AKCESK
AUTORITETI KOMBËTAR PËR
CERTIFIKIMIN ELEKTRONIK
DHE SIGURINË KIBERNETIKE

SIGURIA KIBERNETIKE NË SEKTORIN E ENERGJISË

Mbeshtetur nga:

RisiAlbania
Partner for Growth

Një projekt i Agjencisë Zvicerane për Zhvillim dhe Bashkëpunim SDC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Agjencia Zvicerane për Zhvillim dhe Bashkëpunim SDC

Ky publikim është realizuar nga Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike me mbështetjen e RisiAlbania, një projekt i Agjencisë Zvicerane për Zhvillim dhe Bashkëpunim SDC.

June 2021

Tabela e përmbajtjes

Tabela e figurave

Lista e shkurtimeve

DMZ	Demilitarized Zone
ICS	Sistemet e Kontrollit Industrial
OT	Teknologjia Operacionale

I. Hyrje

Fusha e sigurisë kibernetike ndryshon vazhdimisht me shfaqjen e kërcënimeve të reja. Sektori i Sektori energjetik si pjesë e infrastrukturave kritike, është pa dyshim një mjedis i rëndësishëm, kompleks, pasi shumë sektorë të tjerë varen nga ai, në ofrimin e shërbimeve thelbësore. Ai siguron funksionimin normal të shoqërisë moderne dhe shërben si shtyllë për aktivitetet ekonomike. Prandaj, mungesa e këtij shërbimi çon në ndikime të mundshme te luhatjeve ekonomike.

Lidhja e internetit me shpejtësi të lartë e ka bërë botën një vend më të vogël. The Internet of things ka ndryshuar mënyrën se si vendet ndërveprojnë me njëri-tjetrin dhe ka sjellë një revolucion në procesin e biznesit. Ky dixhitalizim në rritje e bën sistemin e energjisë më të zgjuar dhe u mundëson konsumatorëve të përfitojnë nga shërbimet inovative të energjisë.

Në të njëjtën kohë, dixhitalizimi krijon rreziqe nga një ekspozim ndaj sulmeve kibernetike dhe incidenteve të sigurisë kibernetike, duke rrezikuar potencialisht sigurinë e furnizimit me energji ose privatësinë e të dhënave të konsumatorit.

Sot, siguria kibernetike ka një rol shumë të rëndësishëm në agjendën politike dhe Komisioni Evropian ka qenë shumë aktiv në trajtimin e sfidave të sigurisë kibernetike. Kërcënimet po bëhen serioze, më të sofistikuara, këmbëngulëse, komplekse. Për të kuptuar plotësisht dinamikën e sulmeve kibernetike, është e rëndësishme të kuptohen dimensionet e hapësirës kibernetike. Motivimi i sulmuesve me kalimin e kohës ka evoluar, i nxitur nga perfitimet financiare. Kjo ka rezultuar në një treg të mirë-organizuar të krimit për tregtimin e malware dhe informacionit të vjedhur.

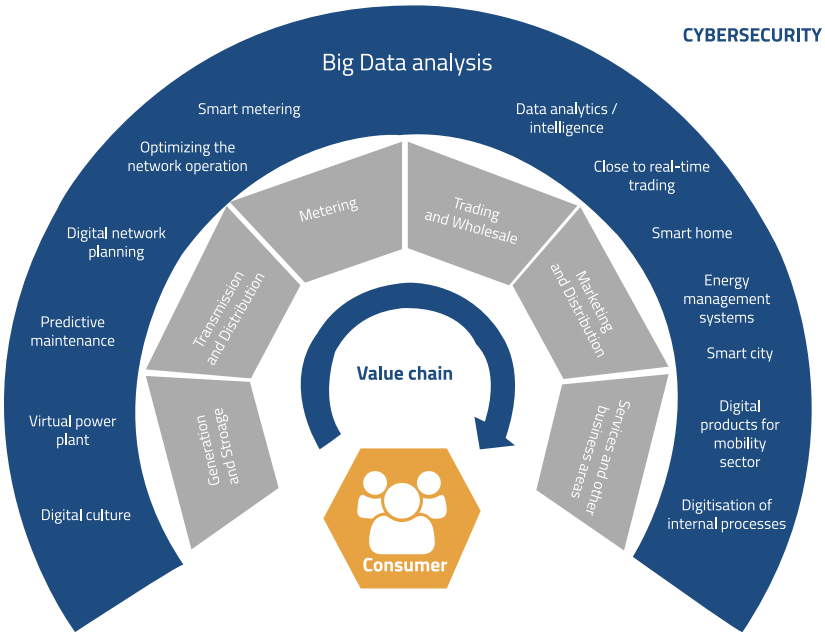

Figure 1 Ilustrimi i digjitalizimit të Sektorit Energjitik

II. Rreziqet në sigurinë kibernetike të sektorit energjitik

Për të përjetësuar zhvillimet dhe inovacionet në fushën e sigurisë kibernetike, kërkohen investime të mëdha. Zhvillimi i teknologjisë është i nevojshëm për të përmirësuar vazhdimisht efikasitetin e sigurisë kibernetike, duke qene në koherencë me kompleksitetin e kërcënimeve kibernetike.

