Informacijska sigurnost u energetskim sustavima

Predrag Pale
Laboratorij za sustave i signale
Zavod za elektroničke sustave i obradbu informacija
Fakultet elektrotehnike i računarstva
Sveučilište u Zagrebu
Unska 3, Zagreb
Telefon: +385 1 6129-911 Fax: +385 1 6129 652 E-mail: Predrag.Pale@FER.hr

Informacijska sigurnost je posebno važna u elektroenergetskim sustavima kao dijelu kritične nacionalne infrastrukture. Stoga je poznavanje tog područja, a prije svega prijetnji, ranjivosti i tehnika napada od posebnog značaja za profesionalce u ovom području. Procesni sustavi i njihovi SCADA podsustavi imaju svoje posebnosti o kojima treba voditi računa. To su relativno neiskustvo osoblja u području informacijske sigurnosti, spore promjene i osvježavanje operacijskih sustava i aplikacija, nedovoljno zaštićeni udaljeni pristup, umreženost s drugim poslovnim sustavima, nepostojanje sustava zaštite, javnost informacija i neodgovarajuća tehnička i fizička zaštita objekata i opreme. Smatra se da najveću prijetnju SCADA sustavima čine zlonamjerni programi, namještenici, hakeri i teroristi. Tehnike zaštite se sastoje od prevencije, otkrivanja, rješavanja incidenata i oporavka sustava. Za SCADA sustave prioritet je u prevenciji, stvaranju organizacijskih preduvjeta i vođenja računa o ljudskom faktoru

I. UVOD

Informacijska sigurnost neizostavni je dio projektiranja, izgradnje i održavanja svih informacijskih sustava. Posebnu težinu ima kod sustava koji služe upravljanju procesima u stvarnom vremenu, a od sudbonosnog su značaja za kritičnu nacionalnu infrastrukturu kojoj pripadaju i elektroenergetski sustavi.

U Hrvatskoj ne postoje posebni propisi koji bi se bavili niti kritičnom nacionalnom infrastrukturom, pa tako ni informacijskom sigurnošću elektroenergetskih sustava. Međutim, standardi, dobra praksa, iskustvo i stavovi drugih zemalja i međunarodnih tijela dovoljni su da profesionalci u ovom području imaju jasan pregled i upute za svoj rad.

II. INFORMACIJSKA SIGURNOST

Informacijsku sigurnost čini skup mjera: pravila, postupaka, resursa; koje osiguravaju da su informacije i informacijska infrastruktura u svakom trenutku raspoloživi, cjeloviti i dostupni samo ovlaštenima. Informacijsku infrastrukturu čine računala, mreže, pravila, postupci i ljudi.

Podrazumijeva se da treba štititi primarne informacije, one koje su dio ili se odnose na poslovne ili proizvodne procese, dakle informacije ko je su suštinske za poslovanje organizacije. Međutim i meta informacije treba štititi. To su informacije o informacijama, tj. podaci o vlasništvu podataka, datum nastanka, promjene ili korištenja podataka, prava pristupa i sl. Pored svega toga, osjetljive su i sekundarne informacije kaje nisu u izravnoj vezi sa sadržajem poslovanja. Tipično su to podaci o zaposlenicima, infrastrukturi, resursima, sustavima potpore i sl.

III. ELEMENTI INFORMACIJSKE SIGURNOSTI

Za potpuno razumijevanje područja informacijske sigurnosti potrebno je razumjeti prijetnje, ranjivosti te tehnike napada.

A. Prijetnje

Za razumijevanje prijetnji potrebno je sagledati: napadače, žrtve, svrhe, ciljeve i mete napada.

Ozbiljnu prijetnju informacijama čine profesionalci i lopovi. Oni imaju jasnu eksternu motivaciju za napad na sigurnost, koriste sve poznate spoznaje o mogućnostima ugrožavanja sigurnosti, brišu tragove za sobom i uporni su. Vjerojatno najopasniju skupinu napadača ipak čine teroristi i vandali. Bezobzirni su, u pravilu nastoje nanijeti štetu žrtvi. Ponekad im nedostaje znanja no to nadomještaju strašću, emocijama i predanošću zadatku. U posebnu, gotovo simpatičnu, skupinu svrstavaju se umjetnici i istraživači. Njihova namjera u načelu nije nauditi žrtvi, već otkriti nešto novo ili stvoriti neku zamišljenu kreaciju ili šalu. Šteta u pravilu nastaje kao nehotična posljedica ili nepromišljenost u pripremi ili tijekom njihova djelovanja. Postoji još jedna skupina napadača: posrednici. Oni su zapravo žrtve, jer su napadači iz prethodnih skupina iskoristili ranjivost posrednikovog sustava da preko njega izvode napad.

