Informačná bezpečnosť z bodu nula

Ako ukazuje naša prax v oblasti informačnej bezpečnosti, stále existuje množstvo organizácií bez ohľadu na veľkosť alebo príslušnosť (štátna, súkromná, zahraničná), ktoré sa doteraz nad informačnou bezpečnosťou nezamýšľali a neriešili ju. Vzhľadom na svoju činnosť a zameranie by sa ňou však zaoberať mali. Predmetom tohto článku nie je presviedčať, že túto oblasť treba riešiť. Skôr či neskôr si každý vyskúša dôsledky opomenutia tejto oblasti a je len na ňom, či je a bude na podobné situácie aspoň trochu pripravený. Veľkosť dosahu bude priamo úmerná závislosti od funkčnosti a dostupnosti informačných technológií pre chod príslušnej organizácie, ale tiež od dávky šťastia či nešťastia.

Ako teda začať riešiť informačnú bezpečnosť v organizácii na zelenej lúke? Dobrou správou je, že bez ohľadu na to, že ste túto oblasť doteraz neriešili, určité jej prvky vo vašej organizácii už máte. Sú spravidla súčasťou už používaných technológií, treba ich len vhodne využiť. Ďalšou dobrou správou je, že túto oblasť často možno riešiť bez potreby veľkých finančných investícií. Odhliadnuc od štandardného návrhu realizácie úvodnej analýzy počiatočného stavu úrovne zabezpečenia, ktorá poukáže na nedostatočne pokryté či vôbec nepokryté oblasti, si dovolím navrhnúť postupnosť nasledujúcich krokov, zoradených podľa dôležitosti ich riešenia.

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

zajicek@dcit-consulting.sk

Budovanie informačnej bezpečnosti je nikdy sa nekončiaci proces. Okrem toho, že si stanovíte úroveň/hĺbku, do akej budete túto oblasť pokrývať, je nevyhnutné realizovať opakovanie jednotlivých krokov. Techniky a spôsoby útokov sa neustále vyvíjajú so zvyšujúcou sa komercializáciou, čoho výsledkom je napr. neustále sa zvyšujúci počet nevyžiadanej pošty v našich emailových schránkach. Stále citlivejšou bude táto oblasť neustálym zvyšovaním závislosti organizácií od funkčných informačných technológií a dát v elektronickej podobe. Zmena kurzu riešenia informačnej bezpečnosti z „možno" na „je nevyhnutné" čaká skôr či neskôr nás všetkých.

POKRYTIE LEGISLATÍVNYCH POŽIADAVIEK

Legislatívne požiadavky sú možno neočakávane na prvom mieste. Môže za to najmä problematika ochrany osobných údajov zasahujúca takmer všetky organizácie. Zákon 428 o ochrane osobných údajov vznikol v roku 2002, pričom poslednou významnou novelizáciou prešiel v roku 2005. Upravuje podmienky, za akých možno spracúvať osobné údaje, prípadne osobitnú kategóriu osobných údajov. Medzi najdôležitejšie podmienky patrí vymenovanie a zaregistrovanie tzv. zodpovednej osoby, požadovanie súhlasu so spracúvaním osobných údajov, povinnosť preškolenia a tiež vytvorenie bezpečnostného projektu ochrany osobných údajov. Konkrétne podmienky je však potrebné riešiť individuálne vzhľadom na rozsah a spôsob spracúvania osobných údajov príslušnej organizácie. Motivačnou časťou už zmieňovaného zákona je § 49, ktorý definuje možnosti uloženia pokuty v minimálnej výške 1 666 €, pričom horná hranica sa končí až pri sume 333 333 €. Množstvo aj vyššie menovaných povinností sa viaže nielen na vlastníka dát, v zmysle zákona definovaného ako prevádzkovateľa, ale aj na subjekty, ktoré spracúvajú dáta v mene prevádzkovateľa. Tí sú v zmysle zákona definovaní ako sprostredkovatelia. Aké sú typické agendy spadajúce pod ochranu osobných údajov? Najčastejšie ide o personálnu a mzdovú agendu či obchodnú agendu spracúvajúcu osobné údaje fyzických osôb.

