

NOVI IZAZOVI



Uskladiti poslovanje sa zahtjevima regulatora i spriječiti prijevare glavni su zadaci financijskih institucija s informacijskog aspekta. Kako bi reagirali što brže, "financijaši" traže partnere u renomiranim informatičkim kućama

Piše **Tomislav Hrisoho**
predsjednik Uprave RECRO-NETA

Tehnološki napredak je omogućio, a tržišna utakmica nametnula, ponudu novih usluga korisnicima banaka i osiguravajućih kuća (internetske i mobilne usluge), kao i optimizaciju tehnoloških aspekata poslovanja (IP telefonija, virtualizacija, sigurna pohrana podataka...). Regulativa u vidu smjernica HNB-a i HANFA-e te međunarodnih standarda (PCI DSS) proaktivno nameće zatvaranje sigurnosnih rupa u sve izloženijim informacijskim sustavima.

Financijske institucije drže korak i paralelno razvijaju svoj IT portfelj - aplikacije internetskog i mobilnog bankarstva, info pultove, virtualne poslovne - i mjere zaštite, od revizije IT sustava, pohrane podataka, zaštite od malicioznog softvera, redundantne infrastrukture do nadzora dnevničkih zapisa.

Rokovi nadležnih državnih institucija, revizije Basel, Solvency i PCI DSS standarda ne znaju za predahe, kao ni informatički sve pismeniji i zahtjevniji profil krajnjih korisnika.

Neizbježno je osigurati potpunu sukladnost s regulativom. Većini financijskih institucija slijedi posvećivanje područjima kao što su upravljanje kontinuitetom poslovanja, stroža kontrola udaljenog pristupa informacijskim sustavima, upravljanje korisničkim pravima pristupa, kontrola performansi mrežnih usluga i aplikacija, aktivno upravljanje sustavima na temelju nadzora dnevničkih zapisa i aktivnosti korisnika, sustavno upravljanje HW i SW imovinom itd.

Incidenati koji dopijuu u javnost ukazuju na sve veću potrebu za tehnički potpomognutim rješenjima sprečavanja financijskih prijevara, zaštite od visokospecijaliziranih napada na elektroničke

usluge te uspostave pričuvnih lokacija ICT sustava, u optimalnom odnosu (visokih) ulaganja i poslovnih potreba.

Osigurati neprekinutost poslovanja

Struka i trendovi nude brojna rješenja koja kombinacijom preventivnih, detektivnih i korektivnih aktivnosti čine IT sustave sigurnijima.

Osiguranje neprekinutosti pružanja ICT usluga zasniva se na analizi utjecaja IT resursa na poslovanje, izbora opcija pričuvne pohrane podataka, redundantnosti i visoke raspoloživosti IT sustava te uvježbavanja osoblja.

Brojni vektori napada čine problematiku upravljanja financijskim prijevarama gotovo znanstvenom disciplinom. Srećom, analize uobičajenih oblika poslovanja te uočenih anomalija i propusta rezultirale su softverskim rješenjima, čiju je razrađenu logiku moguće u razumnom vremenu prilagoditi potrebama pojedinih korisnika.

Interne i vanjske revizije već duže vrijeme uključuju tehnički aspekt, no opseg revizije ne dopušta dubinsku analizu. Sukob interesa rezultira potrebom za neovisnom procjenom stanja sigurno-

sti kroz analizu raskoraka, provjeru IT ranjivosti i penetracijsko testiranje. Sve te usluge potpomognute su ICT alatima, ali pravu vrijednost pružaju u obradi i interpretaciji prikupljenih rezultata. Kako financijskim institucijama nedostaje vremena za analizu tržišta i testiranje rješenja uspostavljaju strateške partnerske odnose s renomiranim informatičkim kućama poput RECRO-NET-a.

Našim korisnicima zadovoljstvo jamčimo svojim iskustvom u pružanju konzultantskih i specijaliziranih tehničkih usluga implementacije i održavanja, u partnerstvu s vodećim svjetskim proizvođačima. Cisco, DenyAll i Palo Alto su tvrtke prepoznatljive po svojim rješenjima mrežne zaštite; OpenTrust je francuska tvrtka posvećena rješenjima zasnovanim na infrastrukturi javnog ključa, koja omogućuju usluge sigurne prijave korisnika IT sustava, digitalnog potpisa, sigurnog prijenosa podataka i slično; Intellinx je proizvođač specijaliziranog softvera za sprečavanje prijevara, kroz mehanizme uspostave redovitih i izvanrednih obrazaca ponašanja, nadzora aktivnosti korisnika, alertiranja i forenzičke analize zapisa.