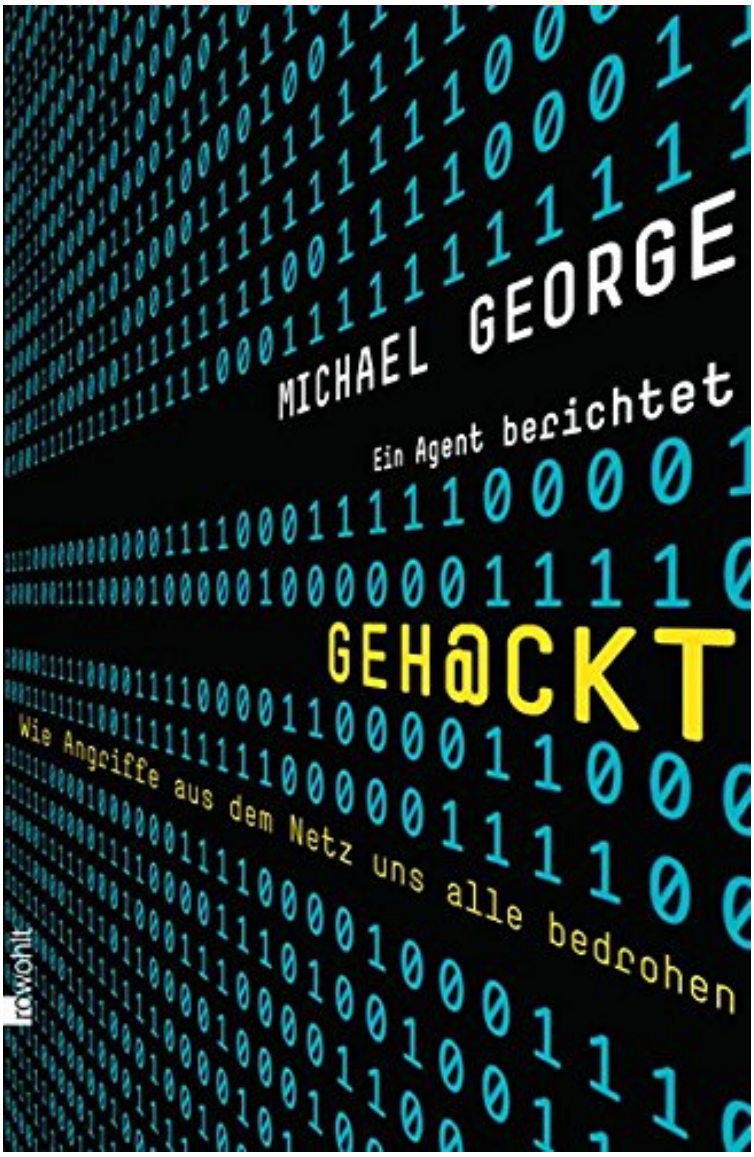
Geh@ckt: Wie Angriffe aus dem Netz uns alle bedrohen: Ein Agent berichtet

Von Michael George
*ebooks | Download PDF | *ePub | DOC | audiobook*



Produktinformation -Verkaufsrang: #488178 in BcherVerffentlicht am: 2013-12-02Erscheinungsdatum: 2013-12-06Abmessungen: 8.70 x .98b x 5.83l, Einband: Gebundene Ausgabe256 Seiten | File size: 71.Mb

Von Michael George : Geh@ckt: Wie Angriffe aus dem Netz uns alle bedrohen: Ein Agent berichtet before purchasing it in order to gage whether or not it would be worth my time, and all praised Geh@ckt: Wie Angriffe aus dem Netz uns alle bedrohen: Ein Agent berichtet:

KundenrezensionenHilfreichste Kundenrezensionen3 von 3 Kunden fanden die folgende Rezension hilfreich.

