Sicherheit im Internet fr alle

Von Thorsten Petrowski
*ebooks | Download PDF | *ePub | DOC | audiobook*

Produktinformation -Verkaufsrang: #527413 in BcherVerffentlicht am: 2013-06-27Abmessungen: .91 Pfund Einband: Gebundene Ausgabe256 Seiten | File size: 68.Mb

Von Thorsten Petrowski : Sicherheit im Internet fr alle before purchasing it in order to gage whether or not it would be worth my time, and all praised Sicherheit im Internet fr alle:

KundenrezensionenHilfreichste Kundenrezensionen6 von 6 Kunden fanden die folgende Rezension hilfreich.

Fallstricke im InternetVon Raumzeitreisender"Sicherheit im Internet" ist laut Vorwort des Autors Thorsten Petrowski ein Ratgeber fr durchschnittliche Nutzer des Internet, die mit den weit verbreiteten Plattformen Windows 7 oder 8 arbeiten. Es ist kein Buch fr IT-Experten. Damit ist der Rahmen hinreichend abgesteckt. Nun gilt es noch, sich selbst als Leser des Werkes entsprechend zu klassifizieren. Diesem Zweck dient der kleine Wissens-Check, bestehend aus 23 Fragen, zu Beginn des Buches. Dieser Test kann als Hilfsmittel herangezogen werden, um zu entscheiden, welche Kapitel fr einen selbst Prioritt haben sollten.Das Internet ist vergleichbar einem Haifischbecken; wer sich auffllig verhlt und viele Spuren hinterlsst, luft Gefahr, "gefressen" zu werden. Thorsten Petrowski klrt auf ber Wege ins Netz, Schadsoftware, Cyberangriffe und Abofallen. Er warnt vor leichtfertigem Umgang mit Passwrtern ("Das Passwort NIEMALS an andere weitergeben."). (68) Je mehr persnliche Daten freigegeben werden, umso grer ist die Gefahr gestohlener Identitten. Auf einmal liegen Rechnungen fr Dienste im Briefkasten, die nie beauftragt wurden.Petrowski klrt darber auf, wie Surfer ihre Spuren verwischen knnen. Dazu gehren u.a. das Lschen des Browser-Verlaufs, der Einsatz eines Proxy-Servers, der Aufbau von VPN-Verbindungen oder das Surfen ber ein anonymisierendes Tor-Netzwerk. Die Anonymisierung ist mit Einschrnkungen verbunden, wie der Autor humorvoll deutlich macht. "Man wollte absolut sicher gehen, dass die mhsam "erkmpfte" Anonymitt nicht durch "plaudernde" Plug- In-Zusatzprogramme wieder zunichte gemacht wird." (239)IT-Experte Petrowski verweist auf einige serise Adressen im Internet, die bei der berprfung der Sicherheit und Konfiguration von Sicherheitseinstellungen hilfreich sein knnen. Zu den wichtigen Seiten gehren die des Bundesamtes fr Sicherheit in der Informationstechnik, das seit Jahren ber Sicherheitsaspekte aufklrt. Die Erluterungen in dem Buch sind zielgruppengerecht. Die Bilder sind teilweise recht klein und damit schwer lesbar. Dennoch werden die Leser durch das Buch ber ein wichtiges Thema aufgeklrt und dafr sensibilisiert, Sicherheit als Dauerthema zu betrachten.10 von 11 Kunden fanden die folgende Rezension hilfreich. Das Wichtige verstndlich dargestelltVon juryDie grte Sicherheitslcke bei Computeranwendungen wird durch naive Anwender aufgetan. Thorsten Petrowski spricht in seinem kompakten Buch "Sicherheit im Internet fr alle" genau diesen Otto Normalverbraucher an, der zwar tglich liest, wie wieder einmal Datendiebstahl im Groen betrieben wurde, aber fest berzeugt ist, dass das mit seinem PC zuhause nichts zu tun hat.Systematisch fhrt das Buch durch alle relevanten Bereiche, vermeidet dabei weitgehend technischen Jargon und betont vor allem immer wieder die Gefahren des Leichtsinns. "Sicherheit" beschrnkt sich dabei nicht nur auf Datensicherung, sondern auch auf Fallen, die dem Anwender durch unserise Anbieter und gierige