AKCESK
AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

SIGURIA KIBERNETIKE NË SEKTORIN FINANCIAR

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

API	Application Programming Interface
BaaS	Backend as a Service
DDoS	Distributed denial-of-service
DPI	Deep Packet Inspection
ENISA	Agjencia e Bashkimit Evropian për Sigurinë Kibernetike
HTTPS	Hypertext Transfer Protocol Secure
IT	Teknologjia e Informacionit
TIK	Teknologjia e Informacionit dhe Komunikimit
XSS	Cross Site Scripting
WAF	Web Aplication Firewall
SCADA	Supervisory Control and Data Acquisition

I. Hyrje

Fusha e sigurisë kibernetike ndryshon vazhdimisht me shfaqjen e kërcënimeve të reja. Sektori i Siguria kibernetike është problemi kryesor për çdo organizatë, pavarësisht nga madhësia dhe natyra e industrisë. Edhe pse çdo industri është e kërcënuar nga sulmet kibernetike, sektori financiar, sidomos ai bankar, është më i ndjeshëm ndaj sulmeve të sigurisë për shkak të sensitivitetit të të dhënave që përpunon. Kërcënimet e sigurisë kibernetike ndaj institucioneve bankare rezultojnë në humbje të ndryshme, të cilat përbëjnë një ndikim serioz në stabilitetin ekonomik të tyre, humbjen e besimit të klientëve nga vjedhja e të dhënave dhe ndër të tjera kërcënim për reputacionin e bankës.

Zhvillimet industrial kanë sjellë rreziqe të ndryshme të sigurisë, ndaj sigurimi i aseteve dhe informacionit është sfida kryesore në fushën digjitale. Kërcënimet janë të formave të ndryshme, të jashtme ose të brendshme, në formën e punonjësve të pakujdesshëm, nga mungesa e protokolleve të sigurisë ose firewalls, etj. Ekspertët e sigurisë besojnë se kërcënimet e brendshme paraqesin kërcënim të lartë për organizatat, pavarësisht industrisë ku operojnë, si sektori bankar, mikrofinanciar, tregu i sigurimeve, fintech etj.

II. Rreziqet në sigurinë kibernetike në sektorin financiar[1]

Incidentet e sigurisë kibernetike që prekin firmat financiare, paraqesin rreziqe specifike në financim dhe likuiditet. Më poshtë listohen katër "kanalet" nga të cilat këto rreziqe transmetohen, duke çuar në kriza sistemike.

1. Mungesa e zëvendësueshmërisë (financiare):
Sistemi financiar varet nga disa qendra kryesore, zakonisht firma ose shërbime të caktuara (p.sh. sisteme elektronike tregtare, shkëmbime), që kryejnë një funksion jetësor për të gjithë industrinë. Shembuj të këtyre funksioneve përfshijnë ruajtjen e letrave me vlerë, menaxhimin e kolateralit, konfirmimin dhe kryerjen e tregtisë, të cilat janë të gjitha procese të automatizuara me anë të teknologjisë. Pra, "industria e shërbimeve financiare mbështetet në një infrastrukturë të fuqishme të Teknologjisë së Informacionit dhe Komunikimit (TIK)" për të përfunduar transaksionet ose për të kryer pagesa". Do të ishte e vështirë për zëvendësimin e këtyre institucioneve ose sistemeve, nëse një incident do të ndikonte tek to.

[1]https://www.brookings.edu/research/the-future-of-financial-stability-and-cyber-risk/

2. Humbja e besimit:
Sulmet në mënyrë të përsëritur ndikojnë tek konsumatorët pasi një "vjedhje me shtrirje më të gjerë ... mund të shkaktojë një humbje më të madhe të besimit". Humbja e besimit nuk mund të vijë vetëm nga vjedhja e të dhënave të një konsumatori, por nga një sërë sulmesh si sulme ndaj makinave ATM, dërgimi i emaileve kompromentuese nga bankierët ose shpërndarja e llogarive. Humbja e besimit te konsumatoreve ndikon tek biznesi I subjekteve financiare.

3. Integriteti i të Dhënave:
Cilësia e të dhënave të konsumatorit të ruajtura në sistmet financiare mund të korruptohen nga ndërhyrjet kibernetike, duke bërë që sistemi të ndërpresë punën derisa të rikthehen të dhënat e ruajtura në backup. Riparimi mund të zgjasë më shumë sesa pritej dhe kjo do të shkaktonte humbje të besimit ose ndikime të tjera sistemike, "veçanërisht për tregjet që përpunojnë me porositë e shpejta".

4. Mungesa e Zëvendësueshmërisë (TIK):
Sektori i financave varet nga sistemet dhe infrastruktura TIK. Pjesa më e madhe e ofruesve të shërbimeve cloud (korporata të IT) operojnë me të njëjtat sisteme operative dhe aplikacione dhe varen nga të njëjtat protokolle themelore të Internetit, si TCP / IP ose DNS.
Ndaj nëse ndodh një ndërprerje lokale si pasojë e sulmit kibernetik do të ndërpriten shërbime financiare të një rajoni ose të disa industrive.

Rezultatet e një sondazhi[2] treguan se 95% e organizatave përjetojnë ndërprerje të papritura, prej afro 10% të serverave të tyre, të cilët kanë të paktën një ndërprerje në vit dhe ndërprerja mesatare zgjat nën dy orë. Ndikimet ekonomike të kohës joproduktive janë të mëdha. Një orë e ndërprerjes së aplikimit kushton një mesatare të vlerësuar prej 64,647 $. Pra, ndërsa koha joproduktive është e pashmangshme, ndikimi i saj është i patolerueshëm. Për ta kapërcyer këtë, organizatat duhet kenë një qasje drejt modernizimit për të krijuar më shumë pika rikuperimi, duke minimizuar kohën joproduktive.

III. Statistika të Evropës për sulmet dhe dëmet në sektorin financiar

Në ditët e sotme, industria e shërbimeve financiare në Evropë dhe kudo, është më kritike se kurrë. Shoqërisë i ofrohen shërbimet profesionale të tilla si investimi, huazimi dhe menaxhimi i parave dhe pasurive. Digjitalizimi i shërbimeve financiare është rritur me shpejtësi që nga individët privatë deri tek tregu dhe tregëtia globale, dhe ky fakt është shfrytëzuar nga kriminelët kibernetikë.

