HRVATSKI OGRANAK MEĐUNARODNE
ELEKTRODISTRIBUCIJSKE KONFERENCIJE
2. (8.) savjetovanje
Umag, 16. – 19. svibnja 2010.

SO3 – 17

mr. sc. Ante Martinić, dipl. ing. rač
KONČAR – Inženjering za energetiku i transport d.d., Zagreb
ante.martinic@koncar-ket.hr

Juraj Ljubešić, mag. ing. el., CISA, CISM
KONČAR – Inženjering za energetiku i transport d.d., Zagreb
juraj.ljubesic@koncar-ket.hr

Marko Šmalcelj, mag. ing. el., CISSP
KONČAR – Inženjering za energetiku i transport d.d., Zagreb
marko.smalcelj@koncar-ket.hr

# USPOSTAVA MEHANIZAMA NADZORA I UPRAVLJANJA INTEGRIRANIM INFORMACIJSKIM SUSTAVOM

## SAŽETAK

Suvremeno poslovno okruženje zahtjeva implementaciju sve složenijih poslovnih procesa podržanih različitim aplikacijama, često uz interakciju s vanjskim svijetom. Mehanizmi integracije aplikacija moraju osigurati integraciju heterogenih informatičkih sustava uz zadržavanje mogućnosti dodavanja novih radi potpore novim poslovnim funkcijama. Osim samih aplikacija integrirani informacijski sustavi uključuju i sistemsku programsku podršku te sklopovsku i mrežnu opremu.

U cilju osiguranja sigurnosti, učinkovitosti i kontinuiteta rada integriranog informatičkog sustava potrebno je osigurati mehanizme nadzora i upravljanja sustavom kao cjelinom. Takvi mehanizmi prate ispravnost rada aplikacija, operacijskih sustava, sklopovlja i računalne mreže a sposobni su i poduzimati predodređene korektivne akcije. Polazna točka pri implementaciji ovakvog sustava nadzora i upravljanja je uspostava sustava za upravljanje informacijskom sigurnošću. U članku će biti opisana uspostava upravljanja i nadzora integriranih informacijskih sustava i tehnička rješenja koja se pri tome koriste.

**Ključne riječi:** informacijski sustav, nadzor i upravljanje, sigurnost, ISO/IEC 27001

# IMPLEMENTATION OF MONITORING AND MANAGEMENT PROCEDURES AND TECHNOLOGIES FOR INTEGRATED INFORMATION SYSTEM

Modern business environment requires implementation of complex business processes supported by various applications, frequently communicating with the outside world. Application integration mechanisms need to enable integration of heterogeneous information systems maintaining openness with the addition of the new ones intended to support new business functions. Apart from the applications, integrated information systems include operating systems, hardware and network equipment.

In order to maintain security of the integrated information system monitoring and management mechanisms must be implemented. Such mechanisms monitor correctness of operation of applications, operating systems, hardware and network and are capable of initiating predefined corrective actions. Starting point for implementation of such monitoring and management system is always Information Security Management System. This article describes implementation of monitoring and management procedures and technologies for integrated information system.

**Key words:** information system, monitoring and management, security, ISO/IEC 27001

## 1. UVOD

Informatički sustavi u elektroenergetskim tvrtkama inicijalno su se bitno razlikovali od klasičnih informatičkih sustava. Informatički su tradicionalno bili dizajnirani i implementirani na način da zadovoljavaju ograničene zahtjeve na performanse, pouzdanost, sigurnost i fleksibilnost. To znači da je osnovni cilj bio je zadovoljavanje stabilnog rada elektroenergetskog sustava, dok se informacijskim i komunikacijskim tehnologijama pridavala manja pažnja. Informatički sustavi su u većini slučajeva bili fizički odvojeni od ostalih računalnih mreža i temeljeni na proizvođački specifičnom sklopovlju, programskoj podršci i komunikacijskim protokolima. Takve tehnologije uključivale su osnovne mehanizme detekcije i ispravljanja pogrešaka, ali nisu imali podršku za sigurnu razmjenu informacija u suvremenim integriranim informatičkim okruženjima temeljenim na širokopropusnim računalnim mrežama. Pažnja se posvećivala pouzdanosti i raspoloživosti u smislu performansi i kvarova elektroenergetskog sustava, dok se potrebe za informatičkom sigurnošću kakvu danas poznajemo nisu uzimale u obzir. Osiguranje informatičkih sustava u energetskim kompanijama podrazumijevalo je onemogućavanje fizičkog pristupa mreži, poslužiteljima i radnim stanicama preko kojim se upravljalo elektroenergetskim sustavom.

Danas se sve više primjenjuju informatička rješenja koja omogućavaju jednostavno povezivanje i komunikaciju između različitih poslovnih subjekata kao i udaljeni pristup korisnika. Sustavi su dizajnirani i implementirani korištenjem standardnih računalnih komponenti, operacijskih sustava i mrežnih protokola. Osim sustava namijenih nadzoru i upravljanju tehničkim sustavom (npr. SCADA sustavi) uvodi se i niz novih aplikacija namijenjenih radu na otvorenom tržištu električne energije. U njihovoj implementaciji primjenjuju se otvorene tehnologije, omogućava se pristup vanjskim korisnicima te se dijelovi sustava eksponiraju prema internetu. Kao potpora poslovanju i poslovnom odlučivanju uvode se sustavi kao što su ERP (eng. *Enterprise Resource Planning*) i skladišta podataka (eng. *Data Warehouse*). Takvi sustavi pohranjuju podatke koji za kompaniju imaju veliku vrijednost i njihova kompromitacija može tvrtkama nanijeti veliku štetu.