Rechtsanwlte gestellt werden.Das alles bewegt sich auf einfachem, verstndlichen Niveau und knnte damit genau den Bedrfnissen der breiten Masse der Anwender gengen - jedenfalls, wenn diese Klientel sich bewegen lsst, ein solches Buch zu kaufen und zu lesen. Daran drfen Zweifel bestehen, was man natrlich nicht dem Autor anlasten muss. Fr Computeranwender, die gelegentlich in eine Fachzeitschrift oder die Wikipedia hineinschauen, wird die Lektre dieses Buchs wohl selten neue Einsichten ffnen; aber irgendetwas, was man noch nicht gewusst hat, findet man bekanntlich immer.Das Bchlein wirkt bersichtlich und aufgerumt. Durch eine gute Gliederung, ein Register und ein durchdachtes Inhaltsverzeichnis findet man bei spterem Nachschlagen das Gesuchte berraschend leicht.print-jury 5* A1166 20.7.2013 ABR 11.517 Rezensionsexemplar40 von 48 Kunden fanden die folgende Rezension hilfreich. Erster Eindruck, eine sehr trgerische Sicheheit, denn solange Windows oder MacOS-X auf dem Rechner ist, liest BIG-BROTHER mit!Von TheoHabe die Homepage besucht und festgestellt das auch closed-source Produkte dabei sind und empfohlen werden.Besonders von Microsoft, das ist etwa so, als ob man dem Fuchs sagt, er solle den Hhnerstall bewachen!Warum?Vorweg gesagt, kann ich hier leider keine Links als Beleg fr meine Aussagen angeben, da diese von gelscht werden.Ansich ist die Idee des Autors gut gemeint, nur bringt sie nicht DIE Sicherheit die man letzten Endes erwartet,besonders wenn es sich um das Absichern von PCs handelt auf denen sich mglicherweise patentrelevante Datenz.B. Konstruktionen und deren Berechnungen befinden.Wer sich einen neuen Rechner im Handel kauft findet meist Windows in irgend einer Variante vorinstalliert. (Auch bei Firmen-PCs)Auffllig in nahezu allen Fllen ist, dass dieses Windows mit Administrator-Rechten ohne Passwort-Schutz luft und in Sachen Eindring-Schutz so offen ist wie ein Scheunentor!Das hat aber NICHTS mit dem Herstellungsprozess zu tun, wenn das Windows in der Fabrik automatisch aufgespielt wird, sondern diese offene Daten-Scheune ist gewollt!Natrlich zum Schaden des Kufers / Benutzers, besonders wenn es um Brorechner von Firmen geht.Jeder Virenscanner besitzt intern eine aktualisierbare Tabelle, worin (scheinbar) vertrauenswrdige Softwarehersteller eingetragen sind.Wenn also von drauen via Internet ein Windows-Update rein kommt, merkt der Virenscanner das und schlgt KEINEN Alarm, weil er Microsoft als vertrauenswrdig einstuft.Und was ist, wenn Microsoft in dem Update von der NSA/CIA vorgegebene Spionage-Routinen versteckt hat?Genau dann ist nmlich Schluss mit lustig, wie ich im Folgendem noch zeigen werde.Dass diese NSA/CIA-Schnffelei auch fr ahnungslose unbescholtene Brger durchaus gefhrlich werden kann, zeigt der Fall des Trken Murat Kurnaz (Wikipedia), der unschuldig 4 Jahre in Guantanamo gefoltert wurde!So was kann sehr viel schneller gehen als manche Leute denken, ganz zu schweigen von den ganzen illegalen Geheimgefngnissen (meist mit Folter), die die Amis rund um die Welt betreiben!Ehrlich gesagt erstaunt mich, warum sich erst jetzt alle ber diese Spionage aufregen?Ich wusste schon seit Juli 1999 also seit rd.~15 Jahren von dieser Spionage, nur hat niemand auf mich gehrt, nicht mal die Polizei!Ich war seinerzeit als Dipl. Informatiker Teamleiter einer kleinen Wartungstruppe in einem Logistik-Unternehmen, dass als Subunternehmer fr die Fa. Kaufhof fungierte.Zu jener Zeit gab es eine Zeitschrift namens PC-Tricks, die sich offenbar aber spter nicht mehr am Markt