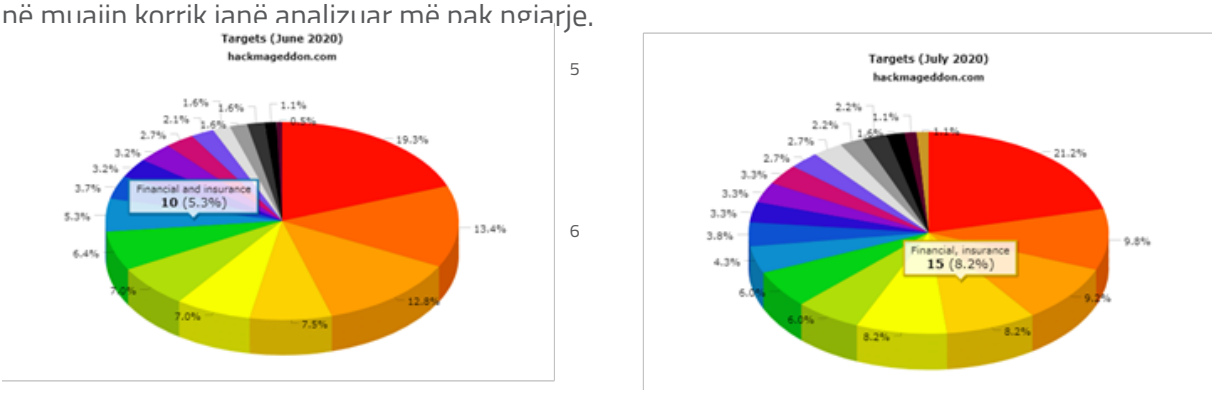
Statistikat Kibernetike në Shërbimet Financiare[3]
Nga anketimet e kryera nga institucione të ndryshme në vitin 2019 janë raportuar të dhënat e mëposhtme:

[2]Data protection trends for financial services. https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/-pdf-7-w-6933.pdf
[3]https://www.finextra.com/blogposting/19411/6-cyber-related-stats-in-financial-services

- 70% nga institucionet financiare e renditën sigurinë kibernetike si prioritet.
- Kostoja e një sulmi kibernetik është më e larta në industrinë bankare, duke arritur 18.3 milion dollarë në vit për çdo kompani.
- 70% e kompanive financiare kanë përjetuar një incident të sigurisë kibernetike gjatë 2019.
- 10% e buxhetit të IT-së është shpenzuar për sigurinë kibernetike.
- 26% e institucioneve financiare pësuan një sulm kibernetik destruktiv. Një rritje prej 160% krahasuar me vitin 2018.

Gjithashtu, në faqen zyrtare të Hackmageddon, në të cilën paraqiten statistika në format grafik për incidente të raportuara të sigurisë së informacionit nga vendet evropiane në muaj specifik, është vënë re një rritje e ndjeshme e sulmeve kibernetike në sektorin financiar.[4]
Në grafikun e mëposhtëm paraqiten statistikat e sulmeve kibernetike në muajin qershor dhe korrik 2020. Në muajin korrik janë analizuar 175 ngjarje, ndërsa në muajin qershor 187 ngjarje.

Sipas grafikut të mëposhtëm përqindja e sulmeve ndaj institucioneve financiare është rritur nga 5.3% në muajin qershor (10 organizata) në 8.2% në muajin korrik 2020 (15 organizata), edhe pse në muajin korrik janë analizuar më pak ngjarje.



5

6

Qershor 2020

Korrik 2020

Figura 1 Sulmet ndaj institucione financiare

Institucionet financiare po përballen me sfida të shumta të lidhura me sigurinë kibernetike
Për shkak të pandemisë së COVID-19 Banka Qendrore Evropiane dhe institucionet e tjera financiare kanë pësuar një rritje të konsiderueshme të sulmeve kibernetike. Ashtu si në sektorët e tjerë, pandemia ka shkaktuar një rritje të papritur dhe të shpejtë të numrit të punonjësve që punojnë nga shtëpia. Gjithashtu, nevoja për digjitalizim të shërbimeve bankare është rritur.

[4]Hackmageddon.com
[5]https://www.hackmageddon.com/2020/09/24/july-2020-cyber-attacks-statistics/
[6]https://www.hackmageddon.com/2020/08/13/june-2020-cyber-attacks-statistics/

Në raportin [7] e ENISA (Agjencia e Bashkimit Evropian për Sigurinë Kibernetike) për periudhën Janar 2019-Prill 2020, paraqiten statistikat të incidenteve sipas sektorëve specifik të raportuara nga vendet anëtare, për të kuptuar dinamikën e evolucionit të kërcënimeve, motivet e kundërshtarëve dhe ekspozimin e pasurive. Në këtë raport jepen trendet e incidenteve në sektorin financiar/bankar/sigurimeve për disa kategori sulmesh:

1. sulmet e aplikacioneve Web;
2. kërcënimi i brendshëm (abuzimi i paqëllimshëm);
3. malware;
4. vjedhja e të dhënave.

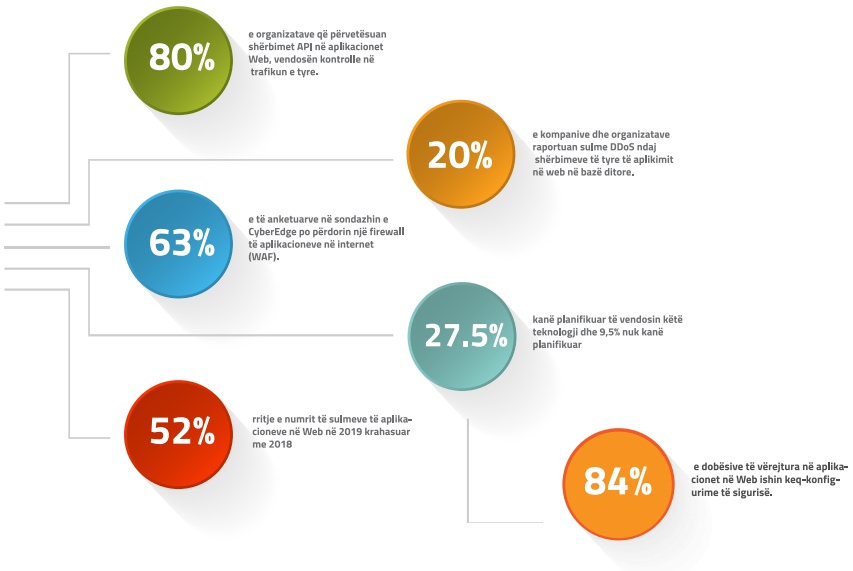
Në vijim paraqiten të dhënat statistikore për secilin nga kategoritë e sulmeve.

