Informačná bezpečnosť – dosiahnutie rovnováhy medzi rizikom a výkonnosťou

Lukáš Neduchal, FCCA, CISA
lukas.neduchal@sk.ey.com

Existuje názor, že čím viac sa veci menia, tým viac zostávajú rovnaké. Platí to aj v oblasti bezpečnosti. Už tisíce rokov sa ľudia usilujú ochrániť svoj majetok. Civilizácie stavali vysoké múry, obrovské pevnosti, využívali rôzne mechanizmy a tajomstvá na chránenie svojich cenností. Niekedy sa však zároveň chceli podeliť o ich krásu s inými – bez ohľadu na to, o aký predmet išlo, alebo aká vysoká bola jeho hodnota. Rovnaké základné princípy bezpečnosti sa dnes dajú aplikovať do nových technológií, na nových trhoch a v nových organizáciách. V dnešných časoch sa ústredné zásady týkajú dôvernosti, integrity a dostupnosti informácií a zdrojov.

Desiaty ročník Globálneho prieskumu spoločnosti Ernst & Young o informačnej bezpečnosti sa v tejto súvislosti zameriava na aktuálny stav informačnej bezpečnosti a najmä na faktory, ktoré formujú jeho budúcnosť. Úlohou tohto prieskumu je pomôcť organizáciám hlbšie porozumieť aktuálnym trendom v oblasti informačnej bezpečnosti, ako aj nasmerovať ich úsilie do oblastí, ktoré podľa nás najviac vyžadujú zlepšenie.

VÝSLEDKY PRIESKUMU

Pri vyhodnocovaní prieskumu bolo zaujímavé pozorovať, ako organizácie zabezpečujú súlad medzi informačnou bezpečnosťou a podnikateľskými cieľmi, čo je hnacou silou potreby zlepšení v oblasti informačnej bezpečnosti, ako organizácie riadia funkcie informačnej bezpečnosti a ako zabezpečujú pokrytie informačnej bezpečnosti ľudskými zdrojmi. Informačná bezpečnosť vždy bojovala so skutočnosťou, že bola oddelená od podnikania. Úsilia o harmonizáciu oveľa viac pootvorili dvere funkciám informačnej bezpečnosti a umožnili jej plne sa zblížiť s podnikaním.

Globálny prieskum ukázal, že spoločnosti naďalej zlepšujú svoju informačnú bezpečnosť. Stále však nedokážu nájsť presnú rovnováhu medzi úsilím zmierňovať riziko a iniciatívami sústredenými na výkonnosť.

INFORMAČNÁ BEZPEČNSŤ A PODNIKANIE

V predchádzajúcich prieskumoch sme sa stretávali s čoraz vyšším počtom respondentov, podľa ktorých by mal byť prístup k bezpečnosti informácií viac aktívny a menej reaktívny. Náš prieskum ukázal, že implementátori bezpečnosti informácií čoraz lepšie zladťujú svoje podnety so strategickými cieľmi organizácie a stávajú sa tak proaktívnymi účastníkmi v procese riadenia celkového rizika v rámci svojich organizácií.