Žrtve napadača pripadaju u jednu od nekoliko kategorija, prema načinu na koji ih napadač izabire. Poznate žrtve su one čiji je identitet dobro poznat napadaču i koje su namjerno poimenično izabrane. Izvedene žrtve su odabrane zbog nekog svog svojstva i sam identitet napadaču nije važan, pa možda čak niti poznat. Slučajne žrtve nisu izabrane ni zbog svog identiteta, niti zbog nekog svog svojstva već posve slučajno. Žrtve mogu biti i postranične (kolateralne), tj. mogu biti napadnute kao posljedica glavnog napada na žrtvu iz neke druge kategorije ili kao posljedica osvete napadaču.

Tri su moguća razloga tj. svrhe napada. Na prvom je mjestu osobna korist. Uspješnim napadom napadač za sebe ili naručitelja može osigurati izravnu ili posrednu novčanu korist ili korištenje resursa žrtve: računala, komunikacija, alata, podataka. Posebnu kategoriju i u medijima najviše prikazivanu čine motivi za (samo)dokazivanjem i

stjecanjem ugleda u javnosti ili među istomišljenicima. Najčešći protagonisti su iz kategorije neprilagođenih kojima je također i uzbuđenje jak razlog za napade.

Stjecanje novih znanja i istraživanje bio je prvi razlog zbog kojeg su ljudi krenuli u napade na informacijske sustave. Tada je i skovan naziv „hacker“ koji se danas koristi zapravo za kategoriju neprilagođenih i vandala.

Drugu veliku skupinu razloga za napad čini želja da se naudi nekom drugom čak i ako to napadaču ne donosi izravnu osobnu korist. Šteta za žrtvu može biti novčani gubitak, gubitak resursa ili ugleda. Posebno oblikovani napadi mogu biti usmjereni na znanje žrtve. Kada je znanje napadnuto, žrtva donosi krive zaključke i odluke čak i kad su joj svi resursi ispravni i dostupni.

Treću skupinu napada čine oni koji i nisu imali neki osobit razlog. Iako ima argumenata da i ovi napadi onda spadaju u neku od navedenih kategorija, prije svega neprilagođenih i vandala ili istraživanja, ipak zbog vrlo niskog intenziteta motivacije, koju je teško prepoznati i u tijeku napada i kasnije kod forenzičke analize, ovaj razlog zaslužuje posebnu kategoriju.

Dok je svrha napada važna za analizu napada i njegovu prevenciju, cilj napada je ključan za reakciju dok napad traje. Svi se napadi mogu svesti na samo jedan ili kombinaciju tri temeljna cilja: pribaviti ili oštetiti informaciju te na kontrolu sustava. Kad je cilj pribaviti informaciju, to može biti na potpuno „nevidljiv“, skriven način ili vrlo javno. Kod oštećivanja informacije radi se o njenoj izmjeni na skriven ili javan način, potpunom brisanju ili nedostupnosti legalnom korisniku. Stjecanjem kontrole nad informacijskim sustavom žrtve, napadač može ostvariti i druge ciljeve te sve svrhe napada. Tipično napadač osigurava budući pristup u sustava na način koji ne ostavlja tragove i ne može se pratiti, proširuje doseg svoje kontrole na druge sustave, te priskrbljuje alate potrebne za daljnje faze napada. Kontrola sustava i ne mora biti izvedena izravnom kontrolom tehničkih sustava, već na primjer promjenom postupaka koje provode ovlašteni korisnici i administratori sustava.

Stoga se kao meta napada mogu pojaviti: računala, komunikacije, procesi i ljudi. Kod napada na računala, meta može biti hardver: poslužitelji ili korisnička oprema poput stolnih i prijenosnih računala, mediji i telefoni; ili softver bilo da je riječ o operacijskim sustavima ili aplikacijama. Kad su meta napada komunikacije, to može biti oprema: telefonske centrale, računalni usmjerivači; ili tijek podataka: fizički medij ili eter. Pored tehničkih sustava, meta napada mogu biti procesi ili ljudi.

