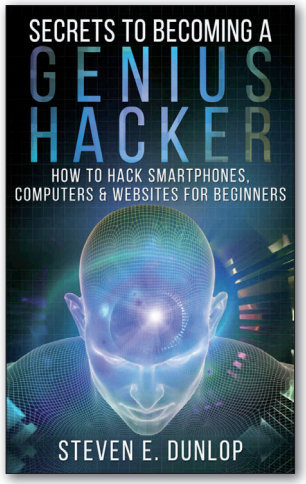
Aktuální normy a publikace o bezpečnosti

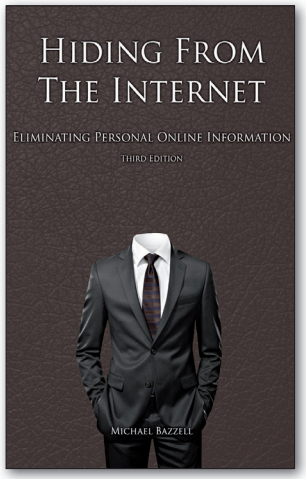
Jak se stát geniálním hackerem



Publikace *Hacking: Secrets To Becoming A Genius Hacker: How To Hack Smartphones, Computers & Websites For Beginners* je stručným, ale uceleným úvodem do světa hackingu. I přesto, že je tato kniha poměrně krátká, má pouhých 36 stran, obsahuje řadu zajímavých a skvěle podaných informací a tipů, jak se stát etickým hackerem. Vysvětluje nejběžnější typy útoků a na konkrétních příkladech popisuje např. hacknutí androidího smartphonu, prolomení hesla k WiFi síti zabezpečené WPA/WPA2 přes slabinu WPS, hacknutí počítače či webové stránky. Pro začínající hackery autor uvádí základní tipy čeho se vyvarovat a na druhé straně postupy, které by měl začínající hacker dodržovat.

https://www.amazon.com/

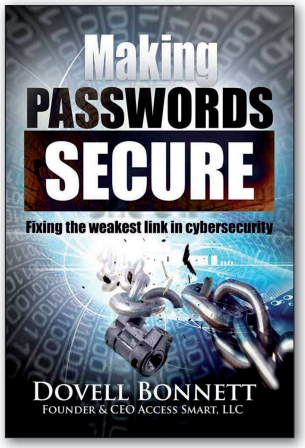
Jak se stát neviditelným na internetu



Kniha *Hiding from the Internet: Eliminating Personal Online Information* je určená všem, kteří si cení svého soukromí. Jedná se o výjimečnou publikaci, která by měla čtenářům ukázat, jak získat lepší kontrolu nad osobními daty v prostředí internetu. Autor nejprve uvádí postupy, jak identifikovat standardní informace, které jsou o vás na internetu k dispozici. A hned z kraje s upozorněním neprovádět tato vyhledávání v okamžiku, kdy máte spuštěný např. Gmail nebo Facebook. Postupně prochází konkrétní služby a úložiště vašich údajů a uvádí postupy jak omezit údaje, které o sobě uvádíte a jak odstranit ty, které jsou někde uvedené. Pro podporu návodů uvedených v této knize autor vytvořil také stránku: https://inteltechniques.com/.

https://www.amazon.com/

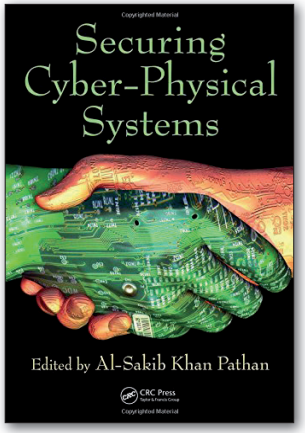
Hesla nejsou mrtvá



Hesla nejsou problém. Skutečnou noční můrou je však jejich správa, tedy vytváření, uchování a použití. Autentizace uživatele je nejvíce ignorované riziko v rámci počítačové bezpečnosti. Alespoň to tvrdí autor v úvodu knihy *Making Passwords Secure - Fixing the Weakest Link in Cybersecurity*. Na 170 stranách dokazuje, že vytvářet bezpečná hesla je nejen možné, ale že hesla se mohou stát účinným a cenově efektivním prvkem celkové kyberbezpečnosti. Kniha představuje novou metodu s názvem Infrastruktura správy a distribuce hesel (Password Authentication Infrastructure, PAI). Metoda je založená na silných a komplexních heslech, která jsou často měněna nástrojem pro správu hesel, který využívá pokročilé šifrovací algoritmy a bezpečné komunikační protokoly. Dále je založena na multifaktorové autentizaci a zejména na tom, že uživatel již není v roli správce hesel.

