AKCESK
AUTORITETI KOMBËTAR PËR
CERTIFIKIMIN ELEKTRONIK
DHE SIGURINË KIBERNETIKE

SIGURIA KIBERNETIKE NË NDËRMARRJET E VOGLA E TË MESME

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

DDoS	Distributed Denial of Service
GDPR	General Data Protection Regulation
IASME	Information Assurance for SME
IT	Teknologjia e Informacionit
NVM	Ndërmarrjet e Vogla e të Mesme
TIK	Teknologjia e Informacionit dhe Komunikimit

I. Hyrje

Në ditët e sotme ndërmarrjet e madhësive të ndryshme përdorin gjerësisht shërbimet të ndryshme që ofrohen në internet si posta elektronike, faqet e internetit të organizatave, online banking etj. Adoptimi i sistemeve TIK dhe interneti u kanë ofruar mundësi të konsiderueshme organizatave për të zgjeruar horizontin e tyre të biznesit, por ka rritur riskun e ekpozimit të tyre ndaj kërcënimeve kibernetike. Në ditët e sotme të zhvillimit të biznesit, siguria kibernetike përfaqëson një nga sfidat kryesore me të cilat përballen sipërmarrjet e IT-së, veçanërisht Ndërmarrjet e Vogla e të Mesme (më tej referuar si NVM), të cilat duhet të gjenerojnë vazhdimisht ide konkuruese për të siguruar qëndrueshmërinë në tregje.

NVM-të janë një nxitës i rëndësishëm për inovacionin dhe rritjen ekonomike të vendit ku veprojnë. Në të njëjtën kohë, NVM-të duhet të përfitojnë sa më shumë ngainovacionet teknologjike dhe të vlerësojnë nevojën dhe përfitimin nga implementimi i përshtatshëm dhe ekonomik i risive teknologjike në fushën TIK. Duke marrë në konsideratë sigurinë kibernetike, NVM-të jo gjithmonë janë të vetëdijshme për rreziqet dhe pasojat e biznesit për zhvillimin e teknologjive në mungesë të aplikikimit në nivelin e duhur të mbrojtjes ndaj sulmeve potenciale kibernetike.

Sulmet kibernetike si humbja e të dhënave, sulmet DDoS dhe ransomëare janë rritur dhe pasojat e humbjeve financiare deri tek dëmtimi i reputacionit mund të jenë një dëm i konsiderueshëm për NVM. Pavarësisht faktit se ndërmarrjet e mëdha kanë rritur alokimin e buxhetit për tu përballur me sulmet kibernetike, kur bëhet fjalë për NVM është më e vështirë për tu përballur dhe zbatuar masa efikase të sigurisë në infrastrukturat e tyre TIK. Masat e sigurisë shpesh herë perceptohen si tepër komplekse, që marrin kohë dhe kërkojnë nivel të lartë njohurish teknike.

Për të garantuar nivelin e duhur të sigurisë kibernetike në NVM është e rëndësishme të aplikohen të paktën disa kërkesa minimale sigurie sipas rekomandimeve të udhëzuara nga AKCESK. Një arsye tjetër që ndikon nëcënimin e sigurisë kibernetike është mungesa e ekspertizës së NVM-ve në zbatimin e funksionaliteteve të sigurisë përditësimin e zgjidhjeve të sigurisë si në përgjigje të situatës kibernetike, për tu përballur dhe zbatuar masa efikase të sigurisë në infrastrukturat e tyre TIK, si dhe planifikimin e investimeve afatshkurta dhe afatmesme të nevojshme.
Ekzistojnë plaftorma të ndryshme, të cilat ofrojnë zhvillime të zgjidhjeve kosto-efektive të mjeteve të sigurisë kibernetike. Këto zgjidhje mbështetin NVM-të në proceset e menaxhimit të rreziqeve të sigurisë kibernetike dhe identifikimin e mundësive për zbatimin e teknologjive të sigurta dhe inovative për tregun digjital.

