Kibernetska varnost energetskega sektorja v Sloveniji

Damir Orlić, dr. Ciril Kafol
Informatika d.d., Hajdrihova ulica 2, Ljubljana
E-pošta: damir.orlic@informatika.si

Povzetek: Kibernetska razsežnost sveta v katerem živimo je ključnega pomena za normalno funkcioniranje sodobne družbe ter tudi za njen nadaljnji razvoj. Zaradi tega ne presenečajo intenzivne dejavnosti v kibernetskem prostoru, ki enim prinašajo dobiček, drugim pa škodo. Pred sodobno družbo so tako postavljeni novi izzivi, kot je potreba po zaščiti kritičnih točk kibernetske ranljivosti. Študije poudarjajo izjemno veliko izpostavljenost energetskega sektorja kibernetskim tveganjem, saj je energetski sektor zanimiv tudi kot sekundarni oz. infrastrukturni cilj kibernetskega napada.

Energetski sektor potrebuje učinkovit sistem za obvladovanje kibernetskih tveganj ter kibernetsko zaščito, ki bo temeljila na dobrih praksah in bo ekonomsko vzdržna. Zato je smiselno razmišljati o skupnem varnostno operativnem centru, ki bi sočasno skrbel za več energetskih podjetij. Pri tem gre za dejansko učinkovitost na področju kibernetske varnosti in ne zgolj za zniževanje stroškov.

Ključne besede: kibernetska tveganja, kibernetska varnost, varnostno operativni center

Cyber Security in the Energy Sector in Slovenia

Abstract: Cyber-dimension of the world in which we live is essential for the normal functioning of modern society as well as for its further development. It is therefore not surprising that there are intensive activities in cyberspace, which brings a profit for one, while others lose. Modern society has new challenges such as the need to protect critical points of cyber vulnerabilities. Studies highlight the extremely high exposure of the energy sector to cyber risks, because the energy sector is also interesting as a secondary i.e. infrastructure target of cyber attacks.

The energy sector needs an effective and economically viable system for managing cyber risks and cyber-security, based on best practices. So it makes sense to think about common security operations center, which would be simultaneously responsible for several energy companies. This is for real effectiveness in the field of cybersecurity, not only to reduce costs.

Keywords: Cyber risks, Cyber security, Security operations center

1 UVOD

Nekdanji direktor obveščalne agencije CIA general Michael Hayden je kibernetski prostor opisal kot peto dimenzijo, ki smo je ustvarili ljudje in sicer z besedami: "Bog je ustvaril štiri dimenzije, mi pa smo peto." Kibernetska razsežnost je dejstvo, ki se mu ne da več izogniti, kot se, v tej razsežnosti, ne moremo izogniti zlorabam, grožnjam, napadom, nevarnostim, tveganjem, krajam, vohunjenju, vojni....

Zatiskanje oči in nepripravljenost za soočanje z realnostjo le te ne spremeni. Pravočasno ukrepanje je nujno. Potrebno je predvideti možne scenarije in tako minimalizirati možnosti realizacije kibernetskih tveganj. S tem se sočasno ščitijo država, gospodarske družbe in državljani.

2 SPLOŠNO O KIBERNETSKI VARNOSTI V SLOVENIJI

Zavedanje o potrebi po učinkovitem sistemu obvladovanja kibernetskih tveganja v Sloveniji še vedno ni na tako visoki ravni kot v ZDA in EU, čeprav se to spreminja. Namreč tudi Republika Slovenija, kot članica EU, si bo prizadevala za vzpostavitev skupnega sistema učinkovitega obvladovanja kibernetskih tveganj v okvirih EU in sicer s sodelovanjem z drugimi članicami na podlagi »Direktive o ukrepih za zagotovitev visoke skupne stopnje varnosti omrežij in informacij v Uniji« [8], ki je bila sprejeta 6.7.2016 in je v uporabi od avgusta 2016.

Izhodišče za sistemsko ureditev vprašanja kibernetske varnosti je vsekakor »Strategija kibernetske varnosti Republike Slovenije« [5], ki jo je sprejela Vlada RS na seji 25.2.2016. Ta strategija je integralen del širše strategije nacionalne varnosti [6] in strategije EU »Odprt, varen in zavarovan kibernetski prostor« [7].

