geheimnisse besitzt. Wenn er gehackt wird, stürzen Regierungen, Börsen crashen und die Formel für die sagenhafte Tera-Bombe gerät in die Hände von Superschurken, die meist Handschuhe tragen, Kätzchen streicheln und ihre Bediensteten in Haifischbecken zu entsorgen pflegen …

Betrachten Sie bitte diesen Benutzertyp – genau wie ich – mit einem gewissen Augenzwinkern. Denn er existiert vor allem symbolisch und steht für den Benutzer, der einer theoretisch größtmöglichen Bedrohung ausgesetzt ist.

Warum dieser fiktive Benutzertyp? Weil es zahlreiche und kostenlose Methoden zur Erhöhung Ihrer persönlichen Sicherheit gibt, die vollkommen ausreichen. Mehr braucht kein normaler Anwender. Doch immer finden sich ganz besonders kluge Mit-

menschen, die darauf hinweisen, dass hier oder dort dieses oder jenes gehackt werden könnte ...

Abbildung 1.3: US-Geheimdienst NSA, Schwerpunkt IT

Und sie haben damit Recht: Wer satt ausgestattet ist mit Material und Geldmitteln (in der Popkultur meist der US-Geheimdienst NSA, *www.nsa.gov*), der kann hypothetisch alles. Webforen sind voll von entsprechend paranoiden Behauptungen.

Die Frage ist nur: Welcher Aufwand wäre eigentlich damit verbunden?

Verschlüsselungsprogramme gelten zum Beispiel als das A und O der Sicherheit. Der Erfinder einer (noch theoretischen, aber gewiss ungemein wertvollen) „Formel zur billigen Herstellung von Mineralöl aus Sonnenlicht“ hat also garantiert einen völlig verschlüsselten Computer, um seine Formel zu schützen. Doch jede Verschlüsselung, das hat die Vergangenheit gezeigt, wird irgendwann geknackt (und die, die bisher nicht geknackt wurden, sind nur so lange „sicher“, bis sie das gleiche Schicksal ereilt – siehe auch Kapitel 7). Ergo kann der theoretische

Super-Geheimdienst natürlich auch jeden Schlüssel dieses Erfinders knacken, dank ausgefeilter Supercomputer und …

Doch das kostet natürlich Geld. Viel Geld. Und viel Personal. Und Material.

Deutlich billiger wäre es, eine Edel-Prostituierte (männlich oder weiblich, je nach Zielperson) zu engagieren. Die soll den Erfinder so lange bezirzen, bis sie irgendwie an die Zugangsdaten herankommt. „Schatz, ich will dir mal was zeigen, können wir mal kurz ins Internet …“ (Wimper-Klimper).

Der theoretische Geheimagent würde das vielleicht noch als Angriff erkennen. Aber welcher Mann in der Mitte seines Lebens würde sich nicht der (falschen) Hoffnung auf einen zweiten Frühling hingeben? Die Geschichte ist voll von Beispielen, hinzu kommen Erpressung und natürlich einfache Bezahlung, garantiert erfolgreich bei unzufriedenen Angestellten …

Anders gesagt: Außer Geheimagenten braucht niemand Geheimagenten-Sicherheits-Werkzeuge. Sanfte Methoden, im Jargon auch *Social Engineering* genannt, funktionieren oft viel besser und billiger – auch davon wird noch die Rede sein.

Drei ganz alltägliche Horror-Szenarien

Die folgenden drei Szenarien können als typisch gelten für große Sicherheitskatastrophen, wie sie alltäglich Tausenden passieren. Für alle nachgenannten Probleme gibt das Buch Anleitungen, wie Sie sie im Vorfeld abwehren und im Fall des Falles möglichst schnell wieder beheben können.

Szenario 1: Malware-Infektion

Der Student Florian Z. speichert seine Daten auf seinem PC. Besonders wichtig ist ihm seine Semesterarbeit, die schon fast fertig ist und in einigen Tagen abgegeben werden muss. Für die Recherche ist er auf eine schnelle Internetverbindung angewiesen.

Gestern hatte Florian Besuch von einem Freund. Gemeinsam machte man sich den Spaß, auf einigen „Rotlicht"-Webseiten herumzusurfen. Heute stellt Florian Z. fest, dass der Rechner bockt und viele Funktionen nicht mehr zur Verfügung stehen. Task-Manager, Eingabeaufforderung und Registry-Editor lassen sich nicht mehr starten. Das Internet ist schneckenlahm.

Ganz offensichtlich hat Florian seinen PC mit einer Malware infiziert.

