

Ispunjenje regulatornih uvjeta za izdavanje dijela poslovanja informatičkih procesa u hrvatskim bankarskim institucijama

Detekcija kao jamstvo sigurnosti

Financijski se sektor sa svojom potrebom intenzivne i precizne obrade podataka oduvijek oslanjao na tehnološka rješenja kao potporu poslovnim procesima. Informatička tehnologija neizbježna je i sve kompleksnija. No uz nove mogućnosti javljaju se i određeni sigurnosni rizici, pojam bankarskom resoru poznat koliko i uporaba sofisticiranih i složenih informatičkih sustava. Sve češće izdavanje dijela poslovanja svojevrsno je otvaranje bankovnih informacijskih sustava prema vanjskim partnerima.

Propisi

S obzirom na to da su jedno od sigurnosno najosjetljivijih područja poslovanja, hrvatske bankarske institucije u temeljnom financijskom poslovanju tradicionalno nadziru brojni zakonski akti. Rast poslovnih zahtjeva iziskuje integraciju tehnoloških rješenja, među ostalim i u sigurnosnim zahtjevima. Kao logično rješenje održanja najviše razine zaštite informacijskih resursa nameće se potpuna izolacija sustava obrade i razmjene informacija u sigurnom okruženju organizacije. Potreba za sve užim specijalističkim tehničkim znanjem, koje kreditne institucije često nisu spremne osigurati u svojim redovima, zbog čega često angažiraju vanjske stručnjake, kao i nužnost sigurne razmjene podataka s trećim stranama - konflikt su

apsolutne sigurnosti i nužnosti profitabilnog poslovanja.

Prvi dokument koji se detaljno pozabavio problematikom eksternalizacije bile su 'Smjernice za adekvatno upravljanje rizikom eksternalizacije' (HNB, listopad 2005.), koncentrirane većinom na procjenu rizika prilikom odabira eksternalizacijskog partnera. Godinu dana poslije HNB je izdao opsežnije 'Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika'. Sve do srpnja 2007. svi su ti naputci bili isključivo savjetodavnog karaktera, što se mijenja donošenjem 'Odluke o primjenom upravljanju informacijskim sustavom'. Njome su odredbe dopunjene i poprimaju obvezni karakter, s preciznim rokovima primjene (od kojih su neki već prošli, a ostali slijede u tekućoj i sljedećoj godini).

Preduvjeti uspjeha

Iako su tim dokumentom pokriveni brojni aspekti informacijskih sustava, dobro je pozabaviti se samo

dijelom koji se odnosi na zahtjeve spram eksternalizacije. Preduvjet dugotrajnog sigurnog poslovnog odnosa banke i partnera valjan je odabir vanjskog pružatelja usluga. Objektivna i strukturirana procjena rizika osigurava izbor optimalnih kandidata. Praksa je međutim pokazala da to samo po sebi nije dovoljno jak temelj bezuvjetnom povjerenju. Tehnička ograničenja pristupa vanjskih suradnika informacijskim sustavima banke utemeljena na načelu posjedovanja minimalnih ovlasti potrebnih za obavljanje posla također ne osiguravaju miran san ako ih ne prate odgovarajući postupci nadzora. Tako se stiže do važnog segmenta upravljanja eksternalizacijom obrađenog regulativom. Učestalost korištenja vanjskim uslugama, brojnost uključenih i sve zastupljenije opcije daljnjskog pristupa IT sustavima uvelike smanjuju učinkovitost tradicionalne metode tzv. gledanja preko ramena, pa se nameće potreba za tehničkim, automatiziranim načinima kontrole unajmljenog rada.

Odabrano rješenje nadzora mora zadovoljiti i zahtjeve prikupljanja odgovarajućih zapisa. Svrha je dvojaka: uporaba arhivskog materijala za forenzičku analizu i mogućnost statističke obrade legitimnih radnji eksternalizacijskih partnera (što pak osigurava neprekidno ocjenjivanje kao preduvjet optimalnog poslovanja). Odlukom HNB-a pokriven je i prateći proces upravljanja incidentima, čija se uspostava temelji upravo na egzaktnim rezultatima nadzora i omogućuje 'pravodoban i učinkovit od-



govor u slučaju narušavanja sigurnosti i funkcionalnosti resursa informacijskog sustava koji podržavaju odvijanje poslovnih procesa'.