Na operativni ravni obstajajo zmogljivosti, toda na strateški ravni ne obstaja koordinacijsko telo, ki bi sistemski povezovalo bistvene deležnike kibernetskega varnostnega sistema:

- Nacionalni odzivni center za omrežne incidente – SI-CERT
- Sektor za informacijsko varnost v okviru Direktorata za Informatiko na Ministrstvu za javno upravo
- Ministrstvo za obrambo za sisteme na področju obrambe in varstva pred naravnimi in drugimi nesrečami
- Agencijo SOVA na področju protiobveščevalnega delovanja
- Policijo v Uradu za informatiko in telekomunikacije in v Upravi kriminalistične policije, predvsem v Centru za računalniško preiskovanje in zatiranje kibernetskega kriminala

Kandidat za koordinacijo na strateški ravni naj bi bil Urad Vlade RS za varovanje tajnih podatkov, ki naj bi postopoma prevzel pristojnosti Nacionalnega organa za kibernetsko varnost ter nalogo strateške koordinacije med deležniki sistema kibernetske zaščite.

Vsekakor je treba omeniti tudi delovanje Sekcije za kibernetsko varnost v okviru Združenja za informatiko in telekomunikacije pri Gospodarski zbornici Slovenije. Načrt sekcije je združevanje in usklajevanje interesov uporabnikov in ponudnikov kibernetske varnosti.

3 KIBERNETSKA VARNOST ENERGETSKEGA SEKTORJA

Po rezultatih analiz ICS-CERT centra, ki deluje v okviru Centra za nacionalno kibernetsko varnost in komunikacije, je prav energetski sektor najbolj izpostavljen kibernetskim grožnjam. Zato ne preseneča, da je Ministrstvo za energetiko ZDA že leta 2006 sprejelo akcijski načrt »Roadmap to Secure Control Systems in the Energy Sector« [4], ki je ena od izhodiščnih točk za posodobitev sistema kibernetske varnosti v energetskem sektorju ZDA.

Mednarodne študije [9-12] poudarjajo izpostavljenost energetskega sektorja kibernetskim tveganjem, saj je energetski sektor zanimiv tudi kot sekundarni oz. infrastrukturni cilj kibernetskega napada. Prav zato je treba poudariti, da je varnost energetike steber varnosti celotne družbe, kar je zapisano tudi v nacionalni strategiji kibernetske varnosti [5].

Slovenska elektrodistribucijska podjetja že imajo zaščito in sicer uporabljajo: postopke za preprečevanje izgub podatkov, požarne pregrade, protivirusno zaščito, sisteme za zaznavanje in preprečevanje vdorov. Izvajajo se redne posodobitve programske opreme, uporabljajo se navidezna zasebna omrežja in tehnike šifriranja. Čeprav je uporaba teh komponent varnosti še naprej nujna, nikakor ni zadostna.

Izkušnje kažejo potrebo po aktivnem načinu varovanja, ker pasivni način varovanja več ne zadostuje. Z drugimi besedami zaželjeno je zaznati kibernetsko grožnjo še preden se incident zgodi in posledično pride do dejanske škode. Takšno stopnjo varovanja je mogoče ustvarti le s koncentracijo znanj in orodji v varnostno operativnem centru, ki bo v sodelovanju z drugimi varnostno operativnimi centri izvajal kibernetsko zaščito, s poudarkom na procesu nenehnih izboljšav in dvigovanja ravni zrelosti varnostnega sistema.

Vzpostavitev in delovanje varnostno operativnega centra je povezano s stroški. Zato je smiselno in popolnoma upravičeno vprašanje ekonomskega ravnovesja med stroški in koristmi.

4 DOBRE PRAKSE

V postopku vzpostavitve in delovanja varnostno operativnega centra (v nadaljevanju VOC) je smiselno uporabiti obstoječe dobre prakse drugih organizacij doma in po svetu. Izpostavljenih je deset točk na katere je treba obrniti pozornost, ker imajo velik vpliv na uspeh izvedbe VOC-a.