Pre vybrané sektory je tiež relevantnou oblasť utajovaných skutočností a požiadavky nevyhnutné na prístup k príslušnej kategórii. A špecifickou oblasťou je aj štátna správa.

ZABEZPEČENIE EXTERNÉHO PRIPOJENIA A INTERNETOVÝCH SLUŽIEB

Druhým najdôležitejším bodom, na ktorý je nevyhnutné zamerať svoju pozornosť, je pripojenie na internet a internetové služby, ktoré poskytujete alebo využívate. Treba si uvedomiť, že používaním internetu sa stávate súčasťou obrovského virtuálneho sveta, v ktorom sa denne uskutočňuje nepredstaviteľné množstvo pokusov o prienik, o zneužitie informácií či infraštruktúry. Bez ohľadu na veľkosť a zameranie organizácie ste aj vy cieľom nespočetných úsilí rôznych automatizovaných nástrojov, ktoré skúmajú, hľadajú a evidujú typy, verzie služieb, prípadne vyhľadávajú špecifické chyby, ktoré následne zneužívajú na to, aby mohli napr. prostredníctvom vašich zariadení zasielať nevyžiadanú poštu, ukladať pornografiu či realizovať rôzne typy zdieľaných útokov. A odtiaľ je už naozaj blízko k tomu, že vám prestanú fungovať zablokované emailové služby, alebo sa objaví neohlásená návšteva bezpečnostných zložiek s následným odvozom serverov a pracovných staníc za účelom vyšetrovania. Netreba sa báť. Spravidla vám ich za niekoľko týždňov či mesiacov vrátia aj s odovzdávacím protokolom. Ak medzitým viete pracovať s papierovým notesom a farebnými fixkami si viete nakresliť logo na faktúry či iné dokumenty, nemusí to byť až taký problém.

Základnou prevenciou je realizácia externého penetračného testu či špecifického preverenia príslušnej internetovej služby, ktoré preveria odolnosť vašej infraštruktúry voči vyššie naznačeným typom útokov. Ak máte viacčlenný tím IT špecialistov, nebojte sa zrealizovať takýto test v tzv. skrytej forme, pri ktorej o ňom nebude informovaný nikto okrem jeho zadávateľa. V takom prípade preveríte nielen odolnosť infraštruktúry, ale aj reakčné mechanizmy. Ak je na oddelení IT pohodová atmosféra a v emailovej schránke vás čaká email informujúci, že na vašom disku je uložený súbor bol_som_tu.txt, treba len dúfať, že realizátor penetračného testu je primerane viazaný mlčanlivosťou. Po zrealizovaní testov je samozrejme nevyhnutné veľkú pozornosť venovať odstráneniu nálezov. Z veľkej časti ide o kroky, ktoré súvisia so zmenou konfigurácie a teda nie je potrebné obstarávať nové zariadenia. V prípade preverovania internetových služieb, akou je napr. internetová aplikácia (obchod,

objednávkový portál, atď.) však môžu byť potrebné úpravy ich funkcionality.

Náročnejšou oblasťou je práca s užívateľmi a primerané nastavenie prístupových práv. Stále veľký počet z nich si neuvedomuje, že ich delí naozaj iba jedno kliknutie od toho, aby sa na ich počítači začali diať zvláštnosti spomaľujúce celú pracovnú stanicu. O nejaký čas vypadne server a lavína sa spúšťa. A to je možno ten lepší prípad podobný poruche vodovodného potrubia, keď je často lepšie, keď voda strieka, ako keď voda uniká po malých kvapkách. Je na mieste upozorniť na antivírovú ochranu. Je síce riešením v tejto oblasti, no už dávno nie je postačujúca a univerzálna.

Nič nebráni tomu, aby ste napr. do povinného preškolenia v oblasti ochrany osobných údajov zahrnuli aj pár informácií z tejto sféry a podporili to záväznou smernicou obsahujúcou zodpovednosť i sankcie.

