Najslabšie miesta informačnej bezpečnosti

Obsah tohto článku vychádza z analýz, ktoré sme uskutočnili v posledných rokoch na Slovensku, ale aj v Českej republike. Tieto analýzy sa uskutočnili v organizáciách, kde sa informačná bezpečnosť už v minulosti riešila, ale aj v organizáciách, ktoré sa problematike informačnej bezpečnosti primerane nevenovali.

Martin Zajíček
Autor je konzultantom na informačnú bezpečnosť v spoločnosti DCIT Consulting

zajicek@dcit-consulting.sk

Primárnym cieľom bolo posúdiť úroveň informačnej bezpečnosti voči norme ISO/IEC 27002 v súčasnosti sa nachádzajúcej v skupine noriem ISO 27000, vychádzajúcich z normy BS7799, ktorá bola neskôr prepracovaná na ISO 17799. Ide podľa môjho názoru o rozumný základ, ktorého zohľadnením sa zaručuje, že v posudzovaných oblastiach sa na nič dôležité nezabudlo. Je vhodné spomenúť, že táto norma je v súčasnosti súčasťou STN s označením STN ISO/IEC 27002. Norma pokrýva jedenásť oblastí, ako napríklad bezpečnosť ľudských zdrojov, fyzická bezpečnosť, riadenie prevádzky a ďalšie.

Ktoré oblasti informačnej bezpečnosti v zmysle STN ISO/IEC 27002 teda patrili medzi najslabšie pokryté?

RIADENIE INCIDENTOV

Táto sféra sa vo všeobecnosti takmer ignoruje. Často nie je dostatočne procesne pokrytá a pracuje podľa zásady: „Ak niečo nefunguje, zavolám nášho IT-čkára a on to

už nejako opraví.“ Čím je organizácia väčšia, tým viac chaosu a problémov môže takéto „riešenie“ spôsobovať a je traumatizujúcim nielen pre užívateľov, ale aj pre pracovníkov IT. Takýmto štýlom nielen opakovane dochádza k rovnakým problémom, ale keď nastanú, riešia sa rovnako, ako by sa stali prvýkrát, najmä ak ide o rozdielnych riešiteľov.

Riadny systém riadenia incidentov informačnej bezpečnosti by mal pokrývať systém nahlasovania a riadenia. Pre nahlasovanie by sa malo vytvoriť jedno centrálne kontaktné miesto, umožňujúce jednoducho nahlásiť akýkoľvek problém a túto požiadavku distribuovať relevantnému riešiteľovi. Okrem odstránenia problému je, samozrejme, potrebné jednotlivé udalosti spracovať s cieľom minimalizovať opakovaný výskyt, ale tiež štandardizovať prípadné opakované riešenie. Rovnako by výstupy mali byť súčasťou systému analýzy a zvládania rizík či podkladom napr. pre definovanie a kontroly SLA.

RIADENIE KONTINUITY ČINNOSTI

Stále sa často stretávame s organizáciami, ktoré v rámci tejto oblasti nezrealizovali ani len analýzu vplyvov (Business Impact Analysis - BIA). Až na základe jej výsledkov možno vytvoriť relevantné a efektívne opatrenia v podobe návrhov scenárov a ich následného rozpracovania havarijných plánov a plánov obnovy. Takže ak si aj niekto skrátil cestu a prešiel priamo na tvorbu konkrétnych postupov bez toho, aby vedel, aké sú požiadavky prevádzky, môže mať problém – či už v podobe preplatených a predimenzovaných záložných riešení, alebo ich poddimenzovaním v podobe zbytočných strát.

Aký je teda náš odporúčaný postup pre oblasť IT? Jednoznačne treba začať s analýzou vplyvov. Jej výstupom by mal byť prehľad kritických činností pre organizáciu, ich závislosť na funkčných a dostupných častiach informačného systému organizácie, vývoj finančných a nefinančných vplyvov plynúcich z nedostupnosti činností v čase (t.j. mať jasné odpovede na otázky, čo by spôsobil výpadok činnosti X napr. po uplynutí určitého času) a množstvo ďalších informácií. Na základe toho možno získať požiadavky prevádzky na dostupnosť jednotlivých činností a teda aj častí infraštruktúry, ktoré sú pre ne nevyhnutné a tiež mať sumárny prehľad strát súvisiacich s ich nedostupnosťou.