B. Ranjivosti

Ranjivi dijelovi sustava su isti oni opisani kao i mete: hardver ,softver, komunikacije, podaci, procesi i ljudi te okolina informacijskog sustava: fizički prostor, energetski sustav i sl. Ranjivosti su ključne za zaštitu sustava i sprečavanje napada, a kod njihova razmatranja važno je proučiti uzroke ranjivosti. Dijelimo ih na tehničke, organizacijske i ljudske.

Tehnički uzroci ranjivosti su greške u arhitekturi sustava, dizajnu ili izvedbi tehničkih dijelova i uređaja. To su također i starost opreme i loše održavanje. Organizacijski uzroci leže u nepostojećim ili loše definiranim procesima. Ljudski uzroci su u greškama i propustima te neznanju, a najteži oblik je zla namjera.

C. Tehnike napada

Tehnike napada ovise o svrsi i cilju, žrtvi i napadaču. Osim kod su napadači umjetnici ili istraživači, težnja je ka što lakšem i jednostavnijem ostvarenju cilja pa su i tehnike jednostavne i preuzete iz „običnog“ svijeta. Tako je jedna od tehnika i obična krađa bilo da se radi o krađi podataka ili opreme. Krađa dokumenata ili njihova sadržaja može biti izvedena i kopiranjem pa žrtva ne mora (odmah) primijetiti krađu. Kad se radi o krađi opreme i ona može biti zamijenjena sličnom ili „kulisom“ koja će na neko vrijeme zatvarati žrtvu da ne primijeti krađu odmah.

Druga „obična“ tehnika napada je provala: fizički, neovlašteni ulazak u prostor, opremu ili dijelove opreme.

Treći i vjerojatno najčešći oblik napada je zlouporaba ovlasti ili povjerenja.

Opisane tehnike napada su identične onima i za druge ne-informacijske sustave i obično ne zahtijevaju posebno informatičko znanje ili iskustvo. Za razliku od njih prijevara, prisluškivanje, „otključavanje“ ili korištenje „rupa“ podrazumijevaju određenu količinu znanja i iskustva.

Prijevare su nenasilne interakcije s ovlaštenim korisnicima informacijskog sustava smišljene da navedu korisnika da napadaču otkriju važne informacije iz ili o sustavu. Žrtva u pravilu nije svjesna da dobrovoljno odaje povjerljive podatke. „Otključavanje“ je onaj tip napada koji se najčešće opisuje u filmovima i beletristici: gotovo čaroban način da se prodre do najčuvanijih tajni. U stvarnosti se radi o dekriptiranju (dešifriranju) podataka, ključeva ili lozinki za pristup podacima. U najvećem broju slučajeva se ne pronalazi algoritam za njihovo razbijanje već se šifre pogađaju. Za alate koji pogađaju šifre važno je prikupiti što više podataka o sustavu pa se obično ovi napadi kombiniraju i s prijevarama i prisluškivanjem. Korištenje „rupa“ je iskorištavanje sigurnosnih propusta u arhitekturi, dizajnu, izvedbi ili konfiguraciji tehničkih sustava ili uređaja. Kako se radi o vrlo složenim uređajima i još složenijim sustavima, praktički ih je nemoguće ispitati tako da budu 100% sigurni, naročito kad se radi o širokim i prilagodljivim primjenama. U stručnoj je javnosti neprekidna diskusija jesu li sigurniji otvoreni sustavi kod kojih svatko može otkriti i iskoristiti sigurnosni propust, ali ih i mnogi uklanjaju, ili zatvoreni sustavi kod kojih mali broj pojedinaca ima pristup izvornom kodu, ali je i uzak krug onih koji propuste uklanjaju.

IV. SCADA sustavi

Pored opisanih općenitih svojstava informacijske sigurnosti, treba razmotriti i posebnosti SCADA sustava. Njih čine još i mjerni instrumenti, uređaji i sustavi, izvršni članovi, lokalna računala koja prikupljaju lokalne podatke te obavljaju autonomno upravljanje, središnja računala koja prikupljaju globalne podatke, obavljaju daljinski nadzor i središnje upravljanje; te komunikacije kratkog dometa u perimetru objekta i one dalekog dometa koje povezuju udaljene lokacije.

SCADA sustavi su informacijski sustavi pa su teoretski izloženi istim prijetnjama kao bilo koji drugi informacijski sustav. U praksi je to malo drugačije zbog nekih njihovih posebnih svojstava. To su sustavi koji se sporo ili nikako ne mijenjaju, s ciljanim životnim vijekom preko dvadeset

godina. Pored toga u njima nema podataka koji se mogu unovčiti kao niti obilnih i „uzbudljivih“ resursa.

