# SIGURNOSNI ASPEKTI PRISTUPA INFORMACIJAMA U BAZI PODATAKA O ODRŽAVANJU TRANSFORMATORSKIH STANICA 110 kV I 35 kV

Tamara Cvjetićanin, "EPS Distribucija" d.o.o Beograd, Srbija
Svetlana Međo, "EPS Distribucija" d.o.o Beograd, Srbija

## KRATAK SADRŽAJ

U ovom radu razmatraju se sigurnosni aspekti pristupa informacijama sadržanih u bazi podataka za praćenje poslova na održavanju transformatorskih stanica 110 kV i 35 kV. Dat je osvrt na rizike pri razmeni podataka između različitih organizacionih celina kojima su ovi podaci potrebni pri radu. Baza podataka se koristi prevashodno na računarima u Službi za pripremu i nadzor održavanja i omogućava unos podataka u bazu, izradu izveštaja o radnom zadatku sa dnevnim poslovima, revizijama, remontima transformatorskih stanica, izradu zahteva za dobijanje dozvole za rad, izradu zahteva za remont uz saradnju sa Službom relejne zaštite, prijavu štete osiguranju na elektroenergetskim objektima. Cilj rada je da pokaže kako se zaštitom od neovlašćenog pristupa bazi podataka, odnosno sprečavanjem menjanja i brisanja podataka usled greške ili zlonamernog upada, postiže zaštita transformatorskih stanica i same elektrodistributivne mreže. Razmatra se nivo poverljivosti informacija u bazi podataka i vrednost koju one imaju za rad Službe za pripremu i nadzor održavanja, kao i celog preduzeća. Rad razmatra vrednost baze podataka kao vrstu informacione imovine koju je potrebno zaštititi kao takvu, kao i pri eventualnoj izradi nove aplikacije sa sličnom funkcionalnošću,a koja bi koristila ovu bazu podataka. Takođe je dat osvrt na rizike, njihovu procenu i moguće štete koje bi nastale usled korišćenja netačnih podataka pri obavljanju poslova održavanja transformatorskih stanica 110 kV i 35 kV.

**Ključne reči:** pristup, baza podataka, informaciona imovina, rizik, transformator

## SUMMURY

This research paper considers security aspects of access to the data base which contains information about monitoring of maintenance activities for 110 kV and 35kV transformers. The resarch paper also brings into view the risks of data exchange between different departments whose work requires those data. The data base is mainly used within the Department for preparation and maintenance monitoring, it allows user to input data, create reports about work tasks with daily activities, revisions, transformer reparations, create request for work permission, create request for reparation in collaboration with the Department for relay protection, submit the damage entry form when it comes to insurance of objects within electric power distribution system. The goal of this research paper is to point out that protecting the data base from unauthorised access and preventing unauthorised change of data and deleting, by mistake or as a result of malicious breach, leads to the protection of transformers and the entire distribution system. The confidentiality level of information within the data base is considered, also the value which they have for the Department for preparation and maintenance monitoring and the entire company. The research paper considers this data base as a sort of information asset which needs to be protected, as is, or during the process of creation of a new application with similar features, which uses information from this data base. The paper also brings into view the risks, their evaluation and possible damages that could take place as a result of using incorrect data during maintenance acitivities for 110 kv and 35 kV transformers.

**Key words:** access, data base, information asset, risk, transformer

Tamara Cvjetićanin, tamara.cvjeticanin@epsdistribucija.rs, 064 8354- 265
Svetlana Međo, svetlana.međo@epsdistribucija.rs, 064 8974-607

## UVOD

Bezbednost informacija i zaštita obrade podataka često se povezuju sa uzbudljivim scenarijima hakerskih napada, koji obuhvataju upotrebu najsavremenijih tehnologija za očitavanje otiska prsta ili irisa, kao i za prepoznavanje lica, u svrhu identifikacije korisnika računara, odobravanje ulaska u zaštićene zone pristupa i slično. Koliko to zaista ima veze sa organizacijama u kojima radimo danas? Od uređaja za očitavanje kartica na ulazu zgrada ili server sala, do čitača otiska prsta na uređajima koje koriste zaposleni i upravljanja lozinkama, prisutni su opšte poznati primeri iz sistema menadžmenta bezbednosti informacija u organizacijama koje su sertifikovane prema standardu ISO/IEC 27001:2013.

Iako krađa skeniranog otiska prsta od zaposlenog u nekoj organizaciji koja barata sa osetljivim podacima, radi ulaska u zone sa ograničenim pristupom i neautorizovanog pristupa računaru, operativnom sistemu, bazama podataka i aplikacijama više liči na scenario za film, ostvariv je u savremenom svetu. Zbog toga je potrebno posvetiti pažnju IKT sistemima od posebnog značaja, u delatnostima od opšteg interesa, gde pripada i distribucija električne energije, pored proizvodnje i prenosa električne energije, poslovanja finansijskih institucija, zdravstvene zaštite, upravljanja nuklearnim objektima (kako to navodi Zakon o informacionoj bezbednosti). Primeri iz sveta i domaće prakse ilustruju ovaj stav. Nerazjašnjen smrtni slučaj oficira za bezbednost belgijske nuklearke, dogodio se 2016. godine, kada je ukradena identifikaciona kartica za pristup centrali. Krajem marta 2018. godine dogodio se incident u Lazarevcu, kada je došlo do fizičkog napada na radnika EPS Distribucije dok je radio na otklanjanju kvara, o čemu je izveštavano i putem Intranet portala i putem sredstava javnog informisanja. Sprečavanje ovakvih incidenata povećava nivo bezbednosti radnika što je stalni cilj organizacije.

