ISMS – systém řízení bezpečnosti informací

řešení požadavků zákona o kybernetické bezpečnosti

Autor

Ing. Zdeněk Vaněk, CSc., e-mail: vane@dcit.cz

V České republice je od 1. 1. 2015 platný prováděcí předpis k zákonu o kybernetické bezpečnosti č. 181/2014 Sb. vydaný formou Vyhlášky NBÚ č. 316/2014 Sb. Z §30 zákona o kybernetické bezpečnosti jednoznačně vyplývá povinnost zajistit plnění požadavků specifikovaných výše uvedenými předpisy do 1 roku ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou. To je náročný úkol, když uvážíme čas nutný na určení rozsahu informačního systému řízení bezpečnosti (dále ISMS), analýzu informačních aktiv a rizik, návrh a zpracování potřebných postupů, proškolení pracovníků, zkušební provoz a zpracování výsledné dokumentace ISMS.

Standardní postup sestává ze 7 etap

Etapa 1 – Vymezení ISMS: Specialista ISMS se seznámí se systémem s kritickou infrastrukturou a vymezí jeho rozsah. Není výjimkou, že během této etapy zjistí závažné nedostatky v informační bezpečnosti i, které si vzhledem k tzv. provozní slepotě správce informačního systému neuvědomuje. Autor se ve své praxi setkal například s příklady, kdy dodavatel software měl nekontrolovatelný přístup k systému včetně dat, kdy vlivem organizačních změn celým skupinám delimitovaných pracovníků nebyl odebrán přístup do systému, kdy probíhala nezabezpečená výměna dat s externí organizací. Výsledkem této etapy je jednoznačné vymezení rozsahu ISMS a případné upozornění na závažný bezpečnostní nedostatek.

Etapa 2 – Analýza rizik: Cílem této etapy je zpracování popisu informačních aktiv a analýza rizik. Výčtová analýza aktiv včetně určení vlastníků je zpravidla bezproblémová. Jenom si musíme uvědomit, že aktiva nejsou jen informace v počítačové formě, ale veškeré informace včetně těch v papírové formě. Odborně nejnáročnější činnost představuje analýza rizik, která v podstatě určuje kvalitu a efektivnost výsledného ISMS. Zpracovatel analýzy by měl zahrnovat pouze reálná rizika (například nemá smysl analyzovat riziko pádu meteoritu) a hrozby ohrožující podstatné procesy u správce ISMS, protože v každé zahrnuté riziko rozšiřuje složitost a administrativní náročnost budovaného ISMS. S velkou výhodou lze pro zmenšení počtu analyzovaných rizik využít princip zakotvený v novelizované normě ISO 27001, podle kterého musí být zpracován postup pro případ, že reálně nastane riziko, které není v seznamu analyzovaných rizik. Tím je vlastně zakotven samoopravný mechanismus, který napravuje případné vynechávky reálných rizik při prvotní analýze. Druhé zjednodušení pro zpracování rizik představuje fakt, že rizika lze rozčlenit na 4 typy:

- Rizika, která jsou skoro stejná v každé organizaci (typicky personální rizika, spisová služba, řízení přístupu do systému, archivace a zálohování),
- rizika v případě, pokud mají na základě smluvních nebo zákonných vztahů do systému přístup externí uživatelé (dodavatelé software, zaměstnanci jiných organizací, občané),
- rizika, která souvisí s perimetrem a parametry budovy,
- specifická rizika, která se týkají jen toho konkrétního správce ISMS.

Toto rozlišení výrazně urychlí zpracování rizik, pokud je provádí pracovník s ověřenými vzory zpracování a řízení rizik, protože zejména první 2 typy rizik pouze lokalizuje pro konkrétního správce ISMS.

Etapa 3 – Tvorba dokumentace: Cílem této etapy je zpracování postupů a zejména ověření jejich reálnosti a akceptovatelnosti pracovníky správce ISMS při školení, během kterého školitel simuluje situace řešené příslušným postupem.

Etapa 4 – Zkušební provoz: Cílem této etapy je zkušební provoz a doladění ISMS. Při zkušebním provoze se zpravidla odhalí situace, kdy zaměstnanci správce všelijak obcházejí stanovené postupy s výmluvou na administrativní náročnost, přičemž často mají pravdu a administrativu lze v těchto situacích zjednodušit, aniž by to snížilo účinnost ISMS.

Etapa 5 - Vyhodnocení: Cílem této etapy je vyhodnocení zkušebního provozu a to zejména výsledků monitoringu pro řízení a zlepšování ISMS.

Etapa 6 - Finalizace: Cílem této etapy je zpracování definitivní dokumentace ISMS a předání do plného provozu.

Etapa 7 – Certifikace (nepovinná): Tato etapa zatím není povinná a spočívá v tom, že je u externí akreditované organizace podána žádost o prověření a certifikaci provozovaného ISMS.

Výše uvedené etapy vycházejí z principu, že cílem těchto prací není formální splnění požadavků legislativy na bezpečnost provozovaných kritických informačních systémů, ale vybudování fungujícího systému ISMS akceptovaného zaměstnanci a pokud možno minimalizující náklady a administrativu spojenou s provozem ISMS. Určité zjednodušení představuje analogie s fyzickou ostrahou prostor správce systému. Tu lze také řešit formálně vydáním směrnice o vstupu do prostor a cedulek „Nepovolaným vstup zakázán!“ bez dalších opatření a riskovat krádeže a vstupy nepovolaných osob anebo zavést čipy, centrální recepci a čidla napojená na PCO pro efektivní zabezpečení vstupu. Analogicky se tato rozhodnutí vztahují i na ISMS s tím, že vlivem bouřlivého rozvoje ICT technologií jsou rizika mnohem sofistikovanější a v čase dynamická. Vznik případných problémů v informačním zabezpečení nelze vyloučit, ale funkční systém ISMS by měl zabránit, aby se opakovaly. A podobně jako efektivní fyzická ostraha perimetru není úkolem pro amatéry, tak vybudování efektivního systému ISMS je úkolem pro specialisty z této oblasti.