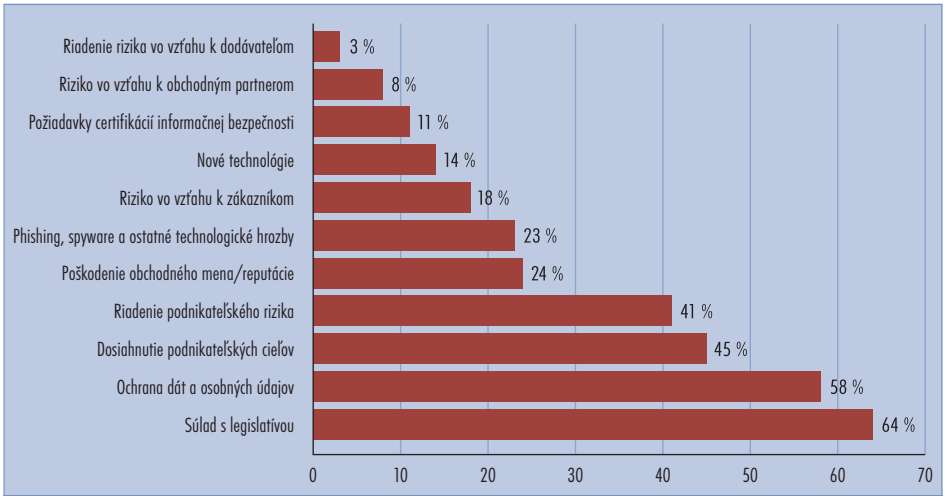
Kľúčovou výzvou pre riadiacich pracovníkov v oblasti bezpečnosti informácií je ich schopnosť nastoliť rovnováhu medzi taktickými požiadavkami, reagovať na zmeny, udržiavať prevádzkové činnosti a zároveň pozdvihnúť úlohu informačnej bezpečnosti tak, aby sa stala súčasťou strategických rozhodovacích procesov korporátnych, ako aj sektorových lídrov. Informačná bezpečnosť musí prekročiť prah integrácie s riadením podnikateľských rizík a úsilí o dodržiavanie legislatívnych noriem. Súčasne sa musí zvýšiť spôsobilosť a význam tejto funkcie na čosi viac ako len ochranu majetku.

SÚLAD S LEGISLATÍVOU

V roku 2007 bol súlad s legislatívou opäť číslom jeden medzi hnacími silami informačnej bezpečnosti. Táto otázka je najnaliehavejšia od roku 2005, keď predstihla tému bežných vírusov a červov, ktoré dovtedy poháňali informačnú bezpečnosť. Tlak na súlad s legislatívou však tiež zvýšil povedomie manažmentu o informačnej bezpečnosti. To sa dostalo až do štádia, v ktorom sa funkcia informačnej bezpečnosti pokladá za neoddeliteľnú súčasť podnikateľskej činnosti.

Primárna hnacia sila – zabezpečenie súladu s legislatívou – začína z pohľadu vyspelostného modelu vstupovať do údržbovej fázy. To však neznamená, že nebude aj v nasledujúcich rokoch predstavovať dôležitú hnaciu silu. Práve naopak, stane sa štandardným prevádzkovým režimom organizácií. Očakávame, že regulačné a harmonizačné prostredie bude naďalej ovplyvňovať agendu informačnej bezpečnosti. Je tu teda príležitosť, aby informačná bezpečnosť nastolila rovnováhu medzi súladom s legislatívou a podporou podnikateľských cieľov. Vytvorením nepretržitého harmonizačného programu si môže informačná bezpečnosť upevniť pozíciu reagujúcu na zmeny v legislatíve a zároveň si zachovať svoje zameranie na podnikanie.

Súlad s legislatívou je silným katalyzátorom toho, aby spoločnosti investovali do zmiernenia podnikateľského rizika prostredníctvom nepretržitého harmonizačného programu. Ako pomoc pri vývoji a udržiavaní nepretržitých harmonizačných programov by organizácie mohli využiť štandardizované modely informačnej bezpečnosti, ktoré definuje ISO 27002, ako aj Štandard pre osvedčené praktiky v oblasti informačnej bezpečnosti vydaný Fórom Informačnej bezpečnosti (ISF).

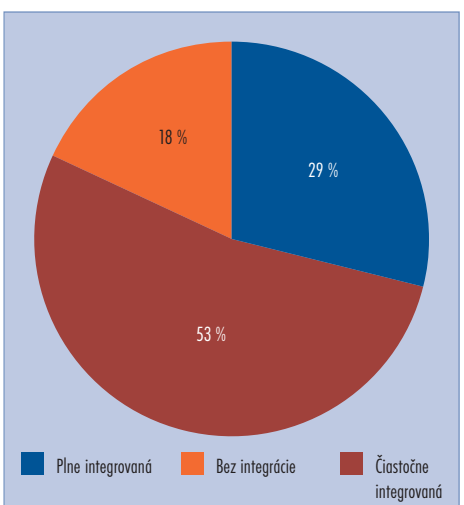


Graf 1: Ako organizácie hodnotia tri najvýznamnejšie faktory, ovplyvňujúce oblasť informačnej bezpečnosti