Pored toga, dosadašnji SCADA sustavi su bili zasnovani na starim, specifičnim tehnologijama, sporim vezama i bili su odsječeni od vanjskih sustava (Internet). Kao takvi bili su zaštićeniji od napada zbog pomanjkanja informacija koje bi napadači mogli koristiti. Danas se to mijenja, jer su sustavi zasnovani na standardnim osobnim računalima i poslužiteljima, koriste standardne operacijske sustave, povezani su standardnim komunikacijskim protokolima i uređajima, a sve češće su barem u jednoj točci povezani s internetom. Ove promjene znače da se i dosadašnje prijetnje i ranjivosti SCADA sustava mijenjaju.

A. Prijetnje SCADA sustavima

Uzevši u obzir sve rečeno, smatra se da su četiri osnovne prijetnje budućim SCADA sustavima: zlonamjerni programi, osoblje, hakeri i teroristi. Zlonamjerni programi su: virusi, crvi ,trojanski konji i tzv. spyware. To je svojevrstan „neusmjereni“ napad jer u načelu tvorci ovih programa nemaju interes u SCADA sustave. Šteta nastaje time što mogu oštetiti podatke, preopteretiti komunikacije, prisluškivati operacije te daljnje smanjivati sigurnost sustava. Ovakvi programi mogu doprijeti u sustav kroz veze s Internetom, preko prijenosnih računala ili podatkovnih medija. Svojstvo ovih programa je da se sami šire jednom kad se aktiviraju unutar sustava.

Osoblje je i najopasnija prijetnja, jer najviše zna o samom sustavu i ima najviše ovlasti. Zlonamjerno osoblje ili bivše osoblje može oštetiti podatke, onesposobiti sustav ili ugraditi nekontrolirane ulaze u sustava za iskorištavanje puno kasnije. Osoblje ne mora nužno biti zlonamjerno a da ipak nanese štetu sustavu u situacijama kad si želi olakšati posao neovlaštenim promjenama u sustavu il ikad misli da poboljšava sustav neovlaštenim promjenama. Ponekad osoblje nanese štetu aktivnostima koje radi iz puke dosade.

Hakeri su nekad bili pozitivci koji su gradili nove programske alate usavršavajući svoje sposobnosti. Danas se taj pojam koristi za svakog tko barem naizgled zna više od prosječnog korisnika i zabavlja se pokušavajući probiti sustave zaštite. To što u sustavu nema materijalnih vrijednosti, pa ni tehničkih zanimljivosti nadomjestiti će egzotičnost ili važnost sustava na ljestvici privlačnosti mete jednog hakera.

Teroristi danas uzrokuju najviše straha. Kritična nacionalna infrastruktura zasigurno je jedan od najvažnijih ciljeva mogućih terorističkih napada. Stoga su teroristi jedna od najozbiljnijih prijetnji SCADA sustavima. Osim vlastitim snagama, teroristi mogu napasti i preko posrednika, angažirajući ili prisiljavajući da za njih rade hakere ili osoblje.

B. Posebnosti SCADA sustava

Kad se razmataju ranjivosti SCADA sustava, treba posebno paziti na njihove posebnosti. Neiskustvo osoblja zaduženog za održavanje i upravljanje sustavom, visoko je na listi ranjivosti sustava. Glavnina zadataka osoblja SCADA sustava zahtjeva pouzdanost i raspoloživost sustava. Sigurnosne preporuke i postupci u dobroj su mjeri u suprotnosti s tim osnovnim potrebama SCADA osoblja, pa im se stoga oni često i suprotstavljaju ili ih barem ne provode u potpunosti i dosljedno. Također, njihovo obrazovanje i pažnja orijentirani su prema sustavima kojima upravljaju, a ne prema IKT sustavima i informacijskoj sigurnosti. Stoga je ranjivost u njihovom nedostatnom znanu i prioritetima.

Standardni operacijski sustavi sve su prisutniji i u SCADA sustavima. U IT sustavima opće namjene koji su dobro održavani redovito se provjerava ispravnost komponenti te se otkrivene ranjivosti „krpaju“. U SCADA sustavima prekid rada radi održavanja je nepoželjan pa se odgađa koliko je to moguće, ali i dulje.

