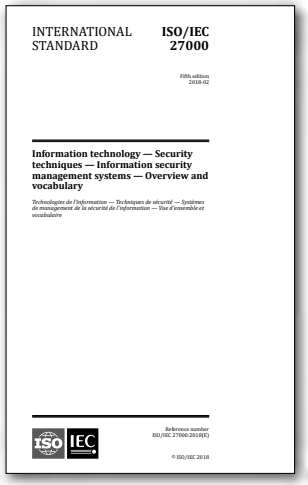
Aktuální normy a publikace o bezpečnosti

Slovník řady 27k popáté


INTERNATIONAL STANDARD
ISO/IEC 27000
Fifth edition 2018-02
Information technology — Security techniques — Information security management systems — Overview and vocabulary
Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire
Reference number ISO/IEC 27000:2018(E)
© ISO/IEC 2018

V únoru byla publikována již pátá verze normy *ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary*. Kromě termínů a definic, které jsou určeny pro použití v celé rodině norem ISMS, obsahuje stručný popis k jednotlivým dosud publikovaným normám řady 27k. Nabízí poměrně dobře zpracovaný úvod do systémů řízení bezpečnosti informací, včetně vysvětlení základních pojmů, jakými jsou bezpečnost informací, systém řízení, procesní přístup apod. V normě jsou vysvětleny jednotlivé činnosti v rámci procesů ustavení, monitorování, udržování a zlepšování ISMS. Drobných úprav v aktuálním vydání doznaly mimo jiné definice kolem monitorování a měření procesů a opatření bezpečnosti informací.

https://www.iso.org/

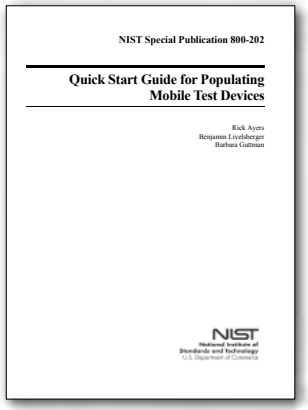
Kybernetická bezpečnost a ISO normy


TECHNICAL REPORT
ISO/IEC TR 27103
First edition 2018-02
Information technology — Security techniques — Cybersecurity and ISO and IEC Standards
Technologies de l'information — Techniques de sécurité — Cybersécurité et normes ISO et IEC
Reference number ISO/IEC TR 27103:2018(E)
© ISO/IEC 2018

Na konci února byla také publikována první letošní novinka z rodiny norem 27k. Technická zpráva *ISO/IEC TR 27103:2018 – Information technology – Security techniques – Cybersecurity and ISO and IEC standards* poskytuje návod, jak mohou být existující standardy řady 27k a další IEC normy využity při zajišťování kybernetické bezpečnosti. Dokument poskytuje informace o tom, proč je důležité vybudovat rámec kybernetické bezpečnosti, který bude založený na riziku, kontextu, prioritách, zaměřený na cíle a komunikaci. Popisuje cíle kybernetické bezpečnosti a zahrnuje mapování na relevantní ISO a IEC, které lze použít k dosažení těchto cílů. Norma je poměrně útlá, má pouhých 23 stran.

https://www.iso.org/

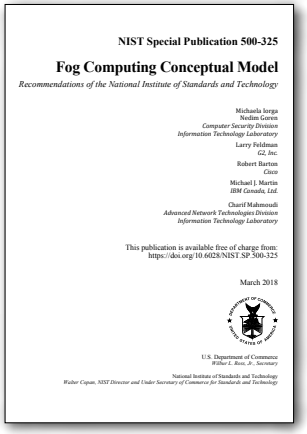
Jak na vyšetřování mobilních telefonů


NIST Special Publication 800-202
Quick Start Guide for Populating Mobile Test Devices
Rick Ayers
Benjamin Livelsberger
Barbara Guttman
NIST National Institute of Standards and Technology U.S. Department of Commerce

Americký národní institut pro standardy a technologii (NIST) v březnu publikoval standard zaměřený na postupy vyšetřování mobilních telefonů a tabletů. *Special Publication 800-202 Quick Start Guide for Populating Mobile Test Devices* obsahuje postupy a doporučení pro přípravu interní paměti mobilních zařízení za účelem testování forenzních postupů a produktů. Cíle standardu jsou dva: 1) poskytnout doporučení pro výběr relevantních dat, které se obvykle nacházejí v paměti mobilního zařízení, 2) poskytnout návod, jak vybraná data efektivně testovat. Příloha B pak obsahuje přehled jednotlivých datových typů a formuláře pro záznam hodnot identifikovaných během forenzního zkoumání.