III.1.1 Sulmet e aplikacioneve Web[8]

Rritja e kompleksitetit të aplikacioneve dhe shërbimeve Web, krijojnë sfida në sigurinë e tyre ndaj kërcënimeve me motive të ndryshme si dëmtimi financiar ose dëmtimi i reputacionit, vjedhja e informacionit kritik ose personal. Aplikacionet dhe shërbimet në Web varen nga bazat e të dhënave për të ruajtur ose shpërndarë informacionin e kërkuar. Sulmet SQL Injection (SQLi) janë lloji më i njohur i kërcënimeve ndaj shërbimeve të tilla. Një shembull tjetër është sulmi i skriptimit ndër-faqesh (XSS) ku keqpërdoren dobësitë në forma ose funksione të tjera të futjes së të dhënave, të cilat e ridrejtojnë përdoruesin në një faqe tjeter webi keqdashëse.

Ndaj shumë organizata që përdorin aplikacione Web kërkojnë me prioritet marrjen e masave për sigurinë e tyre. Kjo përfshin përvetësimin e shërbimeve të reja si Ndërfaqet e Programimit të Aplikimit (API). API-të, krijojnë sfida të reja për organizatat për sigurinë e aplikacioneve në internet, të tilla si marrjen e më shumë masave parandaluese dhe zbuluese.

Për shembull,



[2]Data protection trends for financial services. https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/-pdf-7-w-6933.pdf
[3]https://www.finextra.com/blogposting/19411/6-cyber-related-stats-in-financial-services

Sipas një studiuesi të sigurisë, sasia e sulmeve të aplikacioneve në Web ishte pothuajse e sheshtë krahasuar me 2018 dhe u rrit ndjeshëm më vonë gjatë vitit.

Të dhëna nga studiuesit e sigurisë kanë raportuar që shumica e sulmeve të aplikacioneve në Web janë të kufizuara në SQLi ose LFi, të treguar në figurën e mëposhtme. LFi është Përfshirja e Skedarit Lokal për të mashtruar aplikacionin në Web për të ekzekutuar skedarin me kod dashakeq në serverin e internetit.

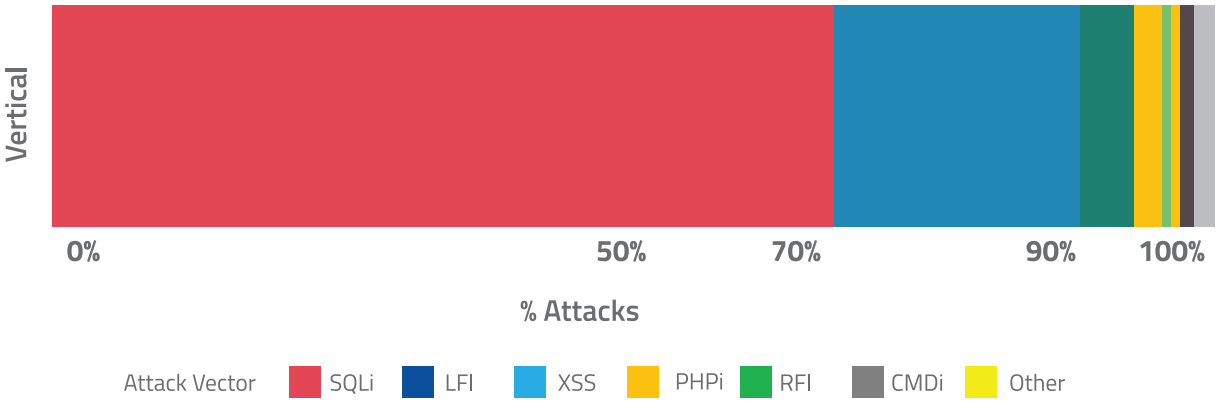


Figura 2 Vektorët e sulmeve, ENISA

III.1.2 Kërcënimi i brendshëm (abuzimi i paqëllimshëm)[9]

Kërcënimi i brendshëm është një veprim që mund të rezultojë në një incident, i kryer nga dikush ose një grup njerëzish që kanë lidhje ose që punojnë për viktimën e mundshme.

Janë pesë lloje të kërcënimit të brendshëm sipas qëllimit dhe objektivave të tyre:

1. punëtorët e pakujdesshëm të cilët keqpërdorin të dhëna, thyejnë politikat e përdorimit të aplikacioneve dhe instalojnë aplikacione të paautorizuara;
2. agjentët e brendshëm që vjedhin informacione për personat e jashtëm;
3. punonjësit e pakënaqur që kërkojnë të dëmtojnë organizatën e tyre;
4. persona të brendshëm që përdorin privilegjet ekzistuese me qëllim të keq për të vjedhur informacione për përfitime personale;
5. palët e treta që rrezikojnë sigurinë përmes inteligjencës, keqpërdorimit ose aksesit keqdashës në ose përdorimin e një aseti.

Tipi më i njohur është (i ashtuquajturi 'keqpërdorim i privilegjit') i cili ndodh kur personat e jashtëm bashkëpunojnë me aktorë të brendshëm për të fituar akses të paaprovuar në asete. Personat e brendshëm mund të shkaktojnë dëme pa dashje nga pakujdesia ose nga mungesa

[9]https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-insider-threat

e njohurive. Meqenëse personat e brendshëm shpesh gëzojnë besim dhe privilegje, njohuri të politikave organizative, të proceseve dhe procedurave të organizatës, është e vështirë të bëhet dallimi i aksesit të tyre në aplikacione në të dhëna dhe sisteme, nëse është i ligjshëm, dashakeq apo i gabuar.

Të pesë llojet e kërcënimeve të brendshme duhet të studiohen vazhdimisht, pasi duhet të përcaktohet strategjia e organizatës për sigurinë dhe mbrojtjen e të dhënave.

- 65% e ndikimit nga kërcënimet e brendshme përfshijnë dëmtimin e reputacionit dhe financave të organizatës.
- 88% e organizatave të anketuara pranojnë që kërcënimet e brendshme janë shkak për tu alarmuar.
- 11,45 milion € është kostoja mesatare vjetore e incidenteve të sigurisë kibernetike të shkaktuara nga një person i brendshëm në organizatë.

Sulmuesit ofrojnë shuma të mëdha parash për personat e brendshëm. Pagesa e personave të brendshëm ndryshon, nga pozicioni i tij në kompani, nga vetë kompania, lloji dhe kompleksiteti i shërbimit që kërkohet, lloji i të dhënave që do të merren dhe niveli i sigurisë në kompani.

Disa nga mënyrat se si sulmuesit rekrutojnë persona të brendshëm janë:

- postimi i një oferte në forume dhe ofrimi i një shpërblimi për informacione të caktuara,
- maskimi i veprimeve të tyre në mënyrë që punonjësit të mos e kuptojnë se po veprojnë në mënyrë të paligjshme, duke zbuluar informacione personale ose duke u përfshirë atë në një aktivitet të brendshëm,
- shantazhi.