Për të rritur ndërgjegjësimin e NVM-ve dhe njohuritë e NVM në këto ccështje është hartuar kjo broshurë e cila përfaqëson një metodologji lehtësisht të aplikueshme nga stafi përgjegjës i NVM. Objektivi kryesor i përdorimit të kësaj broshure është t'u mundësojë NVM-ve të mos e shikojnë sigurinë kibernetike si një pengesë, por si një mundësi për zhvillimin e sigurt të biznesit të tyre. Kjo broshurë paraqet fakte dhe argumenta pse investimi në sigurinë kibernetike është një rast për të zhvilluar biznesin e NVM-ve.

II. Statistika të Europës për sulmet dhe dëmet në NVM

Vitet e fundit si rezultat i zhvillimit të teknologjive të reja është vënë re transformimi i vazhdueshëm i mënyrës së operimit të Qeverisë, bizneseve dhe mënyrës sesi ata ndërveprojnë me njëri-tjetrin. Sipas një raporti të Fireeye të vitit 2020, në Europë, statistikat e krimit kibernetik në NVM arrijnë në rreth 77% të organizatave, prej tyre 44% e tyre nuk e konsiderojnë veten të rrezikuara. [1]

Sipas një studimi të Departamentit për Digjitalizimin, Kulturën, Median dhe Sportin në UK[2] , organizatat më të prekura nga sulmet kibernetike janë ato që përpunojnë të dhëna personale dhe stafi i tyre përdor pajisjet personale për punë.
NVM-të janë shtylla e ekonomisë së Evropës. Rreth 99% ose 25 milion e bizneseve të BE përfshihen në këtë grup. Ata punësojnë afërsisht 100 milion njerëz dhe përbëjnë më shumë se gjysmën e GDP-së së Evropës dhe luajnë një rol të rëndësishëm në jetën ekonomike dhe rritjen e vlerës në çdo sektor të ekonomisë . NVM-të sjellin zgjidhje inovative për sfidat si ndryshimi i klimës, efikasiteti i burimeve dhe kohezioni social dhe ndihmojnë në përhapjen e këtij inovacioni në të gjithë rajonet e Evropës. Prandaj NVM-të janë thelbësore për një ekonomi të qëndrueshme dhe digjitale në Bashkimin Evropian, për konkurencën dhe prosperitetin e Evropës, ekosistemet industriale, sovranitetin ekonomik dhe teknologjik, si dhe qëndrueshmërinë ndaj faktorëve të jashtëm.

Mbrojtja e të dhënave të organizatës jo vetëm që mbron reputacionin e saj, por e vendos atë në një pozicion të sigurt dhe konkurues për të ofruar shërbimet e kërkuara nga klientët. Organizatat të cilat dështojnë në sigurinë dhe ruajtjen e të dhënave nga sulmet kibernetike, nuk vendosin në rrezik thjesht dokumenta. Humbja e të dhënave sensitive mund të ndikojë negativisht në reputacionin e financat e kompanisë, si dhe mundësinë për t'u rritur në treg.
Sipas të njëjtit studim, siguria kibernetike nuk duhet detyrimisht të jetë komplekse dhe të konsumojë kohë.

Disa nga mjetet e rekomandura nëpërmjet të cilave NVM-të mund të sigurojnë një nivel bazik të rekomanduar sigurie janë:

- Krijimi dhe aplikimi i një politike për fjalëkalim të sigurtë e kompleks;
- Instalimi i programit të antivirusit për të gjithë kompjuterat
- Përditësimi i programeve në versionet më të reja.

Pjesa dërrmuese e NVM-ve janë të papërgatitur dhe nuk janë në dijeni për pasojat e sulmeve kibernetike, por klientët janë gjithmonë e më shumë të shqetësuar për sigurinë e të dhënave të tyre.

[1]Fireeye, "Small and midsize enterprises: Stopping cybercrime against small and midsize enterprises," https://www.fireeye.com/offers/stop-cyber-crime-against-small-medium-enterprises.html, 2020.
[2]R. Vaidya, "Cyber security breaches survey 2018: Statistical release," Department for Digital, Culture, Media & Sport, UK, 2018.

II. 1 Ekosistemi kibernetik i NVM-ve në Evropë

Digjitalizimi mund të sigurojë mundësi të mëdha për NVM-të për të përmirësuar efikasitetin e proceseve të prodhimit dhe aftësinë për të sjellë inovacion në produkte dhe modele biznesi. Përdorimi i teknologjive të avancuara, të tilla si Blockchain dhe Inteligjenca Artificiale (AI), Cloud and High Performance Computing (HPC) mund të rrisin në mënyrë progresive konkurrencën midis tyre.