Príkladom je prípad, keď jednodňová nedostupnosť vybranej časti informačného systému vyvolá výpadok niekoľkých činností a spôsobí sumárnu finančnú stratu 10 tisíc eur. Vtedy je neefektívne uvažovať nad budovaním záložného centra v hodnote 100 tisíc eur, pokiaľ primeranú obnovu vieme zabezpečiť servisnou zmluvou zaisťujúcou zrýchlenú dodávku vypadnutej časti infraštruktúry. Primeranú pozornosť treba tiež venovať nefinančným súvislostiam, ako napr. dodržiavanie legislatívneho súladu, keď nesplnením právneho ustanovenia môžu byť nielen vyrubené finančné sankcie, ale môže byť odňatá licencia s následkami obmedzenia alebo až ukončenia činnosti.

Na základe výstupov analýzy vplyvov možno vytvoriť, vybrať a spracovať adekvátne scenáre obnovy. Až v prípade nájdenia súladu alebo aspoň kompromisu medzi požiadavkami a možnosťami ich naplnenia možno uskutočniť preventívne činnosti (napr. úpravou či doplnením SLA, alebo servisnej zmluvy) a spracovať konkrétne havarijné plány a plány obnovy. Po ich praktickom uskutočnení a pretestovaní by mali nasledovať školenia a ostré testy. S odstupom času, prípadne pri významných zmenách v organizácii je potrebné všetky kroky zopakovať – analýza, aktualizácia plánov, školenia, testy. Minimálne sa odporúča pravidelné testovanie.

RIADENIE AKTÍV

Ďalším pomerne častým nálezom sú situácie, keď má organizácia spracovanú bezpečnostnú politiku, nemá však zmapované svoje aktíva.

Ak nepoznáme svoje aktíva, nemáme ich kategorizované (minimálne z pohľadu dôvernosti a dostupnosti), nemáme zadefinovaných vlastníkov dát, ich zodpovednosti, len veľmi ťažko môžeme efektívne a zrozumiteľne riadiť ich bezpečnosť v podobe technických i organizačných opatrení. Okrem zmapovania je potrebné uskutočniť analýzu rizík (často bývajú tieto činnosti spojené), a tým poznať slabé miesta a ohodnotiť ich.

PERSONÁLNA BEZPEČNOSŤ

Do tejto oblasti spadá ľudský faktor ako najzraniteľnejší článok informačnej bezpečnosti. Medzi najčastejšie nálezy patrí absencia požiadaviek preverovania zamestnancov pri kľúčových pozíciách, kam určite patrí aj oblasť IT. Častým nálezom je tiež absencia systému vzdelávania a udržiavania povedomia v oblasti práce s IT i v samotnej sfére informačnej bezpečnosti. Samostatnou kapitolou je absencia postupov ukončenia pracovného pomeru a následného procesu blokovania prístupov do informačných systémov organizácie na úrovni operačného systému i samotných aplikácií. Často sme tiež zaznamenali absenciu evidencie pridelených prístupových práv a akýchkoľvek kontrolných mechanizmov.

Pri posudzovaní celkovej úrovne informačnej bezpečnosti nie je dôležité len pokrytie príslušnej oblasti, ale tiež závažnosť nálezov. Pri posudzovaní stavu informačnej bezpečnosti preto nie je možné posudzovať len pokrytie jej jednotlivých oblasti, ale aj nálezy konkrétnych slabín. To je však námet na článok o inej téme.

Ak nepoznáme svoje aktíva, nemáme ich kategorizované (minimálne z pohľadu dôvernosti a dostupnosti), nemáme zadefinovaných vlastníkov dát, ich zodpovednosti, len veľmi ťažko môžeme efektívne a zrozumiteľne riadiť ich bezpečnosť v podobe technických i organizačných opatrení.