Dëmi i mundshëm nga kërcënimet kibernetike rritet si nga zhvillimet në malware ashtu edhe nga varësia gjithnjë e në rritje e CI nga sistemet e TIK. Vendimet për nivelin e investimeve në sigurinë kibernetike duhet të bëhet në funksion të kostove të mundshme të një sulmi.
Një studim i "Cyber Security Ventures" parashikon që kostot vjetore të krimit kibernetik të rriten nga 3 trilion dollarë në 6 trilion dollarë globalisht midis 2015 dhe 2021, me humbje që rezultojnë nga "dëmtimi dhe shkatërrimi i të dhënave, para të vjedhura, produktivitet i humbur, vjedhja e pronës intelektuale, vjedhja e të dhëna personale dhe financiare, përvetësim, mashtrim,, hetimi mjeko-ligjor, restaurimi dhe fshirja e të dhënave të hakuara dhe sistemet dhe dëmtimi i reputacionit ".

"Cyber Security Ventures" ka parashikuar se shpenzimet globale për produktet dhe shërbimet e sigurisë kibernetike të cilët kalojnë 1 trilion USD në mënyrë kumulative midis 2017 dhe 2021, duke përfaqësuar 12-15% rritje vjetore. Kjo pasqyron rritjen në shpenzimet në lidhje me sigurisë kibernetike. Bota; për shembull, Qeveria e SHBA ka rritur buxhetin e saj vjetor të sigurisë kibernetike me 35%, nga 14 miliardë dollarë të buxhetuar në 2016 në 19 miliardë dollarë në 2017. Në Evropë nga ana tjetër, Këshilli i Evropës ka premtuar të investojë 450 milion EURO në një partneritet publik-privat në sigurinë e informacionit që pritet të arrijë vlerën prej 1.8 miliardë eurosh.

Mënyra e vetme për të mundësuar kuptimin dhe ritmin e nevojshëm për zbulimin dhe ndalimin e një sulmi është përdorimi i AI dhe ekspertiza e automatizuar e domenit. Zbatimi i AI (Inteligjencës Artificiale) për monitorimin dhe zbulimin e kërcënimeve kibernetike në mjedisin operativ OT ndihmon mbrojtësit të krijojnë një pamje të unifikuar të sjelljes anormale dhe të nxjerrin njohuri vepruese për për të ndaluar sulmet. Aftësitë e automatizuara të analizave të drejtuara nga AI deri më tani kanë qenë të kufizuara në operatorët më të mëdhenj të industrisë, ku buxhetet e kërkimit mund të mbështesin zhvillimin e brendshëm. Ndërkohë, shumë kompani të vogla dhe të mesme përpiqen të punësojnë ose trajnojnë personelin e nevojshëm për të siguruar mbrojtjen kibernetike, duke lënë pak buxhet për kërkim. Kjo do të thotë që një pjesë e konsiderueshme e kompanive po lihen pas dhe po bëhen hallka të dobëta në sistemin energjitik.

III. Statistika të Evropës për sulmet dhe dëmet në Sektorin Energjitik

Digjitalizimi i industrisë, përfshirë energjinë, është thelbi i të gjitha iniciativave të Komisionit Europian, si "Digital Single Market", paketa e Unionit të Energjisë (The Energy Union) dhe strategjia e "Single Market". Këto iniciativa synojnë krijimin e kritereve t; duhura për të shoqëruar transformimin e tregjeve, proceset, aktorët dhe për të siguruar përfitime të konsumatorëve në këtë trend të dixhitalizimit.
Një nga sfidat kryesore që e shoqëron këtë trend është siguria kibernetike e operatorëve, pjesëmarrësve të tregut dhe konsumatorëve. Në këtë drejtim, Agjenda Evropiane e Sigurisë 2015-2020 dhe Axhenda e Dixhital Single Market theksojnë nevojën për një qasje të përbashkët për të adresuar kërcënimet kibernetike në të gjithë Evropën, duke u mbështetur në Strategjinë ekzistuese të Sigurisë Kibernetike të Bashkimit Evropian e filluar në 2013 .

