Aktuální normy a publikace o bezpečnosti

Mapování starých norem na nové

Horké letní měsíce letos přinesly kromě jiného také nebývale velký počet nových přírůstků do rodiny norem ISO 27k. Celkem bylo vydáno šest nových standardů. Prvním z nich je ten nejdéle očekávaný *ISO/IEC TR 27023:2015 Information technology – Security techniques – Mapping the Revised Editions of ISO/IEC 27001 and ISO/IEC 27002*. Norma je v podstatě jen oficiální verzí mapování nových verzí dvojice norem ISO/IEC 27001 a ISO/IEC 27002 z roku 2013 na jejich předchůdce z roku 2005. S ohledem na neuvěřitelně dlouhou dobu, kterou technické komisi zabrala publikace jednoduché převodní tabulky, se zdá celý počin skoro zbytečným. Podobná, byť neoficiální mapování se objevila již záhy po publikaci nových verzí norem v roce 2013.

http://www.iso.org/

Nastavení metod vyšetřování incidentů

ISO/IEC 27041:2015 – Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative methods patří do skupiny standardů, které se věnují správným postupům v oblasti digitální forenzní analýzy. Do skupiny souvisejících standardů patří ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042, ISO/IEC 27043 a ISO/IEC 27050. Společným cílem těchto standardů je prosazovat nejlepší praktiky, metody a postupy zajišťování digitálních důkazů, vyhledávání a vytěžování dat pro určité specifické účely v rámci forenzního zkoumání. ISO/IEC 27041 poskytuje konkrétní doporučení a požadavky ohledně ustavení a zavedení správných metod a postupů vyšetřování incidentů bezpečnosti informací.

http://www.iso.org/

Detekce a prevence v sítích

Druhým letním přírůstkem je *ISO/IEC 27039:2015 – Information technology – Security techniques – Selection, deployment and operation of intrusion detection and prevention systems (IDPS)*. Na zhruba padesáti stránkách norma poskytuje doporučení ohledně implementace systémů pro detekci a prevenci průniku (IDPS). Tedy systémů, které monitorují síťový provoz a aktivity operačního systému a odhalují škodlivé činnosti, které by mohly vést k narušení bezpečnosti. S cílem tyto činnosti identifikovat, získat informace o jejich průběhu, nahlásit, případně zablokovat. Norma konkrétně obsahuje doporučení pro jejich výběr, nasazení a provoz IDPS systémů.

http://www.iso.org/

Analýza a interpretace digitálních dat

Dalším ze skupiny forenzních standardů je *ISO/IEC 27042:2015 – Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*. Jak název standardu napovídá, nabízí doporučení ohledně procesu analýzy a interpretace digitálních důkazů. Kromě obvyklých opatření, jako je zajištění důkazního řetězce a pečlivá dokumentace všech kroků, klade standard důraz na integritu celého procesu. Pokud jsou stejné digitální důkazy zpracovávány různými vyšetřovateli, měli by vyšetřovatelé dospět ke stejným závěrům. V každém případě by však mělo být v dokumentaci přesně dohledatelné, proč se posudky liší. Okrajově se standard také dotýká výběru forenzních nástrojů, odborných znalostí a kompetencí forenzních vyšetřovatelů.

http://www.iso.org/

Bezpečné ukládání a archivace dat

Třetím standardem z dílny technické komise ISO/IEC JTC 1, subkomise SC 27 je *ISO/IEC 27040:2015 – Information technology – Security techniques – Storage Security*. Záměrem standardu je poskytnout organizacím doporučení během procesu akvizice a provozování technologií na ukládání a archivaci dat. Konkrétně se věnuje souvisejícím rizikům bezpečnosti informací a návrhu opatření na jejich pokrytí. Rozsahem pokrývá bezpečnost zařízení a médií a s nimi souvisejících činností včetně ukládání a přenosu informací, ať už ze strany aplikací/IT služeb nebo koncových uživatelů. Na standardy řady ISO27k je až nezvykle detailní, má více než sto stran.

http://www.iso.org/

Postupy a kroky vyšetřování incidentů

Posledním ze skupiny forenzních standardů je *ISO/IEC 27043:2015 – Information technology – Security techniques – Incident investigation principles and processes*. Poskytuje všeobecný přehled o principech a různých postupech použitelných v rámci jednotlivých kroků procesu analýzy digitálních důkazů, při vyšetřování jakýchkoli typů incidentů bez toho, aby zacházel do konkrétních detailů. Navazuje tak na doporučení k výběru a ustavení metodik vyšetřování uváděných ve standardu ISO/IEC 27041. Otevřenou otázkou zůstává, jaký má subkomise SC 27 důvod publikovat doporučení k jednotlivým krokům procesu digitální forenzní analýzy jako samostatné standardy. Publikace jednoho vícedílného standardu by možná dávala větší smysl a působila by přehledněji.

http://www.iso.org/

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