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

Konceptuální model mlžných sítí

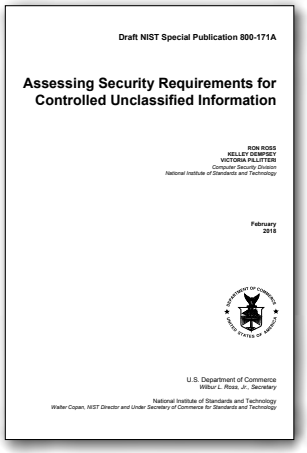

NIST Special Publication 500-325
Fog Computing Conceptual Model
Recommendations of the National Institute of Standards and Technology
Michaela Iorga
Nedim Goren
Computer Security Division
Information Technology Laboratory
Larry Feldman
G2, Inc.
Robert Barton
Cisco
Michael J. Martin
IBM Canada, Ltd.
Charif Mahmoudi
Advanced Network Technologies Division
Information Technology Laboratory
This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-325
March 2018
U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary
National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Dalším z březnových standardů od NIST je *Special Publication 500-325 Fog Computing Conceptual Model, Recommendations of the National Institute of Standards and Technology*. Standard dopodrobna vysvětluje konceptuální model a principy tzv. fog computingu a dává doporučení pro jeho nasazení v praxi. Podstatou fog computingu je, že výpočty neprobíhají na cloudovém serveru, ale na hraničním zařízení (mobilní zařízení, síťový prvek), které je blíže koncovému uživateli. Zpracování dat na zařízeních v místě události výrazně zkracuje dobu odezvy a urychluje odbavení provozu. Mezi další výhody fog computingu patří lokální zpracování, což může být výhodné z hlediska soukromí a bezpečnosti dat.

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

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

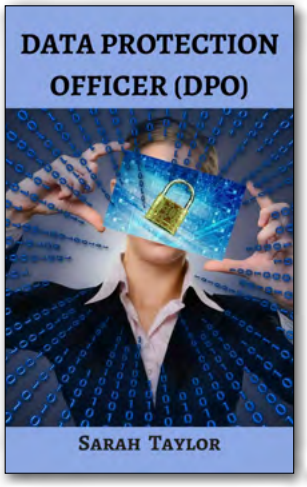
Požadavky na ochranu informací


Draft NIST Special Publication 800-171A
Assessing Security Requirements for Controlled Unclassified Information
RON ROSS
KELLEY DEMPSEY
VICTORIA PILLITTERI
Computer Security Division
National Institute of Standards and Technology
February 2018
U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary
National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Special Publication 800-171A Assessing Security Requirements for Controlled Unclassified Information poskytuje soubor postupů pro posouzení bezpečnostních požadavků uvedených v *SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Jedná se o bezpečnostní požadavky, které musí být splněny, aby byla zajištěna ochrana neklasifikovaných vládních informací zpracovávaných v nevládních informačních systémech a organizacích. SP 800-171A popisuje základní metody a cíle hodnocení pro čtrnáct skupin bezpečnostních požadavků (hodnocení rizik, řízení přístupů, fyzická bezpečnost atd.). Přílohy poskytují další informace související s hodnocením včetně vysvětlení jednotlivých bezpečnostních požadavků. V prostředí České republiky může být standard dobrým zdroje při implementaci požadavků kybernetického zákona.

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

Doporučení pro DPO



Obecné nařízení Evropského parlamentu a Rady (EU) 2016/679 známé jako GDPR s kromě jiného také přináší požadavek na ustavení role pověřence pro ochranu osobních údajů (DPO). I přes často chybnou interpretaci v médiích se povinnost jmenovat pověřence rozhodně netýká všech organizací. Pověřence musí jmenovat všechny orgány veřejné moci a veřejné subjekty. Ostatní správci a zpracovatelé musí DPO jmenovat pokud podstata jejich činností spočívají v rozsáhlém zpracování zvláštních kategorií osobních údajů, případně spočívá v rozsáhlém a systematickém monitorování subjektů údajů. Březnová novinka s výmluvným názvem *Data Protection Officer (DPO)* se věnuje odpovědnostem a povinnostem DPO při dodržování souladu s GDPR, mezi které patří také komunikace s dozorovými úřady a subjekty údajů.

https://www.amazon.com/