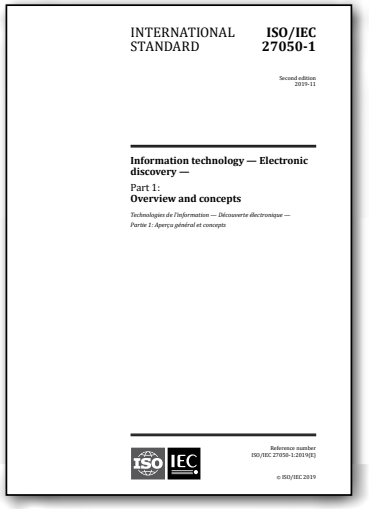
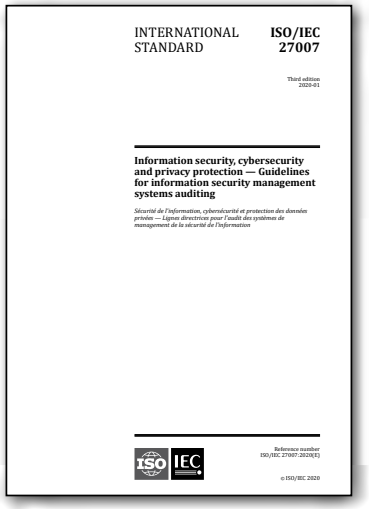
Aktuální normy a publikace o bezpečnosti



Zajišťování elektronických stop

Druhé revidované vydání *ISO/IEC 27050-1:2019 – Information technology – Electronic discovery – Part 1: Overview and concepts* bylo zveřejněno v listopadu 2019. Hlavní změny spočívají v aktualizaci odkazů na normy této řady a sladění terminologie. Normy jsou zaměřeny na postupy zajišťování a zkoumání elektronicky uložených informací, přičemž první část definuje pojmy spojené s identifikací, shromažďováním, zpracováním a analýzou elektronicky uložených informací. Sérii tvoří celkem čtyři normy, kde kromě první části byly publikovány *ISO/IEC 27050-2:2018 Guidance for governance and management of electronic discovery* a *ISO/IEC 27050-3 Code of practice for electronic discovery. ISO/IEC 27050-4 ICT readiness for electronic discovery* je stále ve verzi draft s předpokládaným termínem publikace v roce 2021.

https://www.iso.org/



Doporučení k auditu ISMS

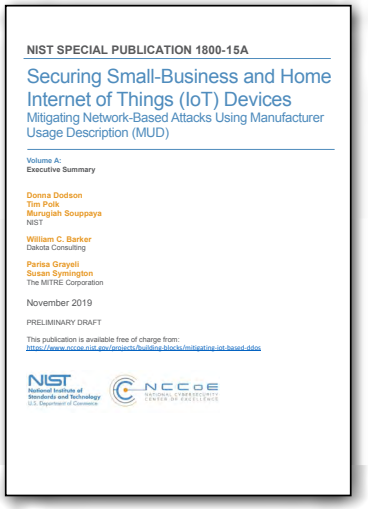
V lednu 2020 bylo publikováno třetí revidované vydání *ISO/IEC 27007:2020 – Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing*, v němž byla tato norma uvedena do souladu s nejnovější verzí ISO 19011: 2018 – *Guidelines for auditing management systems*. Norma obsahuje doporučení pro přípravu programu auditu systému řízení bezpečnosti informací (ISMS) a kontrolu shody s požadavky ISO/IEC 27001:2013. Obsahuje také doporučení a požadavky na kompetence auditorů ISMS, jakož i kritéria pro jejich hodnocení. Obsahově norma čerpá zejména z ISO 19011:2018. V rámci výčtu jednotlivých požadavků se buďto přímo odkazuje na ISO 19011 nebo uvádí požadavky specifické pro auditování ISMS.

https://www.iso.org/

Rámec pro sdílení informací

Letošní novinkou v řadě norem připravovaných technickou komisí ISO/TC 292 Security and resilience je standard *ISO 22396:2020 – Security and resilience – Community resilience – Guidelines for information exchange between organizations*. Činnost ISO/TC 292 je zaměřena na přípravu norem a doporučení pro zvýšení bezpečnosti a odolnosti společnosti. ISO 22396 poskytuje doporučení pro sdílení informací mezi organizacemi. Cílem spolupráce je identifikovat a iniciovat kroky ke zvýšení bezpečnosti a snížení potenciálních zranitelností. Výměna informací o možných rizicích a zranitelnostech pomáhá zvýšit účinnost a efektivitu organizací při řešení obdobných incidentů a mimořádných událostí. Norma zahrnuje zásady, rámec a proces výměny informací. Pro označování a sdílení informací s třetími stranami využívá klasifikaci podle TLP (Traffic Light Protocol).

https://www.iso.org/



Bezpečný provoz IoT zařízení

S tím, jak roste popularita zařízení internetu věcí (IoT), rostou také obavy o jejich bezpečnost. Jedním z nových standardů, které se věnují rizikům spojeným s provozem IoT, je také *SP 1800-15 Securing Small Business and Home Internet of Things (IoT) Devices*. Popisuje pro vývojáře a implementátory IoT přístup založený na standardu MUD (Manufacturer Usage Descriptions), založený na automatickém omezení síťové komunikace výhradně na provoz, který IoT zařízení vyžadují k plnění svých zamýšlených funkcí. Cílem MUD je, aby se IoT zařízení chovala pouze tak, jak bylo zamýšleno jejich výrobcem. Standard připravilo americké národní centrum pro kybernetickou bezpečnost NCCoE ve spolupráci s NIST.

https://csrc.nist.gov/publications/

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