



Rozpočty na informačnú bezpečnosť sa znižujú

Spoločnosti pôsobiace v odvetviach technológií, médií a telekomunikácií (TMT) výrazne znížili výdavky na bezpečnosť. Prieskum ukázal, že 32 % respondentov znížilo rozpočty na informačnú bezpečnosť, 60 % respondentov sa domnieva, že v riešení bezpečnostných rizík zaostávajú alebo stále v poslednej chvíli zachraňujú, čo predstavuje výrazný nárast oproti 49 % takýchto odpovedí v minulom roku.

Z dôvodu rozširovania digitalizácie by sa na bezpečnosť mala vynakladať podstatná časť celkového rozpočtu spoločností pre

oblasť informačných technológií. Pritom iba šesť percent respondentov vynakladá na bezpečnosť informačných technológií sedem

a viac percent zo svojho celkového rozpočtu. Tento rok bol zaznamenaný výrazný pokles oproti predchádzajúcemu prieskumu, podľa ktorého 36 percent respondentov investovalo do bezpečnosti informačných technológií minimálne sedem percent zo svojho celkového rozpočtu.

Prieskum tiež ukazuje, že pokles investícií do bezpečnosti bráni zavádzaniu nových bezpečnostných technológií. Iba 53 % respondentov sa domnieva, že ich spoločnosť si rýchlo osvojuje nové bezpečnostné technológie, alebo že patrí k prvej polovici spoločností, ktoré tak robia. Spoločnosti sa viac sústreďujú na optimalizáciu existujúcich riešení ako na investície do najnovších technológií, na ktorých možno stavať v čase ozdravenia ekonomiky.



Hoci sociálne siete a blogy ponúkajú rôzne možnosti, predstavujú i zvýšenú hrozbu pre vnútornú bezpečnosť spoločností. V súčasnom prepojenom svete sú hrozby zvnútra väčšie ako kedykoľvek v minulosti.

Spoločnosti nemajú k dispozícii potrebné zdroje na riešenie nových zraniteľných miest na sieti. Z celkového počtu opýtaných má iba 47 % v súčasnosti nainštalovaný program na ochranu osobných údajov a iba 44 % má riadiaceho pracovníka zodpovedného za ochranu osobných údajov, pričom minulý rok to bolo 50 %.

Až 56 % respondentov označilo odlišné kultúrne interpretácie za priemernú až veľmi vysokú hrozbu pre ich informačnú bezpečnosť.

Spoločnosti sa viac sústreďujú na optimalizáciu existujúcich riešení ako na investície do najnovších technológií, na ktorých možno stavať v čase ozdravenia ekonomiky.

Ako hrozbu pre informačnú bezpečnosť spoločnosti vníma 83 % respondentov využívanie zraniteľných miest v technológiách označovaných ako web 2.0.

SOCIÁLNE SIETE AKO ĎALŠIA HROZBA

Hoci sociálne siete a blogy ponúkajú rôzne možnosti, predstavujú i zvýšenú hrozbu pre vnútornú bezpečnosť spoločností. V súčasnom prepojenom svete sú hrozby zvnútra väčšie ako kedykoľvek v minulosti. Výsledky prieskumu ukazujú, že ako hrozbu pre informačnú bezpečnosť spoločnosti vníma 83 % respondentov využívanie zraniteľných miest v technológiách označovaných ako web 2.0 a 80 % respondentov uvádza ako hrozbu postupy sociálneho inžinierstva, ako napr. pretexting a phishing.

Okrem toho sú tu aj generačné rozdiely, ktoré majú výrazný vplyv na vnímanie súkromia. Vzájomná výmena informácií medzi najmladšou generáciou pracovníkov v oblastiach TMT môže byť testom obmedzení

tradičných zákonov na ochranu súkromia. Naopak, staršie generácie vnímajú súkromie veľmi odlišne. Respondenti prieskumu si tento problém uvedomujú, pričom 56 % označilo odlišné kultúrne interpretácie za priemernú až veľmi vysokú hrozbu pre ich informačnú bezpečnosť.

Prieskum ďalej uvádza, že v súvislosti s novo sa objavujúcimi zraniteľnými miestami spoločnosti zo sektoru TMT strácajú dôveru vo vlastnú schopnosť čeliť interným bezpečnostným rizikám. Len 28 % respondentov označilo svoje spoločnosti za veľmi spoľahlivé alebo mimoriadne spoľahlivé. Za posledných dvanásť mesiacov zaznamenalo až 41 % respondentov minimálne jedno porušenie pravidiel vnútornej bezpečnosti.

Okrem toho spoločnosti nemajú k dis-

pozícii potrebné zdroje na riešenie nových zraniteľných miest na sieti. Z celkového počtu opýtaných má iba 47 % v súčasnosti nainštalovaný program na ochranu osobných údajov a iba 44 % má riadiaceho pracovníka zodpovedného za ochranu osobných údajov, pričom minulý rok to bolo 50 %. Tento fakt ide ruka v ruku so skutočnosťou, že spoločnosti z oblastí TMT nemajú program na riadenie ochrany súkromia (33 %), písomné pravidlá na ochranu súkromia (28 %) alebo oficiálnu smernicu o likvidácii osobných údajov (28 %).

Informácie a duševné vlastníctvo tvoria podstatu spoločností z oblasti TMT. Najvyššou prioritou by pre ne mala byť ochrana tohto vzácného majetku, ktorý sa často používa v otvorenom prostredí pracovnej spolupráce.