4.1 Podpora uprave

Brez podpore uprave je verjetnost vzpostavitve in delovanja učinkovitega VOC-a minimalna. Uprava mora biti aktivno vključena v procese in jih podpirati. Predvsem mora sodelovati pri: izdelavi vizije in strategije, virih potrebnih za vzpostavitev in delovanje centra, ceni in kazalnikih uspešnosti VOC-a.

4.2 Kadri

Delo v VOC-u zahteva specializirana znanja, široko paleto izkušenj in številne veščine. Prav zato so zaposleni ključnega pomena za uspešno vzpostavitev in delovanje učinkovitega centra. Na splošno primanjkuje ustreznih kadrov, ki jih je praviloma zelo težko pridobiti, še težje pa zadržati. Zaradi dinamičnosti na področju kibernetske varnosti je potrebno poskrbeti za nenehno izobraževanje in usposabljanje kadrov.

4.3 Strategija

Vizija, misija in cilji VOC-a morajo biti jasno definiran del strategije, ki bi morala biti usklajena s poslovno strategijo podjetja in s poslovnimi cilji. Pomembna je tudi organizacijska umeščenost ter pooblastila VOC-a znotraj organizacije. Na ta način se je možno izogniti organizacijski negotovosti ter ustvariti temelj za operativni model VOC-a znotraj celotne organizacije. Poleg tega organizacija mora razviti okvir za upravljanje z dvigovanjem varnostne zrelosti in vrednotenjem vpliva na poslovanje.

4.4 Tehnologija

Nepremišljen nakup tehnološke opreme ima lahko katastrofalne posledice po uspešnost vzpostavitve in delovanja VOC-a. Tehnologija je pomembna, toda nakup mora biti premišljen in mora ustrezati operativnem modelu kibernetske varnosti, poslovnim ciljem ter drugim značilnostim organizacije. O nakupu tehnologije bi na strokovni podlagi morali odločati varnostni strokovnjaki, ki so zaposleni v VOC-u. Zgolj nakup tehnologije zaradi tehnologije same je vedno drag in neučinkovit pristop.

4.5 Procesi

Dobro definirani procesi omogočajo konsistentne operacije s ponovljivimi rezultati. Ena od nalog VOC-a je ustvarjanje, dokumentiranje, implementiranje in upravljanje s procesi v vseh možnih scenarijih. Primeri procesov so: triaža incidentov, analiza incidentov, navodila za odziv na incidente ipd. Skupno načrtovanje procesov je bistvenega pomena, saj se tako izognemo možnim slepim točkam. Tukaj je potrebno omeniti OT segment

(*SCADA*), ki je pogosto izključen iz nadzora s strani VOC-a, kar za organizacijo praviloma pomeni dodatni dvig kompleksnosti upravljanja z varnostnimi tveganji.

4.6 Okolje

Glavni namen VOC-a je omogočiti in zaščititi poslovanje. Zato je razumevanje poslovanja in vrednosti, ki izvira iz poslovne odločitve, ključno za izbor ustreznega odziva na incident. Samo dobro vzdrževan sistem za upravljanje s premoženjem bo VOC-u omogočil doseganje poslovnih ciljev in realno ocenu tveganja. Politike in standardi lahko podprejo usklajevanje operacij VOC-a s cilji organizacije. S komplementarnim primerjanjem poslovno relevantnih informacij in dostopnih tehničnih podatkov lahko VOC ustvari trend, ki omogoči izboljšave na področju poslovnih odločitev, boljše upravljanje s tveganji in neprekinjenost poslovanja.

4.7 Investicije

Pridobitev sredstev je lahko veliki izziv za VOC. Namreč, dokler ni konkretnih rezultatov ali sledenja uspešnosti po sprejetih kazalnikih uspešnosti se lahko zgodi, da ni zadostnega investiranja v obratovanje VOC-a. Zato je v začetku obratovanja potrebno poiskati hitre zmage in demonstrirati dodano vrednost poslovanju.

4.8 Fizični prostor v katerem se nahaja VOC

VOC potrebuje fizični prostor za obratovanje. Ker ta prostor mora biti varovan oz. mora zadovoljiti nekatere varnostne in strokovne standarde, je njegova vzpostavitev povezana tudi s stroški zagotavljanja prostora.