Kako bi se realizirao siguran integrirani informacijski sustav koji će korisnicima omogućiti kontinuirani i pouzdan rad uz minimalnu mogućnost kompromitiranja podataka potrebno je informatički sustav sagledati kao cjelinu. Implementaciji mehanizama nadzora i upravljanja potrebno je pristupiti sustavno te nije dovoljno samo ostvariti sigurnost na razini pojedinih komponenti sustava (poslužitelji, radne stanice). Sustav je potrebno tretirati kao jedinstvenu cjelinu te primijeniti posebne mehanizme kojima se ostvaruju napredne mogućnosti nadzora i upravljanja. Sama instalacija i konfiguracija tehnologija kojima će se u konačnici štititi sustav (npr. vatrozidovi, antivirusi i sl.) samo je jedan od koraka u ostvarivanju sveobuhvatne raspoloživosti i efikasnosti sustava. Implementaciju pouzdanog i sigurnog sustava potrebno je realizirati kao kontinuirani proces uz stalno usavršavanje.

Ostatak rada organiziran je na sljedeći način. U drugom poglavlju ukratko je opisano što se podrazumijeva pod integriranim informacijskim sustavom te koje su osnovne prijetnje njegovom radu. Treće poglavlje opisuje sistematičan pristup uvođenju sustava za upravljanje informacijskom sigurnošću temeljen na standardu ISO/IEC 27001. Četvrto i peto poglavlje opisuju konkretne tehnike i tehnologije koje se primjenjuju u nadzoru i upravljanju integriranim informacijskim sustavom.

## 2. INTEGRIRANI INFORMACIJSKI SUSTAV

Integrirani informacijski sustav omogućuje unos, obradu i korištenje informacija u potpori odvijanju većine poslovnih procesa tvrtke. Obradu informacija obavljaju aplikacije. Složeniji poslovni procesi zahtijevaju rad više međusobno povezanih aplikacija što se najčešće realizira programskom podrškom srednjeg sloja (eng. *middleware*). Sve vrste aplikacija, uključujući i programsku podršku srednjeg sloja i baze podataka, za svoje izvršavanje zahtijevaju platformu. Platformom se smatra komplet sastavljan od računala i pripadajućeg operacijskog sustava, uz eventualni dodatak okruženja kao što su Java ili .NET radno okruženje (eng. *framework*). Povezivanje računala radi omogućavanja protoka podataka obavlja se putem računalne mreže temeljene ne TCP/IP skupu protokola, a potporu sklopovskim sustavima pružaju mehanizmi kao što su: osiguranje neprekidnog napajanja, klimatizacija, sustav za gašenje požara itd.

### 2.1. Radne stanice

Kontakt korisnika sa informacijskim sustavom odvija se uglavnom putem radnih stanica. To su računala prvenstveno usmjerena unosu i prikazu informacija. Radna stanica omogućava čitanje i pisanje

različitih podatkovnih medija te time predstavlja sigurnosni rizik koji se mora odgovarajuće tretirati. Korisnici informacijskog sustava radnu stanicu koriste i za službenu i neslužbenu komunikaciju. Takvom uporabom radna stanica je postala usputna stanica informacija u razmjeni informacija iz i prema vanjskom svijetu što povećava njezinu sigurnosnu izloženost.

### 2.2. Poslužitelji

Poslužitelji pružaju platformu aplikacijama s ciljem realizacije informacijskih usluga na kojima se temelje poslovni procesi. Zbog takvog položaja unutar integriranog informacijskog sustava, poslužitelji su istodobno i visokovrijedni i dobro zaštićeni resursi. U okvirima redovnog korištenja, pristup poslužitelju dozvoljen je isključivo u kontekstu usluge koju pruža, čime se smanjuje njegova izloženost.

Poslužitelji se prema uslugama koje pružaju mogu podijeliti na aplikacijske i općenite. Aplikacijski poslužitelji pružaju platformu aplikacijama namijenjenima automatizaciji specifičnih poslovnih procesa tvrtke. Ovakvi poslužitelji pružaju usluge specifične za određenu tvrtku i njeno područje djelovanja (npr. poslužitelji SCADA sustava). Općeniti poslužitelji pružaju platformu za standardni komplet usluga koji se od tvrtke do tvrtke ne razlikuje puno. U takve općenite usluge spadaju npr. elektronska pošta, pohrana i upravljanje dokumentima.

### 2.3. Računalna mreža

Međusobnu komunikaciju računala omogućuje računalna mreža. Računalnu mreži čini aktivna mrežna oprema (preklopnici, usmjerivači) i pasivni komunikacijski kanali. Treba imati na umu da su uređaji koje nazivamo aktivnom mrežnom opremom u biti specijalizirana računala, da se sastoje od sklopovlja i programa i da, u većoj ili manjoj mjeri, pate od ranjivosti svojstvenih računalu kao takvom.

U današnjem svijetu postoji malo tvrtki koje si mogu dozvoliti posvemašnju odsječenost od okoline po pitanju automatske razmjene informacija. Zbog toga je svaka računalna mreža izravno ili neizravno povezana sa vanjskim svijetom. Takvo stanje nalaže ozbiljnost i metodičnost u pristupu razmatranju sigurnosti računalne mreže.

### 2.4. Prijetnje radu integriranog informacijskog sustava

Informacije se smatraju sigurnima kada posjeduju najmanje slijedeća svojstva: dostupnost, integritet i povjerljivost. Gubitak jednog ili više navedenih svojstava narušava sigurnost informacije te time ugrožava odvijanje pripadajućeg poslovnog procesa. Takva narušavanja uzrokovana su različitim spontanim ili namjernim pojavama unutar informacijskog sustava ili izvan njega. Mehanizmi informacijske sigurnosti suprotstavljaju se takvim prijetnjama. Imajući u vidu konačnost resursa izdvojenih za tu namjenu, nemoguće je postići savršenu sigurnost informacija. Upravljanje informacijskom sigurnošću je postupak kojim se na osnovu procjene rizika određuju kombinacije mjera zaštite informacija kako bi se očekivani gubitak sveo na najmanju moguću mjeru.

Prijetnje mogu nastati spontano (kvarovi, nesavršenosti sustava, nepažnja i sl.) ili namjerno kao posljedica zlonamjerne aktivnosti. Prijetnja koja se uspije materijalizirati uzrokuje privremeni ili trajni gubitak informacije te s tim vezane izravne i neizravne troškove. Funkcioniranje tvrtke u pravilu može podnijeti privremenu nedostupnost nekog dijela informacija bez katastrofalnih posljedica. U skladu s time modeliraju se očekivana vremena do oporavka nakon nastanka pojedine štete, a isto tako i mjera za količinu informacija koja može biti nadomještena u slučaju trajnog gubitka.

#### 2.4.1. Kvarovi

Kvarovi sklopovlja posljedica su mehaničkog trošenja, nesavršenosti materijala ili više sile. Tretiraju se statistički uglavnom kroz očekivani interval vremena prije ili između kvarova, eng. MTBF (eng. *Mean Time Before Failure*).

U proizvodnji programske podrške prihvaćeno je pravilo da u svakom programu ima pogrešaka. Povećanjem napora prema korektnosti procesa proizvodnje programske podrške kao i napora u traženju i ispravljanju pogrešaka, njihov broj može se smanjiti. Suvremena ekonomska realnost uz stalno povećanje kompleksnosti informatičkih rješenja dovodi do praktične nemogućnosti garantiranja potpune ispravnosti programskih sustava.

### 2.4.2. Ljudski faktor

Kao sudionici u procesima baratanja sa informacijama, ljudi unose određenu količinu nesigurnosti. Ovisno o pažnji koja je posvećena procesu rada prilikom implementacije i prilikom izvršavanja, događaju se pogreške, od neispravno upisanih brojeva do masovnih sustavnih pogrešaka kao što je odlaganje magnetskih medija sa podacima u blizinu jakih magnetskih polja.

Posebna kategorija prijetnji su zlonamjerne aktivnosti, bilo da potječu iz same tvrtke ili izvana. Takve aktivnosti imaju obilježja kriminalnog djela kao što su: motiv, sredstvo, prilika i sl.

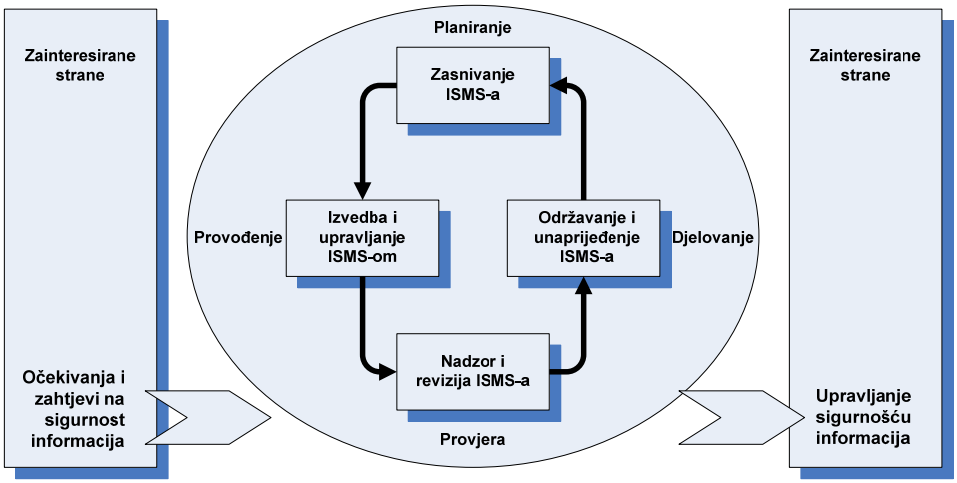
## 3. SUSTAV UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU

Sustavnim pristupom bitno se smanjuje vjerojatnost ispuštanja ili krive obrade nekog elementa sustava koji se želi zaštititi. Sveobuhvatni pristup postignut je implementacijom i primjenom sustava upravljanja na sustave informacijske sigurnosti. To je dovelo do razvoja standardiziranih *sustava za upravljanje informacijskom sigurnošću* (eng. *Information System Management System* - ISMS). Skup normi koji adresira različite aspekte informacijske sigurnosti nosi oznaku ISO/IEC 27000 i prikazan je u tablici I.

Tablica I. Pregled normi iz obitelji ISO/IEC 27000

| Norma | Područje pokrivanja / namjena | Objavljeno |
|---|---|---|
| ISO/IEC 27000:2009 | Pregled, uvod i rječnik | 2009. |
| ISO/IEC 27001:2005 | Zahtjevi sustava upravljanja informacijske sigurnosti | 2005. |
| ISO/IEC 27002:2005 | Kodeks prakse za upravljanje sigurnošću | 2005. |
| ISO/IEC 27003 | Smjernice za primjenu | u pripremi |
| ISO/IEC 27004:2009 | Mjerenja u sustavu upravljanja sigurnošću (sigurnosna metrika) | 2009. |
| ISO/IEC 27005:2008 | Upravljanje rizikom | 2008. |
| ISO/IEC 27006:2007 | Proces certifikacije i akreditacije za certifikacijska tijela | 2007. |
| ISO/IEC 27007 | Smjernice za audit ISMS-a | u pripremi |
| ISO/IEC 27008 | Smjernice za audit kontrola informacijske sigurnosti | u pripremi |
| ISO/IEC 27010 | Smjernice za ISMS u međusektorskoj komunikaciji | u pripremi |
| ISO/IEC 27011:2008 | Smjernice za ISMS u telekomunikacijskim organizacijama | 2008. |
| ISO/IEC 27013 | Smjernice za integriranu primjenu ITIL-a i ISMS-a | u pripremi |
| ISO/IEC 27014 | Upravljanje informacijskom sigurnošću | u pripremi |
| ISO/IEC 27015 | Smjernice za ISMS u financijskim organizacijama | u pripremi |
| ISO/IEC 27031 | Kontinuitet poslovanja usmjereno na ICT | u pripremi |
| ISO/IEC 27032 | Smjernice za cybersecurity | u pripremi |
| ISO/IEC 27033 | Zamjena za IT mrežnu sigurnost u ISO/IEC 18028 | u pripremi |
| ISO/IEC 27034 | Smjernice za aplikacijsku sigurnost | u pripremi |
| ISO/IEC 27035 | Zamjena za upravljanje sigurnosnim incidentima u ISO TR 18044 | u pripremi |
| ISO/IEC 27036 | Smjernice za sigurnost outsorcinga | u pripremi |
| ISO/IEC 27037 | Smjernice za digitalne zapise | u pripremi |
| ISO 27799:2008 | Smjernice za primjenu ISMS u zdravstvu | 2008. |

Najpoznatiji i najopćenitiji sustav za upravljanje informacijskom sigurnošću definiran je međunarodnom normom ISO/IEC 27001:2005 koja opisuje model za zasnivanje, uspostavu, vođenje, nadgledanje, reviziju, održavanje i usavršavanje ISMS sustava. Norma ISO/IEC 27001 je dovoljno općenita da se može primijeniti na bilo koju vrstu organizacije. Upravljanje informacijskom sigurnošću u skladu s ovom normom je ciklički proces koji kontinuirano prolazi kroz sve faze modela Planiraj-Provedi-Provjeri-Djeluj (eng. *Plan-Do-Check-Act* - PDCA) ilustriranog na slici 1.




Slika 1. Model Planiraj-Provedi-Provjeri-Djeluj primijenjen na ISMS

U glavnom dijelu ove norme definirani su obvezni zahtjevi koji moraju biti ispunjeni da bi se mogla deklarirati usklađenost s istom. Tu su definirani opći zahtjevi kao što su uspostavljanje ISMS-a, uvođenje i primjena ISMS-a, nadzor i provjera ISMS-a, održavanje i poboljšavanje ISMS-a, opći zahtjevi koji se odnose na dokumentaciju, opredijeljenost rukovodstva, osiguranje resursa, osposobljavanje, interni ISMS auditi, pregled ISMS-a od strane rukovodstva, te poboljšavanje ISMS-a. U sklopu norme definirano je 133 ciljeva kontrola kao i samih i kontrola grupiranih u 11 područja. Pod kontrolom se podrazumijeva način kojim se adresira određeni sigurnosni rizik.

Tablica II. Pregled grupa ciljeva kontrola i kontrola iz norme ISO/IEC 27001

| Grupa | Naziv grupe | Broj kontrola |
|---|---|---|
| A.5 | Politika sigurnosti | 2 |
| A.6 | Organizacija informacijske sigurnosti | 11 |
| A.7 | Upravljanje imovinom | 5 |
| A.8 | Sigurnost ljudskih resursa | 9 |
| A.9 | Fizička sigurnost i sigurnost povezana s okolišem | 13 |
| A.10 | Upravljanje komunikacijama i radom | 32 |
| A.11 | Kontrola pristupa | 25 |
| A.12 | Nabava, razvoj i održavanje informacijskih sustava | 16 |
| A.13 | Upravljanje sigurnosnim incidentima | 5 |
| A.14 | Upravljanje kontinuitetom poslovanja | 5 |
| A.15 | Usklađenost | 10 |

Norma ISO/IEC 27001:2005 dozvoljava da budu uvedene i kontrole kojih nema izričitom navedenih u normi. Primjer takve dodatne kontrole je definiranje pravila za unošenje opreme u štićene prostore, npr. zabrana unošenja mobitela u štićeni prostor.

Neke od kontrola moguće je realizirati adekvatnom primjenom informatičkih tehnologija. Primjeri parcijalnog korištenja tehnologije u implementaciji ISMS-a su automatsko kreiranje zapisa događaja u sustavu (tzv. logovi), kontrola ulaska u štićene prostorije korištenjem identifikacijskih kartica, zaštita segmenata računalnih mreža vatrozidovima, sustavi detekcije upada u sustav (eng. *Intrusion Detection System* - IDS), zaštita od zlonamjernog koda (antivirusne tehnologije) itd.

Valja voditi računa o tome da uvođenje svake dodatne kontrole može u sustav uvesti nove informacije koje treba štititi, nove prijetnje kojima su informacije izložene, nove razine mogućih šteta, te nove ranjivosti sustava.

U nastavku je opisano na koji način i primjenom kojih kontrola se mogu zaštititi informacije na razini pojedinih elemenata sustava i sustava kao cjeline.

# 4. NADZOR I UPRAVLJANJE ELEMENTIMA INFORMACIJSKOG SUSTAVA

## 4.1. Radna stanica

Konfiguracija radne stanice mora dozvoliti dovoljnu fleksibilnost sa ugodan rad korisnika informacijskog sustava. Istodobno, radna stanica, kao moguća međustanica na putu informacija predstavlja jednu od prvih linija obrane protiv prijetnji koje dolaze kako izvana tako iz same tvrtke.

Osnovni uvjet za sigurnost same radne stanice je ograničenje administrativnog pristupa. Uredan rad sustava kao što su antivirusni klijent, lokalni vatrozid, lokalno otkrivanje upada kritično ovisi o zaštiti koju pruža operacijski sustav. Na računalima na kojima administrativni pristup imaju osobe koje za to nisu ovlaštene sigurnosna kompromitacija samo je pitanje vremena. Kompromitacija radne stanice lančano donosi kompromitaciju korisničkih akreditacija korisnika koji se će se takvom radnom stanicom služiti Zaštitni sustav radne stanice uobičajeno se sastoji od: središnje upravljanih sustava antivirusa, lokalnog vatrozida, lokalnog sustava za otkrivanje upada, sustava za sakupljanje dnevničkih zapisa.