Florian Z. sucht also nach einem Antivirenprogramm und wird auch gleich fündig. Die Panik wird allerdings noch größer, als dieses Antivirenprogramm noch weitere Viren und Würmer auf dem PC findet. Allerdings weigert sich die Software dann, diese auch zu entfernen – dafür müsse man die Vollversion erwerben. Wegen des Abgabetermins für seine Arbeit unter Druck, kommt Florian dem nach – die Viren sind danach weg (es gab sie nie), doch der ursprüngliche Schädling ist immer noch da.

Wie passiert so etwas?

Die typischen Ursachen einer Malware-Infektion:

- ✔ Verwendung von Raubkopien aus dem Internet oder von Freunden
- ✔ Verwendung von Knackprogrammen für kommerzielle Software (Slang: *Crackz*) oder Seriennummern-Generatoren (*Serialsz*)
- ✔ Voreiliger Doppelklick auf angehängte Dateien in Mails, die als Trojanische Pferde arbeiten
- ✔ Voreiliges Klicken auf Links in sozialen Netzen, in Spam-Mails, im Messenger oder in Suchergebnislisten; auf Links, die zu Seiten führen, auf denen bereits das schlichte Betrachten von Flash-Animationen, PDF-Dateien oder ähnlich „Alltäglichem" schon für eine Infektion ausreicht (auf schlecht gepflegten Systemen)

- ✔ Datenaustausch via CD, DVD, USB-Stick oder externe Festplatte mit Freunden oder Kollegen, mit öffentlich zugänglichen PCs und Notebooks, zwischen Zuhause, Universität, Büro, Messe-PCs …
- ✔ Nutzung von (unsicheren) Anonymisierungs-Systemen
- ✔ Und, und, und
- ✔ Plus: Panik – immer eine ganz schlechte Grundlage für Entscheidungen

Wie real ist die Gefahr?

Dieses Problem ist absolut real und alltäglich. Vorsichtiges Verhalten kann die Gefahr minimieren, aber schon wer einen Webbrowser benutzt, setzt sich automatisch Risiken aus, die er heutzutage eigentlich nicht mehr selbst kontrollieren kann.

Besonders perfide ist, dass eine wachsende Zahl von „Antivirenprogrammen“ im Web auftaucht, die so gut wie keine Wirkung haben, aber gutgläubige Nutzer zur Kasse bitten.

- ✔ Abhilfe schaffen echte Antivirenprogramme und Security-Suiten von namhaften Anbietern. Auch regelmäßige Updates und eine Änderung des eigenen Nutzerverhaltens minimieren das Risiko, ebenso Browser-Erweiterungen, die Ihnen helfen, gefährliche Websites schneller zu erkennen – siehe Kapitel 4.
- ✔ Backups helfen, im Fall des Falles schnell wieder die Arbeitsfähigkeit herzustellen – siehe Kapitel 5.

Szenario 2: Netbook-Crash

Julia H. hat sich sehr über ihr Netbook gefreut. Es war recht günstig und ist besonders kompakt, sie hat es immer dabei.

Dank 160-GByte-Festplatte hat sie alles Mögliche draufgepackt: Die Fotos ihrer Kinder liegen ebenso auf dem Netbook wie Fotos von ihrem Mann und Videoclips, die ein Freund auf der Hochzeitsfeier aufgenommen hat.

Doch dann geschieht das Unglück: Das kleine Netbook fällt herunter, die Festplatte ist kaputt. Die Festplatte selbst kann man austauschen, selbst der Ersatz des gesamten Geräts ist bei einem Preis von unter 400 Euro kein Problem.

Doch was ist mit ihren Passwörtern, ihren Briefen, ihren Mails und ihren Fotos? Mit dem Gerät verschwindet heute auch die gemeinsame Erinnerung, die sich in wachsendem Maße im „digitalen Gedächtnis" befindet.

Wie passiert so etwas?

Typische Gründe für einen kompletten Datenverlust am PC:

- ✔ Das Gerät wird gestohlen oder verloren.
- ✔ Das Gerät fällt herunter und wird völlig zerstört.
- ✔ Die Festplatte fällt aus, zum Beispiel weil ganz einfache Netbooks gerne im geöffneten Zustand durch die Welt getragen werden – was den eingebauten Festplatten schadet.
- ✔ Die Festplatte wird versehentlich gelöscht, weil man ein zweites Betriebssystem wie Ubuntu installieren wollte.
- ✔ Eine Schadsoftware löscht das System.

Wie real ist die Gefahr?

Die Gefahr ist absolut real. In jeder Minute verschwindet ein mobiler Rechner in Kaffeehäusern, Hotelzimmern, Schulen und Universitäten. Das wäre halb so schlimm, enthielte nicht mindestens die Hälfte der Net- und Notebooks vertrauliche Daten. Die Studie „Airport Insecurity – The Case of Lost Laptops" (Ponemon, *wwww.ponemon.org*) nennt 16.000 verschwundene Notebooks pro Jahr – und das allein auf US-amerikanischen Flughäfen.

