Nehádejte, měřte!

Víte, jak silná je vaše firemní bezpečnost? Ne? Tak ji změřte! A jak na to?

Takřka pod vánoční stromeček nadělila bezpečnostním expertům mezinárodní organizace pro normalizaci ISO finální verzi normy ISO/IEC 27004, která pojednává o měření bezpečnosti. Splnila tak přání mnoha manažerů, kteří bezvýsledně hledali způsob, jak objektivně hodnotit efektivitu Systému řízení bezpečnosti informací (ISMS). Cílem článku je provést stručnou charakteristiku zmíněné normy a uvést její cíle.

V prosinci minulého roku vydaný mezinárodní standard (celým názvem ISO/IEC 27004 – Information technology – Security techniques – Information security management – Measurement) přináší doporučení, jak vytvářet a používat metriky či měření při hodnocení efektivity zavedeného ISMS a bezpečnostních opatření specifikovaných v normě ISO/IEC 27001. Doporučení lze aplikovat na všechny typy firem bez ohledu na jejich zaměření či velikost. K uplatnění výše uvedeného standardu jsou potřeba ještě standardy ISO/IEC 27000 – Overview and vocabulary (slovník) a zejména ISO/IEC 27001 – Requirements (požadavky), jelikož ISO/IEC 27004 na ně navazuje.

Struktura normy

Norma ISO/IEC 27004 popisuje metriky a postupy měření potřebné k hodnocení efektivity ISMS, pomocí kterých pak podnik dosahuje adekvátního řízení bezpečnosti a vyvážených bezpečnostních opatření požadovaných normou ISO/IEC 27001:2005.

Standard ISO/IEC 27004 začíná přehledem programu a modelu měření bezpečnosti (Information Security Measurement Programme a Information Security Measurement Model), pokračuje řízením potřeb pro měření bezpečnosti informací a vše uzavírají koncepty a postupy pro zavádění programu měření bezpečnosti informací.

Norma obsahuje ještě dvě přílohy. Do přílohy A umístili autoři šablonu pro koncept měření, který tvoří prvky Modelu měření bezpečnosti informací. Do přílohy B pak zařadili reálné příklady konceptů měření pro konkrétní opatření nebo postupy ISMS, kde je prakticky použita šablona z přílohy A.

Příklad z přílohy B je uveden v tabulce 1. V daném případě je rozebrán koncept měření ochrany proti vniknutí nebezpečného kódu, kde jsou v levém sloupci tučně zvýrazněny názvy jednotlivých částí modelu, které se dále rozpadají na konkrétní prvky. Do pravého sloupce se pak zapisují samotné hodnoty.

Příklady použití šablon z přílohy B mají organizacím pomoci se zaváděním měření bezpečnosti informací či se zaznamenáním činností měření a jejich výsledků.

Jak sama norma uvádí, účelem měření bezpečnosti informací ve vztahu k ISMS je:

- Vyhodnocení efektivity zavedených opatření.
- Vyhodnocení efektivity zavedeného ISMS.
- Ověření rozsahu vyhovujících požadavků.
- Usnadnění zlepšování bezpečnosti informací v rámci celkových obchodních rizik organizace.
- Poskytnutí vstupů pro manažerská rozhodnutí, aby usnadnily rozhodování spojené se Systémem řízení bezpečnosti informací (ISMS), a pro odůvodnění potřebná ke zlepšení zavedeného ISMS.

Norma dále např. uvádí, že organizace by si měla stanovit cíle měření s ohledem na:

- Roli bezpečnosti informací v celkových firemních obchodních aktivitách a rizicích, se kterými se firma potýká.
- Aplikovatelnost právních, regulatorních a smluvních požadavků.
- Organizační strukturu firmy.