4.9 Stalne izboljšave

Izboljšava je nenehen proces v življenskem krogu varovanja:

- nadzor
- triaža
- analiza
- odziv
- poročilo

Na koncu vsake iteracije se akumulira dodatno znanje, ki ga nato uporabljamo v naslednji iteraciji. Če VOC ne ustvari sistem učenja in bazo znanja, potem hitro postane neučinkovit in drag ter posledično postaja breme za poslovanje organizacije in ne podpora poslovanju.

4.10 Sodelovanje, outsourcing, zunanja pomoč

Sodelovanje med VOC in drugi deležniki kibernetskega varovanja (CERT, CSIRT,...) je imperativ sodobnega časa. Brez sodelovanja ni učinkovite kibernetske zaščite. Včasih je zato smiselno uporabiti zunanjo pomoč in outsourcing tudi na področju kibernetske varnosti. Seveda potreben je tehten premislek, kaj "outsoursati", kaj pa še vedno zadržati.

5 ZAKLJUČEK

Sklepamo lahko, da so tveganja povezana z kibernetskimi grožnjami velika in se povečujejo. Nujno je potrebno razviti strategije in procese, ki nenehno skrbijo za varnostni ščit in lahko aktivirajo postopke omejevanja škode, če do le te pride.

Energetika je izpostavljeno področje, kjer je lahko škoda in vpliv na delovanje države in življenje njenih prebivalcev velika, zato je smiselno, da se hitro in učinkovito izgradijo mehanizmi za obrambo pred kibernetskimi napadi. Glede na vlogo podjetja Informatika d.d. ter dejstvom, da vseh 5 elektrodistribucijskih podjetij ima del skupne IT infrastrukture ter aplikacije pri podjetju bi bilo smiselno, da Informatika d.d. koordinira in izgradi varnostno operativni center za vseh 5 elektrodistribucijskih podjetij in koordinirano s partnerji, vzpostavi mehanizme za obrambo energetskih podjetij pred kibernetskimi napadi. Deležniki iz energetike se lahko vključijo v projekt z različnimi pristopi (celostno, delno ali kot storitve v oblaku), smotrno

pa bi bilo koncentrirati resurse na enem mestu za celotno panogo energetike. Edino koncentracija resursov bo zagotovila, da so mehanizmi obrambe zadosti dobri, da lahko kakovostno ščitijo sisteme v energetiki.

Torej, smiselno in ekonomsko učinkovito je izgraditi skupen varnostno operativni center za energetiko, ter koncentrirati resurse na enem mestu.

REFERENCE

[1] »Security Operations Centers – helping you get ahead of cybercrime«, 2014, http://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf

[2] Ralph Langner, »To Kill a Centrifuge: A technical Analysis of What Stuxnet's Creators Tried to Acchive«, 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

[3] "The National Strategy to Secure Cyberspace", U.S. government via Department of Homeland Security, February 2003. p. 16. Retrieved 2008-05-18, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

[4] Jack Eisnehauer, Paget Donnelly, Mark Ellis, Michael O'Brien, »Roadmap to Secure Control Systems in the Energy Sector«, 2006, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf

[5] »Strategija kibernetske varnosti: vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti«, 2016, Vlada Republike Slovenije,

[6] »Resolucija o strategiji nacionalne varnosti Republike Slovenije« (Uradni list RS, št.27/10)

[7] »Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace«, 2013, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667

[8] »Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji«, http://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32016L1148&from=SL

[9] »Malware Trends«, Industrial Control Systems Emergency Response Team (ICS-CERT), Advanced Analytical Laboratory (AAL), 2016, https://ics-cert.us-cert.gov/sites/default/files/documents/NCCIC_ICS-CERT_AAL_Malware_Trends_Paper.pdf

[10] »NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report«, 2015, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY%202015_Annual_Vulnerability_Coordination_Report_S508C.pdf

[11] »NCCIC/ICS-CERT Year in Review FY 2015«, 2015, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

[12] »Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat«, 2014, http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf