AKCESK
AUTORITETI KOMBËTAR PËR
CERTIFIKIMIN ELEKTRONIK
DHE SIGURINË KIBERNETIKE

SIGURIA KIBERNETIKE NË SHËNDETËSI

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

PHI	Protected Health Information
CT	Computed Tomography
MRI	Magnetic Resonanc Imaging
HIPAA	Health Insurance Portability and Accountability Act
DKIM	DomainKeys Identified Mail
SPF	Sender Policy Framework
GDP	Gross Domestic Product
APT	Advanced Persisten Threat
PII	Personally Identifiable Information
IoT	Internet of Things

I. Hyrje

Fusha e sigurisë kibernetike ndryshon vazhdimisht me shfaqjen e kërcënimeve të reja. Sektori i kujdesit shëndetësor ofron shërbime kritike për jetën, ndërkohë që sulmuesit kibernetik kërkojnë të shfrytëzojnë dobësitë e tij. Industria shëndetësore është një ndër objektivët e sigurisë kibernetike, duke ekspozuar miliona persona në të gjithë botën ndaj kërcënimeve kibernetike. Spitalet, mjekët, kompanitë e sigurimeve etj, janë objektiva kryesorë për hakerat për shkak të informacionit të vlefshëm shëndetësor (Protected Health Information - PHI) që ata ruajnë dhe rolit jetësor që ata luajnë në infrastrukturën kritike të vendit ku ndodhen.

Kur ndodh një sulm kibernetik, pasojat shtrihen përtej humbjeve financiare dhe reputacionit. PHI është i vlefshëm për hakerat dhe ndryshe nga format e tjera të të dhënave, është unik për secilin individ dhe nuk mund të zëvendësohet. Sulmet kibernetike mund të përvetësojnë sistemet kompjuterike dhe të kufizojnë aksesin në të dhëna kritike, të mbyllin sistemet dhe pajisjet e kujdesit shëndetësor dhe madje të shtojnë tumore në skanimet CT dhe MRI.
Pavarësisht rregulloreve si HIPAA të dedikuara për sektorin shëndetësor, zbatimi i masave të sigurisë ka ende nevojë për përmirësim, siç tregohet nga lista e gjerë në "Wall of shame" [1]

89 % e organizatave të kujdesit shëndetësor kanë pasur shkelje të të dhënave në dy vitet e fundit dhe sektori shëndetësor ishte industria kryesore për sulme kibernetike dhe shkelje të të dhënave në 2018. I njëjti trend vijoi në vitin 2019. Por përgjatë 2020[2] transformimi digjital në sektorin e kujdesit shëndetësor dhe pandemia e COVID-19 po krijon një hapësirë të riskuar në lidhje me sigurinë kibernetike. Të dhënat e bazuara në cloud janë në rritje, pasi mjekët, administratorët dhe pacientët kërkojnë qasje të sigurt në informacionet konfidenciale kundrejt një kostoje më të ulët. Sipas të njëjtit burim, pajisjet mjekësore dhe telemjekësia paraqesin rreziqe mbi sigurinë e Internet of Things - IoT dhe zgjerojnë më tej peisazhin e kërcënimeve.

II. Statistika të Evropës për sulmet dhe dëmet në shëndetësi

Përqindja e të moshuarve në Evropë po rritet për shkak të numrit të ulët të lindjeve dhe i rritjes së jetëgjatësisë. Sipas raportit "Ridizenjimi i shëndetësisë në Evropë për 2020 ", kostot e kujdesit shëndetësor në Evropë aktualisht po rriten. Këto kosto në disa vende evropiane janë faktorë rritës të GDP-së, dhe në disa raste një arsye rritjeje e financave publike, që përfaqëson 4% deri 12% të GDP-së në Shtetet Anëtare të BE-së.

[1]Cases Currently Under Investigation: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[2]Health Task Force. Redesigning Health in Europe for 2020. European Union 2012.

Një aspekt tjetër i rëndësishëm i sektorit të shëndetësisë në BE është se rreth 40% e popullsisë mbi moshën 15 vjeç, pra mbi 100 milion qytetarë, raportohet të kenë një sëmundje kronike. Kjo përqindje rritet në 66% për popullsinë që ka arritur moshën e pensionit duke pasur të paktën dy sëmundje kronike. Shtetet Anëtare të BE-së po përballen me një situatë ku janë shpenzuar më shumë se 70% të kostove të shëndetësisë për sëmundje kronike, dhe kjo shifër pritet të rritet në vitet e ardhshme. Për këtë arsye, vendet anëtare të BE-së po përpiqen të arrijnë që të ofrojnë një shëbim të përballueshëm, më efikas dhe kujdes më të personalizuar për qytetarët.