Ochrana proti nebezpečnému kódu	
Identifikace konceptu měření	
Jméno konceptu měření	Ochrana proti nebezpečnému softwaru.
Číselný identifikátor	Specifické uspořádání.
Účel konceptu měření	Hodnocení efektivity ochrany systému proti nebezpečným softwarovým útokům.
Cíl opatření/procesů	Cíl opatření A.10.4 [27001:2005]. Pro ochranu integrity softwaru a informací. (Plánovaný) Pro ochranu integrity softwaru a informací před nebezpečným softwarem.
Opatření/procesy	Opatření 10.4.1 [27001:2005]. Opatření proti nebezpečnému kódu. Opatření odhalení, prevence a obnovení pro ochranu proti nebezpečnému softwaru a vhodné uživatelské procedury, které se budou realizovat.
Objekt měření a atributy	
Objekt měření	1. Hlášení o incidentech. 2. Záznamy o protiopatřeních softwaru proti nebezpečnému softwaru.
Atributy	Incidenty způsobené nebezpečným softwarem.
Specifikace základní metriky	
Základní metrika	1. Množství bezpečnostních incidentů způsobených nebezpečným softwarem. 2. Celkový počet zablokovaných útoků od nebezpečného softwaru.
Metoda měření	1. Spočítá množství bezpečnostních incidentů způsobených nebezpečným softwarem v záznamech incidentů. 2. Spočítá množství záznamů zablokovaných útoků.
Typ metody měření	1. Objektivní.2. Objektivní.
Měřítko	1. Celá čísla od nuly do nekonečna. 2. Celá čísla od nuly do nekonečna.
Typ měřítka	1. Pořadové číslovky. 2. Pořadové číslovky.
Jednotka měření	1. Bezpečnostní incident. 2. Záznamy.
Specifikace odvozené metriky	
Odvozené metriky	Síla ochrany proti nebezpečnému softwaru.
Funkce měření	Množství bezpečnostních incidentů způsobených nebezpečným softwarem/množstvím zjištěných a zablokovaných útoků způsobených nebezpečným softwarem.
Specifikace indikátoru	
Indikátor	Trend odhalených útoků, které nebyly zablokovány během hlášeného období.
Analytický model	Porovnává současnou hodnotu s minulou (v %).
Popis rozhodovacích kritérií	
Rozhodovací kritéria	Trendové linky by měly zůstávat pod určitou mírou. Výsledný trend by měl být sestupný či konstantní.
Výsledky měření	
Interpretace indikátoru	Výsledný trend by měl být sestupný či konstantní. Vzestupný trend signalizuje zhoršování souladu s opatřením, klesající trend signalizuje zlepšování souladu s opatřením. Když se trendová linka nápadně zvýší, mělo by začít vyšetřování příčiny, případně další potřebné protiopatření.
Formy hlášení	Trendová linka, která zobrazuje poměr odhaleného a odstraněného nebezpečného softwaru s trendovými linkami z předchozích období.
Zainteresované strany	
Zákazník měření	Management bezpečnosti.
Recenzent měření	Management bezpečnosti.
Vlastník informace	Systémový administrátor.
Osoba/organizační jednotka odpovědná za sběr dat	Bezpečnostní management, Systémový administrátor, Síťový manažer.
Osoba/organizační jednotka odpovědná za analýzu dat a hlášení výsledků měření	Koordinace služeb.
Frekvence/Perioda	
Frekvence sběru dat	Denně.
Frekvence analýzy dat	Měsíčně.
Frekvence hlášení výsledků měření	Měsíčně.
Termín revize	Každoročně.
Perioda měření	Jednou ročně.

- Náklady a přínosy zavedení měření informační bezpečnosti.
- Firemní kritéria pro akceptaci rizik.
- Potřebu porovnat několik ISMS v jedné organizaci.

Program měření bezpečnosti informací

Aby organizace dosahovala stanovených cílů měření, měla by zavést a řídit Program měření bezpečnosti informací. Organizace by si také měla osvojit koncept měření, aby docílila opakovatelných, objektivních a užitečných výsledků měření založených na Modelu měření bezpečnosti informací.

Program měření bezpečnosti informací a zavedený koncept měření by měl zajistit, aby organizace efektivně dosahovala cílů, opakovatelných měření, a rovněž by měl poskytnout výsledky měření zainteresovaným stranám k identifikaci potřeb pro zlepšování zavedeného ISMS včetně jeho rozsahu, politik, cílů, opatření, procesů a procedur.

Organizační a provozní struktura Programu měření bezpečnosti informací by měla vyplývat z rozsahu a složitosti ISMS nebo jeho částí. Za všech okolností by v Programu měření bezpečnosti informací měly být role a povinnosti explicitně přiřazeny kompetentní osobě. Měření vybraná a zavedená Programem měření bezpečnosti informací by měla přímo souviset s činností ISMS, zbývající měření pak s podnikovými procesy. Měření může být integrováno do běžného provozu aktivit nebo vykonáváno v pravidelných intervalech stanovených v řízení ISMS.

Tab. 1: Příklad konceptu měření ochrany proti vniknutí nebezpečného kódu demonstruje, jak v praxi použít normu ISO/IEC 27004 prostřednictvím šablony uvedené v příloze A normy. (Zdroj: [1] příloha B. 6 Protection against Malicious Code).

Model měření bezpečnosti informací

Norma obsahuje též Model měření bezpečnosti informací, který představuje strukturu spojující informační potřeby se souvisejícími objekty měření a jejich atributy. Objekty měření mohou zahrnovat plánované či zavedené procesy, procedury, projekty a zdroje. Model měření bezpečnosti informací popisuje, jak významné atributy jsou kvantifikované a převedené na indikátory, které poskytují základ pro rozhodování. Více viz obr. 1, v modelu použité termíny jsou vysvětleny v tabulce 2.