Autentikacija u SCADA sustavima je daleko i od razine koja se zahtjeva za uredske sustave, a kamoli za kritičnu infrastrukturu. Rutinska je praksa da se za različite dijelove sustava koriste iste lozinke, te da veći dio osoblja koristi zajedničke lozinke. Lozinke se rijetko mijenjaju pa je sasvim uobičajeno da ih zna bivše osoblje koje već godinama radi u nekoj drugoj organizaciji. Dodatni problem je otežana primjena biometrijskih metoda autentikacije. Ometaju ih zaštitna oprema i radni uvjeti: zaštitne naočale, maske, rukavice, zamazana lica, ruke. Pored toga, osoblje često koristi otvorene komunikacije kojima se prenose i informacije potrebne za pristup sustavima.

Mnogi dijelovi sustava rade bez stalnog osoblja. Pristup tim dijelovima sustava, bilo kao glavna ili rezervna veza, osiguran je daljinskim putem: telefonskim linijama, javnim mrežama za prijenos podataka ili radio putem. Svi su oni izloženi pokušajima napada ili prisluškivanja.

Umreženost jednog SCADA sustava s drugima ili s poslovnim sustavima kupaca, dobavljača i partnera također su ranjivost. Slabost ili sigurnosni rizik tog drugog sustava, prenosi se na sve sustave s kojima je povezan.

Do sada instalacija sustava za otkrivanje (IDS) ili sprečavanje (IPS) napada , vatrozida te antivirusnih zaštita nije bila uobičajena za SCADA sustave. Osoblje je malobrojno i nije osposobljeno da redovito prati dnevnike (logove) iz kojih i moglo otkriti ranjivost ili napad. Stoga se može govoriti o nepostojanju zaštite.

SCADA softver u pravilu ima skromne sigurnosne elemente i brojne nedostatke u dizajnu koji ne bi bili važni u miroljubivom svijetu.

Vlasnici SCADA sustava u prošlosti su često izvještavali javnost o svojim sustavima uključujući i tehničke informacije koje može iskoristiti napadač. Slično je i s izvođačima i dobavljačima koji za potrebe svoje promocije ili dobivanja novih poslova, objavljuju informacije o sustavima na kojima su radili.

Ni najbolja sigurnosna oprema i ni najstroži propisi neće pomoći ako nije osigurana fizička zaštita: ako napadač može lako pristupiti opremi ili komunikacijskim medijima. Dok su dijelovi sustava bez posade, gotovo u pravilu na izoliranim lokacijama zaštićeni običnim bravama i lokotima, ulaganje u druge oblike zaštite gotovo da i nije potrebno.

V. TEHNIKE ZAŠTITE SCADA SUSTAVA

Tehnike zaštite razvrstavamo u jednu od četiri kategorije: prevencija, otkrivanje, reakcija na incident i oporavak.

Tehnike prevencije su u širokom rasponu: od jednostavnog redovitog obnavljanja aplikacija i operacijskih sustava (update), preko sustava lozinki i

biometrijskih zaštita pristupa, vatrozida, pa sve do antivirusnog softvera.

Otkrivanje sigurnosnih incidenata zasniva se na promatranju aktivnosti računala i korisnika te prometa u komunikacijskim kanalima. Na osnovi promjene stanja resursa ili obrazaca ponašanja aplikacija i korisnika, otkrivaju se potencijalno opasne situacije o kojima se onda obavještavaju nadležni.

I najbolje zaštićeni sustav može ipak biti uspješno napadnut. Dovoljan je najmanji propust, najnevjerojatniji splet okolnosti ili neracionalno složen i skup napad. Ovakvi se događaji u stvarnosti ne mogu spriječiti. Za njih je potrebno previše resursa da bi ih se uklonilo kao osnovu za napad. Stoga se ni ne provode mjere zaštite od njih, ali se nastoje otkriti. No, najvažnije je da se takvi napadi mogu i moraju planirati. A obavezno se moraju planirati mjere za rješavanje sigurnosnog incidenta. Kad se incident dogodi i bude otkriven, postupak njegova rješavanja mora biti potpuno jasan.

Nakon što se zaustavi napad i saniraju glavne posljedice, slijedi postupak oporavka. I on mora biti unaprijed projektiran, resursi spremni, a osoblje uvježbano. Pripreme za oporavak počinju davno prije napada, a provode se svakodnevno: sigurnosne kopije podataka i programa (backup), osvježavanje i prilagođavanje postupaka, obavještavanje i obrazovanje osoblja.