Një ish-inxhinier softueri që punonte në një ofrues të shërbimit cloud shfrytëzoi një firewall të konfiguruar gabimisht të aplikacioneve në Web dhe aksesoi më shumë se 100 milion llogari të klientëve dhe rekordet e kartave të kreditit. Kompania e ofrimit të shërbimit cloud që atëherë e ka rregulluar cënueshmërinë dhe ka deklaruar se 'asnjë numër llogarie të kartavë të kreditit ose kredencialet e loginit të tyre nuk janë kompromentuar'.

Ky rast i kërcënimit të brendshëm është interesant sepse ish-punonjësi i kthyer në haker nuk ishte i shqetësuar për fshehjen e identitetit. Hakeri ndau metodën e hakerimit me kolegët nga Capital One në chat.

Hakeri gjithashtu postoi informacionin në GitHub (duke përdorur emrin e plotë) dhe u mburr në mediat sociale për këtë. Kjo lloj sjelljeje psikologët e quajnë "përhapje"'përmes së cilës personat e brendshëm që komplotojnë për të dëmtuar organizatën zbulojnë planet e tyre. Capital One[10] pret që shkelja të kushtojë deri në 150 milion USD (rreth 127 milion €).
Fushat e biznesit të ndikuara nga incidentet e kërcënimit të brendshëm.

[10]capitalone.com

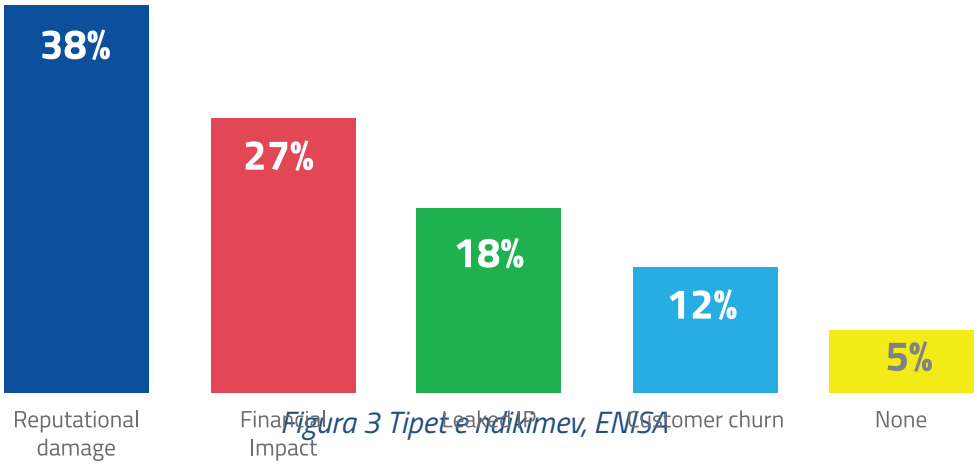


Figura 3 Tipet e ndikimev, ENISA

Sic shihet në grafik sektori financiar preket në 27% nga incidentet e kërcënimit të brendshëm.

III.1.3 Malware[11]

Malware është lloji më i zakonshëm i sulmit kibernetik në formën e softuerit dashakeq. Familjet e malware përfshijnë kriptominer, viruse, ransomware, worms dhe spyware. Objektivat e tyre të përbashkëta janë vjedhja e informacionit ose identitetit, spiunazhi dhe ndërprerja e shërbimit.

Gjatë vitit 2019, kriptominuesit ishin një nga familjet më të përhapura të malware, duke rezultuar në kosto të larta të IT, rritje të konsumit të energjisë elektrike dhe ulje të produktivitetit të punonjësve. Ransomware pati një rritje të lehtë në 2019 krahasuar me 2018, megjithëse mbetet ende në fund të listës së llojeve të malware.[12]

Edhe pse zbulimet globale të sulmeve kanë mbetur në nivelet e vitit të kaluar, ka pasur një zhvendosje të dukshme të sulmeve nga konsumatorët tek bizneset.

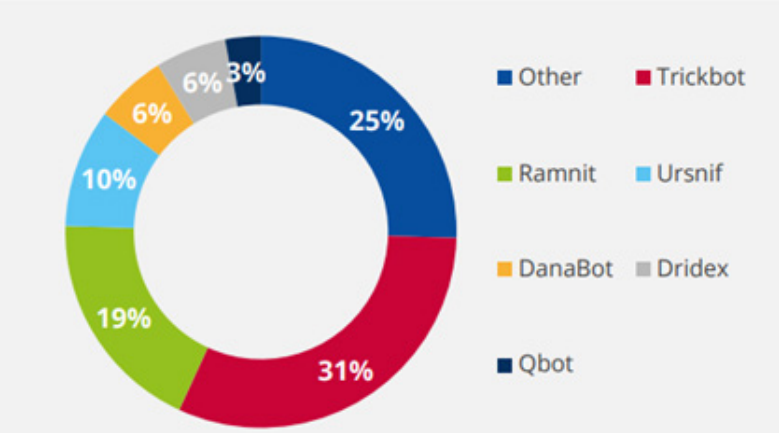
- 400.000_zbulime të spyware dhe adware të para-instaluar në pajisjet mobile.
- 71% e organizatave përjetuan veprimtari malware që përhapen nga një punonjës te tjetri.
- 46,5% i të gjithë malware të mesazheve të gjetur të postës elektronike janë në llojin e skedarit '.docx'.
- 50% rritje të malware të krijuar për të vjedhur të dhëna personale.

- 67% e malware u përhapën përmes lidhjeve të koduara HTTPS.

Edhe pse zbulimet e malware në mbarë botën ishin në të njëjtat nivele si në 2018, u vu re një rritje prej 13% të sulmeve ndaj bizneseve ku ndër sektorët më të prekur ishin shërbimet, arsimi dhe shitja me pakicë. U vlerësua se mbi një e treta e sulmeve malware bankare në

[11]https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-malware
[12]ENISA

2019 shënjestruan përdoruesit e korporatave, me synimin për të kompromentuar burimet financiare të kompanisë. Pesë llojet kryesore të malware që synojnë bizneset ishin: Trojan. Emotet, Adware.InstallCore, HackTool.WinActivator, Riskware.BitCoinMiner dhe Virus.Renamer. Sulmet e Ransomware që synojnë sektorin publik u rritën në 2019 për shkak të mundësisë së tij për të paguar shpërblime më të larta. Meqë kriminelët kibernetikë synojnë shënjestra me vlera monetare të mëdha, krijuan lloje të reja të malware për t'u përhapur brenda rrjetit të korporatave sesa përmes internetit.



Global banking malware detections in 2019. Source: CheckPoint[3]

Në gjysmën e parë të vitit 2019 u rrit me 50% numri i aplikacioneve celular të dizenjnuar për të vjedhur të dhëna kredenciale dhe fonde nga llogaritë bankare të viktimave. Sulmuesit përdorën teknika të mashtrimit për të marrë kredenciale bankare, duke shfaqur një faqe të rreme që imitonte faqen login të bankës ose duke prezantuar aplikacione celular të rreme që ngjajnë me aplikacionet origjinale bankare.

