

Informacijska sigurnost nije tajni sastojak uspješnog poslovanja

Bilo da je sadržana u materijalnim oblicima ili postoji kao realizirana ili potencijalna vrijednost u ljudskim resursima, informacija je ključna vrijednost organizacije koja omogućuje razvoj poslovanja u većini djelatnosti

Na žalost, nije riječ o tajnom sastojku uspješnog poslovanja, čime su informacije, zbog izvjesne ranjivosti uzrokovane svojom prirodom i načinom korištenja, izložene stalnim prijetnjama po temeljnim atributima sigurnosti.

Kombinacija ranjivosti informacijskog resursa i vanjske prijetnje tvori sigurnosni rizik, čije eventualno ostvarenje rezultira određenom negativnom posljedicom po sigurnosna svojstva informacije, a s time i povezane poslovne procese, koji osiguravaju dugotrajnu profitabilnost i ugled organizacije. Mehanizmi procjene i principi upravljanja rizikom služe upravo u svrhu otklanjanja ili smanjenja tih negativnih utjecaja.

Vođenje računa o zaštiti osjetljivih informacija nameće se kao obavezan dio osnovne djelatnosti organizacije, inherentno prisutan kao sredstvo održanja i unaprje-

đenja poslovanja. Dok je sâm pojam dobro poznat, mada i pod drugim terminima, konzistentni i održavani sustav upravljanja informacijskom sigurnošću (Information Security Management System, ISMS) upravo je dodana vrijednost koju tvrtka RECRO-NET nudi tim dijelom svoga portfelja. Riječ je o sustavnom pristupu upravljanju sigurnošću informacija koje služe kao osnova i podloga kritičnim poslovnim procesima te obuhvaća sveukupne resurse organizacije, tj. ljude, procese i ICT (Information and Communication Technology) sustave. Temeljen na procesnom pristupu, podrži upravljačkih tijela, kontroli dokumentacije te podvrgnut redovnim nezavisnim unutarnjim i vanjskim revizijama, ISMS je jamstvo kvalitetnog i sigurnog poslovanja.

Uz konzultantske usluge uspostave sustava upravljanja informa-

cijskom sigurnošću, RECRO-NET pruža brojna tehnološka rješenja implementacije sigurnog okruženja. Također, provjera postojećih mjera zaštite sigurnosti informacija, u vidu revizije (auditing) sustava, pa sve do tehničkih ispitivanja rezistencije IT sustava (penetration testing), spadaju u opis posla međunarodno certificiranih stručnjaka Odjela sigurnosti RECRO-NETa.

Penetracijsko testiranje

Iako sustav upravljanja sigurnošću informacija ne mora nužno pratiti međunarodno utvrđenu metodologiju, pri čemu spomenuti standard nije jedina raspoloživa referenca u svijetu informacijske sigurnosti, slijede određene koristi od korištenja smjernica i certificiranja upravo po HRN ISO/IEC 27001:2006 standardu, poput posjedovanja konkurentne prednosti pri ispunjavanju formalnih

zahtjeva poslovanja prema trećim stranama te referentne garancije kvalitete upravljanja informacijskim resursima kao ključnim elementima poslovanja.

Informacijski su sustavi dinamička okruženja čije se komponente često mijenjaju mijenjajući ponekad i svoj utjecaj na sigurnost cjelovitog sustava, stoga je revizija sigurnosti stalna briga odgovornih stručnjaka. Reviziju valja provoditi vodeći se sigurnosnom politikom samih korisnika, međunarodnim standardima i dobrom in-dustrijskom praksom uz tijesnu suradnju s IT osobljem i otvoren pristup tehničkoj dokumentaciji i konfiguraciji svih uređaja. Detaljno se pregledava dizajn informacijskog sustava, postavke računala i komunikacijske opreme u cilju pronalazanja sigurnosnih slabosti. Revizija rezultira izvješćem o stanju sustava s preporukama za otklanjanje uočenih slabosti.

Unatoč sve većoj pažnji koja se pridaje sigurnosti proizvoda u IT svijetu kod projektiranja, proizvodnje, implementacije i korištenja bilo da je riječ o softveru, hardveru ili uređajima koji objedinjuju oboje, još uvijek je prisutan dovoljan broj sigurnosnih propusta koji omogućava zloćudne pristup, krađu podataka, uskraćivanje resursa. Osim sigurnosnih propusta u proizvodima, nedostaci se mogu pronaći i u procedurama, pravilima korištenja ili implementaciji sustava tako da sitni, najčešće neznatni propusti, posredno omogućuju put do većih koji u konačnici mogu ozbiljno narušiti opću sigurnost sustava.

Uz provjeru razine sigurnosti sustava u skladu sa sigurnosnim pravilnicima, standardima i regulatorskim tijelima nezaobilazno je i penetracijsko testiranje. To je metoda testiranja sigurnosti informa-

cijskih sustava u kojem se kontrolirano simulira napad na sustav kao što bi to učinio zloćudni korisnik. Na taj način aktivno se analizira sigurnost sustava kao jedne cjeline, uključujući sve tehničke aspekte te cjeline i pojedinih komponenti; potencijalni propusti u hardveru i softveru, te pasivni i aktivni sustavi zaštite.

Najčešće se kao cilj penetracijskog testiranja postavlja dolazak do određenog podatka iz testiranog sustava ili postizanje nepri-mjerenih ovlasti unutar sustava.