Selbst wenn die Geräte „ersetzbar" und die Daten darauf „entbehrlich" sind, so sollten die Inhalte in der Regel nicht in falsche Hände gelangen.

Prominentes Beispiel: Im August 2009 wurde das Notebook des Fußball-Managers Christoph Daum auf einem Flughafen gestohlen. Die Langfinger wussten, was sie taten, und forderten vom Fußballtrainer 100.000 Euro Lösegeld, andernfalls werde man Daten von seinem Mobilrechner veröffentlichen, offensichtlich solche, denen irgendeine Brisanz innewohnt.

Natürlich hat nicht jeder „brisante" Daten auf seinem Rechner. Aber jeder Verlust von Kundendaten sollte dringend vermieden werden, auch wenn man kein Arzt mit digitalen Patientenakten oder Anwalt mit Falldateien ist. Und wer die Baby-Bilder seiner kleinen Tochter auf dem Gerät speichert, möchte sicher auch nicht unbedingt, dass diese jemandem in die Hände fallen, der sie in unerwünschtem Zusammenhang verwendet – zum Beispiel als Tauschmaterial für den Kinderporno-Untergrund.

Die Gefahr von Diebstahl, Verlust oder Missbrauch persönlicher oder geschäftlicher Daten ist also höchst real.

- ✔ Abhilfe schaffen Verschlüsselungsprogramme, die dafür sorgen, dass den Dieben nur die Hardware, nicht aber die Inhalte des mobilen Computers in die Hände fallen – siehe Kapitel 7.

Der Crash ist deutlich seltener und auf den ersten Blick auch weniger problematisch. Eines Morgens gibt das Gerät einfach den Geist auf, das war's dann.

- ✔ Abhilfe schafft ein regelmäßiges Backup der Daten des tragbaren PCs auf einer Festplatte, die zu Hause bleibt. Erleichterung verschafft die Nutzung von webbasierten Diensten und Cloud-Services, die den Benutzer unabhängig vom konkret vorhandenen Gerät machen. Beispiel: Wenn Sie GMX-Mail verwenden, so können Sie das auf jedem PC tun – siehe Kapitel 5.
- ✔ Problematisch ist nur, wenn ein defektes Gerät zur Reparatur gegeben wird, denn dann ist wie beim verlorenen oder gestohlenen Notebook die Privatsphäre über Verschlüsselungsmaßnahmen zu schützen – siehe Kapitel 7.

Der völlige Datenverlust durch Malware (Viren, Würmer, Schadprogramme) ist heutzutage eher selten, weil sich der Schwerpunk eines Angriffs verlagert hat: Wollten die Hacker früher noch zerstören, so soll heute ja vor allem die Schadsoftware weiterverbreitet werden, wofür ein einigermaßen reibungslos laufendes System unabdingbar ist.

Szenario 3: Online-Raubüberfall

Der Facharbeiter Thomas S. stellt eines Tages fest, dass jemand auf seine Kosten einkauft. Es sind nur kleine Summen, per Kreditkarte ebenso wie per Bank, doch zusammengenommen ergeben sich hohe Beträge.

Nachforschungen ergeben, dass eine Person im europäischen Ausland unter seinem Namen, aber mit einer weiteren Adresse eine zweite Identität eingerichtet hat und nun auf seine Kosten shoppt und sogar telefoniert.

Beim Versuch, das zu stoppen, kommt Thomas S. in die bizarre Lage, dass er selbst nachweisen muss, dass er der wahre Besitzer der Kontodaten ist.

Er wurde zum Opfer eines Identitätsdiebstahls oder -missbrauchs.

Wie passiert so etwas?

Typische Ursachen eines Identitätsmissbrauchs:

- ✔ Verwendung zu kurzer oder unsicherer Passwörter in verschiedenen Systemen
- ✔ Ein Mobil-Computer mit enthaltenen Zugangsdaten wurde gestohlen oder verloren.
- ✔ Es liegt ein gezielter Angriff eines Mitmenschen vor (nicht so selten, wie es klingt).
- ✔ Nachlässiger Umgang mit persönlichen Daten, auf dem Computer und auch außerhalb

Wie real ist die Gefahr?

Der erfolgreiche Sandra-Bullock-Film „Das Netz“ vermittelt einen passablen Eindruck von diesem Szenario – wenngleich verwässert von Hollywood-Klischees. Noch eindringlicher ist das in dieser Hinsicht lesenswerte Buch „Talk Talk“ von T.C. Boyle, bei dem sich die Opfer eines Identitätsbetrügers allerdings überzeichnet dumm verhalten.