Në vitin 2019, kriminelët kibernetikë u bënë më kreativë, si në rastin e Trojan-Banker.AndroidOS. Gustuff.a, i cili ishte në gjendje të kontrollonte një aplikacion të ligjshëm bankar duke keqpërdorur funksionet e aksesit të sistemit operativ për të automatizuar transaksione të dëmshme. Një risi që u zbulua në 2019 ishte aftësia e një malware për të përdorur sensorë lëvizjeje, i cili aktivizohej vetëm kur smartphone ishte në lëvizje, siç u përdor nga trojani bankar Anubis duke u përpjekur për të gjetur një ambient me sandbox (një pjesë të softuerit) që ka qasje vetëm në disa burime, programe dhe skedarë brenda një sistemi kompjuterik.).
Malware_ë bankarë më popullor gjatë vitit 2019 ishin Asacub (44,4%), Svpeng (22,4%), Agjent (19,1%), Faketoken (12%) dhe Hqwar (3,8%). [13]

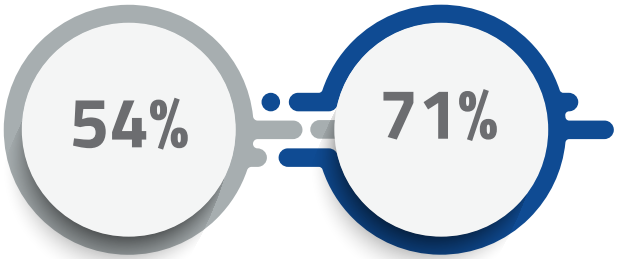
III.1.4 Vjedhja e të dhënave[14]

Thyerja e të dhënave (data breaches) është një lloj incidenti i sigurisë kibernetike në të cilin informacioni (ose një pjesë e një sistemi informacioni) aksesohet pa autorizimin e duhur, zakonisht me qëllim të keq, duke çuar në humbje të mundshme ose keqpërdorim të këtij informacioni. Ai gjithashtu përfshin 'gabimin njerëzor' e cila ndodh gjatë konfigurimit dhe

[13]ENISA
[14]https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl2020-data-breach

instalimit të shërbimeve dhe sistemeve të caktuara, dhe mund të rezultojë në ekspozim të paqëllimtë të të dhënave. Në shumë raste, kompanitë ose organizatat nuk janë në dijeni të një thyerje të të dhënave që ndodh në mjedisin e tyre si pasojë e sofistikimit të sulmit dhe ndonjëherë nga mungesa e dukshmërisë ose mos klasifikimi në sistemin e tyre të informacionit. Bazuar në kërkimet, duhen afërsisht 206 ditë për të identifikuar një thyerje të të dhënave në një organizatë.Kështu që duhet shumë kohë, për të riparuar dhe rikuperuar të dhënat për t'u kthyer ato në gjëndjen normale.Pavarësisht nga të gjitha rreziqet e hasura, organizatat mbajnë shumicën e të dhënave duke përdorur infrastrukturën e magazinimit në re dhe pajisje komplekse të brendshme.

Këto mjedise janë më të ekspozuara ndaj rreziqeve të reja dhe të ndryshme, në përputhje me ndjeshmërinë e informacionit të ruajtur. Nuk është për t'u habitur që, numri i shkeljeve të të dhënave u rrit në 2019 dhe 2020. Gjetjet e reja kanë nxjerrë që ndikimi nuk ndihet menjëherë sapo zbulohen shkelje e të dhënave - impakti financiar mund të vazhdojë për më shumë se 2 vjet pas fillimit të incidentit.



rritje në numrin e përgjithshëm të shkeljeve nga mesi i vitit 2019 krahasuar me 2018.

e shkeljeve të të dhënave ishin për arsye financiare.

Një raport i ENISA përmend që mashtrimi është në krye të listës së kontribuesve kryesorë të thyerjeve të të dhënave. Raporti gjithashtu përmend që posta elektronike është mënyra kryesore e shpërndarjes së malware - 70% e shkeljeve të të dhënave ekspozohen nga postat elektronike. Edhe pse emri i përdoruesit dhe fjalëkalimet (d.m.th. kredencialet) ndryshohen më lehtët në krahasim me detajet personale (d.m.th. data e lindjes), thyerja e të dhënave ndodh kryesisht tek këto të dhëna.

Eshtë e vështirë të rritësh sigurinë në mjedisin në re (cloud) sepse duhet të ruhet fleksibiliteti që ka kjo teknologji në infrastrukturë dhe burime.
Një keqkonfigurim mund të rezultojë në ekspozimin e të gjithë të dhënave sensitive të bazës së të dhënave. Një studiues i sigurisë beson se shumica e thyerjeve të të dhënave në cloud janë rezultat i konfigurimit të gabuar të cilat kryesisht janë të paqëllimta. Disa shembuj, ndër shumë të tjerë janë Netflix, Ford dhe TD Bank.

Megjithatë thyerjet e të dhënave që rezultojnë nga përpjekje dashakeqe ende kushtojnë më shumë se shkeljet e shkaktuara nga defektet e sistemit ose gabimet njerëzore dhe arrijnë në një kosto të konsiderueshme mesatarisht 3,24 milion USD (rreth 2,74 milion €).
Kostoja e thyerjeve të të dhënave për ndërmarrjet ose organizatat e mëdha me më shumë se 25.000 të punësuar është 204 dollarë amerikanë (rreth 173 €) për punonjës. Shuma totale është rreth 5,11 milion USD (rreth 4,33 milion €). Ndërsa për ndërmarrjet e vogla (500-1.000 punonjës) kostoja mesatare është rreth 3.533 dollarë amerikanë (rreth 3.000 €) për punonjës. Kostoja totale është rreth 2,65 milion USD (afro 2,24 milion €) për bizneset e vogla, sipas ENISA.

Aktorët e kërcënimit të jashtëm janë shkaku kryesor i thyerjes së të dhënave, dhe mund të përfshijë aktivitete të tilla si botnet. Përfitimi financiar është motivi kryesor për thyerjen e të dhënave që bëhen nga këto grupe aktorësh. Spiunazhi gjithashtu është një nga motivet kryesore prapa thyerjeve të të dhënave, por jo aq sa përfitimet personale ose financiare.