Sigurnosna rješenja

Jedna od glavnih podjela te vrste testiranja je prema početnoj (priključnoj) točki izvođenja; kod vanjskog testiranja pristupa se iz javne mreže (interneta), dok se kod unutarnjeg kreće iz točke u mreži tvrtke čija se sigurnost testira. (Statistike pokazuju da je 80% zloćudnih radnji dolazi 'iznutra'.) Osim prema početnoj točki, penetracijsko testiranje se dijeli i prema početnim informacijama testnog tima o meti, odnosno upoznatosti mete s provođenjem testiranja. Naime, ako se testira znanje i iskustvo testera, tada se kreće s nikakvim ili samo osnovnim spoznajama o meti, odnosno ako se uz testiranje sigurnosti sustava testira i spremnost osoblja i sustava na reakciju, tada osoblje zaduženo za zaštitu nije upoznato s provođenjem testiranja.

Penetracijsko testiranje mora biti izvedeno temeljito, s posebnom pažnjom prema detaljima. Naime, ne smije se zanemariti da je ponekad dolazak do cilja moguć na više načina.

Standardi

Krovni standard vezan uz informacijsku sigurnost Međunarodne organizacije za standardizaciju ISO (International Organization for Standardization) i Međunarodne elektrotehničke komisije IEC (International Electrotechnical Commission), oznake ISO/IEC 27001:2005 i naziva Informacijska tehnologija - Sigurnosne metode - Sustavi upravljanja informacijskom sigurnošću - Zahtjevi (Information technology - Security techniques - Information security management systems -

Sigurnosna politika tvrtke temeljni je dokument oko čijih postavki se gradi obrana i uvode sigurnosni mehanizmi u IT infrastrukturu svake tvrtke.

Prva linija obrane na mrežnoj strani obično je odgovarajuće konfiguriran i nadziran firewall sustav, koji može nositi i dodatnu funkcionalnost detekcije i prevencije napada poput Cisco ASA obitelji proizvoda i odgovarajuće dodatne module. Siguran pristup udaljenih korisnika zahtijeva odgovarajuće dizajniran i nadziran VPN sustav, čemu opet može poslužiti Cisco ASA.

Javno dostupne internetske poslužitelje potrebno je dodatno štiti od mrežnim upadima ili DoS napada, pri čemu RECRO-NET nudi rješenja tvrtke IronPort i Arbor Networks kao posebne uređaje za filtriranje e-mail poruka, web zahtijeva i provjeru standardnoga mrežnog prometa (www.ironport.com, www.arbornetworks.com).

Sustav upravljanja elektroničkim identitetom svakako je središnje mjesto oko kojega se gradi svaki moderni informacijski sustav: OpenTrustova (www.opentrust.com) rješenja za upravljanje pametnim karticama, jednokratnim lozinkama, sustavom sigurne razmjene kriptiranih podataka, digitalnih potpisa i digitalno potpisanih dokumenata te kompletnom PKI infrastrukturom primijenjena su i unutar RECRO-NETa kao kućni standard sustava digitalnih identiteta.

Uvijek valja razmišljati o nekoliko prstena obrane koji obuhvaćaju kvalitetna backup/restore rješenja za pohranu i povrat važnih

podataka i antivirusnu i malware zaštitu na mjestima koja su prepoznata kao kritična.

Antivirusna i malware zaštita svakako je alat koji svako korporacijsko osobno računalo mora imati i takav se alat mora svakodnevno ažurirati. RECRO-NET nudi Symantecova antivirusna rješenja koja uz osnovnu antivirusnu zaštitu omogućuju i uvode centralno upravljanje sigurnosno spremanje i povratak podataka na računalo čime se uvodi dodatna funkcionalnost na korisničko računalo. Tako kontrolirano računalo omogućuje nadzirano korištenje USB uređaja za pohranu podataka i forsiranje odgovarajuće sigurnosne politike kroz tzv. crne liste nedopuštenih aplikacija i servisa na korporacijskim računalima.

Praćenje rada aktivne mrežne opreme, korisničkih računala i kritičnih poslužitelja podrazumijeva kvalitetan i redovit nadzor log datoteka, pri čemu je prepoznat problem odgovarajućeg tamčenja pojedinih događaja i stanja na nadziranim uređajima. TriGEO uređaj (www.trigeo.com) omogućuje praćenje logova većeg broja nadziranih uređaja i dovođenje pojedinih događaja na raznim uređajima u odgovarajuću korelaciju, čime se mnogo lakše sjele sveobuhvatan uvid u stanje računalne infrastrukture. TriGEO Active Response klijent omogućuje definiranje odgovarajućih odgovora na uočene nepravilnosti ili napade na informacijski sustav, pa se virusnom zaraženo računalo može isključiti iz mreže, isključiti nedopušteni USB uređaj, prijaviti zlonamjerni pokušaj upada na korisničko računalo ili datotečne poslužitelje...

Rješenja za sve probleme

RECRO-NET je informatička tvrtka koja ispunjava sve korisničke zahtjeve za rješenjima iz područja informacijsko-komunikacijskih tehnologija s korisnicima u cijeloj regiji Jugoistočne Europe i na Bliskom istoku. Misija RECRO-NETa je kroz inovativnost i optimizaciju stalno stvarati nove vrijednosti za svoje korisnike, poslovne partnere, zaposlenike i opću društvenu sredinu.

RECRO-NET trenutačno ima stotinjak zaposlenih u Hrvatskoj i BiH te je tvrtka s najviše visoko certificiranih pojedinaca u regiji. ■