Kërcënimet kibernetike me të cilat përballen kompanitë e energjisë elektrike, përfshijnë sulmet tipike që prekin edhe industritë e tjera, si për shembull: vjedhja e të dhënave, mashtrimi i faturimit dhe ransomware për kompanitë private. Disa karakteristika specifike të sektorit të energjisë rrisin rrezikun dhe ndikimin e kërcënimeve kibernetike kundrejt operatorëve që veprojnë në këtë fushë.

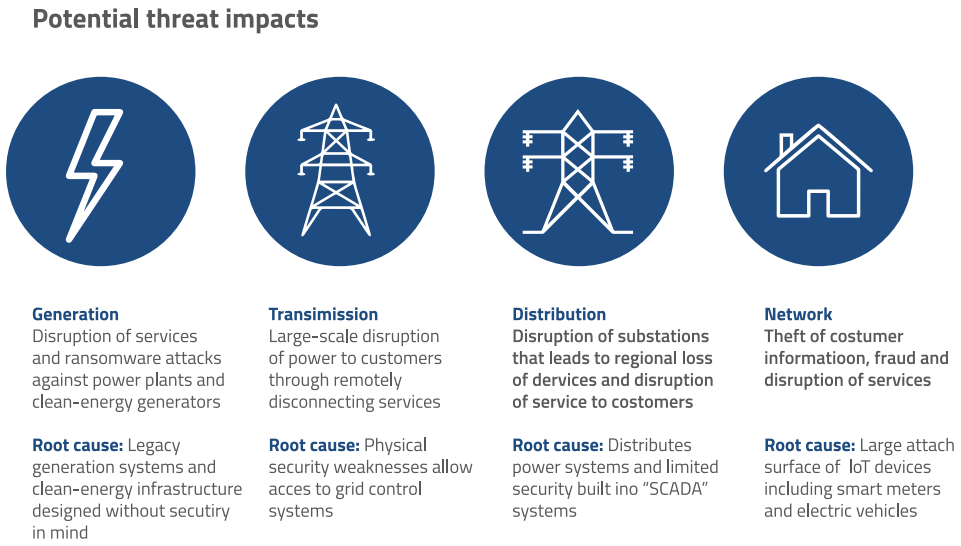

Figura 2 Ndikimi i rreziqeve në zinxhirin e furnizimit

Sistemet e Kontrollit Industrial (ICS) në Evropë, sipas Kaspersky, kanë pësuar bllokim për shkak të malware-ve në tremujorin e parë të vitit 2020 në nivel krahasimisht të njëjtë me tremujorin e katërt të vitit 2019, ndërsa përqindja e të gjithë kompjuterëve ICS në Evropë të bllokuar me malware në tremujorin e parë të 2020 është dukshëm më e ulët se e njëjta përqindje për tremujorin e katërt të vitit 2019.

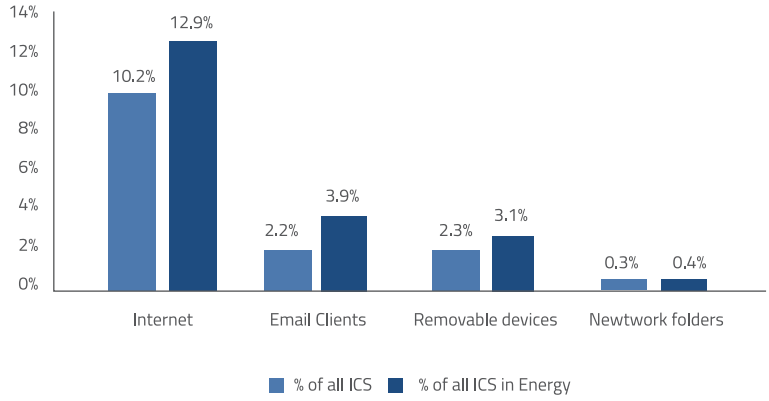

Figura 3 Burimet e kërcënimeve, ICS vs ICS ne Sektorin Energjetik, Evropë, Q1 2020

Figura e mëposhtme tregon përqindjen e Malware-ve që kanë sulmuar kompjuterat ICS në sektorin e Energjisë në Evropë, nga tremujori i funditit i 2019 deri në tremujorin e pare të 2020, ku vihet re një rënie e vogël. Konkretisht përqindja e kompjuterëve ICS në sektorin e energjisë që u prekën nga kërcënimet në internet ishte 2.7 % më e lartë se përqindja për të gjithë kompjuterët e ICS. Në të 2 njëjtën kohë, përqindja e kërcënimeve me e-mail ishte 1.7 % më të larta.