VI. NAJVAŽNIJI ELEMENTI ZAŠTITE SCADA SUSTAVA

Svi opisani sustavi zaštite jednako su važni i potrebno je raditi na svima. Međutim, u slučajevima kad treba izgraditi informacijsku sigurnost za sustav koji je praktički nema, potrebno je odrediti prioritete. Početi treba od prevencije, a pri tome treba voditi računa o organizacijskim preduvjetima i ljudskom faktoru.

A. Prevencija

Prevencija je najobimniji dio zaštite informacijskih sustava. Sastoji se od administrativnih mjera, obrazovanja, tehničkih mjera i posebnih sustava.

Administrativne mjere su okvir koji omogućava da se sve ostale mjere primijene i slože u skladnu cjelinu bez propusta. Tehničari zaziru od administracije, a profesionalni administrativci često nemaju dovoljno tehničkih znanja za definiranje potrebnih postupaka, dokumenata, politika i mjera. Međutim, bez njihove kvalitetne izrade, ali i održavanja, ni jedan tehnički sustav neće dati očekivani rezultat.

Još važniji su kadrovi, koji prije svega trebaju biti svjesni informacijske sigurnosti, njene važnosti i svojstava, kao i svoje uloge u njoj. Nakon toga treba ih sustavno obrazovati. To znači da mora biti potpuno jasno tko i kada što mora znati, kako će to naučiti i kako će se provjeriti stupanj znanja i vještina.

Tehničke mjere su već opisane i u suštini se sastoje od redovitog održavanja operacijskih sustava i aplikacija, pažljivog podešavanja parametara sustava, te praćenja dnevnika poslužiteljskih programa.

Za visoki stupanj prevencije napada na informacijske sustave nužno je upotrijebiti i posebnu opremu: specijalizirane komunikacijske uređaje, uređaj ili softver za prevenciju provala. Njihovo korištenje ne daje puni rezultat bez pažljivog projektiranja sustava sigurnosti, odabira pravih komponenti i njihove integracije u cjelokupni informacijski i poslovni sustav organizacije.

B. Organizacijski preduvjeti

Organizacijski preduvjeti su: strategije, politike, pravila, postupci, sigurnosni procesi i odvraćanje. U strateške odluke spadaju temelji: hoće li organizacija sama graditi informacijsku sigurnost, ili će ju kupiti od profesionalne organizacije ili pitanje je li organizacija spremna pod nekim uvjetima propustiti mogućem ucjenjivaču.

Politike vezane uz informacijsku sigurnost prvenstveno definiraju nadležnosti i odgovornosti te postavljaju glavne okvire za definiranje pravila i postupaka.

Pravila su konkretizacija politika u smislu da na provedbenoj razini definiraju ne samo kako se radi informacijska sigurnost, već i kako radi organizacija općenito.

Postupci koji se odnose na poslovanje organizacije moraju biti usklađeni sa sigurnosnim politikama i pravilima, a sigurnosne procedure se moraju tako definirati da u potpunosti osiguravaju potrebe definirane strategijama.

Čitav niz mjera se može osmisliti koje će odvratiti napadača. One mogu biti usmjerene na to da smanje privlačnost mete napadaču, da izazovu strah kod mogućeg napadača ili, pak, da se napadačeva energija usmjeri na neki drugi cilj,

C. Ljudski faktor

Ljudski je faktor apsolutno najvažniji. Čak i uz slabije organizacijske i tehničke mjere i sa skromnijim resursima mogu se postići zadovoljavajućoj rezultati, ako je ljudski faktor na visokoj razini.

Obezglavljena vojska uvijek gubi. Stoga je ključno definiranje službenih uloga s aspekta informacijske sigurnosti. Rukovoditelji moraju razumjeti svoju ulogu i koliko je opasno kad se sigurnosna pravila i postupci suspendiraju, krše ili zanemaruju čak i kad je to u svrhu povećanja učinkovitosti ili brzog rješavanja incidentne situacije u poslovanju. Također je loše ako se nekim poslom bavi tko stigne ili svi. Zato se mora definirati odgovorne osobe za pojedine funkcije u sustavu informacijske sigurnosti i to mora biti poznato svim zaposlenicima.