Doch jenseits dieser Klischees sprechen die Fakten für sich: Das Bundesamt für Sicherheit in der Informationstechnik (BSI, *bsi.bund.de*) beobachtet seit Jahren eine Zunahme der Cyberkriminalität im Umfeld des Identitätsmissbrauchs. Das Bundeskriminalamt (BKA, *www.bka.de*) stellt jährlich eine wachsende Zahl von digitalen Identitätsdiebstahlen fest. An der Spitze stehen dabei mehrere Tausend Fälle der missbräuchlichen Nutzung von Accounts von Telekommunikationsdiensten, wobei Zugangsdaten ausgespäht und anschließend missbräuchlich verwendet werden. Die Zahl der jährlichen „Account-Takeovers“ ging ebenfalls bereits 2009 in die Hunderte, inzwischen dürfte sie noch höher liegen. Dagegen ist die Zahl der „Carding“-Opfer, bei denen Kreditkartendaten entwendet wurden, vergleichsweise gering. Zieht man allerdings in Betracht, dass Mitte 2011 der Firma Sony von Hackern mehrere Millionen Zugangsdaten entwendet wurden, bestätigt sich die Aussage des BKA, wonach die Dunkelziffer gewiss weit höher liegt.

- ✔ Abhilfe schafft eine Änderung des Nutzerverhaltens, vor allem beim Umgang mit Passwörtern – siehe Kapitel 6.
- ✔ Spezielle Tools helfen bei der Abwehr von Spionage-Werkzeugen und Schnüffeleien, etwa Verschlüsselung – siehe Kapitel 7.
- ✔ Auch der Spurenlöschung kommt Bedeutung zu, denn aus den Spuren eines Benutzers lässt sich ebenfalls auf sein Verhalten schließen – siehe Kapitel 8.

Früher üblich (und auch heute noch praktiziert): das sogenannte *Dumpster Diving*, zu Deutsch etwa „Tauchen im Müllcontainer". Papier-„Hacker" wühlen dabei im Müll, meist in dem von Firmen, auf der Suche nach deren (und Ihren) Geheimnissen. Kein Witz! Der Sage nach soll der ehemalige Microsoft-Chef Bill Gates auf diese Weise in den Besitz von Programmcode gelangt sein. Machen Sie sich mal den Spaß und werfen Sie bei trockenem Wetter einen Blick ins Altpapier und prüfen Sie, wie viele Adressen, Bankverbindungen und Unterschriften Sie zusammenkriegen würden. Man muss sich gar nicht in den Computer eines Opfers hacken, man muss nur warten, bis der Betreffende sein Altpapier vor die Tür stellt …

Eine neue Art von Sicherheit

Allgemein gesagt ist Ihr PC niemals sicher. Jeder Virenscanner erkennt zum Beispiel (vereinfacht dargestellt) digitale Schädlinge an ihren Mustern. Scanner erkennen daher nur Schädlinge, die sie erkennen können, weil sie deren Suchmuster kennen – neue Schädlinge kennen sie systembedingt nicht. Daher hilft auch der beste Scanner nichts, wenn Sie der erste Mensch auf Erden sind, der mit einer nagelneuen Schadsoftware konfrontiert wird.

Hier springen „verhaltensbasierte Schutzprogramme" in die Bresche. Sie versprechen, beliebiges Schadverhalten ganz allgemein zu erkennen, ohne diesen einen Virus speziell schon über sein Muster identifizieren zu können. Funktioniert auch, oft. Doch wie unterscheidet sich das Posten eines Links bei Facebook durch Sie vom gleichen Vorgang durch einen Wurm in Ihrem PC? Und selbst wenn es funktioniert, so fällt Ihnen vielleicht das Notebook herunter, Ihre Festplatte ist ein Montags-Fabrikat oder ein Erdbeben findet völlig überraschend statt.

Kurz: Sie sind sowieso nie sicher.

Ergo ist es am besten, sich vom Gedanken an irgendeine Art von „100-prozentiger Sicherheit“ gleich zu verabschieden.

Hat man das einmal verinnerlicht, stellt sich nämlich die viel wichtigere Frage: Was können Sie tun, um nach einem Crash, egal welcher Art, schnellstmöglich wieder den vorherigen Zustand herstellen?

Dieser Punkt ist mir sehr wichtig, denn wir stehen in Sachen Sicherheit meiner Meinung nach vor einem Paradigmenwechsel weg von „Abwehrmaßnahmen“ hin zu „Wiederherstellungsvorbereitung“.

Der Crash kommt so oder so. Klug ist daher derjenige, der sein System so ausgelegt hat, dass er eine Stunde nach dem Crash einfach weiterarbeiten kann.