Sistemi za upravljanje bezbednošću informacija u organizacijama treba u većoj meri da posvete pažnju onim manje uzbudljivim scenarijima, koji za razliku od prethodna dva primera, imaju veliku verovatnoću da se ostvare i veću učestanost pojavljivanja. To su: zaboravljene ili izgubljene lozinke, snimanje važnog dokumenta u formatu koji nije čitljiv korisnicima ili ostavljanje elektronskog odnosno papirnog dokumenta dostupnim svima, uprkos principu praznog stola i praznog ekrana, koji se navodi u politici bezbednosti informacija organizacije. Kada se iskoriste ove ranjivosti, preduzeće može biti izloženo pretnjama koje dovode u pitanje njegovo funkcionisanje. Pogrešna odluka u upravljanju distributivnim elektro-energetskim sistemom, usled netačnih informacija, mogla bi ugroziti kontinuitet u distribuciji električne energije, što dalje ugrožava finansijski rezultat i reputaciju organizacije, znači prouzrokuje materijalne i nematerijalne štete. Upravljanje bezbednošću infomacija treba to da spreči, smanjivanjem verovatnoće da se pretnje ostvare odnosno svođenjem rizika na prihvatljiv nivo. Standard ISO/IEC 27001:2013 zahteva zapise koji se odnose na analizu i procenu rizika u oblasti bezbednosti informacija, a upravljanje rizicima, u širem smislu, obuhvata rizike osnovne delatnosti. Zbog toga su izveštaji iz oblasti upravljanja distributivnim elektro-energetskim sistemom, kao izveštaji o prekidima u isporuci električne energije, kvarovima, stanju vozila (što je posebno bitno za zahtev kontinuiteta poslovanja u zimskom periodu) važan ulaz u proces analize rizika. Kada prekidi u isporuci električne energije obuhvate i lokacije preduzeća na kojima se čuvaju i obrađuju podaci, mogući su informacioni incidenti koji će onda testirati koliko su efikasni načini oporavka sistema. Primer je situacija iz 2012. godine, kada je došlo do otkaza blade servera posle nestanka električne energije, što je onemogućilo funkcionisanje finansijskog i drugih informacionih sistema, kao i Intranet-a. Incident je rešen pozajmicom blade servera od poslovnog partnera, do trajnog rešenja odnosno nabavke ove skupe komponente računarskog sistema.

## ODGOVOR ORGANIZACIJE NA IZAZOVE – OD SITNIH RANJIVOSTI DO ZNAČAJNIH NOVINA U OBLASTI ZAŠTITE INFORMACIJA

Savremeni modeli računara često imaju mali metalni senzor blizu tastature ili monitora koji očitava otisak prsta korisnika. Mobilni telefoni koriste pored otiska prsta, prepoznavanje lica korisnika radi otključavanja uređaja. Zaposlenima je ova mogućnost dostupna bilo da se radi o službenim uređajima, bilo privatnim, koje koriste za svrhe posla (tzv. „BYOD“ što je skraćenica od „Bring your own device“ i odnosi se na upotrebu ličnih uređaja za poslovne svrhe). Treba napomenuti da je u politikama bezbednosti informacija neophodno napraviti podelu na imovinu koja je u vlasništvu organizacije i onu koja je u ličnom vlasništvu zaposlenog, a zaposlene obavezati na zaštitu informacija organizacije pri korišćenju obe grupe uređaja. Potrebno je obuhvatiti i probleme koje ove novine sa sobom nose (sličan lik otključava mobilni telefon). Zašto bi bilo pogodno korišćenje otiska prsta za identifikaciju korisnika u organizaciji? Otisak se registruje koristeći „Register fingertips“, zatim se otisak kao podatak povezuje sa nalozima korisnika, tako da kasnije korisnik uradi samo identifikaciju otiska prsta i tako dobije pristup operativnom sistemu i aplikacijama, a bez unošenja korisničkih imena i lozinki ponaosob. U praksi bi to moglo biti korisno za radnika koji treba da uđe u trafo stanicu i obavi određeni posao na udaljenoj radnoj stanici SCADA-e, jer bi bio dovoljan samo jedan podatak – otisak prsta, da bi brzo prošao sigurnosne