Por NVM-të nuk përfitojnë plotësisht nga të dhënat që ato disponojnë, të cilat janë thelbi i ekonomisë digjitale. Një pjesë e tyre nuk janë të vetëdijshme për vlerën e të dhënave që krijojnë dhe administrojnë, si dhe nuk janë të mbrojtur mjaftueshëm nga sulmet potenciale kibernetike. Vetëm 17% e NVM-ve kanë aplikuar dhe integruar në mënyrë të suksesshme teknologjitë digjitale në bizneset e tyre, krahasuar me 54% të kompanive të mëdha.

Rezultatet e një studimi të Cyber Streetwise dhe KPMG[3] treguan se për 23% të NVM-ve siguria kibernetike është një ndër shqetësimet kryesore të tyre, e cila po kthehet në një mënyrë për të bërë biznes; 83% e konsumatorëve të marrë në studim janë të shqetësuar për faktin se cili biznes ka akses në të dhënat e tyre dhe 58% e tyre u shprehën se një thyerje sigurie do t'i dekurajonte për të përdorur të njëjtin biznes edhe në të ardhmen.

Statistikat e tjera të studimit tregojnë se për 94% të menaxherëve të prokurimeve, standartet e sigurisë kibernetike janë të rëndësishme kur një NVM realizon një shërbim ose projekt, 86% e tyre do të konsideronin penalizimin dhe prishjen e kontratës në rast shkeljeje.Nëse u vlerësua që 60% e NVM-ve kanë pësuar një thyerje sigurie, vetëm 29% e atyre që nuk kanë patur një eksperiencë të tillë theksuan dëmtimin e reputacionit si të rëndësishëm dhe për t'u marrë në konsideratë.

Impakti i një sulmi dhe thyerjeje të sigurisë mund të jetë i madh dhe me pasoja afatgjata. 89% e bizneseve të vogla të marra në studim të cilët kanë pësuar një thyerje sigurie, shprehen se kishte një ndikim në reputacionin e tyre. Ato të cilët janë sulmuar thonë se 31% kanë pësuar dëmtim të markës, 30% kanë humbur klientët dhe vetëm 29% e tyre kanë siguruar rritje të biznesit. NVM-të të cilat kanë pësuar sulme kibernetike dhe thyerje të sigurisë kanë deklaruar se 26% kanë pësuar vonesa tek klientët dhe 93% e tyre kanë patur impakt mbi mënyrën e operimit të biznesit.

NVM-të tradicionale, shpesh janë të pasigurta për të implementuar strategji biznesi digjitale, për shkak të vështirësive në mirëmbajtjen e bazave të të dhënave të mëdha dhe u shmangen përgjegjësive për të përdorur aplikacione dhe mjete të avancuara të Inteligjencës Artificiale. Në të njëjtën kohë, ata janë konsideruar si më vulnerable ndaj kërcënimeve kibernetike.

[3]KPMG, 2018 "Small business reputation and cyber risk"

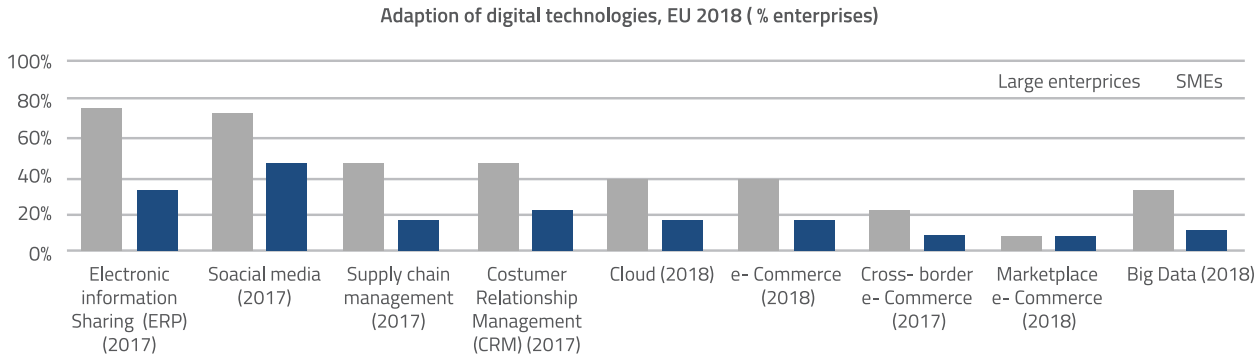

Figura 1 Adoptimi i teknologjive Digjitale, Eurostat 2018

II.2 Miti dhe realiteti i sigurisë

Gjysma e bizneseve (51%) të marra në studim mendojnë se nuk mund të ndodhë asnjëherë që ata të jenë objekt i një sulmi kibernetik. Kjo ndoshta mund të shpjegojë faktin se rreth 33% e bizneseve janë plotësisht të përgatitur për një sulm. Për më tepër, 68% e bizneseve që nuk kanë qenë kurrë pjesë e një sulmi, mendojnë se nuk janë pothuajse fare të riskuar, sipas të njëjtit studim nga KPMG. 6 në 10 nga bizneset e vogla të marra në studim kanë patur një eksperiencë me sulmet kibernetike.

Bizneset e vogla po vendosin veten në rrezik duke nënvlerësuar ndikimin e madh që një sulm kibernetik mund të ketë në reputacionin e tyre. Pavarësisht faktit se një pjesë e madhe e bizneseve të marra në studim mendojnë vazhdimisht për reputacionin e tyre, ata nuk e konsiderojnë faktin se si një sulm kibernetik mund të ndikojë në biznesin e tyre. Në fakt, 23% e kompanive të vëzhguara që nuk kanë patur eksperienca të mëparshme me sulmet kibernetike shprehen se dëmi që shkakton një sulm kibernetik duhet marrë në konsideratë.

Më pak se gjysma e këtyre bizneseve mendojnë se një sulm kibernetik mund t'i dekurajojë konsumatorët për të qëndruar si klient në të ardhmen. Në realitet, bizneset e vogla janë duke e nënvlerësuar impaktin e vërtet që sjell një sulm kibernetik. Pjesa më e madhe e konsumatorëve (58%) të marrë në studim shprehen se një thyerje e sigurisë do t'i dekurajonte për vazhdimësinë e biznesit.

***Bizneset të cilët kanë pësuar një sulm kibernetik, kanë patur këto pasoja:**

1. Dëmtim të markës;
2. Humbje klientele;
3. Kanë humbur mundësinë për të tërhequr klientelë të re;
4. Kanë humbur mundësinë për të zgjeruar aktivitetet e tyre.

III. Situata në Shqipëri me referenca statistikore

NVM janë operatorë potencialë për t'u identifikuar në listën e Infrastrukturave Kritike e të Rëndësishme të Informacionit për shkak të volumit dhe sensitivitetit të të dhënave që ato përpunojnë.

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 NVM arrin në nivelin 740. Vlerësimi i sigurisë paraqet një mesatarizim të vlerësimit të sistemeve të kompromentuara, Diligjenca dhe sjellja e përdoruesve të NVM. 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.

Në këtë platformë, për NVM në Republikën e Shqipërisë, vulnerabilitetet më të shpeshta gjenden në grafikun e mëposhtëm:

Top Infections (% of IPs)

Name	Last 30 Days	Last 7 Days ↓	Change
Gamarue	66.7 %	100.0 %	-50.0 %

Figura 2 Top infections, Bitsight

Gamarue lejon sulmuesit të aksesojnë në distancë pajisjet e kompromentuara. Ai përhapet kryesisht përmes postës elektronike (spam). Në nivel rajonal, Shqipëria renditet e treta për nivelin e rankimit të sigurisë së NVM, duke lënë pas Serbinë dhe Maqedoninë e Veriut.