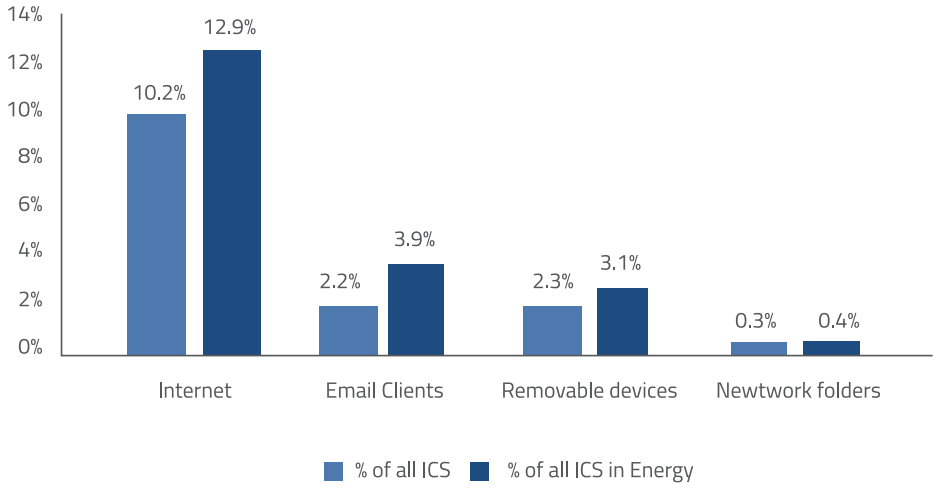

Figure 4. Malware-t e Sektorit Energjitik Q4 2019- Q1 2020

Në figurën e mëposhtme paraqiten tipet e kërcënimeve që kanë një rritje në përqindje midis të gjithë kompjuterëve në ICS dhe kompjuterëve në ICS për Energjinë.

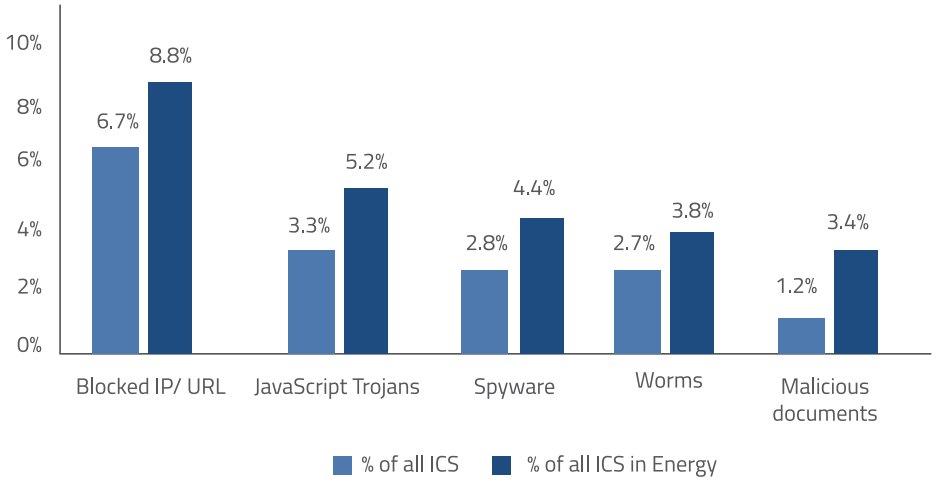

Figure 5 Tipet e Sulmeve ICS vs ICS ne Sektorin Energjitik, Europe, Q1 2020

IV. Siguria kibernetike në sektorin e energjisë në Shqipëri

Shqipëria ka realizuar hapa pozitivë përsa i përket identifikimit të sektorit të energjisë në listën e infrastrukturave kritike të informacionit. Në Vendimin e Këshillit të Ministrave Nr.553/2020 "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit" janë të listuar operatorë që ushtrojnë veprimtarinë e tyre në këtë sektor në Republikën e Shqipërisë.

Autoriteti Kombëtar për CESK në kuadër të rritjes së nivelit të sigurisë në hapësirën kibernetike merr informacione të vazhdueshme nga partnerët ndërkombëtarë mbi aspekte të ndryshme të sigurisë kibernetike. Një prej tyre është Bitsight, një kompani vlerësimesh mbi sigurinë kibernetike që analizon kompanitë, agjencitë qeveritare dhe institucionet arsimore. Vlerësimet e sigurisë që jepen nga BitSight përdoren nga autoritetet përkatëse për të krijuar një panoramë të gjendjes së sigurisë kibernetike në nivel kombëtar dhe për të shpërndarë paralajmërime në raste sulmesh.