III. 2 Çfarë do të ndodh në të ardhmen e afërt?

Në tabelën e mëposhtme jepen statistika të thyerjes së të dhënave sipas sektorit dhe madhësisë së organizatës. Në tablë vihet re që sektori financial zë vendin e tretë ndër sektorët e tjerë me më shumë thyerje të të dhënave, me 207 thyerje të të dhënave, ku 26 prej tyre kanë ndodhur në organizata të vogla dhe 19 në organizata të mëdha.

Incidents	Breaches	Small	Large	Unknown
Accommodation	61	34	7	20
Administrative	17	6	6	5
Agriculture	2	2	0	0
Construction	11	7	3	1
Education	99	14	8	77
Entertainment	10	2	3	5
Finance	207	26	19	162
Healthcare	304	29	25	250
Information	155	20	18	117
Management	2	1	1	0
Manufacturing	87	10	22	55
Minning	15	2	5	8
Other Services	54	6	5	43
Professional	157	34	10	113
Public	330	17	83	230
Real Estate	14	6	3	5
Retail	139	46	19	74
Trade	16	4	8	4
Transportation	36	3	9	24
Utilities	8	2	0	6
Unknown	289	0	109	180
Total	2.013	271	363	1.379

Figura 5 Statistika sipas sektorëve, Verizon 2019

IV. Siguria kibernetike në sektorin financiar në Shqipëri

Autoriteti Kombëtar i Certifikimit Elektronik dhe i Sigurisë Kompjuterike për të vlerësuar performancën e sigurisë të kompanive që administrojnë Infrastruktura kritike dhe të rëndësishme të informacionit përdor platformën BitSight.

Të dhënat e Sigurisë BitSight përshkruajnë sjelljen e sigurisë kibernetike të një kompanie, shërben si matëse e rrezikut dhe paraqet sesi kompanitë menaxhojnë rrezikun e sigurisë duke përdorur të dhënat, për të vlerësuar efektivitetin e sigurisë së një kompanie. Kategoria e rrezikut të Sistemeve të Kompromentuara tregon praninë e malware ose softuerit të padëshiruar, e cila tregon që kontrolli i sigurisë është i pamjaftueshëm. Kategoria e rrezikut të kujdesit (Diligence) vlerëson hapat që ka marrë një ndërmarrje për të parandaluar sulmet, zbatimin e praktikës më të mirë dhe zvogëlimin e rrezikut (p.sh. konfigurimet e serverit) për të përcaktuar nëse praktikat e sigurisë së një organizate janë ndër praktikat më të mira. Kategoria e rrezikut e Sjelljes së Përdoruesit vlerëson aktivitetin e punonjësve, të tilla si shkëmbimi i skedarëve dhe ripërdorimi i fjalëkalimeve. Këto lloj aktivitetesh mund të fusin malware në një organizatë ose të rezultojnë në shkelje të të dhënave.
Për periudhën nëntor 2019-nëntor 2020 nga platforma Bitsight u nxorrën të dhënat e sigurisë së mëposhtme të kompanive financiare, përkatësisht bankar, mikrofinanciar, sigurime, tatimet. Rangu i të dhënave të sigurisë kategorizohet në bazik, me vlerën e sigurisë së të dhënave në intervalin (240-640), mesatar (640-760), avancuar (900-740).

Nga 12 kompani bankare asnjë prej tyre nuk e ka rangun e të dhënave të sigurisë në nivelin bazik.

- 3 prej tyre e kanë rangun e të dhënave të sigurisë në nivel mesatar (mesatarisht 676). 9 prej tyre e kanë rangun e të dhënave të sigurisë në nivel të avancuar (mestarisht 735).
- 3 kompani të mikrofinancës e kanë rangun e të dhënave të sigurisë në nivelin e avancuar (mestarisht 740).
- 6 kompani të sigurimeve e kanë rangun e të dhënave të sigurisë në nivelin mesatar (mestarisht 660).
- 2 kompani të tatimeve kanë rangun e të dhënave të sigurisë në nivelin mesatar (mestarisht 680).

Sipas Bitsight, për sektorin financiar 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	71.4 %	66.7 %	-7 %
CVE- 2020 - 3452	28.6 %	33.3 %	+17 %
FREAK	14.3 %	16.7%	+17 %

Figura 6 Vulnerabilitetet kryesore, Bitsight

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 nivelin më të ulët të sigurisë së sektorit financiar.

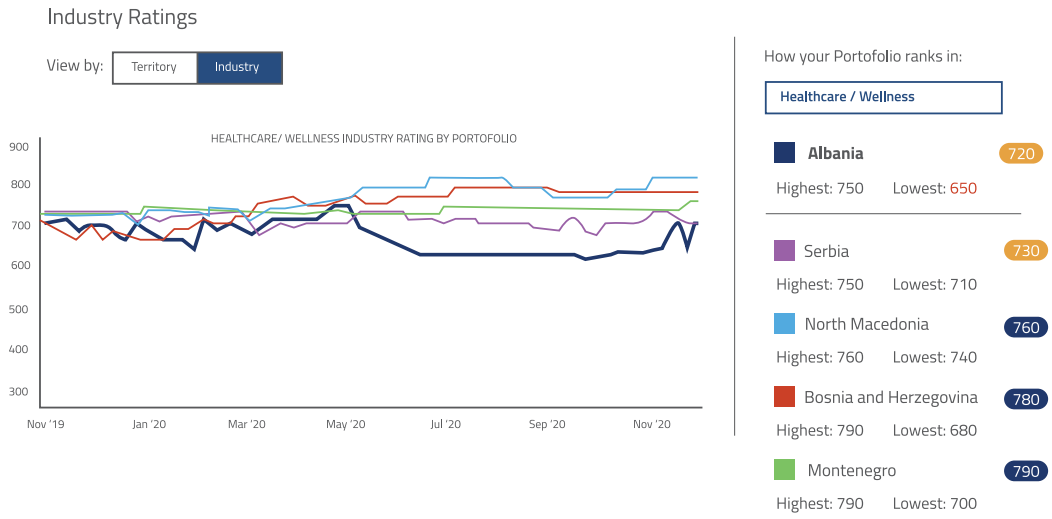


Figura 7 Rankimi rajonal, Bitsight

Ekipet e përgjigjet ndaj incidenteve kibernetike në sektorin e shërbimeve financiare po trajtojnë kërkesa më të shumta në numër për shkak të pandemisë globale COVID-19. Puna në distancë dhe shtimi i numrit të shërbimeve që ofrohen online, ka sjellë rritjen e kërcënimeve, përfshirë kërcënimet e brenshme.