behaupten konnte.Ich hatte das Glck seinerzeit eine Ausgabe in die Hnde zu bekommen in der das Microsoft-Home-Betriebssystem Windows 98 teilweise diassembliert gezeigt wurde.Kurze Erluterung fr Laien:Sprachcompiler wie C++ / Pascal / Ada / PL1 etc. bersetzen Hochsprachen-Programme in Maschinensprache.Da sieht dann eine Addition z.B. so aus:Addiere (BefehlsNr.= 5) den Inhalt von Speicherstelle 18 zu dem der Speicherstelle 13.5 13 18Assembler ist eine vermenschlichte Maschinensprache in dem man die Befehlsnummer hier die 5 mit einem aussagekrftigen Namen belegt z.B. ADDAlso:ADD 13 18 ; Ab dem Semikolon kann man Kommentare zur Operation schreibenSo muss der Assemblerprogrammierer keine Nummern auswendig lernen.Diassemblieren ist der umgekehrte Vorgang, der Maschinencode wird in Assembler zurckverwandelt wie in unserem ADD-Beispiel.In den USA ist diassemblieren verboten, aber in Europa erlaubt.So konnte man dann auch Windows 98 diassemblieren wobei entdeckt wurde, dass Windows-98 eine Hintertr besa, durch die sich die NSA jederzeit ohne Bemerken des Eigentmers bzw. legalen Benutzers in den laufenden Rechner via Internet einloggen und wertvolle Daten wie patentrelevante Informationen abgreifen konnte.Microsoft hat sich nicht mal die Mhe gemacht die Kommentare der Programmierer auszulschen, so das man den in der Zeile wo der Zugangscode der NSA startete tatschlich in englischerSprache lesen konnte ZUGANG NSA.Da es sich bei Windows 98 um ein Home-Betriebssystem handelt, kann man nur erahnen das sich zum gleichen Zeitpunkt selbige Spionageroutinen in den Profisystemen Windows NT und Windows 2000 befunden haben.Der polizeinahe Autor Udo Ulfkotte schrieb zur selben Zeit 1999 ein Buch mit dem Titel:'Marktplatz der Diebe. Wie Wirtschaftsspionage deutsche Unternehmen ausplndert und ruiniert'Die Rede ist in dem Buch von damals 40 Milliarden DM also heute ~20 Mrd. Euro Schaden und 50.000 vernichteten Arbeitspltzen pro Jahr!Mittlerweile drfte in 2013 der jhrliche Schaden bei 50 Milliarden Euro liegen und bei 125.000 jhrlich vernichteten Arbeitspltzen!Man kann also mit sehr hoher Wahrscheinlichkeit davon ausgehen, das die Regierenden in Deutschland egal welcher Parteien, diesen Sachverhalt gewut haben und ganz bewusst keine Gegenmanahmen ergriffen haben, um ber den Umweg des Auslands ihre eigenen Landsleute auszuspionieren, unter voller in Kaufnahme der groen wirtschaftlichen Schden, die dadurch bis zum heutigen Tage entstanden sind.Bedenkt man das nach 202a StGB - Aussphen von Daten, jedem Cyberkriminellen bis zu 3 Jahre Knast angedroht werden, ist diese Spionageaffhre ein Fall der seines gleichen sucht und mit einer zynischen Doppelmoral einhergeht!Insbesondere wegen der wissentlichen Duldung seitens der jeweiligen deutschen Regierungen zurck verfolgbar seit 1999. (Zeitschrift PC-Tricks mit diassembliertem Win-98)Dies erfllt wegen des grundgesetzlichen Eides unter Artikel 56 des Grundgesetzes einen schweren Versto gegen die Vereidigung (Kanzler+Minister) das deutsche Volk vor Gefahren zu schtzenund seinen Nutzen zu mehren! Da hilft auch keine Ausrede (Merkel) das das Internet ja Neuland wre. Neuland nach mindestens 15 Jahren?Meinen damaligen Arbeitgeber schien das nicht zu stren obwohl z.B. die US-Konkurrenz wie Wall Mart anhand der Logistikdaten durchaus eine eigene Verkaufslogistik ableiten konnte,denn wenn andere das Lehrgeld bezahlt haben in Form von Ladenhtern etc. kann man durchaus davon lernen und solche teuren Fehler der Konkurrenz vermeiden.Diesen Sachverhalt habe ich auch schon mehrmals zur Polizei gesendet mit obiger Begrndung, Reaktion = NULL, was offensichtlich darauf hindeutet, das von ganz oben ein Ermittlungsverbot bestand.Was die Amis interessiert, sind vor allem patentfhige Entwicklungen!Der Deutsche gibt diese erst frei, wenn zu 99,9% alles ausgereift ist. Der Ami hingegen wirft schon 80% marktreife Produkte auf den Markt, z.B. mit geklauten deutschen Patenten und sichert sich dann die Patente bevor der Deutsche der beklaut wurde es kann.Man darf mit 100% Sicherheit davon ausgehen, das in spteren Systemen wie XP/Vista/7/8 noch weit verbesserte Hintertren existieren, die von KEINEM Virenscanner erkannt werden weil sich diese als Systemrelevant unter dem Deckmantel von Microsoft ausgeben, wie in dem Update-Beispiel oben.Geplante neuere Methoden der Amis, vor allem INTEL und AMD, sie machen das zuknftig ber den Prozessor internen Mikrocode!Der Mikrocode ist ein winziges Programm, welches sich auf dem Prozessor-Chip befindet und dort seine Arbeit verrichtet.Es steuert die funktionalen Einheiten des Prozessors, Arithmetik und Logik-Einheit, die Speichermanagement-Einheit, die den Hauptspeicher im PC verwaltet usw. Jeder Befehl,den das Betriebssystem oder eine Anwender-Software an den Prozessor gibt, muss letztlich ber den Mikrocode umgesetzt werden.Da spielt es dann keine Rolle mehr ob man Linux, Windows, FreeBSD, MacOS-X oder sonst was installiert ist.Dann knnen die Amis alles auslesen, weil der Schutz ber ein anderes spionagefreies Betriebssystems nicht mehr greift!Das geht sogar so weit das die (vermeintlich) ausgeschaltete PCs im stand-by Modus hacken knnen, denn kommt ein Impuls ber die Netzwerkkarte fhrt die Kiste wieder hoch und es beginnt eine neue Runde im Daten-Roulette! Gerade dann, wenn der Eigentmer der Kiste nicht davor sitzt!Grundstzlich gilt fr Privatleute, besorgt Euch Linux, oder PC-BSD, das die die grafische Variante von FreeBSD, PC-BSD bzw. FreeBSD kann auch Linux-Programme ausfhren!Das chinesische Militr benutzt ebenfalls FreeBSD. Dann kann Euch nichts mehr passieren, jedenfalls bis in die mittlere Zukunft.Einziger Wermutstropfen, die Bcher zu FreeBSD sind meist alle in 'Inglisch' und das zu lesen ist im Regelfall zeitraubender als deutsch.Linux-Bcher gibt es hingegen satt auf deutsch.Natrlich ist das fr Windows-Fetischisten mit Arbeit verbunden, aber wer sich z.B. vor berfllen schtzen will, lernt entweder eine Kampfsportart, oder besorgt sich Trnengas, oder im hrtesten Fall auch eine echte Knarre. Ergo ist bei einem System-Umstieg auch etwas Arbeit ntig, was sich aber in einer erheblich strker geschtzten IT-Privatsphre bezahlt macht,denn dann hat BIG-BROTHER (NSA/CIA/BND) ausgesprochen schlechte Karten!Hier noch ein paar Tipps zu Softwareprodukten, mit denen man der NSA und ihren Schnfflern das Leben schwerer machen kann.Eine WEB-Seite