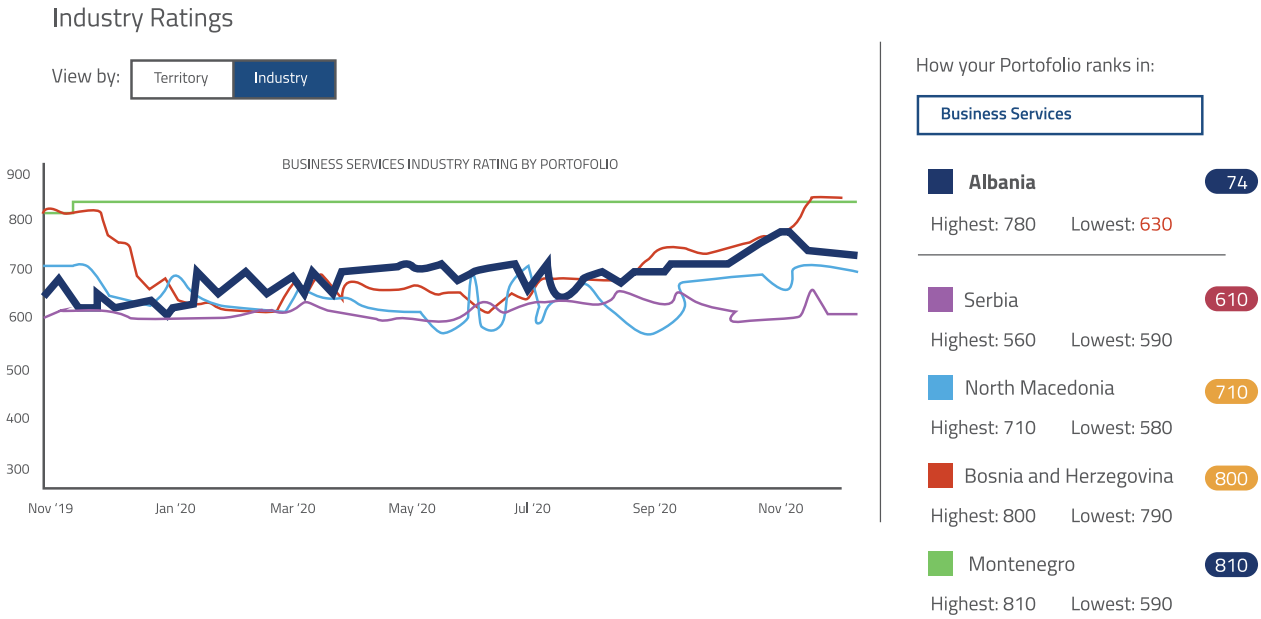

Figura 3 Rankimi rajonal, Bitsight

Si çdo aktivitet biznesi, informacionit në NVM duhet të menaxhohet dhe mbrohet në mënyrë strategjike. Drejtuesit e NVM-ve duhet të kuptojnë vlerën e informacionit që përpunohet në sistemet e tyre dhe të implementojnë korniza për vlerësimin dhe zbatimin e sigurisë së informacionit.

Zakonisht, për shkak të zhvillimit dinamik, integrimi dhe siguria nuk adresohen në fazën e ndërtimit. Për këtë arsye, planifikimi i sigurisë së informacionit dhe rikuperimi pas sulmeve janë thuajse inekzistente. Shpesh ndodh që rreziku i sigurisë kibernetike për NVM-të nuk shtrihet përtej viruseve dhe programeve anti-virus. Në vendin tonë, ashtu si në Evropë, shumica e drejtuesve të NVM-ve e konsiderojnë sigurinë e informacionit vetëm si një ndërhyrje teknike për të adresuar kërcënimet ndaj viruseve dhe back up (kopjet) e të dhënave. Nga ana tjetër programet e trajnimit dhe ndërgjegjësimit të personelit shpesh neglizhohen.

IV. Benefitet e investimeve në siguri kibernetike të NVM dhe masat mbrojtëse

I[illegible]xhimi i sigurisë kibernetike mund të jetë sfidues dhe kërkon kohën e nevojshme. Automatizimi i proceseve të sigurinë kibernetike ndihmon në mënyrë efektive biznesin që të përballojë kërcënimet dhe sulmet potenciale.

Mediat sociale dhe interneti kanë arritur të integrojnë çdo familje, shkollë dhe NVM brenda shoqërisë moderne dhe ekosistemit kibernetik. Interneti ka ndryshuar pozitivisht shumë

aspekte të jetës, siç janë ofrimi i mundësive të reja për të bërë biznes, mundësimi i zgjerimit të atij aktual, sidhe rritja e përfitimit financiar.