U cilju zaštite od kvara sklopovlja, u radnu stanicu se ugrađuju udvojene kritične komponente kao što su tvrdi diskovi i mrežna sučelja. U uvjetima dobro organiziranog informacijskog sustava, kvar pojedinačne radne stanice, osim privremeno, ne dovodi do bitnog gubitka podataka budući da se sve informacije kritične za poslovanje nalaze na poslužiteljima.

## 4.2. Poslužitelj

S obzirom na ulogu u obradi informacija, poslužiteljsko računalo je visoko vrijedan resurs. Budući da se na njemu odvijaju samo točno specificirane aktivnosti, lakše ga je zaštititi restriktivnim pristupom sigurnosti.Za poslužitelje je prva linija obrane tzv. očvršćivanje (eng. *hardening*). Ovim se postupkom poslužiteljskoj platformi suzuje dostupnost kako bi se umanjila površina izloženosti ugrozama. Taj se postupak provodi za svaku razinu platforme posebno.

Drugi bitni sustav zaštite poslužitelja je sustav otkrivanja upada. Taj sustav, osim praćenja anomalija u ponašanju računala prema metrikama kao što su oblik mrežnog prometa, uzorak promijene opterećenja procesora i potrošnje radne memorije, prati i integritet binarnih datoteka programa i operacijskog sustava koji se izvršavaju na poslužitelju.

Sustav sakupljanja dnevničkih zapisa primijenjen na poslužitelju, osim dnevnika operacijskog sustava, nadzire i dnevnike aplikacija koje se izvršavaju na poslužitelju. Na taj način središnji nadzorni sustav može pratiti urednost izvršavanja aplikacija u potpori poslovnim procesima tvrtke.

Antivirusni sustav također je poželjni čimbenik sigurnosti poslužitelja. Međutim, treba imati na umu da u pojedinim slučajevima antivirusni sustav može ometati rad specifičnih aplikacija koje se izvršavaju na poslužitelju.

Zaštita od kvara sklopovlja kod poslužitelja se provodi sustavnim udvajanjem kritičnih komponenti. Tako su uobičajeno udvojeni sklopovi za napajanje, tvrdi diskovi su zaštićeni paritetom, udvojena su mrežna sučelja, ponekad se udvajaju i banke radne memorije. Dodatna zaštita platforme koju pruža poslužitelj sastoji se od udvajanja čitavih poslužitelja u grupe (eng. *cluster*).

## 4.3. Računalna mreža

Tehnologija računalne mreže napredovala je od pojedinačnih fizičkih segmenata spojenih čvorovima do današnjih kompleksnih mrežnih uređaja koji u sebi sadrže proizvoljan broj virtualnih segmenata, preklopnika, usmjerivača i ostalih mrežnih čvorova. Time je omogućena velika fleksibilnost konfiguracije, mogućnost udvajanja fizičkih uređaja kao i ostvarivanje naprednih sigurnosnih usluga. U suvremenim mrežama, računala su sa mrežnim uređajima spojenu u topologiju točka – točka, dok su mrežni uređaji međusobno spojeni višestrukim prespojima.

Na najnižoj razini, mrežni uređaju su visoko specijalizirana računala koja pate od karakterističnih problema sa sklopovljem i programskom podrškom kao i računala opće namjene, uz razliku da je kontrola kvalitete i za sklopovlje i za programe mrežnih uređaja bitno stroža nego za klasična računala.

Prilikom planiranja mrežne infrastrukture obavlja se segmentiranje u skladu sa mrežnim protokolom koji će se koristiti. Na taj se način omogućuje optimizacija upravljanja prometom. Spomenuti segmenti su virtualni a računala koja pripadaju različitim segmentima spojena su na isti fizički uređaj. Segmenti koji povezuju visoko kritične sustave obavezno se odvajaju od segmenata sa manje kritičnim

sustavima putem posebnih segmenata tzv. demilitariziranih zona - DMZ. Kod takvih je segmenata pravilo da komunikacija uvijek kreće iz segmenta više razine sigurnosti prema razinama niže sigurnosti (npr. iz segmenta gdje se nalazi SCADA sustav prema poslovnom segmentu). Moguće je od najsigurnijeg segmenta do spoja sa vanjskim svijetom imati više ulančanih kompleta DMZ-a.

## 5. NADZOR I UPRAVLJANJE CJELOVITIM INFORMACIJSKIM SUSTAVOM

Da bi se ostvarilo učinkovito upravljanje sigurnosnim mehanizmima u informacijskom sustavu funkcije upravljanja je potrebno generalizirati i centralizirati. To je potrebno kako bi se postigla dosljednost i smanjio prostor za pogreške. U tu svrhu se primjenjuje skupina sustava namijenjenih potpori upravljanju informacijskim sustavom (eng. *information system management*). Iako većina njih nije prvenstveno sigurnosno usmjerena, njihova ispravna uporaba bitno doprinosi postizanju i održavanju visoke razine sigurnosti informacijskog sustava. Ustroj upravljačkih sustava koje se najčešće primjenjuju ilustrirane su na slici 2.

### 5.1. Upravljanje ovlastima korisnika

Sigurnost u radu sustava ovisi njegovim interakcijama sa okolinom u kojoj se nalazi. U ovom kontekstu okolinom se smatraju unutarnji i vanjski korisnici te administratori informacijskog sustava.