OCHRANA ÚDAJOV AKO KONKURENČNÁ VÝHODA

Čoraz viac organizácií venuje pozornosť dôsledkom straty alebo odcudzenia údajov. Túto tému podnietili zverejnené incidenty, pričom výkonní pracovníci začali brať svoj podiel na zabezpečovaní dostatočných kontrol a ochrany vážne. Značne vyšší podiel respondentov v prieskume – 58 % v porovnaní so 41 % v roku 2006 – označil ochranu súkromia a údajov ako jednu z troch najsilnejších hnacích síl v podnikaní, pričom 73 % výkonných riaditeľov a 64 % riaditeľov IT kládlo veľký dôraz na dôležitosť ochrany súkromia a dátového majetku.

Spomedzi hlavných otázok informačnej bezpečnosti sa práve ochrana súkromia stáva čoraz výraznejšou hnacou silou, a to najmä vďaka svojej orientácii na spotrebiteľa. Medializované príbehy o narušení súkromia, odcudzení identity ako aj o strate osobných údajov nielen vystupňovali uvedomelosť spotrebiteľov, ale zároveň stimulovali zmysel osobnej zodpovednosti vedúcich pracovníkov a absolútnu potrebu postaviť ochranu súkromia a osobných údajov do popredia. Ak sa informačná bezpečnosť vykonáva správne, majú organizácie prvú možnosť rozšíriť kontroly vyvinuté v úsilí zosúladiť postupy s legislatívou a využiť ochranu súkromia a údajov ako konkurenčnú výhodu.



Graf 2: Stupeň integrácie funkcie informačnej bezpečnosti v celkovom riadení rizík spoločnosti

Podnikateľské subjekty, ktoré preukážu skúsenosti so zavádzaním zabezpečovania silnej ochrany a uskutočňovania kontrol dodržiavania bezpečnosti v praxi, môžu rozvíjať tieto atribúty vo svojom podnikaní a tým sa pozitívne odlíšiť od konkurencie, zvýšiť svoj podiel na trhu, zlepšiť si povesť a zvýšiť zisk.

PLNENIE PODNIKATEĽSKÝCH CIEĽOV

Treťou najvýznamnejšou silou poháňajúcou informačnú bezpečnosť bolo plnenie podnikateľských cieľov. Tento výsledok podporuje silnejúci trend vytvárania súladu informačnej bezpečnosti s podnikateľskými cieľmi. Tradičné hnacie sily ako technologické pokroky a napadnutie technickej stránky systému sa tým odsunuli, alebo sa pokladali za súčasť úsilia zabezpečiť súlad s legislatívou. Informačná bezpečnosť takto dostáva možnosť sústrediť sa na podnikateľské iniciatívy, čo potvrdil aj náš prieskum, keďže menej ako 15 % respondentov pokladá technológiu za dôležitú hnaciu silu.

INTEGRÁCIA DO CELKOVÉHO RIADENIA RIZIKA

Najdôležitejší odkaz z výsledkov prieskumu poskytuje pomer respondentov, ktorí udávajú, že sčasti alebo úplne integrovali funkcie informačnej bezpečnosti do systému riadenia rizika (82 %, v porovnaní so 40 % v roku 2005 a 43 % v roku 2006). Silným integračným stimulom bol aj súlad s právnymi normami, na základe ktorého sa počet organizácií, ktoré plne integrovali obe funkcie takmer zdvojnásobil a to z 15 % v roku 2006 na 29 % v roku 2007.