Sipas statistikave të ofruara nga Bitsight, vlerësimi i sigurisë për sektorin e energjisë arrin në nivelin 730. Vlerësimi i sigurisë paraqet një mesatarizim të vlerësimit të sistemeve të kompromentuara, Diligjenca dhe sjellja e përdoruesve të operatorëve të sektorit të energjisë.
Komponenti i sistemeve të kompromentuara përfaqëson pajisjet e rrjetit të organizatës që tregon simptomat e aktiviteteve dashakeqe. Komponenti i diligjencës tregon hapat një kompani

ka ndërmarrë për të parandaluar sulmet. Komponenti i sjelljes së përdoruesve (user behavior) kërkon për aktivitete dashakeqe në sistemet e kompanisë, për shembull shkarkimi i skedarëve të infektuar.

Sektori i energjisë është veçanërisht i prekshëm nga kërcënimet kibernetike për shkak të tre arsyeve kryesore. Së pari, numri i kërcënimeve kibernetike është në rritje për shkak të aktorëve shtetërorë ose të sponsorizuar nga shtetet të cilët kanë si qëllim të shkaktojnë humbje ekonomike dhe dëmtim të infrastrukturave kritike kombëtare. Së dyti, për shkak të shtrirjes gjeografike dhe organizative, natyra e decentralizuar e menaxhimit të sigurisë kibernetike rrit kompleksitetin e trajtimit të incidenteve kibernetike në operatorët e infrastrukturave kritike të këtij sektori, edhe në vendin tone. Së fundi, ndërvarësia midis infrastrukturës fizike dhe kibernetike i bëjnë operatorët e sektorit energjitik të prekshëm ndaj sulmeve, duke përfshirë mashtrimet e faturimit me "matës të mençur" wireless, komandimin e sistemeve të ndryshme në distancë etj.

Në platformën Bitsight, për sektorin e energjisë në Republikën e Shqipërisë, vulnerabilitetet më të shpeshta gjenden në grafikun e mëposhtëm:

Top Vulnerabilities (% of IPs)

Name	Last 30 Days	Last 7 Days ↓	Change
POODLE	100.0 %	100.0 %	-

Figure 6 Top vulnerabilities

Në 30 ditët e fundit vulnerabiliteti më i shpeshtë është POODLE, i cili lehtëson sulmet man-in-the middle, i cili është një sulm kibernetik ku sulmuesi transmeton fshehurazi dhe ndryshon komunikimet midis dy palëve që besojnë se komunikojnë drejtpërdrejt me njëri-tjetrin.
Në nivel rajonal, Shqipëria renditet në nivelet më të larta të sigurisë së sektorit të energjisë, duke lënë pas Serbinë.