Një pjesë e madhe e NVM-ve po përditësojnë dhe integrojnë teknologjitë digjitale të reja në proceset e tyre të biznesit për të qenë konkurues dhe të suksesshëm në treg. Procesi i përditësimit dhe ofrimit të shërbimeve me teknologjitë e reja digjitale shoqërohet me një risk të ekspozimit të vulnerabiliteteve të tyre. Kjo është arsyeja se pse NVM duhet të planifikojnë dhe investojnë në Sigurinë Kibernetike.

Benefitet e investimeve në sigurinë kibernetike		
1.	Kosto e ulët	Automatizimi i proceseve të sigurisë kibernetike redukton kostot e IT, të cilat zakonisht janë fikse dhe relativisht të larta kur është një punonjës i brendshëm që kryen të gjitha funksionet e IT
2.	Zhvillimi hap pas hapi	Rekrutimi i një punonjësi të kualifikuar në siguri kibernetike, nuk ofron mbrojtje totale nga sulmet potenciale kibernetike. Nga ana tjetër, me anë të një softueri të sigurisë kibernetike, biznesi juaj siguron udhëzues dhe instruksione hap pas hapi, të cilat e bëjnë të drejtpërdrejtë adresimin e kërcënimeve kibernetike dhe strategjitë e minimizimit të impaktit të këtyre kërcenimeve.
3.	Avantazh konkurues për NVM	Ndryshe nga bizneset e mëdha, NVM-të nuk mund të përballojnë mbështetje dhe zgjidhje të problemeve kibernetike nga punonjësit e brendshëm. Nga ana tjetër duke zgjedhur të automatizosh kërkimin për dobësi në sistem, mund të përfitosh të njëjtin nivel sigurie si firmat dhe bizneset e mëdha.
4.	Kontroll i përhershëm	Njësoj si investimet e tjera të biznesit, të drejtosh një zgjidhje sigurie kibernetike nga vetë biznesi, mbart një risk të konsiderueshëm që duhet vlerësuar. Gjithsesi me njohuritë dhe ekspertizën e duhur në çështjet e sigurisë, softëare i kontraktuar do të sigurojë kompaninë tuaj dhe do i ofrojë besueshmëri dhe kredibilitet për një periudhë kohe të caktuar.
5.	Përditësimi me teknologjinë e re	Ndryshimet në kërkesën e tregut mund të kërkojnë zgjerimin e biznesit. Hakerët gjithashtu kanë gjetur mënyra të ndryshme të shfrytëzimit të masave të sigurisë të vendosura nga bizneset. Sidoqoftë, në rastin e operimit me një softuer, ju do të merrni raporte javore mbi statusin e biznesit tuaj, duke ju sjellë në vëmendje çdo çështje për të cilën ju duhet të keni kujdes ose duhet të merrni masa.

Masat mbrojtëse që nevojitet të implementohen	
1. Mbro biznesin dhe konsumatorët	Një sulm i suksesshëm, jo vetëm që dëmton biznesin, por ndikon në mënyrën sesi konsumatorët do e shohin kompaninë tuaj dhe në mënyrë direkte zgjedhjen e një kompani alternative me më shumë besueshmëri. Sulmet Kibernetike shkatërrojnë reputacionin e biznesit tuaj. Të gjithë bizneset kanë bazën e tyre të të dhënave, të cilat përfshijnë informacione sensitive, të cilat mund të jenë pre e aksesit të paautorizuar dhe humbjes nëse nuk implementohen kriteret e duhura të Sigurisë Kibernetike. Bizneset që nuk arrijnë të menaxhojnë të dhënat personale që lkrijon dhe përpunon në përputhje me GDPR mund të penalizohen me sanksione rregullatore.
2. Qëndro koherent për sulmet më të reja	Ruajtja e të dhënave personale duhet të jetë një prioritet për biznesetsepse dështimi në implementimin e kritereve dhe normave të Sigurisë Kibernetike dhe Mbrojtjes së të dhënave (GDPR, IASME), vendos klientët në një risk masiv të privatësisë së tyre. Edhe nëse mendon se biznesi juaj është i mbrojtur, sulmet kibernetike janë rritur në numër të konsiderueshëm dhe po bëhen gjithnjë më të sofistikuar duke arritur në disa raste që të sulmojnë sistemet më të avancara të sigurisë.
3. Rrit nivelin e sigurisë kibernetike në rrjetet / sistemet	Duke ndjekur dhe ndërmarrë masat fillestare për të mbrojtur më mirë biznesin, veten dhe klientët, ju krijoni një biznes më të sigurt dhe një imazh të besueshëm për klientët. Krimi kibernetik do të vazhdojë të evolojë, duke zhvilluar kërcënime të reja çdo vit. Për këtë arsye biznesi duhet të vendosë si prioritet kryesor marrjen e masave për të parandaluar sulmet kibernetike. Në ditët e sotme shkalla e evolimit të sulmeve kibernetike, po e tejkalon nivelin e sigurisë që bizneset kanë implementuar. Për këtë arsye siguria kibernetike tani konsiderohet si më e rëndësishme se kurrë për NVM-të. Duhet të jemi të ndërgjegjshëm se një sulm kibernetik ka të bëjë më shumë me pyetjen “Kur” dhe jo “Nëse”.