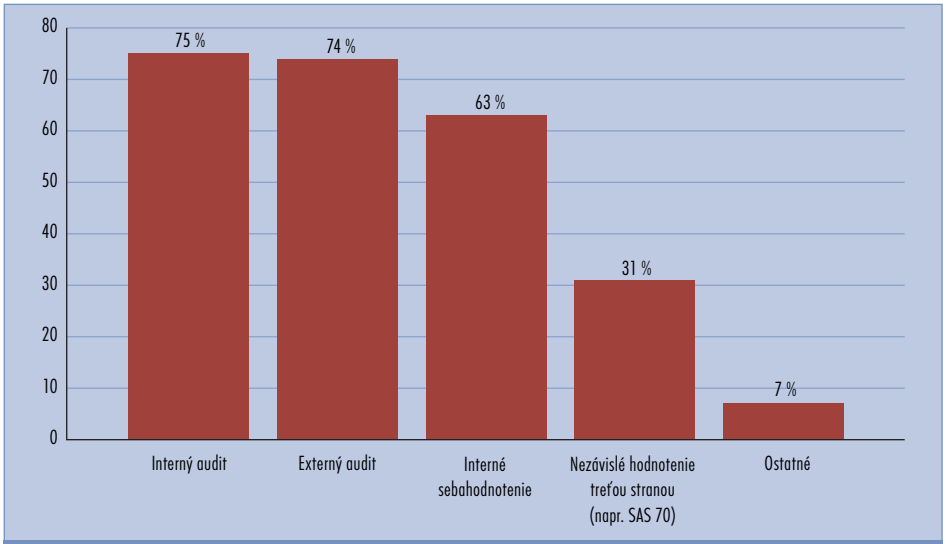
Znamená to, že informačná bezpečnosť už nebude súčasťou funkcie IT? Nemyslíme si to. Tento výsledok opodstatňuje rastúci trend integrácie funkcie informačnej bezpečnosti so strategickými/riadiacimi líniami týkajúcimi sa súladu s legislatívou, ako aj s prevádzkovými a architektonickými líniami v rámci funkcie IT. Tento trend poháňa nielen potreba zabezpečenia súladu s legislatívou, ale akceleruje aj z hľadiska rozširujúcich sa hraníc vymedzenia bezpečnosti. Napriek značnej integrácii bezpečnosti do procesu celkového riadenia rizika existujú obavy, že túto integráciu poháňajú skôr iniciatívy ako strategické smerovanie riadenia. Prieskum ukázal, že pravdepodobnosť stretnutia tímu informačnej bezpečnosti s vedením IT raz mesačne je trikrát vyššia ako v prípade stretnutia špecialistov informačnej bezpečnosti s vedúcimi pracovníkmi spoločnosti a vedúcimi divízií. Zriedkavosť stretnutí či inej interakcie medzi špecialistami na informačnú bezpečnosť a senior manažérmi nešťastne naznačuje, že informačná bezpečnosť stále nie je tak úzko prepojená s vedúcimi pracovníkmi, ako by bolo vhodné. Väčšina funkcií informačnej bezpečnosti sa stretáva s vedením menej ako jedenkrát za štvrťrok, pričom 20 % respondentov uviedlo, že ich skupiny informačnej bezpečnosti sa nestretávajú s riadiacimi pracovníkmi alebo vedúcimi divízií vôbec.

Zahrnutie úvah o informačnej bezpečnosti do aktivít strategického plánovania spoločnosti, ako ich neoddeliteľnej súčasti, prináša množstvo výhod. Tento proces sa začína vtedy, keď funkcia informačnej bezpečnosti využíva vzťahy s kľúčovými vedúcimi pracovníkmi na úrovni spoločností, ktoré rozvíja – aj keď tieto vzťahy prekračujú tradičné, predpísané reportovacie línie. Skorá účasť umožňuje funkciám informačnej bezpečnosti pomôcť organizácii identifikovať a vyriešiť alebo aspoň poukázať na otázky ktoré ovplyvňujú dosiahnutie strategických podnikateľských cieľov. Očakávame, že sa táto úloha ešte posilní, pretože spoločnosti naďalej zlepšujú svoje schopnosti v oblastiach riadenia rizika a súladu s legislatívou.

RIADENIE INFORMAČNEJ BEZPEČNOSTI

V roku 2002 iba 21 % účastníkov prieskumu uviedlo, že outsourcovali akékoľvek činnosti súvisiace s informačnou bezpečnosťou tretej strane.