Krajnje je opasno kad zaposlenici pomisle da je briga o informacijskoj sigurnosti isključivo na nadležnima. Stoga je jako važno jačati i svijest i znanje i vještine samozaštite. Svaki zaposlenik mora i vjerovati i razumjeti da je njegova sigurnost, sigurnost njegova posla i njegovih resursa i rezultata upravo njegova briga. Da svi ostali djeluju samo kao pomagači.

Jednako je tako opasno, kad zaposlenici vode brigu o svojim resursima, ali ne i o resursima kolega i zajedničkim resursima, smatrajući da to nije njihov posao.

I po tom pitanju je ključ u svjesnosti, znanju, i sustavima potpore. Svaki zaposlenik mora osjetiti svoju odgovornost za sigurnost zajednice i znati kako joj može doprinijeti.

VII. ZAKLJUČAK

Informacijska sigurnost veliko je područje od suštinske važnosti za energetske sustave. Potreba razina informacijske sigurnosti postiže se planiranjem , oslanjanjem na kadrove i sustavnim višegodišnjim radom. Potrebno je unijeti promjene u gotovo sve aspekte poslovanja. Uvođenje mjera informacijske sigurnosti čini poslovanje složenijim i skupljim, no danas ni jedan sustav ne može ignorirati potrebu za informacijskom sigurnosti. Kad se radi o sustavima koji su dio kritične nacionalne infrastrukture, kao što je energetski sustav, onda se o tome ni ne raspravlja. Informacijska sigurnost je od najvišeg značaja, ravnopravna je sa osnovnom djelatnošću.

LITERATURA

[1] Byres, Eric P., J. Lowe. "The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems." 4 Oct. 2004. 20 Feb. 2005 <http://www.tswg.gov/tswg/ip/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf>.

[2] "CSX Blames Virus for Delays". Washington Post. 20 Aug. 2003: E05. 12 Feb. 2003 <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A23020-2003Aug20&notFound=true>.

[3] The Center for SCADA Security. Home page. 21 Feb. 2005 <http://www.sandia.gov/scada/home.htm>.

[4] „INEEL's SCADA Test Bed." Idaho National Engineering and Environmental Laboratory. 21 Feb. 2005 <http://www.inel.gov/nationalsecurity/factsheets/scada_test_bed.pdf>.

[5] Harrold, Dave. "Get Safe: Prepare for Security Intrusion". Control Engineering. March 2003. 20 Feb. 2005 <http://www.manufacturing.net/ctl/article/CA283196>.

[6] The Instrumentation, Systems and Automation Society. Security Technologies for Manufacturing and Control Systems. Technical Report ISATR99.00.01-2004. 11 Mar. 2004.

[7] Lemos, Robert. "E-Terrorisim, Safety: Assessing the Infrastructure Risk." 26

[8] "NCASSR Project: SCADA Protocol Authentication Project." National Center for Advanced Secure Systems Research. 21 Feb. 2005 <http://www.ncassr.org/projects/scada.html>.

[9] North American Electric Reliability Council. Urgent Action Standard 1200 –

[10] Cyber Security. 13 Aug. 2003. 22 Feb. 2005 <ftp://www.nerc.com/pub/sys/all_updl/standards/rs/Urgent_Action_Standard_1200_Cyber_Security.pdf>.

[11] Poulsen, Kevin. "Slammer Worm Crashed Ohio Nuke Plant Network." SecurityFocus News. 19 Aug. 2003. 24 Jan. 2005 <http://www.securityfocus.com/news/6767>.

[12] Stamp, Jason et al. "Sustainable Security for Infrastructure SCADA." Sandia Corporation. 2003. 21 Feb. 2005 <http://www.sandia.gov/scada/documents/SustainableSecurity.pdf>.

[13] Verton, Dan. "California Hack Points to Possible IT Surveillance Threat." ComputerWorld. 12 Jun. 2001. 19 Feb 2005 <http://www.computerworld.com/industrytopics/energy/story/0,10801,61313,00.html>.

[14] "We Have Your Water Supply, and Printers' – Brumcon Report." The Register 20 Oct. 2003. 13 Feb. 2005 <http://www.theregister.co.uk/2003/10/20/we_have_your_water_supply/>.

[15] Willoughby, Mark. "Panel: Authentication has a Long Way to Go at Industrial Sites." Computerworld. 3 Jun. 2003. 20 Feb. 2005 <www.computerworld.com/securitytopics/security/story/0,10801,81764,00.html?nas=SEC-81764>.