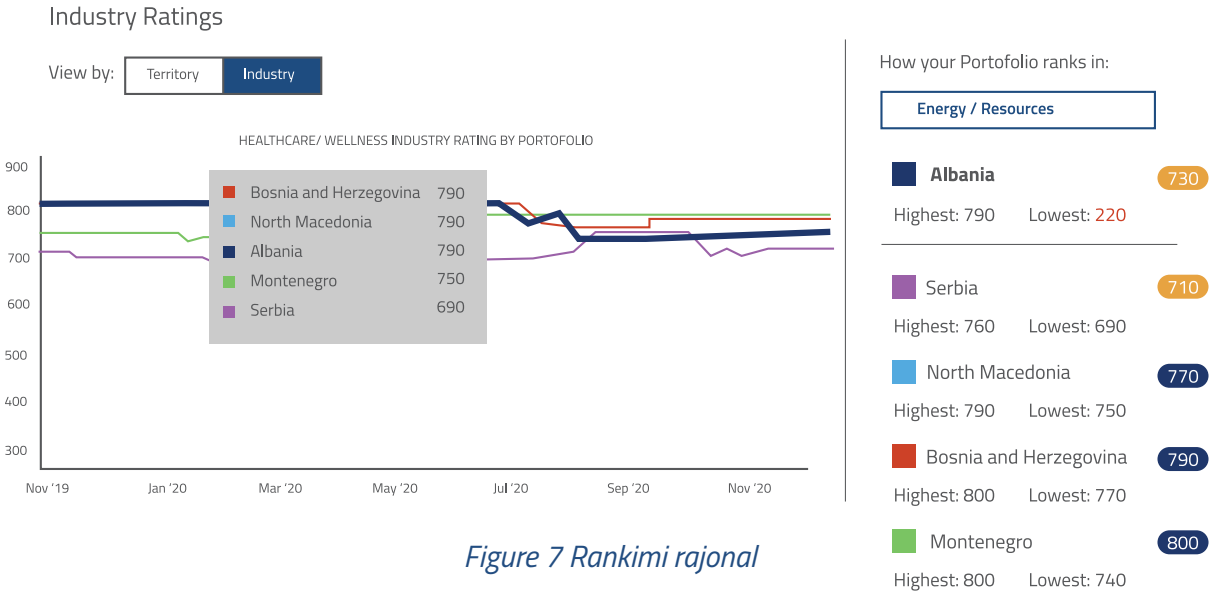

Figure 7 Rankimi rajonal

V. Përfitimet e investimeve në sigurinë kibernetike

Për të siguruar të gjithë ekosistemin e energjisë, industria ka nevojë për shërbime të përballueshme të mbikëqyrjes së sigurisë kibernetike të drejtuar nga AI në mënyrë që të forcohen objektivat OT pavarësisht nga madhësia e tregut. Duke kombinuar teknologjitë AI të ndërveprueshme dhe duke shfrytëzuar në mënyrë efikase ekspertizën njerëzore të lindur në OT, kompanitë e vogla dhe të mesme të energjisë mund të fitojnë qasje në aftësitë e monitorimit, zbulimit dhe parandalimit të sulmeve kibernetike.
Vetëm duke siguruar të gjitha hallkat në zinxhirin e vlerës së energjisë, industria në tërësi mund të vazhdojë të zhvillojë infrastrukturë inteligjente, mjete elektrike dhe gjenerim të decentralizuar të energjisë.

Më poshtë është paraqitur një model biznesi për një organizatë që vepron në sektorin e energjisë në Republikën e Shqipërisë. Përafrimet janë bazuar në kostot mesatare të investimit në sektor si dhe vetëdeklarimet e operatorëve për secilin prej zërave të tabelës si shpenzimet aktuale mesatare për një sulm kibernetik, numri i sulmeve në vit, investimi fillestar, kosto të tjera jo të drejtpërdrejta.

ENERGJI	**EUR**
Shpenzimet aktuale	
Numri i sulmeve mesatare per nje sulm kibernitik	30.000
Numri i sulmeve per nje vit	0.5
Totali i shpenzimeve per nje vit	15.000
Skenari I- Investim i brendshëm	10.000
Servera	4000
Infrastruktura e rrjetit	12.000
Ndertimi i Telefonise VOIP	8.000
Routers dhe switches	4.000
Firewall	5.000
Software te ndryshem	**43.000**
Totali	2.000
Mirembajtja	
Skenari II	
Kosto e sherbimit	11.500
Kosto e indirekte	2.000

Figure 8 Business Case

Metodologjia e përllogaritjes së kostos së kapitalit

Kosto e Kapitalit është bazuar në Modelin e Çmimit të Aseteve Kapitale, ku:

- norma pa risk është konsideruar norma e interesit të obligaconit 10-vjeçare e qeverisë Shqiptare;
- primi i riskut të tregut (beta) është bazuar sipas Demodaran;
- primi i riskut të madhësisë sipas Duff and Phelpsë
- primi specifik i kompanisë është konsideruar midis 1-2%, në mënyrë që të përfshihen të gjitha rreziqet e tjera të lëna jashtë.

Formula e kostos së Kapitalit

Kosto e Kapitalit = Norma pa risk + beta (primi i riskut të tregut + primi i riskut të madhësisë + primi specifik i kompanisë).

Kosto e Borxhit është bazuar në detyrimet afatgjata të denominuara në monedhën Lekë sipas Bankës së Shqipërisë, duke konsideruar efektin e taksës për tatimin mbi fitim prej 15% për kompanitë në Shqipëri.

Struktura e Financimit (Kapital + Borxh) është bazuar sipas strukturës mesatare të tregut nga Damodaran.

Bazuar në këta indikatorë është krijuar modeli financiar, i cili tregon se për një kompani të tillë norma e kthimit të investimit arrin në vlerën e 23%.

Kthimi nga projekti - ENERGJI	*Inflation*	*2,3%*	*3,2%*	*3,0%*	*3,1%*	*3,1%*	*3,1%*	*3,1%*	*3,1%*	*3,1%*	*3,1%*
EUR	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Shpenzimet e kursyera	15.000	15.345	15.836	16.311	16.817	17.338	17.876	18.430	19.001	19.590	20.197
Investimi fillestar	(43.000)										
Mirembajtja	(2.000)	(2.046)	(2.111)	(2.175)	(2.242)	(2.312)	(2.383)	(2.457)	(2.533)	(2.612)	(2.693)
Demtim imazhi	(2.000)	(2.046)	(2.111)	(2.175)	(2.242)	(2.312)	(2.383)	(2.457)	(2.533)	(2.612)	(2.693)
Fluksi I lire I parase	**(32.000)**	**11.253**	**11.613**	**11.961**	**12.332**	**12.715**	**13.109**	**13.515**	**13.934**	**14.366**	**14.811**
Kosto e kapitalit te projektit 12,4%											
Periudha	-	0,5	1,5	2,5	3,5	4,5	5,5	6,5	7,5	8,5	9,5
Faktori I skontimit	1,00	0,94	0,84	0,75	0,66	0,59	0,53	0,47	0,42	0,37	0,33
Viera e skontuar e fluksit te lire te p	**(32.000)**	**10.614**	**9.745**	**8.930**	**8.191**	**7.514**	**6.892**	**6.322**	**5.799**	**5.319**	**4.879**
Tregues kryesore financiare											
Viera aktuale neto (NPV)	42.205										
Norma e brendshme e kthimit (IRR)	*23%*										
Periudha e shlyerjes (PBP) ne vite	6										
Flukset e akumuluara	(142.243)	(126.168)	(103.314)	(74.222)	(39.269)	1.163					
Viti i shlyerjes se investimit	-	-	-	-	-	6					