Informačná bezpečnosť naplnila kruh bezpečnostných funkcií a od decentralizovaného modelu na začiatku deväťdesiatych rokov sa vrátila späť k modelu centralizovanému. V súčasnosti až 82 % účastníkov nášho prieskumu uviedlo návrat k centrálne štruktúrovanej funkcii, čo nie je prekvapujúce vzhľadom na silné tlaky na zosúladenie s legislatívou a rozširujúcu sa úlohu riadenia rizika v oblasti informačnej bezpečnosti. Organizácie hľadajú spôsoby, ako odhadovať a merať efektivitu svojej informačnej bezpečnosti. Prieskum ukázal, že veľa organizácií hodnotilo efektivitu svojho bezpečnostného programu vlastným odhadom, „benchmarkom“, interným a externým auditom, ako aj nezávislým hodnotením treťou stranou. Až 63 % organizácií hodnotí svoje funkcie informačnej bezpečnosti vlastným odhadom. Z týchto spoločností 91 % využíva korporátne zmluvy, postupy a interné štandardy ako základ takéhoto hodnotenia. Takmer tri štvrtiny respondentov sa spoliehajú na výsledky formálneho externého



Graf 3: Ako organizácie hodnotia svoj stav informačnej bezpečnosti

a interného auditu. Šesť z desiatich firiem hodnotí svoj prístup k riadeniu bezpečnosti, jeho implementáciu a kontrolu prostredníctvom uznávaných sektorových štandardov pre informačnú bezpečnosť ako napríklad ISO 27001: 2005 a 27002: 2005. Na záver treba konštatovať, že takmer 40 % respondentov používa nezávislé techniky ako sú SAS 70 alebo iné odhady tretích strán na hodnotenie svojho bezpečnostného programu.

ČORAZ VIAC VZŤAHOV S TRETÍMI STRANAMI

Informačné technológie, rovnako ako informačná bezpečnosť vytvárajú stále viac vzťahov s tretími stranami. Buď formou strategických obchodných vzťahov, outsourcingom prevádzkových výkonov, rozšírením zdrojov, alebo podporou pri vykonávaní taktických iniciatív. Tieto vzťahy však so sebou prinášajú zvýšené riziko. Schopnosti informačnej bezpečnosti a požadované kontroly na ochranu organizácie sa nesmú využitím tretích strán alebo služieb nimi poskytovanými oslabiť. Náš prieskum ukázal značný rast požiadaviek na tretie strany, obchodných partnerov a dodávateľov v oblasti dodržiavania politiky, postupov a štandardov klientskej organizácie (zvýšenie o 12 percentuálnych bodov zo 66 % v roku 2006 na 78 % v roku 2007).

Vyše polovica respondentov zároveň vyžadovala, aby organizácie tretej strany mali zavedenú vlastnú informačnú bezpečnosť, ako aj zásady a postupy na zachovanie súkromia – rast o sedem percentuálnych bodov – na to, aby vôbec mohli spolupracovať s klientskou organizáciou.

Trendom nasledujúcich rokov tak bude zrejme proaktívny, neustály monitoring funkcií a kontrola informačnej bezpečnosti. Riadenie informačnej bezpečnosti sa stane dôležitejším, pretože nebude predstavovať len spôsob zberu informácií, ale aj ich vykazovania. Bezpečnostné panely sa budú stávať bežnými, pretože organizácie sa budú usilovať vylepšiť obraz o ich pozícii z hľadiska bezpečnosti v očiach výkonného manažmentu a podnikateľského prostredia.

ĽUDSKÉ ZDROJE

Efektívne riadenie ľudských zdrojov v akomkoľvek sektore, a to najmä nábor a udržanie talentov je nevyhnutné pre úspech každej organizácie. Tento aspekt je extrémne dôležitý pre informačnú bezpečnosť a sleduje sa už od roku 1997. Účastníci prieskumu v roku 2007 uviedli, že obmedzenia v oblasti ľudských zdrojov z pohľadu IT, ako aj informačnej bezpečnosti sú jednou z najvýznamnejších výziev, s ktorými sa organizácie stretávajú pri odovzdávaní projektov informačnej bezpečnosti.