Spionage heute: ein Insider berichtetVon GoldtimeComputer bestimmen unseren Alltag wie nie zuvor - sie steuern unsere Stromversorgung, Wasser und Abwasser, sogar U-Bahnen, sie koordinieren die Lebensmittelversorgung ber Kontinente hinweg und dienen unserer Kommunikation.Wir speichern vertrauensselig unsere Fotos, Textdateien, Musik, GPS-Daten und Kontaktadressen - und sind lngst davon abhngig, dass Smartphone und Laptop reibungslos funktionieren.Viren, Wrmer und Trojaner - nie wurden so viele Daten gestohlen und mibraucht wie heute. Selbst ein Gert im Stand-by-Modus kann zur berwachungsanlage umprogrammiert werden.Gefahren durch Hackerangriffe? Wir haben doch lngst einen Virenschutz!... - Doch was, wenn Hacker unsere sorgsam ausgetftelte Infrastruktur lahm legen? Wie gefhrdet sind unser Stromnetz, wie realistisch Horror-Szenarien aus Romanen wie "Blackout"?Und wie gefhrdet ist unsere Privatsphre bereits?Michael George, geb. 1968, absolvierte eine Ausbildung beim BND und arbeitet seitdem bei verschiedenen Nachrichtendiensten in der Spionageabwehr - ein Vollprofi also, der in seinen Publikationen und Vortrgen ber reale Gefahren und notwendige Sicherheitsvorkehrungen im Internet aufklrt.In seinem aktuellen Buch "Geh@ckt" beschreibt er auf uerst spannende, anschauliche Weise, welche Flle er tatschlich erlebt hat - und wie sich ganze Staaten, aber auch jeder einzelne vor Datenspionage schtzen kann.Ich bin keine IT-Spezialistin, lese aber fters Publikationen rund ums Internet sowie Thriller, die damit zusammenhngen (z.B. "ZERO"). "Geh@ckt" hat mich total begeistert, weil es eine Kombination aus beidem ist: authentische Flle von IT-Kriminalitt, so spannend wie ein Thriller, sowie investigative Aufklrung UND praktische Tipps. Dazu fand ich es leicht verstndlich geschrieben, auch ohne Insider-Kenntnisse.Nach der Lektre habe ich alle meine angeblich "100% sicheren" Passwrter gendert und etliche Kundenkonten gelscht. Ich werde in Zukunft noch viel vorsichtiger sein, wem ich welche Daten preisgebe.Fazit: ein superspannendes, lehr- und hilfreiches Buch - fr alle, die sich in dieser schnen neuen Welt nicht den bestens organisierten Internet-Kriminellen ausliefern wollen.5 von 5 Sternen und eine absolute Lese-Empfehlung!2 von 2 Kunden fanden die folgende Rezension hilfreich. Informationssicherheit in seiner ganzen BreiteVon Jan KlingelGehackt ist ein wundervolles Buch, welches das Thema Informationssicherheit in seiner ganzen Breite beleuchtet. Nicht fr den erfahrenen Sicherheitsfachmann, aber fr all diejenigen, die sich zum Beispiel als Verantwortliche in mittelstndischen Firmen nebenbei um die Absicherung dessen kmmern mssen, was auch weiterhin einen groen Teil der Bruttowertschpfung in Deutschland ausmacht: unsere Innovations- und Fortschrittskraft. Was wir schtzen mssen liegt heute in digitaler Form vor und lsst sich auf eine fingernagelgroe Speicherkarte packen: Forschungsergebnisse, Designstudien, Konstruktionsplne sowie strategische Konzepte.Unser Leben wird mobiler und digitaler, die Bedrohungen wachsen damit stndig. Das Problem damit? Cyber-Angriffe und ihre Gegenmanahmen sind von der Allgemeinheit schwer zu verstehen.Whrend ich dies tippe ist einer meiner Finger eingeschient. Die Bedrohung auf Leib und Leben beim Snowboarden, kombiniert mit der Schwachstelle mangelndes Knnen, hat zu einem Kapselriss gefhrt, ein Risiko, welches ich vorher bewusst eingegangen bin. Meine einzige risikoreduzierende Manahme, der Helm, hat Schlimmeres verhindert.Die Angriffe auf unsere Informationen kommen aber meist nicht sichtbar auf uns zu und verursachen auch keinen Initialschmerz. Der Schmerz kommt erst spter wenn wir herausgefunden haben, dass ein Fremder mit unseren Kreditkartendaten online einkaufen war. Wollen wir proaktiv Gegenmanahmen dagegen ergreifen, so sind diese oft schwer zu verdauen: Microsoft Deutschland spricht bei der letzten Sicherheitsschwachstelle im Internet Explorer - mit Gru an den Duden - von Remotecodeausfhrung. Bevor ein Patch fr diese Sicherheitsschwachstelle verfgbar war, waren vom Anwender kryptische Befehle einzugeben, deren Auswirkung nur noch wenige nachvollziehen knnen.Wer glaubt, dass Informationssicherheit a gmahde Wiesn ist, muss sich nur mal im nicht IT-affinen Bekanntenkreis umhren: wer ist der Empfehlung des BSI gefolgt und hat einen alternativen Browser installiert, wer hat auf seinem Smartphone ein Gerte-Passwort installiert und wer schtzt die Vielzahl an verwendeten Internet-Passwrtern effektiv?In Gehackt versteht der Autor, Informationssicherheit leicht verstndlich und greifbar den Lesern nher zu bringen, die eingebauten Anekdoten lockern den Text immer wieder auf.10 von 12 Kunden fanden die folgende Rezension hilfreich. Blackout - Gefahren aus dem NetzVon RaumzeitreisenderDass im Internet Gefahren lauern, ist mittlerweile nicht nur fr IT-Fachleute, sondern auch fr durchschnittliche Nutzer des Internet eine Binsenweisheit. Geflschte Rechnungen, unberechtigte Abmahnungen, gestohlene Identitten u.v.a.m. sprechen eine deutliche Sprache. Nicht zuletzt durch die NSA- Affre ist jedem Brger klar geworden, dass smtliche digitale Kommunikation berwacht wird und dass das persnliche Profil ein offenes Buch ist. Dennoch werden Gefahren unterschtzt.Computer und Internet haben sich in einem solch rasanten Tempo entwickelt, dass fr Sicherheitsfragen keine Zeit mehr blieb. "Facebook, Twitter und E-Mails zu verbieten ist eine ebenso gute wie sinnvolle Empfehlung wie die, das Atmen einzustellen, weil die Luft verschmutzt sein knnte." (10) Autor Michael George bringt das Dilemma auf den Punkt.IT-Experte George kennt sich mit Sicherheitsfragen aus. Er ist in verschiedenen Funktionen bei deutschen Nachrichtendiensten ttig. Dabei arbeitet er fr die Spionageabwehr des Bayerischen Landesamtes fr Verfassungsschutz und untersttzt Unternehmen sowie Behrden bei der Abwehr von Cyber- Attacken. Er klrt ber Gefahren auf und bietet Lsungen an.Die Vernetzung elektronischer Steuerungstechnik von Versorgungseinrichtungen mit dem Internet fhrt zu einer Potenzierung realer Gefahren. Was passieren knnte, wenn Hacker das Stromnetz lahmlegen, hat jngst Marc Elsberg in seinem Roman "Blackout" beschrieben. Wir wrden im Chaos versinken. "Untersuchungen haben ergeben, dass wir uns nach etwa achtundvierzig Stunden am Rande des Chaos befnden, zu stark ist mittlerweile die Abhngigkeit von Elektrizitt", schreibt IT-Fachmann George. (19) Folglich