Táto oblasť je z pohľadu počtu útokov najexponovanejším, hoci nie najzraniteľnejším miestom. To obsahuje ďalší bod.

ZABEZPEČENIE VNÚTORNÉHO PROSTREDIA ORGANIZÁCIE

Najzraniteľnejším miestom v oblasti informačnej bezpečnosti je nesporne vnútorné prostredie. Ak aj dôjde v tejto oblasti k incidentu, má spravidla vysoký dosah. Preto je potrebné tejto oblasti venovať pozornosť a neignorovať ju. Je jasné, že je veľmi ťažké brániť sa pred zlomyseľným či nevedomým zamestnancom. Ešte ťažšie však pred zlomyseľným administrátorom. Najčastejším problémom je úplná otvorenosť infraštruktúry smerom do vnútra organizácie a takmer úplná absencia najzákladnejšieho pravidla v oblasti prístupových práv o prideľovaní minimálnych prístupových práv a ich zvyšovanie len v prípade oprávnenej požiadavky.

Jednou z možností, ako zistiť možnosti potenciálneho útočníka z radov zamestnancov (ale tiež tretích strán, pristupujúcich k vašej vnútornej infraštruktúre), je realizácia penetračného testu v internej podobe. V takomto prípade sa test realizuje vo vnútri siete. V prvom kroku sa preveruje pridelená štandardne nastavená pracovná stanica z pohľadu odolnosti voči zneužitiu a voči úsiliu získať nad ňou plnú kontrolu. Následne sa uskutočnuje preverenie definovanej časti infraštruktúry. Zo skúseností a bez preháňania môžem potvrdiť, že pri tomto type testov nediskutujeme, či môže byť daný útok úspešný v podobe prieniku či získania vyšších práv, ako boli pôvodne pridelené. Diskutujeme len o tom, ako a za aký dlhý čas je útok úspešný. Ojedinelé výnimky potvrdzujú pravidlo.

Existujú možnosti rôznych riešení odstraňujúcich nálezy interného penetračného testu. Ich účinnosť a rozsah sú úmerné úsiliu a vloženým finančným prostriedkom. Veľa možno uskutočniť v oblasti nastavenia už zmieňovaných prístupových práv či zmenami v nastaveniach testovaných zariadení. Ďalšou oblasťou je oblasť zadefinovania zodpovedností a povinností užívateľov, samozrejme v kombinácii s primeranými sankciami.

ZMAPOVANIE KĽÚČOVÝCH AKTÍV, PROCESOV A RIEŠENIE KONCEPČNEJ OBLASTI

Ak ste prešli predchádzajúcimi bodmi, veľká časť uskutočnených činností sa realizovala s cieľom zabezpečiť infraštruktúru ako takú. Ďalším logickým krokom je poznať požiadavky vášho biznisu na zabezpečenie vašich aktív a činností, ktoré každý deň vykonávate. Znalosť požiadaviek znamená to, aby sme o nich vedeli a poznali požiadavky na ich zabezpečenie voči prezradeniu, zničeniu, neoprávnenej zmene, ale tiež aby sme poznali požiadavky na ich dostupnosť. Možno to znie v tejto zhustenej podobe strašidelne, nie je to však až také zložité na pochopenie. Ide v podstate o to poznať, aké sú vaše kritické aktíva a činnosti. Je potrebné poznať výšku finančných i nefinančných dopadov v prípade ich prezradenia či nedostupnosti alebo nefunkčnosti. Keď tieto informácie máte, viete špecifikovať minimálne požiadavky na zabezpečenie a tiež objem finančných investícií, ktoré možno efektívne investovať na úplné alebo aspoň čiastočné eliminovanie prípadných dosahov. Tu sa už dotýkame oblasti systémového riadenia informačnej bezpečnosti, ktorého súčasťou je zmapovanie aktív, analýza rizík, tvorba bezpečnostnej politiky, analýza dosahov a následné riešenie havarijného plánovania.