NEDOSTATOK SKÚSENÝCH PRACOVNÍKOV

Keďže priority a ciele informačnej bezpečnosti sa presúvajú, nachádzanie vhodných ľudských zdrojov v rámci organizácie alebo mimo nej bude naďalej predstavovať rastúce obavy pre informačnú bezpečnosť. Nedostatok zručných pracovníkov dokáže v konečnom dôsledku narušiť spôsobilosť organizácie vykonávať strategické podnikateľské rozhodnutia a implementovať ich. Prieskum neprekvapujúco ukazuje, že nedostatok kvalifikovaných pracovníkov je dôležitým hľadiskom pri rozhodovaní sa o vyhľadaní pomoci tretej strany. Schopnosť organizácie nájsť a udržať si skúsené a vyškolené ľudské zdroje je ovplyvnená mnohými faktormi, vrátane podnikateľských modelov, technologického pokroku a vyvážených investícií. Každý z týchto faktorov môže klásť iné požiadavky na zručnosti, ktoré buď organizácia má k dispozícii alebo ich musí získať. Zmena nastala najmä v tom, že respondenti prikladajú väčšiu dôležitosť tomu, aby bol v rámci organizácie prítomný skutočne talentovaný personál v oblasti informačnej bezpečnosti, pričom nedostatok schopných pracovníkov sa pokladá za ešte väčšiu prekážku, ako tradične známe finančné a technologické limity.

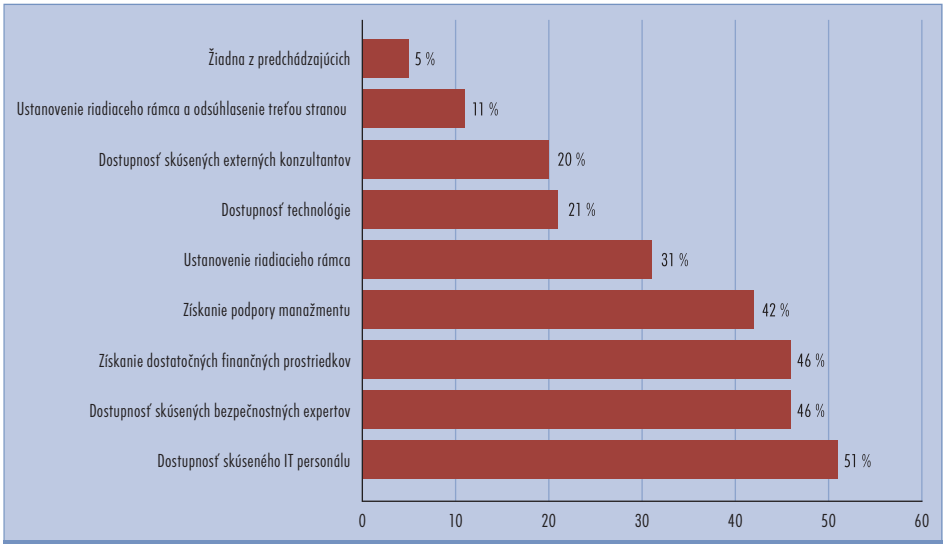
Dostupnosť kompetentných osôb sa umiestnila na prvom a druhom mieste medzi výzvami, pričom získanie vyškolených, skúsených externých konzultantov bolo oveľa jednoduchšie. Navyše existujú určité schopnosti, ktorých outsourcing je výhodnejší z hľadiska nákladov, čo je s najväčšou pravdepodobnosťou dôvod prečo 75 % respondentov využívalo tretie strany na testovanie útokov a penetrácie a 47 % použilo externé zdroje na vytvorenie architektúry informačnej bezpečnosti, vývoj postupov, ako aj na školiace programy.