namens PRISM-BREAK ORG, da findet ihr einiges an alternativer Software, im Regelfall Open-Source-FreeWare, die ohne Verseuchung alla NSA Co daher kommt.Nur wie gesagt auf einem Microsoft-Windows-Betriebssytem

ProduktbeschreibungSicherheit im Internet fr alle

KurzbeschreibungFiese Fallstricke erkennen und vermeiden - unerkannt surfen - sicher kommunizierenDieses Buch gibt einen berblick ber die Sicherheitsrisiken und Gefahren, die im Internet lauern und zeigt, wie man sie vermeidet. Dabei wird auf technische Hintergrnde und Details in einer auch fr Laien verstndlichen Weise eingegangen. Wer das Internet nutzt, ist stndigen Bedrohungen ausgesetzt. Egal ob betrgerische Websites, Hackerangriffe oder staatliche berwachung. Wer nicht aufpasst, fngt sich schnell etwas ein. Viren, Wrmer, Malware unsichtbar und lautlos dringen sie in unsere Computer und Smartphones ein. Sie saugen vertrauliche Informationen ab, manipulieren unsere Bankkonten und locken uns in teure Abofallen. Inzwischen sind die Gefahren so komplex, dass ein normaler Anwender kaum noch durchblickt.Dieses Buch gibt Ihnen Werkzeuge und Tricks an die Hand, um Sie vor diesen Gefahren zu bewahren. Sie profitieren von diesem Buch gleich mehrfach:- kein IT-Fachchinesisch fr Experten, sondern Klartext fr jeden Internet-Nutzer- schnelle und auf den Punkt gebrachte Informationen durch Checklisten, Piktogramme und Illustrationen- hoher Nutzwert durch praktische Tipps so werden Sie selbst zum Sicherheitsexperten- wichtige Empfehlungen fr einen mglichst sicheren Umgang mit sozialen Netzwerken. Sichern Sie sich mit diesem Buch profundes Expertenwissen leicht nachvollziehbar aufbereitet und sofort einsetzbar.Besonders ntzlich: Am Anfang des Buches hilft ein Test, die Prioritten zu identifizieren.Als Extra: Auf der Internetseite zum Buch finden Sie den virtuellen USB-Stick mit ntzlichen Programmen, die das Surfen sicherer machen. Alle diese Sicherheitsprogramme werden regelmig aktualisiert und sind fr Sie als Privatanwender vllig kostenlos!