Figure 9 Kthimi nga projekti

Kthimi nga projekti - ENERGJI	*Inflation*	*2,3%*	*3,2%*	*3,0%*	*3,1%*	*3,1%*	*3,1%*	*3,1%*	*3,1%*	*3,1%*	*3,1%*
EUR	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Shpenzimet e kursyera	15.000	15.345	15.836	16.311	16.817	17.338	17.876	18.430	19.001	19.590	20.197
Kosto e shenbimit	(11.500)	(11.765)	(12.141)	(12.505)	(12.893)	(13.293)	(13.705)	(14.129)	(14.567)	(15.019)	(15.485)
Fluksi I lire I parase	**3.500**	**3.581**	**3.695**	**3.806**	**3.924**	**4.046**	**4.171**	**4.300**	**4.434**	**4.571**	**4.713**
Kosto e kapitalit te projektit 12,4%											
Periudha	-	0,5	1,5	2,5	3,5	4,5	5,5	6,5	7,5	8,5	9,5
Faktori I skontimit	1,00	0,94	0,84	0,75	0,66	0,59	0,53	0,47	0,42	0,37	0,33
Viera e skontuar e fluksit te lire te para	3.500	3.377	3.101	2.841	2.606	2.391	2.193	2.011	1.845	1.692	1.552
Tregues kryesore financiare											
Viera aktuale neto (NPV)	27.111										

Figure 10 Kthimi nga projekti, outsource

Zgjedhja midis insource dhe outsource në sigurinë kibernetike është një dilemë me të cilën përballen shumë organizata. Si shumë dilema të tjera biznesi që duket se adresojnë koncepte abstrakte, tërheqja e një korrelacioni me jetën e përditshme është e dobishme. Vlerësimi i aftësisë së stafit tuaj të brendshëm kundrejt stafit të jashtëm kërkon një analizë të kostos dhe efikasitetit. Sipas analizave të realizuara, skenari i parë është më fitimprurës për organizatat e vogla e të mesme.

VI. Masat mbrojtëse të sigurisë kibernetike së Sektorit Energjitik

Kompanitë e energjisë elektrike janë veçanërisht vulnerabël ndaj sulmeve kibernetike, por një qasje e strukturuar që zbaton kornizat e komunikimit, organizimit dhe procesit mund të zvogëlojë ndjeshëm rreziqet e lidhura me krimin kibernetik. Tre janë karakteristikat që e bëjnë këtë sektor të riskuar ndaj kërcënimeve kibernetike:

1. Së pari është një numër i lartë i personave që e synojnë këtë shërbim: Mund të jenë qytetarë te shtetit që duan të shkaktojnë thyerje të sigurisë dhe ekonomisë, kriminelët kibernetikë që kuptojnë vlerën ekonomike të përfaqësuar nga ky sektor dhe haktivistët të cilët shprehin publikisht kundërshtimin e tyre ndaj projekteve të ndryshme ne energjitikë.

2. Së dyti, si vulnerabilitet listohet rritja e sulmit të ndërmarrjeve si pasojë e kompleksitetit gjeografik dhe organizativ.

3. Së fundmi, ndërvarësitë unike të sektorit të energjisë elektrike midis infrastrukturës fizike dhe kibernetike i bëjnë kompanitë të prekshme nga shfrytëzimi, përfshirë mashtrimin e faturimit me "smart meters", komandimin e sistemeve të teknologjisë operacionale (OT) për të ndaluar turbinat e erës, madje edhe shkatërrimin fizik.