prepreke za ulazak, zaštitio se od neželjenih posetilaca, i bio proveren da njegov otisak odgovara jednom od naloga za autentifikaciju na listi naloga, a pre obavljanja kritične aktivnosti na udaljenoj radnoj stanici.
Koja su to ostala manje uzbudljiva scenarija koja ugrožavaju bezbednost informacija, a imaju veliku verovatnoću da se ostvare? To su: neusaglašenosti sa najnovijim vezijama softvera i baza podataka, neblagovremeni prelazak na web orijentisane verzije softvera, nedovoljna informisanost o prestanku tehničke podrške za pojedine proizvode (npr. Internet Explorer pretraživač, XP operativni sistem), kao i skladištenje podataka na neodgovarajućim i nebezbednim mestima, van aplikacija i baza podataka, a bez izrade rezervnih kopija. Često se dešava da preduzeća drže stare verzije baza podataka, iako nove nude dobre mogućnosti zaštite i to: bolje sisteme za enkripciju, zabranu blanko lozinke pri instalaciji, zabranu da lozinka ili njen deo budu ime host računara, ime korisnika tj naloga, zabrana da lozinka glasi „Admin“, „Administrator“, „Sysadmin“, „Password“, zahtev da lozinke budu duže od 6 karaktera uz upotrebu malih i velikih slova, brojeva i nealfanumeričkih karaktera. Razlog da se preduzeće svesno izlaže riziku, ostavljajući da ove ranjivosti postoje, može biti nedostatak finansijskih sredstava. Međutim neopravdan razlog za izlaganje rizicima su neinformisanost i nizak nivo svesti o ranjivostima organizacije i pretnjama do kojih one mogu dovesti. Potrebno je imati osmišljenu strategiju preduzeća u slučaju da se neki od nepovoljnih scenarija ostvare. Na primer, šta ako se neka aplikacija ne može koristiti na novoj verziji operativnog sistema? Zbog aplikacija koje funkcionišu na XP-u, ali ne i na novijim verzijama operativnih sistema, korisnici se odlučuju da na jednoj particiji računara zadrže instaliran XP, da bi i dalje koristili date aplikacije. Potrebno je osmisliti odgovor organizacije i na ovakve, naizgled trivijalne ranjivosti. Sistemskim uticajem na njih pravi se veliki korak napred u zaštiti informacija.
Na tržištu proizvoda iz oblasti zaštite podataka (koje se brzo razvilo), postoje rešenja koja pružaju podršku za neki proizvod i kada je ona zvanično ukinuta. Ponuđači takvih rešenja vide potencijalnu zaradu u preduzećima koja ne idu u korak s vremenom. Svakako treba biti pažljiv u izboru takve „produžene“podrške koja ne potiče od originalnog proizvođača[1].
Programiranje usmereno na zaštitu privatnosti postaće neophodno, tvrdi fizičar i teoretičar dr Michio Kaku. Razlog za to je činjenica da će svetska populacija koja predstavlja srednju klasu biti prva na meti za krađu identiteta, čime će se ugroziti plaćanja karticama i plaćanja preko Interneta. Već sada je aktuelna tema da se kao uslov za dobijanje vize odnosno ulazak u razvijene zemlje mora dati korisničko ime i lozinka na društvenim mrežama, radi provere. To jasno ukazuje na veliku vrednost koju podaci za autentifikaciju imaju i na to kolika je šteta za pojedinca ako se ukradu odnosno zloupotrebe. Posle ogromne ekspanzije društvenih mreža, koje su do sada bile stalno u centru pažnje i u čijem razvoju leži mnogo novca, radiće se na zaštiti privatnosti organizacija i korisnika. To će biti unosan posao i uticaće na rad preduzeća u novonastalim uslovima poslovanja. Živećemo u svetu gde će svaki kupac zahtevati da zna sve podatke o proizvodu i proizvođaču, a prodavac će znati sve o svom kupcu. Potrošači u Srbiji će uskoro moći mobilnim telefonom da očitaju tagove na namirnicama[2] i informišu se o njihovom poreklu, načinu proizvodnje i transporta do rafova. Ovakav sistem zasnovan je na očitavanju putem radio frekvencije (koriste se NFC tagovi sa QR kodom) i predstavlja unapređenje kod sledljivosti proizvoda, a takođe pozitivno utiče na stavove korisnika o dostupnosti informacija. Potrebno je razmotriti šta će to značiti za za korisnike distributivnog sistema. Sveobuhvatne podatke o distribuciji električne energije, korisnici mogu tražiti po ugledu na informisanje o drugim proizvodima/uslugama. Zato je potrebno predvideti koje će sve podatke da zatraži korisnik distributivnog sistema (na primer koja je njegova izvorna trafo stanica, koliki je broj i trajanje prekida u isporuci električne energije, kakav je kvalitet električne energije koja mu je distribuirana i slično). Potrebno je zapitati se i na koji način će mu se ti podaci učiniti dostupnim, a u cilju zadovoljstva korisnika. Organizacije će biti u situaciji da se pri nabavci susreću sa proizvodima odnosno sistemima za zaštitu informacija, kao i sa uređajima koji imaju karakteristike nastale kao odgovor na nove zahteve tržišta u vezi sa bezbednošću informacija.
U današnje vreme se preko Internet-a lako mogu sakupiti informacije o učesnicima nekog sastanka, internim i eksternim učesnicima uključenim u rad na nekom projektu ili članovima radne grupe formirane u okviru organizacije. Lako su dostupni njihovi kontakt podaci i pozicija na kojoj se nalaze, slike, biografije, saradnici, reference, čak i lična interesovanja. Određene informacije su vrlo korisne za rad, ali gde je granica kada je u pitanju zaštita ličnih podataka i privatnosti? Internet je svima dostupan i pruža brojne informacije, a da bi se postavile granice, Vlade država, banke i drugi subjekti će pribegavati formiranju svojih Intranet mreža. U domaćim organizacijama mogu se sresti rešenja gde su podaci o zaposlenima dostupni samo u okviru lokalnih aplikacija ili Intranet-a (u okviru ODS-a odnosno EPS-a, u pojedinim Ministarstvima). Na taj način se ostvaruje kontrola i sprečava prekomerno ili neželjeno otkrivanje informacija. U budućnosti će se koristiti kvantna kriptografija za zaštitu podataka. Laserski snop će biti nosilac poruke koju niko neće moći da otkrije nijednom poznatom fizičkom metodom. Svaka promena laserskog snopa, menja vektor polarizacije i odmah se zna da neko pokušava da razotkrije poruku. Zbog brojnih afera u svetu, sa presretanjem poruka i prisluškivanjem, ulagaće se

[1] podatak sa Smart E-Government 2015, savetovanje i izložba održano u Crown Plaza-i

[2] Projekat “Upotreba savremenih identifikacionih tehnologija u procesu praćenja proizvoda“, podržan od strane Razvojne agencije Srbije

u sigurne komunikacije, verovatno u internet paralelan ovom današnjem, koji će koristiti kvantnu kriptografiju. Zato ne treba da čudi zahtev standarda 27001 koji se odnosi na kriptografiju, njega tek čeka procvat u praksi. Sve pomenute promene neminovno će se desiti, neke od njih se možda u ovom trenutku ostvaruju, pa nije nikada prerano razmišljati šta će te promene u okruženju značiti za pojedinačnu organizaciju. Zbog čega bi navedene novine imale uticaj na rad preduzeća? Zbog toga što:

1) je neophodno korišćenje Internet-a pri radu, pa svaka promena kod Internet-a ima uticaj na preduzeće

2) je neophodno obezbediti zaštitu komunikacija, pogotovo u uslovima tržišne konkurencije, kroz poštovanje:

   - Uredbe Vlade Srbije o zaštiti tajnih podataka u informaciono telekomunikacionim sistemima, (koja poziva na primenu standarda ISO/IEC 27001 i drugih tehničkih standarda)

   - Zakona o informacionoj bezbednosti (koji je u primeni od februara 2016. godine i prepoznaje IKT sisteme u oblasti distribucije električne energije kao IKT sisteme od posebnog značaja)

   - podzakonskih akata (koji su usvojeni novembra 2016. godine i obuhvataju Uredbu o utvrđivanju Liste poslova u oblastima u kojima se obavljaju delatnosti od opšteg interesa i u kojima se koriste informaciono-komunikacioni sistemi od posebnog značaja, Uredbu o bližem uređenju mera zaštite informaciono-komunikacionih sistema od posebnog značaja, Uredbe o postupku dostavljanja podataka, listi, vrstama i značaju incidenata i postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja)

   - opšte uredbe o zaštiti podataka o ličnosti -EU GDPR, koja se odnosi i na zemlje koje nisu članice EU, a koje rukuju ličnim podacima građana EU (stupila je na snagu 25.05.2018.)

3) mnoga preduzeća imaju Intranet, koji će vremenom dobiti na značaju zbog toga što se lokalno kontroliše i pruža veću sigurnost

4) će organizacije morati da izaberu odgovarajuće proizvode za zaštitu, među mnoštvom na tržištu, a to nisu više samo antivirus i firewall programi, već proizvodi zaštite u oblasti naprednih perzistentnih pretnji (Advanced Persistant Threats[3)], proizvodi za dvo-faktorsku autentikaciju, za upravljanje nalozima za pristup udaljenim radnim stanicama SCADA-e, itd. Obaveza nabavke ovih proizvoda proističe iz dva razloga: imaće ih organizacije sa kojima sarađuju, i što je važnije imaće ih i konkurenti.

5) će postojeći sistemi za upravljanje bezbednošću informacija morati da se uhvate u koštac sa novim zahtevima u oblasti standarda. Sistem upravljanja bezbednošću informacija EPS Distribucije bi trebalo da obuhvati i tehnički izveštaj ISO/IEC TR 27019:2017 koji daje smernice za sprovođenje kontrolnih mera u energetskoj oblasti (pokriva sisteme za kontrolu procesa u distribuciji električne energije).

Koliko vremena će proteći dok se ne oseti uticaj navedenih novina na organizaciju? Za adekvatan odgovor treba se podsetiti primera iz prošlosti, vremena koje je proteklo od prelaska sa Mainframe računara na personalne računare, vremena potrebnog za uvođenje mobilne telefonije i pojave pametnih telefona. Potrebno je sagledati i primere iz sadašnjosti i razmotriti brzinu prelaska na Cloud tehnologiju, pojavu iznuđivanja na Internet-u, koliko je brzo primenjena SmartGrid tehnologija i koliko će trajati razvoj sajber zaštite za SmartGrid (koja je za sada na niskom nivou). Koliko vremena je promenama potrebno da ostvare svoj uticaj? Ne previše.

## SCENARIO OSTVARENJA PRISTUPA NEAUTORIZOVANOG KORISNIKA, ANALIZA RIZIKA I PRIMERI ZAŠTITE

U scenariju koji će ovde biti opisan, prvi korak je kopiranje baze sa servera na kom je smeštena, a potom sledi analiza pretnji koje iz toga mogu proisteći. Sve informacije koje se ovde navode služe isključivo za podizanje

[3] Pristup koji omogućava da se u kontinuitetu prate informacije u okviru preduzeća, u dužem vremenskom periodu.

svesti o oblasti bezbednosti informacija, ne smeju se koristiti u nedozvoljene svrhe, niti za ugrožavanje reputacije proizvođača hardvera, softvera, vlasnika baze podataka, administratora i njenih korisnika. Jedan sasvim moguć scenario jeste da korisnik napravi kopiju baze podataka na neki medijum. Naravno prethodno mora obezbediti fizički pristup lokaciji, što je onemogućeno kontrolom fizičkog pristupa i postojanjem bezbednosnih zona (korišćenje id kartica, portirnice, upisivanje na ulasku u server salu, odobreni spiskovi posetilaca lokacijama sa njihovim podacima koji se prave za sve koji ulaze na lokaciju, a nisu zaposleni – poslovni partneri (pogotovo iz inostranstva), izvođači, saradnici na projektima, studenti na praksi i slično). Ako bi korisnik uspeo da prođe kroz bezbednosne zone, zatim bi morao da obezbediti pristup računarskoj mreži i domenu u kom se računar nalazi. Politika zaštite domena se primenjuje na dati domen ili skup računara odnosno disk jedinica datog sistema. Sistem administratori koriste politiku zaštite domena da bi postavili zaštitne protokole za deo mreže, uključujući tu protokole za lozinke, nivoe pristupa i drugo. Administratori mogu da kontrolišu jačinu lozinki zahtevanih na domenu i utiču na zaštitu domena putem podešavanja u okviru politike sigurnosti domena. Potrebno je praviti razliku između politike zaštite domen kontrolera i politike zaštite celokupnog domena. U EPS Distribuciji, kao i drugim savremenim organizacijama, upravljanje zaštitom je kompleksno jer administrator može biti eksterno lice. Delovi računarske mreže koji su posebno bitni organizaciji, mogu biti izdvojeni. To je svakako slučaj sa SCADA sistemom u EPS Distribuciji, jer je to podrška osnovnoj delatnosti. Zaštita se obavlja posebno, jer se radi o posebnoj celini. Odvojenost i predstavlja svojevrstan vid zaštite. U organizaciji koja se bavi distribucijom električne energije čiji su IKT sistemi označeni kao sistemi posebnog značaja, zasebne celine u računarskoj mreži i zasebna zaštita nisu loše rešenje. Organizacija mora naći tehnička rešenja za zaštitu koja su za nju najpogodnija, a imajući u vidu zakonske odredbe i zahteve standarda. Posebno je složeno pitanje zaštite kada ima više rukovaoca nad sistemom, pa pored zaposlenih iz organizacije rukovaoci mogu biti i drugi, čiji bi rad i zaštita sistema pri radu, trebalo da budu precizno definisani u ugovornim obavezama. Realizacija tih obaveza bi trebalo da bude vrlo efikasna u praksi da bi se govorilo o ozbiljnoj zaštiti.

Neautorizovani korisnik nema odgovarajuće korisničko ime i lozinku za logovanje na mašinu. Ako bi prevazišao prethodno navedene prepreke, sledeći korak je da pristupi serveru na kom se baza podataka nalazi (pretpostavka je da baza podataka nije na lokalnoj mašini). Pokušaj pristupa serveru bi trebalo da rezultira porukom na ekranu da korisnik nema dozvolu za pristup datom serveru, naročito ako se na njemu nalaze podaci najveće važnosti, koji su kritični za poslovanje. Navedene prepreke u praksi pružaju solidnu zaštitu. Podrazumeva se da su sistemi koji su od velikog značaja zaštićeni jakim lozinkama, a veliki broj neuspešnih pokušaja logovanja bi trebalo da bude uočljiv administratoru i zabeležen u logovima sistema. Ako se u radu organizacije koristi veliki broj aplikacija, a među njima i web orijentisanih, potrebno je razmotriti i upotrebu tzv. “Password manager-a” odnosno aplikacija za upravljanje lozinkama. Ovakve aplikacije vrše generisanje lozinki, njihovu enkripciju i čuvanje na sigurnom. Moguće ih je koristiti i na Desktop računarima, ali i na pametnim telefonima. S obzirom da se lozinke čuvaju u bazi podataka kao enkriptovane, korisnik ni ne mora znati svaku od njih, jer je vidi kada se generiše, a dalje upravljanje lozinkama je povereno aplikaciji. Jedan od dobrih primera zaštite u praksi je korišćenje jakih lozinki uz korišćenje dvofaktorske autentikacije. To je dodatni sloj zaštite u kome se posle unosa lozinke, šalje jedinstveni kod na pametni telefon. Svako logovanje ima korak unosa lozinke i korak unosa koda koji je generisan baš za to logovanje. Neautorizovani korisnik bi onda morao da ima i lozinku i da istovremeno ima pristup telefonu na kom je kod, što je malo verovatno. Ovaj sloj zaštite je koristan kod pristupa tajnim informacijama i povećava on-line zaštitu. Naime, upadi putem pecanja, tzv. “phishing”-a, su česta pojava. Sajt deluje da je autentičan, međutim to je lažni sajt sa koga stiže zahtev da se daju određeni osetljivi podaci korisnika – lozinka, lični podaci, podaci o kreditnoj kartici i drugo, uz objašnjenje da je to iz određenog razloga potrebno sajtu pod čijim identitetom se pojavljuje onaj ko “peca”. Dati podaci će naravno biti zloupotrebljeni. Kada organizacije naručuju penetracione testove, obavezni deo je svakako testiranje korisnika na pretnju od “pecanja” njihovih podataka. Rezultati penetracionog testa sprovedenog u EPS Distribuciji 2014. godine, pokazali su pozitivne rezultate na pokušaj ovakve krađe podataka. Na testiranju je bilo “žrtava” i koji su IT struke. Preporuka je pogledati da li je nešto neobično u nazivu sajta, što odstupa od ustaljene adrese, jer to upućuje na moguću prevaru. Takođe otići na sajt koji je naveden, ali ne kroz link u poruci već kroz pregledač i na njemu naći link koji se navodi u elektronskoj poruci. Ako ne postoji, posumnjati na prevaru ili koristiti kontakt naveden na sajtu te organizacije da potvrde da su tražili podatke. Zbog čega su “phishing” napadi opasni? Zato što zaposleni svakodnevno koriste elektronsku poštu odnosno web mail, gde im mogu biti ukradeni podaci za logovanje. Ako organizacija koristi tzv. “single sign-on”, tako da korisnik jednim skupom podataka za logovanje ostvaruje više pristupa – i mašini i nekim aplikacijama, onda ovu pretnju treba ozbiljno razmotriti. Kada se pojave sumnjive elektronske poruke potrebno je upozoriti korisnike kroz odgovarajuće obaveštenje i EPS Distribucija ima ovakvu ustaljenu dobru praksu. Preporuka za ovu situaciju, proistekla iz iskustva organizacije, jeste da obaveštenja budu napisana jasno, za sve korisnike i da se eventualni delovi obaveštenja na engleskom ili sa engleskim izrazima adekvatno prevedu. Originalna upozorenja koja se ubrzo posle zlonamernih događaja mogu naći na internetu su najčešće na engleskom jeziku, mogu se navesti u originalu, ali obavezno i prevesti. Međutim treba realno sagledati stanje po pitanju zaštite, naime u svakoj organizaciji postoje rizici po informacije i informaciona dobra. Na primer uvek postoji broj servera koji su dostupni većem broju zaposlenih,

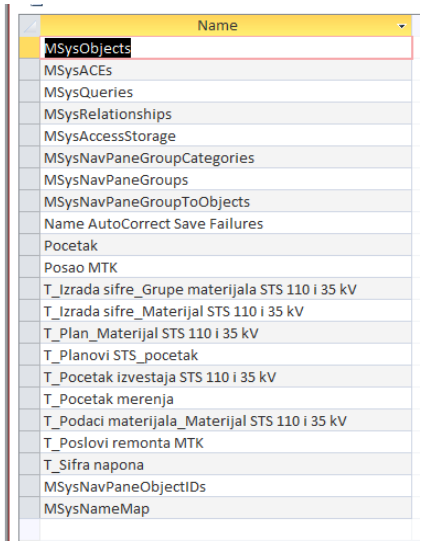
makar zbog toga što nema dovoljno prostora na serverima, pa ga neke organizacione celine moraju zajednički koristiti. Tu se otvaraju druge mogućnosti zaštite, na primer zaštita lozinkom na nivou foldera ili pojedinog dokumenta, ako je procenjeno da sadrže informacije visokog stepena tajnosti prema skali klasifikacije informacija koju primenjuje organizacija.Uvek postoje podaci koji nisu kriptovani iako je to zahtev standarda. Na skupu u organizaciji Fonis-a, na Fakultetu organizacionih nauka, izneti su podaci iz 2015. godine, koji nisu značajno promenjeni do danas prema kojima kod nas ima samo 13-14% servera sa pravilno konfigurisanom enkripcijom, a njih 20% ima validne sertifikate. Često se šalju poruke koje nisu enkriptovane, kao običan tekst (tzv. "plain text"), a sadrže osetljive podatke, pa čak i JMBG. Takođe se često dešava da više organizacionih celina koristi iste informacione resurse, na primer univerzalne uređaje za skeniranje i kopiranje, gde je potrebno obezbediti da skenirani dokument ode na destinaciju u memoriji koja je dostupna samo toj organizacionoj celini. Ovde pretnja nisu zlonamerni upadi, ali je povećana mogućnost greške i premeštanja ili brisanja dokumenta od strane zaposlenih iz drugih organizacionih celina, sa kojima se uređaj deli. U slučaju pristupa većeg broja zaposlenih istom serveru, na kom skladište podatke potrebne za rad, organizaciju od zlupotrebe podataka štiti to što svaki zaposleni ima obaveze u vezi sa rukovanjem podacima. Ako su mu određeni podaci i dostupni, a nisu iz njegovog delokruga rada, obavezan je da ih čuva. Te obaveze zaposlenih mogu biti iskazane u kolektivnom ugovoru, ugovorima o radu, aneksima tih ugovora, pravilnicima iz ove oblasti, izjavama o poverljivosti, u odgovarajućim politikama i procedurama bezbednosti informacija, aktima bezbednosti informacija i slično. Prevazilaženjem svih ovih prepreka, recimo da se radi o nekom autorizovanom korisniku odnosno zaposlenom u organizaciji, on dolazi do baze podataka i može je kopirati. Međutim ako se uređaj sa kopijom baze podataka izgubi, može da se nađe u pogrešnim rukama. Kada neautorizovani korisnik otvori bazu podataka, trebalo bi da naiđe na prepreku – zaštitu lozinkom. Baze podataka i aplikacije koje se koriste lokalno, od strane samo nekoliko zaposlenih, kao podsetnik i pomoć u radu određene službe nemaju visok stepen zaštite. Međutim ako se pokažu kao korisna informatička podrška (na primer u procesima upravljanja i održavanja elektroenergetskih objekata) i ako se neke bitne odluke donose na osnovu njihovih podataka, onda imaju vrednost za preduzeće iako nisu navedeni kao ključne stavke na listi vrednosti informacione imovine(takozvani "krunski dragulji"). Informacije sadržane u bazama podataka koje se koriste u pojedinim organizacionim celinama, makar i samo kao pomoćno sredstvo, mogu biti od koristi na primer za migraciju podataka pri prelasku na neki novi sistem tj. novi softver. Zaključak je da i ovakve baze podataka zahtevaju odgovarajući stepen zaštite. Dodavanje lozinke bazi podataka mora ispoštovati zahteve za pravljenje lozinke u usvojenoj politici bezbednosti informacija preduzeća i zahteve samog proizvođača. U slučaju MS Access baza podataka, jaka lozinka je ona od 8 i više karaktera, uz upotrebu kombinacije malih i velikih slova, brojeva i simbola. Preporuka politika za bezbednost informacija je da lozinka ne bude reč iz rečnika, kao i da se čuva odvojeno od sistema kojeg štiti i najbolje bi bilo da se ne zapisuje. Ipak treba voditi računa, da se u slučaju gubljenja lozinke ona ne može povratiti. Zato je treba pažljivo čuvati i odraditi verifikaciju lozinke kada se ona dodaje. Na primer lozinka "SiUpLo943!" zadovoljava navedene kriterijume, a ako autor zna da se odnosi na tačku standarda iz Aneksa A lako je može upamtiti bez zapisivanja (tačka A.9.4.3 Sistem upravljanja lozinkama). Kada se otvori "mdb" fajl na računaru koji je van mreže preduzeća javlja se poruka o grešci, jer linkovi ka tabelama nemaju potrebnu putanju do svog izvora. U zavisnosti od verzije Access-a kojom se otvara fajl, u poruci o grešci koja se pojavi, može se pročitati ip adresa servera na kom se te tabele nalaze. Zloupotrebe se uglavnom baziraju na tome da se namerno napravi greška, da bi se izgenerisala ovakva poruka iz sistema, a onda se navedene informacije mogu (zlo)upotrebiti. Ponekad poruka osim verzije softvera prikazuje i putanju i slične podatke. Što su novije verzije Access-a, sve je manje takvih podataka u ovim porukama, znači sve je manje ranjivosti. Od verzije 2007 koristi se i Database Splitter (Database Tools → Access Database) kojim se baza podataka deli na dva fajla. U prvom fajlu, čiji naziv ima sledeću strukturu: "ime_baze_podataka_be.mdb", nalaze se tabele. To je tzv. Back-end baza podataka. A u drugom fajlu su forme, upiti, izveštaji, makroi i linkovi ka tabelama. Razvoj novih formi se obavlja u ovom, tzv. Front-end delu. Proces deljenja zahteva da se sve tabele prethodno zatvore (inače se javlja poruka o grešci), relativno je dugotrajan i njegovim prekidanjem može doći do neželjenih posledica. Zato je obavezna izrada rezervne kopije pre procesa deljenja baze podataka. Ovo razdvajanje je svojevrstan vid zaštite, jer se onda odvojeno mogu čuvati i zaštititi podaci iz baze i ostalo. Na ovaj način se unapređuje podela posla i zaduženja (zaposleni zadužen samo za Back-end bazu podataka i zaposleni zadužen za Front-end deo). Oglasi za posao u poslednje vreme sve češće ovu podelu prepoznaju, praktično se radi o konkursu za različita radna mesta. Izbegava se pristup u kom jedna osoba projektuje, administrira bazu podataka, razvija aplikaciju i pruža podršku korisnicima. Praćenje ovakvih novih trendova je bitno za organizacije koje u svojim bazama podataka skladište informacije kritične za njeno funkcionisanje. U nekim manjim bazama podataka, koje se koriste lokalno, u jednoj organizacionoj celini, mogu na primer da se skladište podaci koji mogu biti od važnosti za organizaciju. Posmatrana je baza podataka i aplikacija koja pruža sledeće koristi: podaci o transformatorskim stanicama locirani na jednom mestu (šifra trafo stanice, podaci o elementima, izveštaji o radnim zadacima po radnim nalozima, podneti zahtevi za dobijanje dozvole za rad...). Vrednost informacija nije uvek ista, u nekim okolnostima vrednost informacije poraste, ponekad je i stari spisak zaposlenih koji su prošli odgovarajuću obuku, vrlo važan jer na primer pokazuje ko može u kratkom roku da se uključi u neku vrstu posla. U nekoj situaciji "istorija" neke trafo stanice, odnosno podaci o tome šta se događalo

na mreži, na kom elementu i kako je saniran kvar, mogu biti od velike važnosti za organizaciju. Kvalitetne odluke se donose na osnovu tačnih i pouzdanih informacija. Ne treba zaboraviti da i takve baze podataka treba adekvatno zaštititi. Analizom baze podataka o održavanju transformatorskih stanica 110 kV i 35 kV, procenjeno je da bi pogrešan podatak, bilo da potiče od greške ili zlonamenog upada, imao loš uticaj na aspekt bezbednosti na radu. Ukoliko greškom ne bi bili upisani svi elementi ili se upiše pogrešan element prilikom podnošenja Zahteva za dobijanje dozvole za rad, to direktno utiče na obezbeđenje beznaponskog stanja. Naravno postoje i dodatne kontrole - energetičar iz Operativne energetike će skrenuti pažnju u datoj situaciji.
Ovakve baze podataka su često male i u MS Access-u. Važno je naglasiti da kada se kreira baza podataka u starijoj verziji i u njoj dodeli uloga administratora i korisnika, takva će podela ostati na važnosti i kada se takva baza podataka otvori u novijoj verziji. I iz te novije verzije moguće je pokrenuti alate koji su korišćeni u starijoj verziji (verzija 2007 može da otvori alate 2003, kao što je čarobnjak za korisnički nivo zaštite ili dijalozi za podešavanje korisnika i grupa). Tako da je projektovana zaštita relativno otporna, kada se radi o pojavi novih verzija alata. Ipak treba nastojati da se prate nove verzije i vrši prelazak na iste, jer se onda automatski dobijaju neke nove vrste zaštite i novi alati pogodni za upotrebu. Podrška starim verzijama posle nekog vremena iščezava, pa je teže rešiti problem ako iskrsne, jer ostali korisnici nisu u toj situaciji.
Što se tiče dozvola u ovakvim bazama, one su eksplicitne (dodeljene korisničkom nalogu) i implicitne (dodeljene grupnom nalogu). Kada se korisnik doda grupi, on dobija dozvole grupe, pa je to težnja neautorizovanog korisnika, da postane deo grupe. Ko može da menja dozvole nad objektom baze? To su članovi grupe administratora, vlasnici objekta ili bilo koji korisnik koji ima administratorske dozvole nad objektom. Cilj neautorizovanog korisnika je da ostvari administratorske dozvole nad objektom. Onda može da obavi akciju nad objektom baze, koja mu inače ne bi bila dozvoljena. Administratori i vlasnici objekata imaju dozvole koje im ne mogu biti oduzete (nalog koji je vlasnik baze uvek može da je otvori, nalog koji je vlasnik objekta uvek može dobiti potpunu dozvolu nad objektom, administratori imaju pune dozvole nad objektima kreiranim u radnoj grupi). Administratorski korisnički nalog je isti za svaku kopiju Access-a, pa je potrebna zaštita, inače će svako sa kopijom moći da se loguje u radnu grupu koristeći administratorski nalog i imati pune dozvole nad tabelama, upitima, formama , izveštajima i makroima grupe. To je cilj neautorizovanog korisnika koji bi se dokopao kopije baze podataka. Zato je potrebno definisati administratorski nalog i korisničke naloge vlasnika (može i jedan nalog za oba), a onda iz grupe administratora izbaciti administratorski korisnički nalog. Rezervne kopije bi trebalo izrađivati u nekom određenom, pogodnom vremenskom periodu, jer je to zaštita u slučaju da dođe do neželjenih izmena nad bazom podataka.

