Informační bezpečnost a zdravotnictví

Bezpečnostní incidenty ve světě

Informační bezpečnost již dávno není pouze záležitostí bank a státních institucí. Nestačí jen nainstalovat antivirový software a firewall, aby jste byli chráněni vůči průniku z Internetu.

Jedním z příkladů je únik dat z americké zdravotnické firmy Community Health Services, která oznámila, že její síť se stala cílem rozsáhlého útoku v dubnu a červnu 2014. Během něj byla odcizena data přes 4,5 milionu zákazníků. Byly odcizeny jména, adresy, telefonní čísla a čísla sociálního pojištění.

Dalším příkladem je případ vydírání po úniku dat na britské klinice plastické chirurgie Harley Medical Group. Společnost oznámila, že neznámý pachatel ji vydíral a hrozil zveřejněním údajů o jejích 480 000 zákaznících. Šlo o údaje, které klinika vyžaduje pomocí webového formuláře od potenciálních zájemců o její služby. Data obsahovala nejen typ zákroku, ale i celé jméno, datum narození, e-mail, telefon a místo bydliště.

Situace v České republice

Informace o incidentech zatím nejsou zveřejňovány, i když z naší praxe víme, že existují.

V České republice zatím není stanovena povinnost hlášení bezpečnostních incidentů, ale již schválený zákon č. 181/2014 Sb. o kybernetické bezpečnosti zavede tuto povinnost pro mnoho organizací provozujících kritickou informační infrastrukturu.

Nastavení bezpečnostních procesů a opatření v České republice dále vyžaduje hlavně vyhláška č. 98/2012 Sb. o zdravotnické dokumentaci, zákon č. 101/2000 Sb. o ochraně osobních údajů a zákon č. 499/2004 Sb. o archivnictví a spisové službě, a též soubor norem jako je ISO/IEC 27 000.

Oborová specifika

Při definování rizik a opatření v oboru zdravotnictví je potřeba přihlédnout na určité odlišnosti. Jedná se především o důvěrnost, dostupnost a integritu dat, protože zdravotnická zařízení pracují s velkou koncentrací citlivých osobních údajů pacientů. Tato data jsou rovněž podkladem k rozhodnutím, která můžou rozhodovat o životě a smrti každého z nás.

Na základě našich zkušeností jsou nejčastějšími riziky:

- předstírání identity uživatele;
- používání dat neautorizovanými uživateli;
- politika přinášení vlastních zařízení (BYOD - bring your own device);
- malware šířený mobilními zařízeními a sociálními sítěmi;
- nedostatečné zabezpečení základních subsystémů (server, firewall, router nebo databáze).

Management rizik

Tak jako v životě, ani v oblasti informační bezpečnosti obvykle neexistuje univerzální a jednoduchá metoda, která vyřeší všechny problémy okamžitě a bezbolestně.

Pro řízení informačně bezpečnostních rizik a dodržení legislativních požadavků je nutná analýza současného stavu.

Předpokladem je určení oblastí bezpečnostní analýzy a prostředků, jak bude vyhodnocení probíhat - například prostřednictvím penetračních testů, auditu serverů, prověření komunikační infrastruktury nebo verifikace dokumentace a porovnání existujícího stavu.

Analýza vychází z dokumentace organizace, výstupů testovacích skriptů a nástrojů, podkladů o realizovaných činnostech a řízených rozhovorů.

Správně provedená analýza je základem pro zajištění bezpečnosti a podkladem pro eventuální snížení nákladů na informační bezpečnost.

Žádoucím výstupem je stav, kdy jsou identifikovaná rizika a definovány způsoby, jak tato rizika eliminovat nebo alespoň minimalizovat.

Východiska

Každá situace je řešitelná. Informační bezpečnost je potřeba řešit erudovaně a koncepčně, bez ad-hoc výdajů na nákup hardware a software.

Tímto způsobem lze racionalizovat náklady a předcházet ztrátě důvěry klientů, pokutám od regulačních úřadů a výrazným finančním ztrátám.