ObserveIT

ObserveIT izraelska je tvrtka čiji je istoimeni programski paket specijaliziran za praćenje aktivnosti na računalnim uređajima IT sustava različita obujma, uspješno uveden u organizacije raznovrsnih profila, uključujući, naravno, financijski sektor. Riječ je o isključivo softverskom rješenju (uz uvođenje u infrastrukturu korisnika) koje na temelju određenih parametara snima i u vizualnom formatu pohranjuje sve aktivnosti koje korisnici vide na zaslonu nakon pristupanja održavanom dijelu sustava. Proizvod je agnostičan spram upotrijebljenoga komunikacijskog protokola (podržava Terminal Services, Citrix, Re-

mote Desktop, PC-Anywhere, VNC i NetOP) i klijentske aplikacije kojom korisnik pristupa nadziranom sustavu, čime pokriva snimanje aktivnosti na svim terminalskim, konzolnim i virtualizacijskim računalnim sesijama. Mogućnost praćenja uključuje izravno snimanje na održanim računalima, odnosno dozvolu sigurnog VPN pristupa vanjskim partnerima isključivo na nadzirano računalo, a tek nakon toga s njega na uređaj koji se održava. Kako korisnik, čak ni s administratorskim ovlastima na uređaju, ne može bez trenutačne uz-bune administratoru isključiti snimanje, ispunjen je zahtjev strogog i kontinuiranog nadzora rada. Osim nadzora vanjskih partnera kod osjetljivih se dijelova sustava može javiti potreba za kontrolom i vlastitih zaposlenika, što je, naravno, podržano. Da bi se smanjila količina sni-

mljenog materijala, konfiguracija sustava omogućava definiciju preciznih pravila ispunjenje čijih uvjeta djeluje kao otponac snimanja, ovisno o uključenim korisničkim strukturama, upotrijebljenim aplikacijama, tipovima datoteka, pa čak i sljedovima pritisnutih tipaka na tipkovnici. Radi dodatne uštede prostora sustav prepoznaje vrijeme neaktivnosti korisnika i automatski nakon isteka određenog vremena prekida snimanje, a krajnji se materijal i komprimira.

Cjelovita pokrivenost

Kad je riječ o pohrani prikupljenog materijala, valja uzeti u obzir njegovu količinu, koja u većim sustavima s čestom potrebom za vanjskom linijom ima na tisuće zabilježenih sati na godinu. Deklaracija proizvođača o zauzeću manje od 100 GB za okruženje od tisuću poslužitelja na godinu dovoljno govori

RECRO-NET

Stvaranje novih vrijednosti

Više detalja o rješenju možete pronaći na web-adresi: www.observeit-sys.com. RECRO-NET d.o.o. ima stručno osoblje, iskustvo, projektnu organizaciju i financijsku stabilnost da to rješenje može uvesti u raznovrsne heterogene IT sustave. RECRO-NET d.o.o. jedna je od vodećih ICT tvrtki u području umrežavanja, sigurnosnih i sistem-integracijskih rješenja s poslovanjem i korisnicima u cijeloj Jugoistočnoj Europi i na Bliskom istoku. RECRO-NETOVA je misija inovativnošću i optimizacijom stalno stvarati nove vrijednosti za svoje korisnike, poslovne partnere i cijelu društvenu sredinu.

o izvršnim performansama pohrane podataka tog rješenja.

Sveobuhvatna pokrivenost raznih programskih platformi i optimalan sustav pohrane dva su temeljna preduvjeta učinkovitog sustava nadzora, međutim krajnja korist rješenja sadržana je upravo u mogućnosti efikasne analize silne količine materijala. U tu svrhu program tijekom snimanja analizira stanje na zaslonu i pohranjuje tzv. tekstualne metapodatke kojima se poslije olakšava postupak pretrage na temelju ključnih riječi. Putem web-sučelja dostupan je i iscrpan alat za izradu izvještaja prilagođenih specifičnim zahtjevima korisnika, u čemu se očituje prije spomenuta nužna statistička funkcionalnost rješenja za nadzor.

Osim neovisnog web-sučelja ObserveIT može se integrirati s nekim rješenjima za upravljanje IT sustavima, primjerice Microsoftom, CA Unicenterom, BMC-om, HP Open Viewom i mnogim drugima. Simbioza krovnog upravljačkog sustava s mogućnostima rješenja ObserveIT uvelike skraćuje vrijeme potrebno za traženje, a tako i duljinu odaziva na uočeni problem, što je izravan doprinos zahtjevu procesa upravljanja sigurnosnim incidentima. ■

PSIHOLOŠKI UČINCI

Veća transparentnost

Znajući da su najveća vrijednost, ali i najslabija karika organizacijskog lanca ljudi, valja spomenuti i sveprisutan psihološki učinak. Naime, uz određene negativne konotacije koje

sustav nadzora inherentno povlači, spoznaja o stalnoj kontroli i mogućnosti reprodukcije nehotičnih i namjernih štetnih aktivnosti uvelike će pridonijeti ozbiljnosti pristupa

poslu i odvratanju od malicioznih djelatnosti samih zaposlenika i vanjskih partnera. Povećana transparentnost kao posljedica dodana je vrijednost na korist svim stranama.