Opseg interakcije određen je ovlaštenjima subjekata koji u njoj sudjeluju. Svako dodijeljeno ovlaštenje pojedinačno određuje slijedeće:

- Tko smije pokrenuti - subjekt
- Koju akciju - aktivnost
- Nad kojim dijelom sustava ili skupa informacija - objekt

Već u slučaju malog sustava i malog broja korisnika broj ovakvih ovlaštenja postaje prevelik za pojedinačno uređivanje te se zbog toga koriste različite sheme za pojednostavnjivanje i poopćavanje.

Ovlaštenja se uobičajeno definiraju putem sustava uloga (eng. *Roles Based Access Control* - RBAC). Sustav uloga definira skup uloga koje su uobičajeno vezane za dužnosti koje subjekti obnašaju u okviru svoga djelovanja u tvrtci. Za pojedinu ulogu definiran je skup nužnih ovlaštenja. Na taj se način ovlaštenje ne veže za pojedinu osobu nego za ulogu koja se zatim pridijeli jednoj ili više osoba. Promjena zaduženja kroz promjenu uloge automatski dovodi do primjene ovlaštenja. Na takav način nema opasnosti da bilo tko internom promjenom radnog mjesta zadrži ovlaštenja koja mu više ne pripadaju. Ovakav način rada sa ovlaštenjima olakšava provođenje u djelo principa po kojemu svatko tko stupa u interakciju sa informacijskim sustavom to mora činiti u okviru pripadajućeg jedinstvenog identiteta.

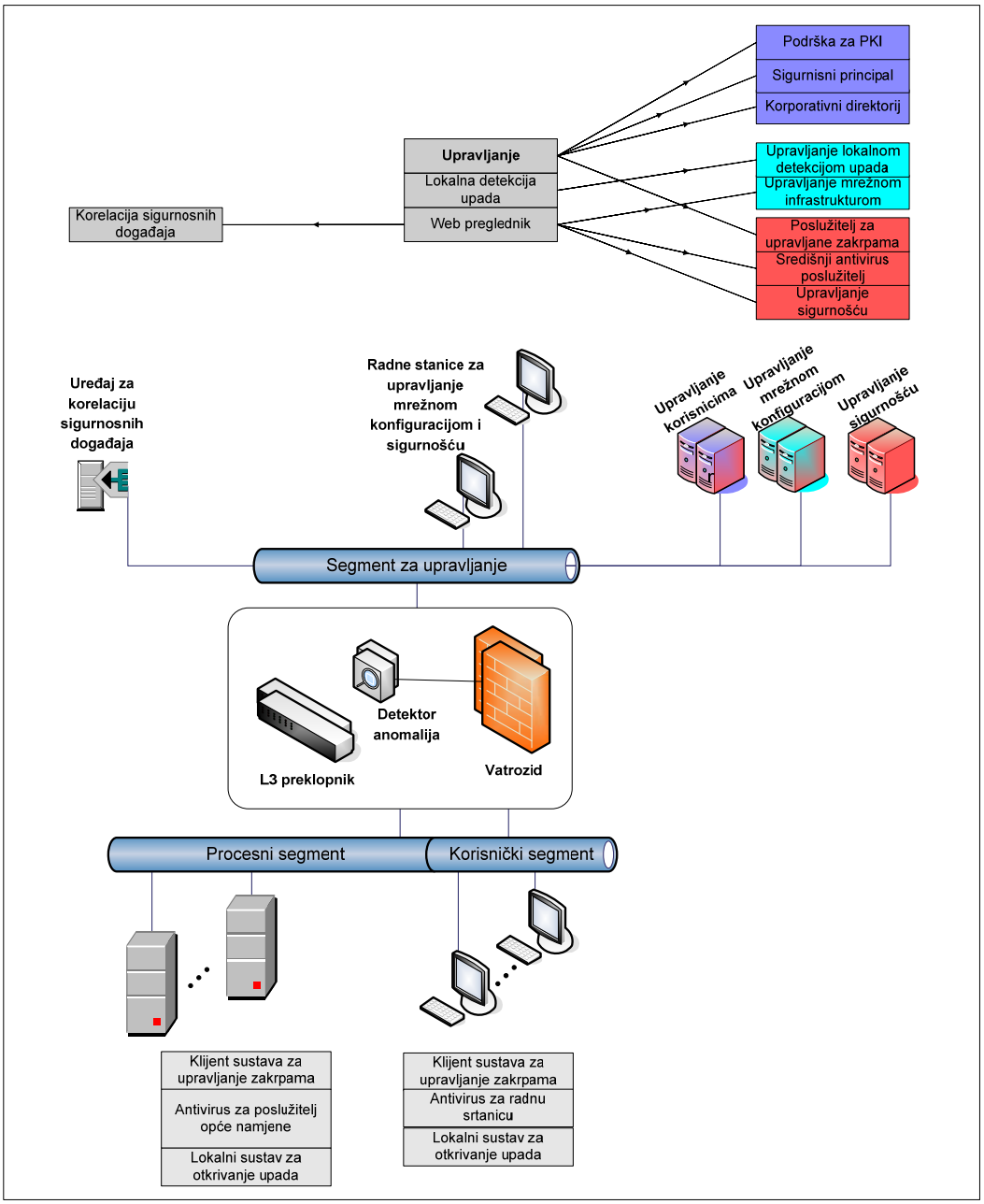
Kako bi se ovlaštenje moglo uporabiti potrebno je nedvojbeno povezati subjekt i identitet za koji subjekt tvrdi da je njegov. Taj se postupak naziva autentikacija i provodi se različitim metodama. Općeniti kriterij uspješnog postupka autentikacije vezan je za tri obilježja ili faktora:

1) Nešto što subjekt posjeduje,
2) Nešto što subjekt zna i
3) Nešto što subjekt jest

U prvu kategoriju spadaju predmeti kao što su magnetne kartice, ključevi, tokeni itd. U drugu kategoriju spadaju informacije kao što su zaporke i PIN-ovi. U treću kategoriju spadaju obilježja subjekta na koja on ne može utjecati kao što su otisak prsta, geometrija ruke, uzorak šara na šarenici itd. Autentikacija se najčešće obavlja uz pomoć dva od tri ili sva tri obilježja. Primjeri za autentikaciju putem dva faktora su token i PIN, magnetska kartica i otisak prsta itd.