Më poshtë është paraqitur një model biznesi për një NVM që operon 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.

NVM	EUR
Shpenzimet aktuale	
Shpenzimet aktuale mesatare per nje sulm kibernetik	20.000
Numri i sulmeve per nje vit	0.5
Totali i shpenzimeve per nje vit	**10.000**
Skenari I- Investim i brendshem	
Servera	6.000
Infrastruktura e rrjetit	1.500
Ndertimi i Telefonise VOIP	12.000
Routers dhe Switches	10.000
Firewall	2.000
Software te ndryshem	9.000
Totali	40.500
Mirembajtja	1.000
Skenari II- Shërbimi nga palët të treta	
Kostot e sherbimit	8.000
Kosto indirekte	1.000

Figura 4 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 24 %.

Kthimi nga projekti - NVM	*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	10.000	10.230	10.557	10.874	11.211	11.559	11.917	12.286	12.667	13.060	13.465
Investimi fillestar	(40.500)										
Mirembajtja	(1.000)	(1.023)	(1.056)	(1.087)	(1.121)	(1.156)	(1.192)	(1.229)	(1.267)	(1.306)	(1.346)
Demtim imazhi	(1.000)	(1.023)	(1.056)	(1.087)	(1.121)	(1.156)	(1.192)	(1.229)	(1.267)	(1.306)	(1.346)
Fluksi I lire I parase	**(32.500)**	**8.184**	**8.446**	**8.699**	**8.969**	**9.247**	**9.534**	**9.829**	**10.134**	**10.448**	**10.772**
Kosto e kapitalit te projektit *14,0%*											
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	0,82	0,72	0,63	0,55	0,49	0,43	0,37	0,33	0,29
Vlera e skontuar e fluksit te lire te parase	**(32.500)**	**7.665**	**6.939**	**6.269**	**5.670**	**5.128**	**4.637**	**4.194**	**3.793**	**3.430**	**3.102**
Treques kryesore financiare											
Vlera aktuale neto (NPV)	18.328										
Norma e brendshme e kthimit (IRR)	*24%*										
Periudha e shlyerjes (PBP) ne vite	7										
Flukset e akumuluara	(32.500)	(24.835)	(17.896)	(11.627)	(5.957)	(829)	3.808				
Viti i shlyerjes se investimit	-	-	-	-	-	-	7				

Figura 5 Kthimi nga projekti

Kthimi nga projekti - NVM	*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		10.000	10.230	10.557	10.874	11.211	11.559	11.917	12.286	12.667	13.060	13.465
Kosto e sherbimit		(8.000)	(8.184)	(8.446)	(8.699)	(8.969)	(9.247)	(9.534)	(9.829)	(10.134)	(10.448)	(10.772)
Fluksi I lire I parase		**2.000**	**2.046**	**2.111**	**2.175**	**2.242**	**2.312**	**2.383**	**2.457**	**2.533**	**2.612**	**2.693**
Kosto e kapitalit te projektit	*14,0%*											
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	0,82	0,72	0,63	0,55	0,49	0,43	0,37	0,33	0,29
Vlera e skontuar e fluksit te lire te parase		**2.000**	**1.916**	**1.735**	**1.567**	**1.417**	**1.282**	**1.159**	**1.049**	**948**	**858**	**776**
Treques kryesore financiare												
Vlera aktuale neto (NPV)		14.707										

Figure 6 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.