## PRIMERI KONKRETNIH BEZBEDNOSNIH ASPEKATA

Ako bi opšti aspekt informacione bezbednosti definisali kao element aktivnosti organizacije, proizvoda, usluge koji može da utiče na informacionu bezbednost organizacije i postoji u svakoj organizaciji, onda bi time bili obuhvaćeni fizički pristup, prazan sto i prazan ekran, upravljanje lozinkama na računarima zaposlenih u opštim službama, održavanje opreme, rashodovanje medijuma, razmena elektronskih poruka, identifikovanje primenljivih zakona itd. Konkretni aspekti bezbednosti bi se mogli definisati kao elementi aktivnosti operatora distributivnog sistema i usluge koju pruža, a koji utiče na informacionu bezbednost organizacije (EPS Distribucije) i njenih korisnika. Time bi bili obuhvaćeni kontrola logičkog pristupa SCADA sistemu, pristup bazi podataka o održavanju transformatorskih stanica 110 kV i 35 kV, prisup bazi podataka sa podacima o mernim mestima, GIS bazi podataka, upravljanje lozinkama na SCADA sistemu, upravljanje lozinkama aplikacije EMS-a koje koriste zaposleni EPS Distribucije, kontrola fizičkog pristupa transformatorskim stanicama, prikupljanje znanja iz incidenata narušavanja bezbednosti informacija sakupljanjem zapisa komisija formiranih za ispitivanje uzroka otkaza rikolozera, otežane komunikacije centralne stanice i udaljenih radnih stanica, prekida voda visokog napona i drugo.
Tabela 1. prikazuje skrivene, sistemske tabele u okviru posmatrane baze podataka o održavanju transformatorskih stanica 110 kV i 35 kV, sledeći podaci su se pojavili kada je izvršen upit:
SELECT Name FROM msysobjects WHERE Type=1.
Ako bi neautorizovani korisnik uspeo da dođe do baze podataka, šteta bi mogla nastati uništavanjem sistemskih tabela. Podaci iz tabela o planovima materijala i podaci o poslovima remonta, bi mogli takođe da se zloupotrebe, da se ugrozi obavljanje posla i kontinuitet distribucije električne energije. Takođe mogla bi da se stvori nelojalna konkurencija eksternih preduzeća koja bi posedovala ove podatke u odnosu na ostala, bez tih saznanja.

TABELA 1



| Name |
|---|
| MSysObjects |
| MSysACEs |
| MSysQueries |
| MSysRelationships |
| MSysAccessStorage |
| MSysNavPaneGroupCategories |
| MSysNavPaneGroups |
| MSysNavPaneGroupToObjects |
| Name AutoCorrect Save Failures |
| Pocetak |
| Posao MTK |
| T_Izrada sifre_Grupe materijala STS 110 i 35 kV |
| T_Izrada sifre_Materijal STS 110 i 35 kV |
| T_Plan_Materijal STS 110 i 35 kV |
| T_Planovi STS_pocetak |
| T_Pocetak izvestaja STS 110 i 35 kV |
| T_Pocetak merenja |
| T_Podaci materijala_Materijal STS 110 i 35 kV |
| T_Poslovi remonta MTK |
| T_Sifra napona |
| MSysNavPaneObjectIDs |
| MSysNameMap |

## ZAKLJUČAK

Kada je zaštita informacija u pitanju, uvek se treba rukovoditi devizom da đavo leđi u detaljima. Naizgled male ranjivosti sistema mogu dovesti do toga da se neka ozbiljna pretnja realizuje i ugrozi rad organizacije. Najčešće rizici ne potiču od velikih napada hakera i zlonamernih kodova, iako u svetu oni uveliko postoje, već od zastarelosti i otkaza opreme, nekompatibilnih komponenti, ljudskih grešaka, nemara, neadekvatne organizacije procesa, nedovoljne stručnosti, manjka finansijskih ulaganja, nedostatka izrade rezervnih kopija, nedovoljne informisanosti i kašnjenja u praćenju razvoja tehnologija, kao i nepotpune primene postojećih zakona, politika i procedura bezbednosti informacija. Kada se prave liste informacione imovine polazi se od onih stavki sa najvećim prioritetom i vrednošću, što je ispravno, ali treba određenu pažnju posvetiti i "manje vrenim" dobrima - bazama podataka i aplikacijama koje se koriste kao pomoć pri radu, u pojedinim organizacionim celinama. Nekada se informacije koje su poverljive skladište upravo u njima. Informaciona bezbednost sistema zavisi od toga koliko je najslabija karika zaštićena, kao što protivpožarna zaštita mora da obuhvati i pomoćnu prostoriju, jer bezbednost cele lokacije zavisi i od nje. Savršena zaštita server sale ne vredi mnogo, ako je ostava pored nezaštićena. Podaci u malim bazama podataka i pomoćne aplikacije mogu pružiti istorijske podatke o trafo stanicama, elementima, načinima sanacije i poslužiti kao osnov za analizu korisnu za organizaciju. Osmišljavanje strategija zaštite primenjivo je i na neke značajnije baze podataka i aplikacije. Potrebno je biti otvoren za razmišljanje zasnovano na riziku koje je postalo aktuelno i opisano je u međunarodnim ISO standardima koji se primenjuju i u EPS Distribuciji. Organizacije posvećuju sve veću pažnju zaštiti, formiraju organizacione celine koje su usmerene isključivo na ovu oblast, a sve je veći broj proizvoda na tržištu koji pružaju informacionu zaštitu sistemima. Nikada nije prerano za analizu promena u okruženju organizacije, a promene u oblasti bezbednosti informacija se brzo odigravaju. Proaktivne organizacije uvek su u prednosti. EPS Distribucija svakako treba da teži da bude takva organizacija i zbog Zakona o informacionoj bezbednosti, koji navodi da su informaciono-komunikacioni sistemi u oblasti distribucije električne energije od posebnog značaja, kao i zbog dugogodišnje tradicije koja je na to obavezuje.

## LITERATURA


1. Duckett C., 2014., "Privacy program boom coming, once we are done with social media: Dr Michio Kaku ", " Tech Republic" - online, 2. April. 2014
2. "Uskoro uz pomoć telefona sve o poreklu proizvoda", Portal kvalitet - online, 25. april 2018.
3. "Set or change Access 2003 user-level security in Access 2007 or higher", Microsoft support - online, https://support.office.com/en-us/article/set-or-change-access-2003-user-level-security-in-access-2007-or-higher-0c6a10e7-966f-44f4-864e-5d2ef79439fa
4. "Domain Controller (DC)", "Techopedia"-online, https://www.techopedia.com/definition/4193/domain-controller-dc

5. “Domain Security Policy”, “Techopedia” - online, https://www.techopedia.com/definition/24028/domain-security-policy
6. Institut za standardizaciju Srbije, SRPS ISO/IEC 27001:2014 (identičan sa ISO/IEC 27001:2013)
7. Moore B., 2008., “Access through access” – research paper, version 1.0