hat Elsberg in seinem Roman nicht bertrieben. Da stellt sich die Frage, ob es sinnvoll ist E-Werke oder Wasserwerke ber das Internet zu warten. Aber selbst bei Trennung vom Netz kann Schadsoftware im Zuge der Wartung ber angeschlossene Notebooks eingeschleust werden.In manchen Unternehmen sind gewachsene Systeme in ihren Abhngigkeiten nicht mehr vollstndig zu durchschauen. "Wir knnen das betroffene System nicht vom Netz nehmen, weil wir nicht wissen, welche Auswirkungen das auf unser Gesamtnetz htte. Es ist zu komplex." (46) Auf der anderen Seite nehmen Angriffe auf Steuerungsanlagen zu, wie z.B. der Angriff auf die iranischen Atomanlagen deutlich macht.Michael George unterscheidet zwischen Angriffen von einzelnen Personen, Gruppierungen und von staatlichen Stellen. Deutsche staatliche Stellen betreiben lt. George keine Wirtschaftsspionage. (80) George erklrt die Unterschiede zwischen Nachrichtendiensten und Geheimdiensten. Erstere unterliegen einer Kontrolle.Die Verffentlichungen von Snowden haben die Ttigkeiten der Geheimdienste in den Fokus gerckt. George macht deutlich, dass Terrorabwehr kein vorgeschobener Grund fr Wirtschaftsspionage sein darf. Auch drfen Daten nicht willkrlich abgehrt werden. Aber wer kontrolliert das? Insofern haben die Dokumente von Snowden eine Diskussion in Gang gesetzt, die lngst berfllig war.Warum ist die Abwehr von Hackerangriffen so schwierig? George geht ausfhrlich auf diese Problematik ein. Erstens sind viele Systeme zu komplex ("Too big to be protected"), zweitens erhlt Sicherheit auch aus Kostengrnden nicht die Prioritt, die ihr zustehen msste, drittens spielt der Faktor Zeit eine groe Rolle ("Hase-Igel-Problem") und viertens berichten Unternehmen nur selten ber Angriffe, um ihrem Image nicht zu schaden.George gibt Tipps fr private Nutzer und fr Firmen im Umgang mit Sicherheit. So sollten z.B. die 5% besonders wichtigen Firmendaten besonders gesichert und einzelne Netze wenn mglich getrennt werden. IT-Sicherheit muss als Unternehmensziel definiert werden. Fr private Nutzer gibt es neben den Mainstream-Produkten zahlreiche Alternativen.In "Die Numerati" thematisiert Stephen Baker, wie Datenhaie Profile auswerten und den Menschen quasi digital nachbilden. Ein Beispiel fr die digitale Datensammelwut liefert auch Gerald Reischl in "Die Google Falle". Diese Szenarien sind wirtschaftlich motiviert und zumindest nicht lebensgefhrlich. Was Michael George aufzeigt geht einen Schritt weiter. Er beschreibt die Folgen von Angriffen auf unsere Infrastruktur - aber auch Mglichkeiten der Gefahrenabwehr.Hinsichtlich der Struktur des Werkes sehe ich Mglichkeiten der Verbesserung, denn die Kapitel wirken beliebig aneinandergereiht. Das Buch richtet sich nicht an IT-Experten, sondern an Interessierte, die sich einen allgemeinen berblick ber das Thema Datensicherheit verschaffen wollen. Diese werden sensibilisiert, sich mit dem Thema intensiver zu beschftigen.