V. Benefitet e investimit në sigurinë kibernetike per sektorin financiar

Edhe pse sulmet kibernetike ndaj institucioneve dhe infrastrukturave financiare janë bërë më të shpeshta dhe të sofistikuara, kanë nxitur investime gjithnjë e më të mëdha në sigurisë dhe rritjen e përqendrimit për të lehtësuar dhe administruar rrezikun kibernetik. Paralelisht me këto përpjekje, sektori financiar dhe qeveritë kombëtare kanë punuar së bashku për të përmirësuar ripërtëritjen dhe stabilitetin e përgjithshëm të këtij sektori. Në shumicën e vendeve të zhvilluara, dhe në disa vende në zhvillim, lojtarët e sektorit privat bashkohen për të ndarë informacione mbi kërcënimet dhe të luftojnë së bashku mashtrimet financiare dhe krimin kibernetik. Një zhvillim tjetër është rritja e produktet të sigurimeve kibernetike midis kompanive të mëdha shumëkombëshe të sigurimeve. Bashkëpunimi ndër-sektorial dhe publik-privat, shihet si një domosdoshmëri për të luftuar krimin kibernetik dhe për lehtësimin e efektive të rreziqeve. Në shumicën e vendeve, ekziston një formë e dialogut publik-privat në sektorët financiarë dhe telekomunikacion.

V1 Organizimi i mbrotjes kibernetike: insource apo outsource?

Modernizimi i backup - ndihmon në menaxhimin e kostove rregullatore dhe kapitale

Modernizimi i backup çliron burimet e angazhuara për mbrojtjen e të dhënave dhe i përqëndron ato në projekte thelbësore të inovacionit për zhvillimin e bizneseve. Përmes modernizimit të Backup, organizatat ulin koston e backup dhe mbrojtjes së të dhënave me 50% dhe arrijnë një rritje prej 55% të efikasitetit në rikuperimit të të dhënave. Me anë të modernizimit të operacioneve dhe proceseve, organizatat mund të kenë një ndikim të rëndësishëm në shërbimin ndaj klientit, uljen e kostos dhe të detyrave të punonjësve. Më shumë se 98% e organizatave të anketuara ishin në proces ose në planifikim e sipër për transformim dixhital; megjithatë, shumë ishin përballur me sfida në arritjen e rezultateve të dëshiruara.

Sfidat e Transformimit Dixhital- Efekti i cloud në modernizimin e backup

Sfidat kryesore për organizatat e shërbimeve financiare që ndjekin transformimin dixhital ishin mungesa e aftësive të stafit të IT (47%) dhe varësia nga sistemet e trashëguara (42%).
Këto pengesa shkaktonin një mungesë të konsiderueshme të kohës dhe buxhetit.

Prandaj, organizatat e shërbimeve financiare po përdorin shërbime në cloud (ruajtje dhe / ose BaaS) për rreth gjysmën e bakup të tyre. Kur u pyetën se cila do të jetë zgjidhja e tyre kryesore e backup-ve deri në vitin 2022, të anketuarit shpjeguan se planifikojnë që backupet të menaxhuar nga BaaS të përbëjnë 41% të rezervimeve, ndërsa rezervat e vetë-menaxhuara që përdorin shërbime cloud do të përbëjnë 34%. Pra, në vitin 2022, organizatat financiare parashikojnë përdorimin e shërbimeve të bazuara në cloud për 75% të backup të tyre si një nga investimet në sigurinë kibernetike.

V.2 Model Biznesi për Investimin Në Siguri Kibernetike

Bazuar në të dhënat e marra me metoda primare dhe sekondare, ka një rast biznesi për të investuar në sistemet e sigurisë kibernetike për sektorin financiar, jo vetëm për bankat, por edhe për nënsektorë të tjerë si mikrofinanca, sigurimet, fintech etj. Vetëm këto investime ofrojnë siguri prë vazhdimësinë e biznesit të tyre.

Më poshtë është paraqitur një model biznesi për një organizatë që vepron në sektorin financiar 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.

Finance	**EUR**
Shpenzimet aktuale	
Shpenzimet aktuale mesatare per nje sulm kibernetik	30.000
Numri i sulmeve per nje vit	0.5
Totali i shpenzimeve per nje vit	**15.000**
Skenari I- Investim i brendshem	
Servera	12.000
Infrastruktura e rrjetit	7.000
Ndertimi i Telefonise VOIP	15.000
Routers dhe Switches	7.000
Firewall	9.000
Software te ndryshem	10.000
Totali	60.000
Mirembajtja	5.000
Skenari II	
Kostot e sherbimit	14.000
Kosto indirekte	2.000

Figura 8 Business Case, Perpunim I Autoreve

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 12 %.

Kthimi nga projekti - FINANCE	*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	(60.000)										
Mirembajtja	(5.000)	(5.115)	(5.279)	(5.437)	(5.606)	(5.779)	(5.959)	(6.143)	(6.334)	(6.530)	(6.732)
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	**(52.000)**	**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 *9,0%*											
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	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Vlera e skontuar e fluksit te lire te parase	**(52.000)**	**8.184**	**8.446**	**8.699**	**8.969**	**9.247**	**9.534**	**9.829**	**10.134**	**10.448**	**10.772**
Tregues kryesore financiare											
Vlera aktuale neto (NPV)	42.262										
Norma e brendshme e kthim it (IRR)	*12%*										
Periudha e shlyerjes (PBP) ne vite	7										
Fluksete akumuluara	(52.000)	(43.816)	(35.370)	(26.671)	(17.702)	(8.455)	1.079				
Viti i shlyerjes se investim it	-	-	-	-	-	-	7				

Figura 9 Kthimi nga projekti

Kthimi nga projekti - FINANCE	*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 sherbimit	(14.000)	(14.322)	(14.780)	(15.224)	(15.696)	(16.182)	(16.684)	(17.201)	(17.734)	(18.284)	(18.851)
Fluksi I lire I parase	**1.000**	**1.023**	**1.056**	**1.087**	**1.121**	**1.156**	**1.192**	**1.229**	**1.267**	**1.306**	**1.346**
Kosto e kapitalit te projektit *9,0%*											
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	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Vlera e skontuar e fluksit te lire te parase	**1.000**	**1.023**	**1.056**	**1.087**	**1.121**	**1.156**	**1.192**	**1.229**	**1.267**	**1.306**	**1.346**
Tregues kryesore financiare											
Vlera aktuale neto (NPV)	12.783										

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 që duhet të aplikohen

Si pasojë e rezultateve nga sulmet e sigurisë kibernetike apo për shkak të rregulloreve të reja, institucionet financiare duhet të rivlerësojnë sjelljen e tyre të sigurisë dhe të bëjnë çdo përpjekje për të zbatuar kontrolle të forta sigurie në mënyrë që të ruajnë informacionin e ndjeshëm, të ruajnë pajtueshmërinë me ligjet dhe rregulloret, dhe të menaxhojnë rrezikun.
Më poshtë listohen disa masa mbrojtëse për sulmet e aplikacioneve Web, për kërcënimin e brendshëm, dhe për vjedhjen e të dhënave.