Dobre známy nedostatok talentov v oblasti IT a informačnej bezpečnosti sa môže stať problémom pre mnohé organizácie, ale zároveň môže predstavovať príležitosť na prehodnotenie toho, ako informačná bezpečnosť reaguje na dopyt po ľudských zdrojoch. Veríme, že súlad so strategickými, riadiacimi, prevádzkovými a architektonickými funkčnými líniami poskytuje príležitosť pre informačnú bezpečnosť využiť nové oblasti zdrojov, ktoré neboli dostupné v minulosti. Napríklad zvýšená integrácia informačnej bezpečnosti a riadenia rizika viedla k tomu, že požiadavky na zdroje sa presunuli z primárne technickej roviny do rizikovej a kontrolnej s technickou „vhodnosťou". Vzhľadom na skutočnosť, že informačná bezpečnosť sa začala čoraz menej sústreďovať na technické a prevádzkové aspekty podnikania, zdroje z iných častí organizácie ako Interný audit sa stali technicky vhodné, pričom tie majú skúsenosti s určovaním rizík a potrieb súladu z oblasti auditu.

Organizácie však musia zabezpečiť aby presun od technických a prevádzkových prvkov nezapríčinil trhliny v tradičnejších oblastiach informačnej bezpečnosti.

ZAVEDENIE POSTUPOV PRI RIADENÍ RIZÍK

Je dôležité uvedomiť si, že zmeny v podnikaní môžu vyžadovať, aby organizácia prehodnotila svoje potreby a schopnosti v oblasti ľudských zdrojov. Toto rýchlo sa meniace prostredie zdrojov je pravdepodobne jedným z hlavných dôvodov, prečo 60 % účastníkov prieskumu zvolilo pri určitých prvkoch informačnej bezpečnosti outsourcing. Organizácie takto znížili potrebu získať a udržať si isté ťažko dostupné zručnosti interne.



Graf 4: Počet respondentov, ktorí vyhodnotili nasledovné oblasti ako najväčšiu výzvu v strategických projektoch informačnej bezpečnosti v ich organizácii

Tretie strany budú naďalej hrať dôležitú úlohu pri vypĺňaní trhlín v ľudských zdrojoch, pričom ich využitie by malo rozšíriť úlohy informačnej bezpečnosti, najmä keď organizácia nechce dlhodobo najímať vysoko kvalifikovaný a skúsený personál. Náš prieskum ukázal, že využitie zdrojov tretích strán môže byť produktívne z hľadiska riadenia nákladov a zároveň dokáže pokryť rastúci dopyt po odborníkoch z oblasti informačnej bezpečnosti.

Využitím vzťahov s tretími stranami, ktoré sa podľa nás budú ďalej rozvíjať, vzniká potreba poskytnúť tretej strane prístup k obchodným systémom alebo informáciám organizácie. S týmto rozvojom prichádza zvýšenie rizika. Organizácie musia toto zvýšené riziko rozpoznať a riadiť prostredníctvom vhodného vedenia vzťahov a zabezpečenia, aby boli externé zdroje v súlade s bezpečnostnými cieľmi organizácie. Napriek tomu, že väčšina organizácií má takéto postupy zavedené, viac organizácií by malo zaviesť formálne dojednania pri riadení vzťahov s tretími stranami. Platí to aj pre využitie nezávislého auditu, ktorý by monitoroval súlad a zvyšoval úroveň istoty, že tretie strany vykonávajú kroky potrebné na ochranu majetku organizácie.

Pracovať viac s menším počtom zamestnancov je pre odborníkov z oblasti informačnej bezpečnosti už roky známa mantra. Tejto výzve sa však treba postaviť. Tradičné modely obsadenia informačnej bezpečnosti ľudskými zdrojmi sa do budúcnosti zmenia, pretože organizácie budú hľadať cesty ako vyplniť trhliny v personalistike. Odborníci na stratégiu v oblasti bezpečnosti budú úzko spolupracovať s odborníkmi na podnikateľské stratégie, pričom budú aktívni v rôznych častiach organizácie. Bezpečnostní architekti budú viac koordinovať svoju činnosť s IT architektmi a funkcie prevádzkovej bezpečnosti sa zmiešajú s funkciami bezpečnosti jednotlivých divízií.