U postupku autentikacije i nakon pristupa sustavu postoji potreba za povjerljivom i ovjerenom komunikacijom između subjekata. Za to se uobičajeno koristi infrastruktura javne kriptografije (eng. *Public Key Infrastructure* – PKI). Javna kriptografija se zasniva na matematičkim funkcijama koje su teško reverzibilne. Na taj način moguće je korištenje parova javnih i tajnih ključeva tako da javni ključ služi za kriptiranje i provjeru potpisa, a tajni za dekriptiranje i potpisivanje.

Opisanim ovlastima korisnika na razini cjelokupnog sustava najčešće su upravlja putem sustava središnjeg imenika kao što je Active Directory.




Slika 3. Ustroj upravljačkog dijela informacijskog sustava

## 5.2. Nadzor stanja sustava

U cilju očuvanja sigurnosti integriranog informacijskog sustava potrebno je o stanju njegovih elementima voditi sustavnu brigu. I za relativno male sustave, takav pothvat nije praktičan bez uporabe automatiziranih alata. Takvi alati najčešće se nazivaju sustavima za upravljanje mrežom iako u današnje vrijeme odrađuju i mnoge druge zadaće.

Programi za upravljanje i nadzor u najvećoj mjeri utemeljeni su na protokolu SNMP (eng. *Simple Network Management Protocol*). Unutar protokola definirana je hijerarhijska struktura podataka kroz koju uređaji izlažu informacije o svom radi i dozvoljavaju upravljanje. Ta se struktura naziva *Management Information Base* - MIB. Upravljački poslužitelj stupa u kontakt sa programskim agentima koji se nalaze na upravljanim objektima te čitanjem ili pisanjem u vrijednosti MIB agenta obavlja željene akcije. Primjena nije ograničena na mrežne uređaje već se može primjenjivati i na razini računala pa čak i programskog modula.

Jedno od važnih obilježja dobro ustrojenog informatičkog sustava je mogućnost automatskog otkrivanja objekata (eng. *discovery*) putem SNMP protokola. Prilikom otkrivanja uređaji daju osnovne informacije o računalima koja su na njih spojena. Daljnjim ispitivanjem računala sustav za upravljanje popunjava sliku informacijskog sustava. Slika stanja informacijskog sustava dobivena automatskim otkrivanjem mora odgovarati planiranom stanju. Svaka nepravilnost može značiti postojanje sigurnosno oslabljenog mjesta.

Osim aktivnog očitavanja i zapisivanja, postoji asinkroni način korištenja SNMP protokola. Tim načinom SNMP agenti, prema unaprijed definiranim kriterijima, izvještavaju nadzorni sustav o interesantnim događajima. Na taj način slika o stanju sustava dobiva na kvaliteti vremenske dimenzije uz istovremeno smanjivanje upravljačkog prometa na mreži. Prilikom korištenja asinkronog izvještavanja ne preporuča se odustajanje od povremenog očitavanja stanja mrežnih uređaja.

Vrhunac vrijednosti upravljačkog sustava je mogućnost upravljanja pojedinim elementima sustava. Takvo se upravljanje koristi kao prethodno definirani odgovor na određeni događaj ili kao pomoć administratoru u provođenju propisanih aktivnosti. Jedan primjer takvog upravljanja je održavanje operacijskih sustava na radnim stanicama koje su izvan radnog vremena ugašene. U takvom slučaju upravljački sustav će pokrenuti paljenje računala, odraditi akciju održavanja i nakon toga pokrenuti gašenje računala.

Stalnim nadzorom radnih parametara objekata informacijskog sustava na mnoge se poremećaje u nastajanju može djelovati preventivno. Nadalje, u slučaju postojanja ugovorne obaveze prema vanjskim subjektima, nadzor kvalitete izdane odnosno primljene usluge dobiva na važnosti.

Komercijalna rješenja za upravljanje informacijskim sustavom su npr. MS SystemCenter, Nagios i HP Openview. Sigurnosnu komponentu donose proizvodi kao što je Cisco Security Agent, a korelaciju sigurnosno relevantnih događaja obavlja i Cisco Security MARS.

### 5.3. Upravljanje programskom podrškom

Slijedom činjenice da se obrada informacija unutar integriranog informacijskog sustava odvija uz pomoć računalnih programa, upravljanje programskom podrškom je od iznimne važnosti za ostvarivanje sigurnosti informacijskog sustava.

Upravljanje programskom podrškom nastoji osigurati poštivanje slijedećih pravila:

a) Na računalima se nalaze potrebni programi.
b) Na računalima se nalaze samo dozvoljeni programi.
c) Revizije programa koji se nalaze na računalima su suvremene.

Odstupanje od bilo kojeg od tih pravila negativno utječe na sigurnost cjelokupnog informacijskog sustava. Automatsko upravljanje programskom podrškom ima smisla za računala koja su po svojoj namjeni mnogobrojna i relativno slična. U tu grupu spadaju prvenstveno radne stanice.

Potreba suvremenosti revizija programa koji se nalaze u uporabi potječe iz činjenice da se niti za jedan programski sustav ne može tvrditi da je proizveden u potpunosti bez pogrešaka. U takvoj situaciji proizvođači programa kontinuirano rade na njihovom poboljšavanju te izdaju nove revizije.