Masat mbrojtëse për sulmet e aplikacioneve Web

1. Duhen përdorur teknikat të validimit dhe izolimit të inputit për tipet e sulmeve të injektimit.
2. Duhen implementuar firewall për aplikacionet në Web si masë parandaluese dhe mbrojtëse (e njohur si patching virtual).
3. Për API-të e aplikacioneve në internet:
   - Duhen enkriptuar komunikimet dhe lidhjet API
   - Duhen siguruar mekanizmat e duhur të autentifikimit dhe nivelet e autorizimit.
4. Duhen përfshirë procese të sigurisë së aplikacionit gjatë zhvillimit të aplikacionit dhe në ciklin jetësor të mirëmbajtjes.
5. Të kufizohet aksesi në trafikun inbound vetëm për shërbimet e kërkuara.
6. Duhet bërë menaxhimi i trafikut dhe bandwidth_it.
7. Duhen kryer vlerësime të cënueshmërisë dhe rrezikut para dhe gjatë zhvillimi të aplikacionit të Webit.
8. Duhen kryer penteste gjatë implementimit dhe shpërndarjes (deployment) së aplikacioneve web.

Masat mbrojtëse për kërcënimin e brendshëm (abuzimi i paqëllimshëm)

1. Duhet përdorur një teknologji e thellë të inspektimit të paketave (DPI) për zbulimin e anomalive e cila u jep përdoruesve industriale një platformë të besuar për monitorimin e rrjedhës dhe kontrollit të proceseve dhe për mbrojtjen nga kërcënimet e jashtme. Në të njëjtën kohë, zvogëlon rrezikun e ndërhyrjeve të 'avancuara' nga inxhinierë të brëndshëm, nga operatorët SCADA ose nga personel të tjerë të brendshëm me akses të drejtpërdrejtë në sisteme.

2. Të hartohet një plan kundërmasash të kërcënimit të brendshëm në strategjinë dhe politikat e përgjithshme të sigurisë. Ky plan të përfshijë një kornizë të menaxhimit të rrezikut, planin e vazhdimësisë së biznesit, programin e rikuperimit të katastrofës, politikat e menaxhimit financiar dhe të kontabilitetit, dhe menaxhimin ligjor dhe rregullator.
3. Të ndërtohet një program sigurie që konsiston në:
   a. kryerjen e aktiviteteve të gjuetisë së kërcënimeve,
   b. kryerjen e skanimit të dobësive dhe penteste,
   c. zbatimin e masave të sigurisë së personelit,

d. përdorimin e masave të sigurisë fizike,
e. zbatimin e zgjidhjeve të sigurisë së rrjetit,
f. zbatimin e masave të sigurisë së të dhënave,
g. zbatimi imasave tëidentitetit dhe aksesimit,
h. implementimi i kapaciteteve të menaxhimit të incidenteve,
i. mbajtja e shërbimeve dixhitale forensic dhe përdorimi i metodave të Inteligjencës artificiale (AI) për të parandaluar sulmet e brendshme.

4. Të hartohet një politikë sigurie rreth kërcënimeve të brendshme, bazuar në vetëdijen e përdoruesit, i cili është një nga kontrollet më efektive për këtë lloj kërcënimi kibernetik.

5. Duhen zbatuar kontrolle të fuqishme teknike. Masat tradicionale të sigurisë përqendrohen në kërcënimet e jashtme, të cilat nuk janë efikase në identifikimin e rreziqeve të brendshme që vijnë nga brenda organizatës. Për të mbrojtur aktivet, duhen zbatuar mjete të tilla si parandalimi i humbjes së të dhënave (DLP- data loss prevention) për të parandaluar marrjen e të dhënave nga persona të jashtëm.

Masat mbrojtëse për Malware

1. Duhet implementuar kontrolli për malware për të gjitha kanalet hyrëse / dalëse, duke përfshirë postën elektronike, rrjetin, sistemet e aplikimit dhe web në të gjitha platformat (d.m.th. serverat, infrastruktura e rrjetit, kompjuterët personalë dhe pajisjet mobile).
2. Duhet kontrolluar trafiku SSL / TLS duke lejuar që firewall të dekriptojë atë që transmetohet në dhe atë që merret nga faqet e internetit, komunikimet me email dhe aplikacionet mobile.
3. Duhen përdorur mjetet e disponueshme për analizën e malware për marrjen e informacionit për malware dhe zvogëlimin e ndikimit të tij.
4. Duhen zhvilluar politika sigurie që specifikojnë proceset që duhen ndjekur në rast infektimi.
5. Duhet kuptuar kapaciteti i mjeteve të ndryshme të sigurisë dhe të zhvillohen zgjidhje të reja të sigurisë. Të identifikohen boshllëqet dhe të zbatohet parimi i mbrojtjes në thellësi
6. Të bëhet filtrimi i email (ose filtrimi i spam) për emailet dashakeq dhe të hiqen bashkëngjitjet e ekzekutueshme.
7. Të monitorohen rregullisht rezultatet e testeve të antivirusit.
8. Duhen monitoruar log_et duke përdorur menaxhimin e incidenteve të sigurisë dhe të ngjarjeve (SIEM-security incident and event management).
9. Duhet caktivizuar ose duhet kufizuar hyrja në funksionet PowerShell.

Masat mbrojtëse për vjedhjen e të dhënave

1. Duhet investuar në mjete hibride
të sigurisë së të dhënave që funksionojnë në modele të përgjegjësisë së përbashkët për mjediset e bazuara në re (cloud).
2. Duhet krijuar dhe mirëmbajtur një plan ndërgjegjësimi për sigurinë kibernetike. Duhen bërë skenarë trainimi dhe simulimi për identifikimin e social engineering dhe fushatave të phishing për stafin.
3. Duhet krijuar një ekip të reagimit ndaj incidenteve dhe të vlerësohen shpesh planet e përgjigjes ndaj incidenteve.
4. Duhet identifikuar dhe klasifikuar të dhënat sensitive/personale dhe të aplikohen

masa për kriptimin e të dhënave të tilla gjatë transmetimi dhe kur janë në ruajtje. Pra, duhet implementuar masa parandaluese të humbjes së të dhënave.

5. Duhen rritur investimet në mjetet e zbulimit, të paralajmërimit dhe në kapacitetin për t'iu përgjigjur një shkelje të të dhënave.
6. Duhet zhvilluar dhe krijuar politika të forta që kërkojnë zbatimin e fjalëkalimeve të forta (menaxhim fjalëkalimesh).
7. Duhet investuar që të krijohen politika dhe plane për t'u angazhuar me ekipet qeveritare dhe ekipet të menaxhimit të rrezikut.