SMEROVANIE K ROVNOVÁHE MEDZI RIZIKOM A VÝKONOM

Globálny prieskum spoločnosti Ernst & Young o informačnej bezpečnosti v roku 2007 ukázal, že mnoho organizácií v súčasnosti vníma informačnú bezpečnosť ako niečo viac než len zmiernenie rizika a od implementácie bezpečnostných iniciatív očakáva skutočné zlepšenie výkonnosti. Bude zaujímavé porovnať výsledky tohto prieskumu s prieskumom stavu informačnej bezpečnosti v Slovenskej republike 2008, na ktorého organizácii a príprave sa podieľajú Ernst & Young, Národný bezpečnostný úrad a časopis DSM – Data Security Management a ktorý je práve vo fáze vyhodnocovania.

Desiaty ročník Globálneho prieskumu spoločnosti Ernst & Young o informačnej bezpečnosti bol vyvinutý s pomocou klientov z oblasti poistenia a poradenstva vo vyše päťdesiatich krajinách. Tohtoročný prieskum sa uskutočnil v máji 2007 až auguste 2007. Zúčastnilo sa na ňom takmer 1 300 organizácií zo všetkých významných odvetví. ■

Autor je manažér oddelenia riadenia technologických a bezpečnostných rizík, Ernst & Young

Zhrnutie kľúčových zistení

Zosúladenie informačnej bezpečnosti s podnikaním
- ★ Informačná bezpečnosť sa čoraz častejšie zameriava na napĺňanie podnikateľských cieľov.
- ★ Informačná bezpečnosť je v súčasnosti viac integrovaná do celkového riadenia rizika.
- ★ Informačná bezpečnosť zostáva odizolovaná od výkonného manažmentu a strategických rozhodovacích procesov.

Hnacia sila informačnej bezpečnosti
- ★ Zlepšenie IT a efektivity prevádzky sa stávajú dôležitými cieľmi.
- ★ Súlad s legislatívou je naďalej hlavnou hnacou silou zlepšení v oblasti informačnej bezpečnosti.
- ★ Súkromie a ochrana údajov sa stávajú čoraz dôležitejšími hnacími silami informačnej bezpečnosti.

Riadenie informačnej bezpečnosti
- ★ Organizácie sa spoliehajú na audity a vlastné odhady pri hodnotení efektivity svojich vlastných programov informačnej bezpečnosti.
- ★ Organizácie požadujú viac od svojich dodávateľov a obchodných partnerov pri riadení vzťahov s tretími stranami.

Ľudské zdroje v oblasti informačnej bezpečnosti
- ★ Najväčšou výzvou pri dodávaní projektov informačnej bezpečnosti zostáva nedostupnosť skúseného IT personálu, ako aj ľudských zdrojov z oblasti informačnej bezpečnosti.

Príležitosti na zlepšenie

Zosúladenie informačnej bezpečnosti s podnikaním
- ★ Využitie obchodných vzťahov na dôslednejšie splnenie podnikateľských cieľov;
- ★ Pokračovanie v zlepšovaní súladu informačnej bezpečnosti s celkovým riadením rizík;
- ★ Zapojenie informačnej bezpečnosti do strategických rozhodovacích procesov spoločnosti;

Hnacia sila informačnej bezpečnosti
- ★ Pristupovanie k informačnej bezpečnosti z pohľadu zdokonalenia podnikania a lepšieho ovplyvnenia investícií;
- ★ Využitie ochrany súkromia a údajov ako konkurenčnej výhody;
- ★ Nadväzovanie na iniciatívy zabezpečujúce súlad a zavedenie udržateľného harmonizačného programu;

Riadenie informačnej bezpečnosti
- ★ Využitie kombinácie vlastného odhadu, interného auditu, externého auditu a benchmarku na efektívne ohodnotenie a monitoring informačnej bezpečnosti;
- ★ Prijatie viacerých formálnych a konzistentných postupov na riadenie rizík vo vzťahoch s tretími stranami;

Ľudské zdroje v oblasti informačnej bezpečnosti
- ★ Preskúmanie alternatívnych personálnych zdrojov na zvýšenie dostupnosti skúsených a vyškolených pracovníkov;