https://www.amazon.com/

Slovník řady 27k

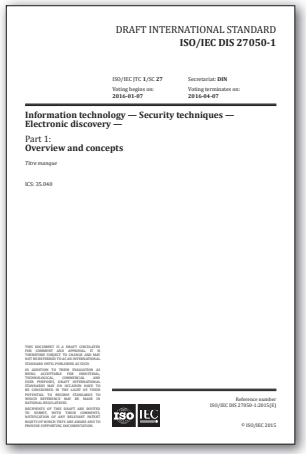


V pořadí již čtvrtá verze normy *ISO/IEC 27000:2016 Information technology – Security techniques – Information security management systems – Overview and vocabulary* byla publikována koncem února letošního roku. Kromě termínů a definic, které jsou určeny pro použití v celé rodině norem ISMS, obsahuje rovněž stručný popis k jednotlivým dosud publikovaným normám řady 27k. Dále poskytuje celkově dobře zpracovaný úvod do systémů řízení bezpečnosti informací vč. vysvětlení základních pojmů, jakými jsou informace, bezpečnost informací, systém řízení a procesní přístup. Jsou vysvětleny jednotlivé činnosti v rámci procesu ustavení, monitorování, udržování a zlepšování ISMS, tedy kroky procesu PDCA.

http://www.crcpress.com

Ing. Libor Široký, CISM, CRISC, AMBCI, *siroky@rac.cz*

Standard pro elektronické stopy

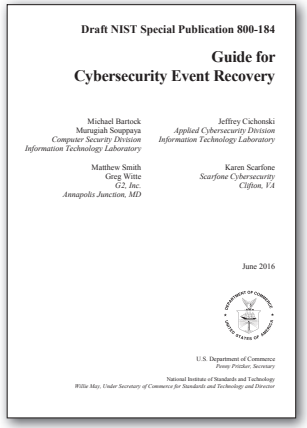

DRAFT INTERNATIONAL STANDARD
ISO/IEC DIS 27050-1

Information technology — Security techniques — Electronic discovery —
Part 1:
Overview and concepts

Pod označením *ISO/IEC FDIS 27050 – Information technology – Security techniques – Electronic discovery* je připravován soubor norem, které se budou věnovat problematice zajištění a zkoumání elektronicky uložených informací. Soubor bude obsahovat celkem čtyři normy: *ISO/IEC 27050-1 Overview and concepts, ISO/IEC 27050-2 Guidance for governance & management of electronic discovery, ISO/IEC 27050-3 Code of practice for electronic discovery, ISO/IEC 27050-4 ICT readiness for electronic discovery*. Hlavním účelem standardů pro digitální forenzní analýzu, které jsou postupně publikovány v rámci řady 27k, je prosazování osvědčených postupů a procesů v rámci celého vyšetřovacího cyklu zajištění dat až po jejich analýzu a reporting.

http://www.iso.org/

Zotavení z kybernetických incidentů


Draft NIST Special Publication 800-184

Guide for
Cybersecurity Event Recovery

June 2016

SP 800-184, Guide for Cybersecurity Event Recovery je připravovaný standard od amerického národního institutu pro standardy a technologii (National Institute of Standards and Technology, NIST) zaměřený na řešení následků způsobených kybernetickými bezpečnostními incidenty. Standard má podpořit organizace při přípravě a zlepšování plánů, procesů a postupů pro zvládání kybernetických událostí. Poskytuje taktické a strategické pokyny týkající se plnění cílů a úkolů při plánování, přípravě scénářů, testování a zlepšování plánů obnovy. Vlastní implementace jednotlivých doporučení je doložena na příkladu scénáře průniku do systému s následkem narušení důvěrnosti citlivých údajů. Standard je momentálně ve fázi veřejného připomínkování, které končí 11. července 2016.

http://csrc.nist.gov/publications/