PressestimmenDer groe Hack ist keine Legende! (FAZ)Ein guter, aber auch bengstigender berblick ber die Cyberkriminalitt. (Gttinger Tageblatt)KurzbeschreibungLahmgelegte Industrie- und Energieanlagen, gestohlene Geheimdokumente und Firmengeheimnisse, ausgesphte Konto- und Personendaten, bedrohte Verkehrs- und Gesundheitssysteme die Abhngigkeit von Computern hat sich zur Achillesferse unseres Lebens entwickelt.ber Internetanschlsse und Smartphones kann jeder, der das ntige Knowhow besitzt, in Wohnungen, Bros und Fabriken eindringen. Wir vertrauen auf unsere Virenscanner und IT-Abteilungen, doch sptestens die Abhr- und Spionageaffre um die NSA zeigt, wie fatal diese Haltung ist. Denn auf dem Spiel stehen tatschlich nicht weniger als die Sicherheit und der Wohlstand unseres Landes und jedes Einzelnen von uns. Grokonzerne wehren Hunderttausende Virenangriffe ab tglich. Internetkriminalitt hat schon ber die Hlfte der deutschen Unternehmen getroffen und setzt inzwischen weltweit mehr Geld um als der Drogenhandel. Jeder zehnte Privat-PC gilt als gekapert und wird unbemerkt fr kriminelle Zwecke missbraucht.Ein Insider schlgt Alarm: Michael George wei so gut wie kaum ein anderer, dass der groe Hack und der Blackout keine Legenden sind, sondern jeden Tag eintreten knnen. Nach Lektre dieses Buches kennen wir das ganze Ausma der Gefahr, wissen aber auch, dass wir dennoch etwas tun knnen.ber den Autor und weitere MitwirkendeMichael George, Jahrgang 1968, ist seit seiner Ausbildung beim Bundesnachrichtendienst in verschiedenen Funktionen bei deutschen Nachrichtendiensten ttig. Derzeit arbeitet er fr die Spionageabwehr des Bayerischen Landesamtes fr Verfassungsschutz und untersttzt Unternehmen sowie Behrden bei der Abwehr elektronischer Angriffe. Er ist verheiratet und lebt mit seiner Familie in Mnchen.