Për të siguruar rrjetet dhe sistemet e informacionit në këtë sektor, sugjerohet të implementohet një strategji mbrojtje me tre hapa:

1. Strategji inteligjente që paraprijnë kërcënimet dhe sulmet në rrjet. Kompanitë duhet të shtojnë masat përtej atyre bazike duke marrë një qasje largpamëse ndaj sigurisë kibernetike e cila integron fuksionin e sigurisë në vendime kritike për kompaninë si përshembull zgjerimi i koorporatave, rritja e infrastrukturës dhe kompleksiteti gjeografik. Paralelisht, administruesit duhet të zhvillojnë plane të sigurta për t'ia adresuar "të panjohurit të njohur" ndërkohë që sulmuesit përpiqen të gjejnë dhe të përdorin vektorë të rinj sulmi.

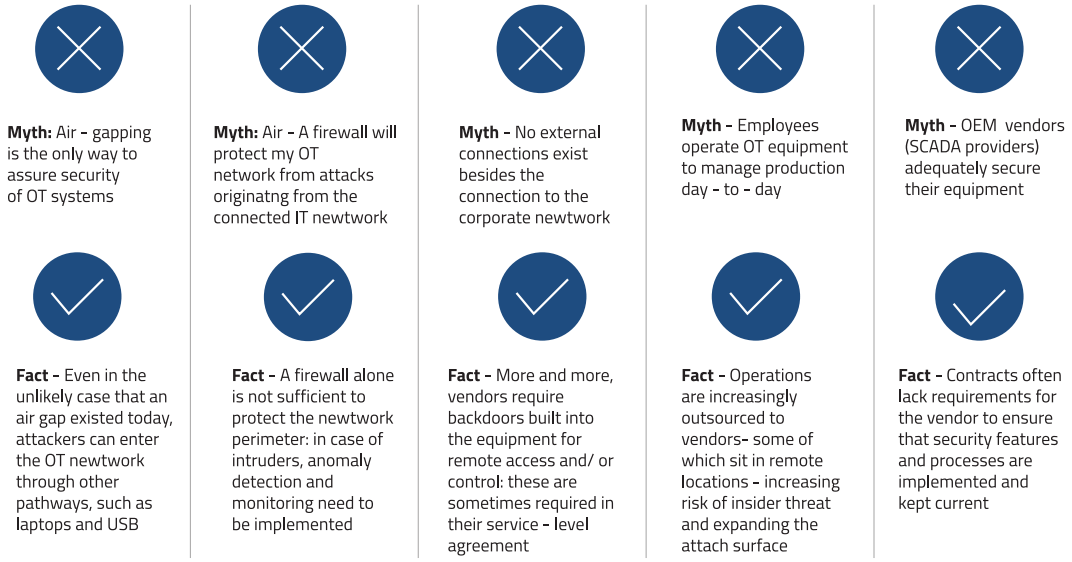

Figure 11 Mit dhe Fakt "Sistemet Operative"

2. Programet për të zvogëluar boshllëqet gjeografike dhe operacionale në ndërgjegjësimin dhe komunikimin, duke krijuar një kulturë të sigurisë. Duhet një aparat me shkallë sigurie të lartë ku punonjësit kryesorë në të gjithë ndërmarrjen, jo vetëm në siguri, të jenë të vetëdijshëm për kërcënimet dhe të kenë akses në procese si raportimi i dobësive apo incidenteve. Për më tepër sistemet teknike duhet të jenë të ndërlidhura me njëra tjetrën pavarësisht pozitës gjeografike ku mund të ndodhen duke ofruar siguri dhe duke patur mundësi të zbulojnë sulmet e koordinuara.

Ilustrative architecture for a power - generation plant

Location	Level							
Headquarters/ office	**Level4 :** IT corporate newtwork		Corporate newtwork domain controller		Corporate newtwork computer		Enterprise resource planning (ERP)	
Plant office	**Level 4 :** IT plant business newtwork		Business network domain controller				Business network computer	
Data center	**Level 3.5 :** DMZ	IT firewall	OT firewall	WEB server	Assets management system		Log location and forwarding	DMZ
Central control room	**Level 3:** Process- control network	Turbine- management system Performance - management system					Emergency shutdown Emergency shutdown system	
Local control room/ plant proceses area	**Level 2:** Supervisory control	Workstation		Local human machine interface		Workstation		Local human- machine interface
Plant process area	**Level 1:** Process control		Field controller				Field controller	
Plant process area	**Level 0:** Field process devices		Turbines				Emergency - shutdown system sensors and actuators	

Figure 12 Zonat e sigurisë

3. Bashkëpunim me të gjithë industrinë për të ndërgjegjësuar rritjen e kërcënimeve fizike dhe virtuale. Partneritetet në industri, duke parë teknologjitë kryesore që mund të implementohen në terren, duhet të përfshihen në dialog sesi të sigurojnë një lidhje të sigurt midis infrastrukturës fizike dhe virtuale si dhe midis teknologjisë së informacionit (IT) dhe rrjeteve OT.