

Recro-net, u strateškom partnerstvu s tvrtkom KPMG pruža usluge provedbe procesa BCM i integraciju tehničkih rješenja za upravljanje kontinuitetom poslovanja, odnosno 'Business Continuity Management'



Upravljanje kontinuitetom poslovanja jedan je od zahtjeva i središnje banke

Predsjednik uprave jednog je poslijepodneva primijetio da slanje i primanje jednostavne elektroničke pošte traje neuobičajeno dugo i da se gubi veza s mail-serverom. Pokušao je nazvati informatičkog direktora, ali na ekranu njegova IP telefona pisalo je 'connecting'... Mobilnim telefonom uspio je dobiti informatičkoga direktora koji mu je objasnio da nema razloga za brigu jer će uskoro ukloniti problem. Prema prvim procjenama bila je riječ samo o prolaznom opterećenju procesora glavnog 'switcha' prouzročenom naglim porastom prometa. Predsjednik uprave tražio je da problem riješe što prije jer mu je otežavao rad, a očekivao je i

važan poziv iz inozemstva. Informatički direktor nazvao je voditelja svog IT odjela i pitao za fazu rješavanja problema. Voditelj mu je odgovorio da intenzivno rade na tome, ali da još nisu pronašli uzrok naglog povećanja prometa. Usput mu je objasnio da se isti problem ponavlja posljednjih nekoliko dana, i to tako da traje kratko i nestane sâm od sebe. Nažalost, ovaj se put stanje nije vratilo u normalu. Uskoro su počeli pozivi mobitelom zaposlenika iz središnjice i poslovnica banke s pritužbama da telefoni ne rade, poslovna aplikacija ne funkcionira i da se na šalterima stvaraju redovi nezadovoljnih korisnika. Postalo je očito da je u mreži nastao problem s nekontroliranim prometom koji ovaj put

neće nestati sâm od sebe... Što se poslije dogodilo, zašto takvi problemi iskrsavaju, kako ih ukloniti te kako izbjeći takve situacije, reći će vam RECRO-NET-ovi stručnjaci s najpriznatijim ICT certifikatima! Upravljanje kontinuitetom poslovanja je usluga planiranja i izrade detaljnih procedura u slučaju rizičnih događaja, promijenjenih poslovnih procesa i procedura radi vraćanja u uobičajeno stanje. Cilj je planiranja jasno definirati moguće rizične događaje i mehanizme za umanjivanje njihova utjecaja, osigurati neprekidnost kritičnih poslovnih procesa i moguće gubitke svesti na prihvatljivu razinu. Upravljanje kontinuitetom poslo-

STANARDI

Što čini upravljanje kontinuitetom poslovanja

Upravljanje kontinuitetom poslovanja u skladu sa standardom BS25999 obuhvaća:

- Analizu utjecaja rizičnih događaja na poslovanje (Business Impact Analysis, BIA)
- Procjenu rizika (Risk Assessment, RA)
- Plan upravljanja kontinuitetom poslovanja (Business Continuity Plan, BCP)
- tehnološkog oporavka (Disaster Recovery Plan, DRP)

vanja jedan je od zahtjeva koje postavlja i HNB. Recro-net u strateškom partnerstvu s konzultantskom tvrtkom KPMG pruža usluge provedbe procesa BCM i integraciju tehničkih rješenja za upravljanje kontinuitetom poslovanja. Tehnička procjena sigurnosti u skladu sa zahtjevom HNB-a i PCI-a usluga je sustavne provjere dizajna sigurnosti, mjera zaštite i konfiguracija komponenti informacijskog sustava.

Sigurnosni pregled

Namjera je procijeniti koliko je sigurnost informacijskog sustava korisnika usklađena s međunarodnim preporukama i politikama sigurnosti korisnika. Penetracijski test jest usluga simuliranog napada na informacijski sustav korisnika koji primjenjuje iste metode napada potencijalnih napadača. Cilj penetracijskog testa je izmjeriti razinu otpornosti informacijskog sustava na napad, stvarnu efikasnost mjera zaštite i identificirati ranjivosti koje je moguće slučajno aktivirati ili namjerno iskoristiti. Rezultati procjene sigurnosti i penetracijskog testiranja jesu dokumenti koji detaljno opisuju pronađene ranjivosti i razinu rizika te daju preporuke za poboljšanja sustava.

Analiza GAP jest usluga analize raskoraka između postojećeg stanja sigurnosti informacijskog sustava i željnog stanja, usklađenog sa zahtjevima međunarodne norme ISO27001. Cilj te analize jest sustavno procijeniti sigurnost informacijskog sustava i u kojim su područjima poboljšanja nužna, i to rabiti kao osnovicu za određivanje prioriteta i potrebnih resursa. Rezultat je analize dokument koji sadrži zahtjeve norme ISO27001, opisuje trenutačno stanje informacijskog sustava, definira razinu usklađenosti i daje smjernice za poboljšanje.

Centralizirani sustav

Radi učinkovitog nadzora uporabe informacijskog sustava na pojedinim je komponentama sustava (aplikacije, baze podataka, operacijski sustavi, mrežna oprema) uključeno generiranje sistemskih poruka. Iste se, u skladu sa za-

htjevom HNB-a i PCI-a, moraju neprekidno analizirati i trajno pohraniti. Budući da je riječ o velikoj količini podataka, bez sustava za centralizirano prikupljanje i korelaciju sistemskih poruka vrlo je teško utvrditi što se u određenom trenutku dogodilo i tko je odgovoran za problem.

End-user-experience (EUE) monitoring sustav podrazumijeva praćenje funkcioniranja poslovnih aplikacija iz perspektive krajnjeg korisnika. Sustav aktivno prati funkcioniranje mreže i aplikacija te daje uvid u percipiranu kvalitetu usluge pojedinog korisnika, identificirajući korisnike zahvaćene degradacijom performansi kritičnih aplikacija i prikazujući trendove degradacije. Rezultat implementacije ovog rješenja jest brza i učinkovita detekcija i izolacija problema u sustavu, čime se otvara mogućnost rješavanja problema prije negoli ga korisnik uopće osjeti, čime se naposljetku sprječava gubitak kredibiliteta korisnika i potencijalni gubitak prihoda.

Suvremeno mrežno okruženje iznimno je dinamično, a sigurnosna politika u praksi se tipično implementira kreiranjem pravila na sustavima firewall i listama access control. Time se kontrola provodi na perimetrima i na takav način se ne obuhvaća ukupni mrežni promet. U takvim okolnostima učinkovito kontroliranje pristupa mrežnim resursima i sukladnosti tokova prometa unutar poslovne mreže s internom sigurnosnom politikom i/ili vanjskim regulatornim zahtjevima postaju pravi izazov. Takav uvid treba pružati informaciju tko komunicira - što komunicira - s kim komunicira.

Ruke stručnjaka

'Vrijeme je novac' izreka je potpuno primjerena za trading dio financijskog sektora. Nadzor i planiranje mrežnih resursa temeljen na 15-minutnim agregiranim podacima nije adekvatan za trading-aplikacije. Učinkoviti trading zahtijeva i praćenje specifičnih parametara kao što su Financial Information eXchange, Multicast

Svjedočanstva

REKLI SU O RECRO-NETU...

DANIJEL BARA,

direktor Sektora informatike Jadranskog osiguranja:

- Recro-net je naš dugogodišnji, pouzdan poslovni partner. Svojom filozofijom koja u osnovu svih aktivnosti postavlja razumijevanje poslovnih potreba korisnika aktivno je uključen već u fazama promišljanja i predlaganja rješenja koja bi optimizirala i unaprijedila poslovanje Jadranskog osiguranja. Takav poslovni odnos daje rezultate koji su često iznad sfere čisto ekonomskih kriterija i kao takav za nas ima neprocjenjivu vrijednost.

BALAZS BEKEFFY,

član Uprave OTP banke:

During long-term collaboration, we found RECRO-NET as our partner that supports OTP bank business needs and actively takes part in creating solutions and services which enhance our business activities. Security and reliability are key characteristics of our information system and RECRO-NET's service is indeed in accordance with that approach. Thus, business relationship that we have with RECRO-NET is inestimable for us.

market feeds, TibCo visibility i drugi.

Infrastruktura javnog ključa (Public Key Infrastructure, PKI) uporabom kriptografije omogućava pouzdanu provjeru identiteta (zahtjev HNB-a i PCI-a), digitalni potpis, neporecivost digitalnih transakcija i sigurnu razmjenu podataka na nesigurnim mrežama kao što je internet. Implementacijom PKI-a povećava se sigurnost informacijskog sustava i smanjuju troškovi uvođenjem poslovanja putem interneta. Većina gotovih aplikacija kao što su programi za mail, web-serveri i preglednici, paket MS Office, MS AD, bežične i VPN mreže već sada omogućava upotrebu PKI sustava i pametnih kartica za pohranu digitalnih certifikata.

Problemi u funkcioniranju poslovnih aplikacija vrlo često nastaju upravo na mrežnoj razini. IT osoblje primarno se fokusira na zaštitu viših razina svojih informacijskih sustava zanemarujući pritom temeljne mehanizme mrežne sigurnosti, čime se znatno narušava sigurnost ukupnoga poslovnog sustava. Mrežna oprema osim osnovne funkcionalnosti prijenosa podataka ima i brojne sigurnosne mehanizme koji, pravilno primijenjeni, mogu znatno podići sigurnosnu razinu ukupnoga informacijskog sustava.

nosne mehanizme koji, pravilno primijenjeni, mogu znatno podići sigurnosnu razinu ukupnoga informacijskog sustava.

Nadzor računalnih sesija

Kako bi se u skladu s HNB-ovim zahtjevom osigurao nadzor aktivnosti vanjskih partnera kojima je prepušten dio poslova i IT osoblja s posebnim ovlastima, nužno je snimati njihove računalne sesije na informacijskom sustavu tvrtke. Cilj je nadzora dvostruk; detektirati pogreške i neovlaštene aktivnosti te djelovati preventivno na njihovu sprječavanju. Snimljene sesije sadrže i meta-podatke na osnovi kojih se može raditi brzo pretraživanje te izvješćivanje prilagođeno potrebama korisnika.

Preпустите се с повјеренјем у руке стручњака!

Recro-netov tim stekao je najcjelovitije certifikate na području informacijske sigurnosti: CISA (Certified Information Systems Auditor), CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), ISO27001LA - ISO 27001 lead auditor i CCIE (Cisco Certified Internetwork Expert) - Security. ■