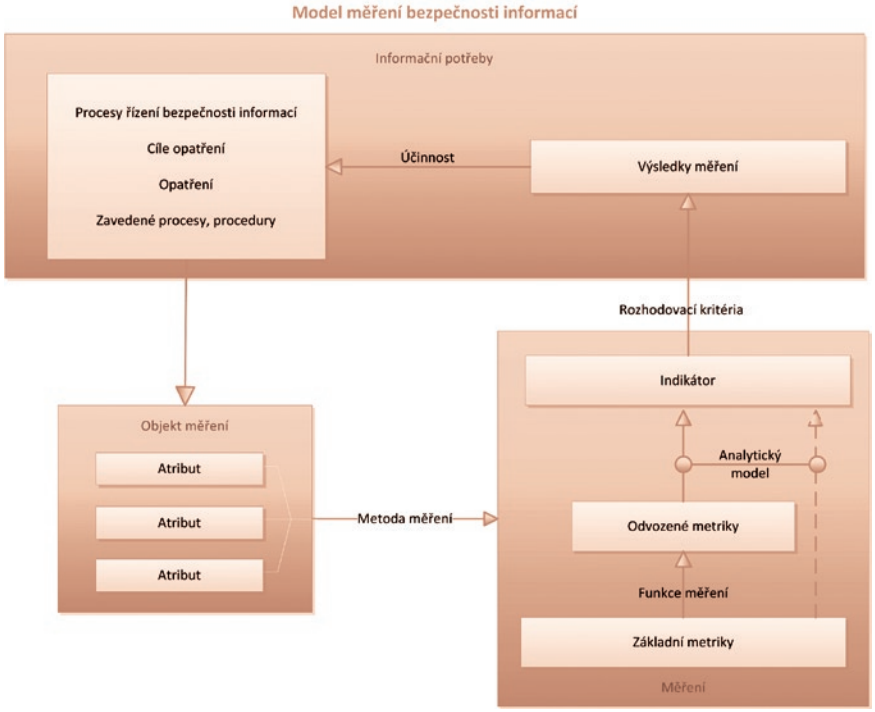
Závěr

Ve stručnosti charakterizovaná norma ISO/IEC 27004 by neměla chybět v knihovně žádného bezpečnostního manažera. Standard přináší řešení jednoho z nejpalčivějších problémů firemní bezpečnosti – jak měřit úspěšnost a účinnost zavedení ISMS. Vytváří tím manažery často požadovanou zpětnou vazbu a argumenty pro investice do bezpečnosti. A navíc v harmonii s rodinou norem 27K.

Zbyněk Marx
marx@rac.cz

Zbyněk Marx

Autor pracuje jako konzultant ve společnosti Risk Analysis Consultants, současně studuje obor Informační technologie a management na Bankovním institutu vysoká škola v Praze.



Obr. 1: Model měření bezpečnosti informací.

Termín	Popis
Analytický model	Algoritmus nebo výpočet kombinující jednu či více metrik a/nebo odvozených metrik s přidruženými rozhodovacími kritérii.
Atribut	Vlastnost nebo charakteristika objektu, která může být rozlišena lidskými či automatizovanými prostředky.
Funkce měření	Provedený algoritmus nebo výpočet kombinující jednu či více základních metrik.
Indikátor	Metrika poskytující odhad nebo ohodnocení specifikovaných atributů získaných z analytického modelu s ohledem na definované informační požadavky.
Informační potřeba	Porozumění nezbytné k dosažení krátkodobých a dlouhodobých cílů, k řízení rizik a zvládání problémů.
Měření	Proces získání informace o účinnosti ISMS a opatření pomocí metody měření, funkce měření, analytického modelu a rozhodovacích kritérií.
Metoda měření	Všeobecně popsaná logická posloupnost operací použitá ke kvantitativnímu určení atributu s ohledem na stanovené měřítko. Pozn.: Typ metody měření závisí na povaze operací použitých ke kvantitativnímu určení atributu. Rozlišujeme dva typy metod měření – subjektivní (kvantitativní určení zahrnuje lidské posouzení) a objektivní (kvantitativní určení je založeno na numerických pravidlech).
Metrika	Proměnná, do které je přiřazena hodnota jako výsledek měření Pozn.: Termín „metriky“ souhrnně odkazuje na základní metriky, odvozené metriky a indikátory. Příklad: porovnání plánované a skutečné naměřené chybovosti a vyhodnocení, zda získaný rozdíl ukazuje či neukazuje na problém.
Objekt měření	Objekt (entita), který je charakterizovaný prostřednictvím měření svých atributů. Objekt může zahrnovat procesy, plány, projekty, zdroje a systémy nebo části systémů.
Odvozená metrika	Metrika, která je definována jako funkce jedné nebo více hodnot základních metrik.
Opatření	Prostředek řízení rizik zahrnuje politiky, směrnice, metodické pokyny, praktiky nebo organizační struktury, které mohou být povahy administrativní, technické, řídicí či legislativní.
Rozhodovací kritéria	Prahy, cíle nebo vzory používané k určení požadavku na činnost či na další zkoumání nebo k popisu úrovně důvěry v dané výsledky.
Výsledky měření	Jeden nebo více indikátorů a jejich interpretace, které poukazují na informační požadavky.
Základní metrika	Metrika definovaná pomocí atributu a metody, která tento atribut kvantitativně určuje. Pozn.: Základní metrika je funkčně nezávislá na ostatních metrikách.

Tab. 2: Popis termínů z Modelu měření bezpečnosti informací. (Zdroj: [1]).

POUŽITÉ ZDROJE

[1] ISO/IEC 27004 – Information technology – Security techniques – Information security management – Measurement.