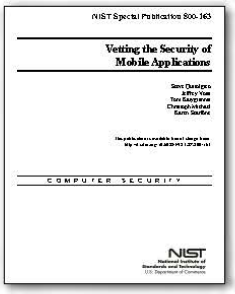
# Aktuální normy a publikace o bezpečnosti

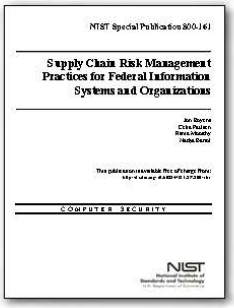
## Prověřování mobilních aplikací




Americký národní institut pro standardy a technologii (National Institute of Standards and Technology, NIST) publikoval v první polovině letošního roku tři zajímavé standardy. Prvním z nich je *SP 800 – 163 Vetting the Security of Mobile Applications*. Účelem standardu je pomoci organizacím pochopit a implementovat proces a postupy prověřování bezpečnosti mobilních aplikací. Vytvořit požadavky na jejich bezpečnost, porozumět zranitelnostem Android / iOS aplikací a metodám, jak tyto zranitelnosti detekovat. Jak nastavit kritéria jejich akceptace ve světle firemních požadavků na bezpečnost. Standard vyzdvihuje zejména ty faktory, které jsou v procesu schvalování aplikací a jejich updatů kritické (např. k jakým datům a periferiím bude mít aplikace přístup).

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

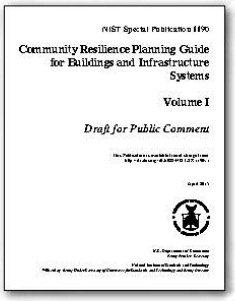
## Řízení rizik dodavatelů




Druhým standardem je *SP 800 – 161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, který je zaměřený na řízení rizik v dodavatelských řetězcích. Standard poskytuje metodiku pro řízení ICT rizik v řetězci dodavatelů (ICT Supply Chain Risk Management, ICT SCRM), a to na všech úrovních organizace. Metodika je postavena na čtyřech pilířích – bezpečnost informací, integrita ICT produktů, kontinuita a kvalita v rámci dodavatelského řetězce. Standard vychází ze základních konceptů již existujících standardů. Zejména *NIST SP 800-30 (Risk Assessments), NIST SP 800-37 (Risk Management), NIST SP 800-39 (Managing Information Security Risk)*, ale také u nás známější normy ISO/IEC 27036 Information Security for Supplier Relationships. Katalog bezpečnostních opatření v rámci dodavatelských vztahů čerpá z *NIST 800-53 (Security and Privacy Controls)*.

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

## Odolnost při krizových událostech

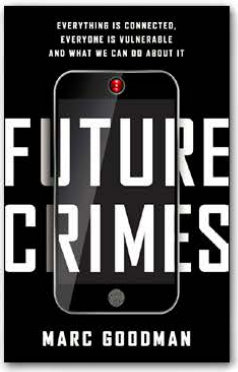



Třetím standardem z dílny NIST je *SP 1190 Community Resilience Planning Guide for Buildings and Infrastructure Systems (Draft)*, který je zaměřen na problematiku resilience (odolnosti) v rámci komunit (společenství lidí žijících ve stejném místě) ve vztahu ke krizovým událostem. Tento dvoudílný standard obsahuje doporučení a best practice pro vytvoření resilientní komunity schopné reagovat a zotavit se z krizových událostí (povodně, blackout, epidemie apod.). Jedním z hlavních záměrů a doporučení standardu je, aby komunity měly vytvořeny své plány odolnosti (resilience plans), které budou koordinovat postupy při mimořádných a krizových událostech. Jde např. o negativní následky týkající se budov, infrastruktury, veřejných služeb apod. První část standardu obsahuje zásady a best practice postupy, jak plány vytvořit. Druhá je detailním zdrojem informací pro jejich implementaci.

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

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

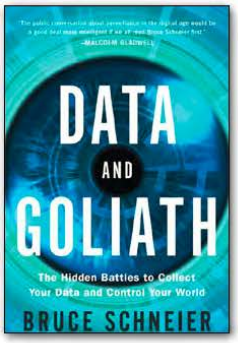
## Zločiny budoucnosti




Další publikací, kterou byste si letos neměli nechat ujít, je kniha *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*. Kniha čtenáře vtáhne do světa digitálního undergroundu. Do prostředí, kde hackeři již nejsou omezeni běžnými počítači a chytrými telefony, ale naopak se jim otevírají zcela nové a v tuto chvíli jen málo tušené příležitosti. Pro běžného člověka jako oběť jsou to znepokojující možnosti, které dnes mají a budou mít zločinci, korporace a vlády některých zemí s použitím nových a vznikajících technologií. Dělají nás zranitelnějšími, než jsme si kdy dokázali představit. Budoucnost kyberzločinu je spjatá s Internetem věcí (Internet of Things, IoT). Střízlivé odhady tvrdí, že kolem roku 2020 bude celosvětově připojeno k Internetu až 50 miliard věcí denní potřeby, o jejichž zabezpečení nebudeme nic vědět.

*http://www.futurecrimes.com/*

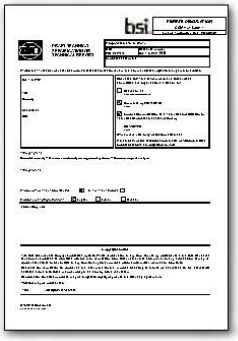
## Data a Goliáš




Neméně znepokojivou je další letošní novinka od americké kapacity na kryptografii a počítačovou bezpečnost Bruce Schneiera *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. Hned zdroje knihy se dozvíte, že jste trvale pod dohledem – postava absolutistického vládce z románu 1984 už není fikcí. Vlády a korporace vybudovaly bezprecedentní systém dohledu nad každým z nás. Mobilní operátor sleduje vaši polohu a ví, kdo je s vámi, internetové obchody mají perfektní přehled o tom, kdy jste nemocní nebo těhotní, Google ví, kdy jste nezaměstnaní a co si myslíte, Facebook zná vaši sexuální orientaci, aniž byste ji kdy zmínili. Korporace manipulují s články a reklamou, vlády používají dohled k cenzuře a omezení svobody projevu. Taková je dnešní situace. Autor nabízí jinou cestu, která si cení jak bezpečnosti, tak soukromí.

*https://www.schneier.com/*

## Analýza dopadů podrobně




Dalším připravovaným standardem z dílny technické komise ISO/TC 223 je *ISO 22317 Societal security – Business continuity management systems – Business impact analysis (BIA)*. Tento mezinárodní standard poskytne podrobné doporučení pro ustavení, implementaci a udržování procesu analýzy business dopadů (BIA) v souladu s tím, jak požaduje certifikační norma ISO 22301 (požadavky na certifikaci BCMS). Nastavuje a upřesňuje kroky, které musí předcházet každé BIA, jako je vymezení kontextu a rozsahu BCM programu apod. Následně pak již dává doporučení směrem k vlastnímu procesu BIA. Čtenáře provádí definicemi rolí a odpovědností, přípravou a provedením vlastního hodnocení dopadů na úrovni produktů a služeb, procesů a činností, které tyto produkty zajišťují, postupy pravidelné revize BIA.

*http://www.iso.org/*