Aplikacije za upravljanje programskom podrškom posjeduju skladište programske podrške pogodne za instalaciju na korisnička računala. U njihovim bazama podataka nalaze se informacije o tome koji programi moraju biti postavljeni na koja računala i koje su njihove revizije trenutno instalirane. Istim putem omogućeno je mijenjanje dostupnosti pojedinih usluga operacijskog sustava korisničkog računala(eng. *policy*), u skladu sa sigurnosnom procjenom. To se npr. odnosi na zabranu korištenja USB prijenosnih memorija za pohranu podataka.

Samostalno i u suradnji sa nadzornim sustavom, aplikacija za upravljanje programskom podrškom obavlja instalacije, deinstalacije i rekonfiguracije korisničkih računala.

Navedena funkcionalnost uključena je u suvremene programske sustave kao što je npr. Microsoft System Center Configuration Manager

### 5.4. Obrana od virusa

Poseban slučaj upravljanja programskom podrškom je obrana od virusa. Ovdje je naglasak stavljen da uklanjanje zlonamjernih i ostalih nedopuštenih programa sa računala. To se obavlja uspoređujući sadržaje pojedinih datoteka sa poznatim uzorcima kao i promatranjem programa prilikom izvršavanja te zabranjivanjem potencijalno opasnih akcija. Zbog brzine širenja virusa, ovakvi sustavi u

tvrtkama sastoje se od središnjeg poslužitelja koji kontinuirano preuzima najnovije virusne definicije i distribuira ih prema antivirusnim klijentima koji se nalaze na štićenim računalima.

Osim primarne namjene današnji antivirusni sustavi sposobni su provoditi i akcije kao što je uklanjanje ilegalnih programa te muzičkih i video zapisa u čemu se donekle preklapaju sa sustavima za upravljanje programskom podrškom.

Antivirusni sustavi koriste se pretežito na korisničkim računalima i poslužiteljima opće namjene. U slučaju aplikacijskih poslužitelja specifične namjene, vrlo malena vjerojatnost zaraze virusom u odnosu na dodatni rizik interferencije antivirusnog sustava sa produkcijskim često ne opravdava korištenje antivirusnog sustava.

### 5.5. Bilježenje sigurnosnih događaja

Tokom rada integriranog informacijskog sustava, upravljačke aplikacije primaju i obrađuju informacije o različitim događajima koji upućuju na uredno ili poremećeno funkcioniranje pojedinih podsustava kao i sustava u cjelini. Pojedine aplikacije koje obrađuju sigurnosno osjetljive informacije za neke od kritičnih operacija prijavljuju identitet njihovog pokretača. U slučaju problema sigurnosne prirode, od velike je važnosti čuvanje zapisa o događajima kako bi se omogućila naknadna analiza te uklonili sigurnosni propusti.

Zapisi o sigurnosnim događajima moraju se sakupljati i čuvati na takav način da, jednom kada su zabilježeni zabilješku više nije moguće promijeniti. Tehnologija za čuvanje zapisa zasniva se na računalima koja su odvojena od ostalih kako bi se spriječilo njihovo sigurnosno kompromitiranje. Također, zaposlenici koji upravljaju takvim sustavima ne smiju biti dijelom ustroja odjela informatike kako bi se izbjeglo udruživanje i neobjektivnost.

## 6. ZAKLJUČAK

Kako bi se omogućio protok informacija nužan za rad u suvremenom poslovnom okruženju različiti informatički sustavi međusobno se integriraju u jedinstvenu cjelinu. Integriraju se pojedinačni informatički sustavi unutar kompanija, ali se ostvaruju i veze s informatičkim sustavima poslovnih partnera. Često su dijelovi sustava izloženi i prema internetu. Za povezivanje informatičkih sustava i razmjenu informacija sve se više primjenjuju standardne i otvorene tehnologije. Povezivanje s poslovnim partnerima, izloženost globalnoj mreži internetu i primjena općepoznatih i standardnih tehnologija rezultira činjenicom da informatički sustavi u elektroenergetskim kompanijama postaju ranjivi na prijetnje kao i svi ostali informatički sustavi bez obzira u kojem se poslovnom području primjenjuju. Zbog kritičnosti infrastrukture s kojom su povezani informacijski sustavi u energetskim kompanijama moraju biti iznimno dobro nadzirani i upravljani. Kako bi se ostvario najviši stupanj sigurnost informacijskog sustava potrebno je implementaciji mehanizama nadzora i upravljanja pristupiti sustavno. Sustavan pristup osigurava se primjenom standarda kao što je ISO 27001:2005. U ovom radu opisan je način na koji je moguće ostvariti sveobuhvatni sustav za upravljanje informacijskom sigurnošću te je dan pregled mehanizama koji se primjenjuju za nadzor i upravljanje kako pojedinim komponentama tako i integriranim informacijskim sustavom kao cjelinom. Takvim sustavnim pristupom i primjenom odgovarajućeg skupa tehnika i tehnologija moguće je ostvariti zadovoljavajuću razinu raspoloživosti informacijskog sustava uz optimizaciju utrošenih sredstava.

## LITERATURA


[1] ISO/IEC 27001:2005, "Information technology – Security techniques – Information security management systems – Requirements", Switzerland, 2005.

[2] A. Martinić, A. Černicki-Mijić, I. Šturlić, "Sigurnost u sustavima procesne informatike", 8. savjetovanje HRO CIGRÉ, Cavtat, RH, studeni 2007.

[3] A. Martinić, M. Šmalcelj, I. Šturlić, "Implementacija sustava za upravljanje informacijskom sigurnošću u sustavima procesne informatike prema standardu ISO 27001", 8. simpozij o sustavu vođenja EES-a (CIGRÉ), Cavtat, RH, studeni 2008.

[4] http://www.iso.org/iso/iso_catalogue/management_standards.htm

[5] http://www.iso27001security.com/
[6] http://www.isaca.org/
[7] CISSP Common Body of Knowledge, http://www.isc2.org/