Për të arritur këtë, aplikimi i Teknologjive të Informacionit dhe Komunikimit është avantazh për sektorin. Përdorimi i konceptit të eHealth luan një rol kryesor për të ruajtur cilësinë e shërbimeve shëndetësore në mënyrë të përballueshme kosto-efektive. Si pasojë, teknologjitë eHealth pritet të rriten ndjeshëm në vitet e ardhshme. Nëpërmjet tyre do të jepen informacione dhe shërbime të lidhura me shëndetin. Nga pikëpamja e sigurisë kibernetike, të gjitha këto tendenca dhe zhvillime teknologjike duhet të analizohen me kujdes. Ato ekspozojnë dhe rritin ndjeshmërinë e sistemeve të informacionit dhe të dhënave të pacientëve përmes sinjaleve monitoruese, statusit shëndetësor dhe historikut të të dhënave të pacientëve në format elektronik. Ky informacion konsiderohet e dhënë konfidenciale dhe e ndjeshme. Prandaj, duhet të vendosen rregulla dhe kërkesa të forta për autentifikime dhe duhet të bëhen përpjekje të vazhdueshme për të mbrojtur informacionin, duke marrë parasysh kërcënimet dhe trendet ekzistuese në sulme kibernetike.

Sulmet kibernetike janë vazhdimisht në rritje. Ato përqendrohen kryesisht në vjedhjen e informacionit financiar, informacionin e faturimit dhe numrat e llogarive bankare duke përdorur pajisje me të dhëna të pa enkriptuara, phishing dhe spam email. Evolimi i teknologjisë ka çuar në luftë kibernetike të avancuar duke përdorur SQL injection, Advance Persistence Threats (APT), sulme zero-day dhe malware të ndryshëm.

Sektori eHealth nuk përbën përjashtim. Mungesa e investimeve në IT nga organizatat e kujdesit shëndetësor dhe mungesa e informacionit për krimin kibernetik kanë ekspozuar dobësitë e organizatave shëndetësore. Ndikimi i sulmeve kibernetike në sistemet spitalore dhe kujdesit shëndetësor vlerësohet të jetë gati gjashtë miliardë në vit[3] .

BitSight ka realizuar një studim në nivel global mbi organizatat e kujdesit shëndetësor. Synimi i studimit ishte të kuptonte më mirë se ku ka nevojë për menaxhim risku më shumë sektori i shëndetësisë, Duke përdorur të dhënat e mbledhura nga ekipi i BitSight's Data Science që nga 1 qershori 2019, u shqyrtuan vlerësimet e përgjithshme të sigurisë së kompanive të kujdesit shëndetësor, si dhe dobësitë e mundshme të tilla si sisteme dhe programe vulnerabël, porta të pasigurta dhe shembuj të sistemeve tashmë të kompromentuara[4] .

Rezultatet ishin të qarta. Të dhënat tregojnë se organizatat në këtë sektor kanë hapësirë për të përmirësuar sjelljet e tyre të sigurisë. Siç tregon grafiku më poshtë, vetëm 50% e kompanive të kujdesit shëndetësor kanë Vlerësime të Avancuara - që do të thotë se ata kanë një mundësi më të ulët të thyerjes së sigurisë. Vlerësimet e Sigurisë së BitSight variojnë nga 250 në 900. Çdo gjë mbi 740 konsiderohet "e Avancuar". Kompanitë me një vlerësim sigurie prej 500 ose më të ulët kanë gati pesë herë më shumë gjasa të përjetojnë një shkelje të të dhënave të zbuluara publikisht.

[3]Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute
[4]Bitsight.com

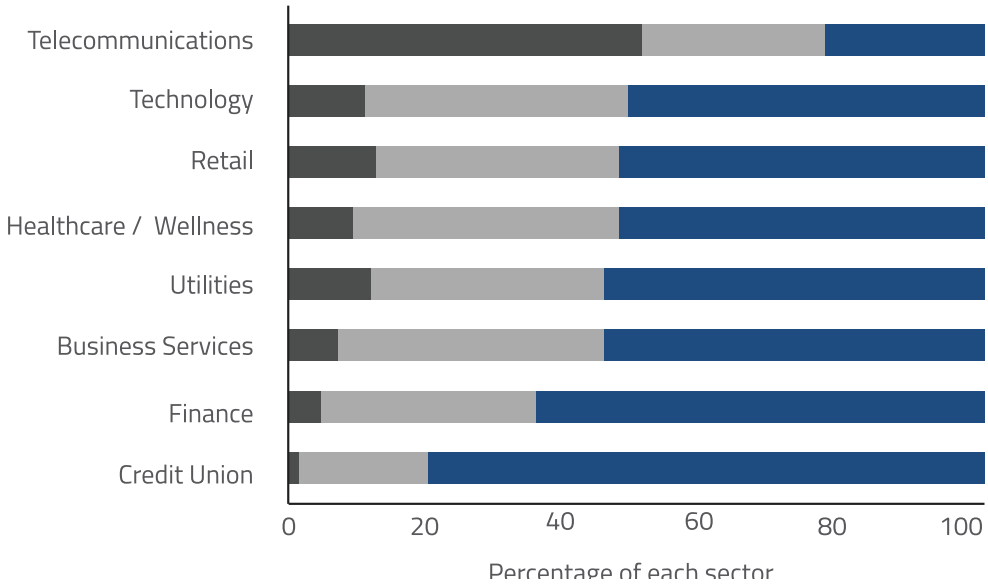

Figura 1 Nivelet e thyerjes së sigurisë për sektor, Bitsight

51% e organizatave të kujdesit shëndetësor përdorin sisteme ose pajisje të papërditësuara, të cilat mund të jenë vulnerabël ndaj sulmeve kibernetike. Në industrinë e kujdesit shëndetësor, pajisjet e tilla shpesh shfrytëzohen nga aktorë dashakeqës për të fituar akses në të gjithë rrjetin.

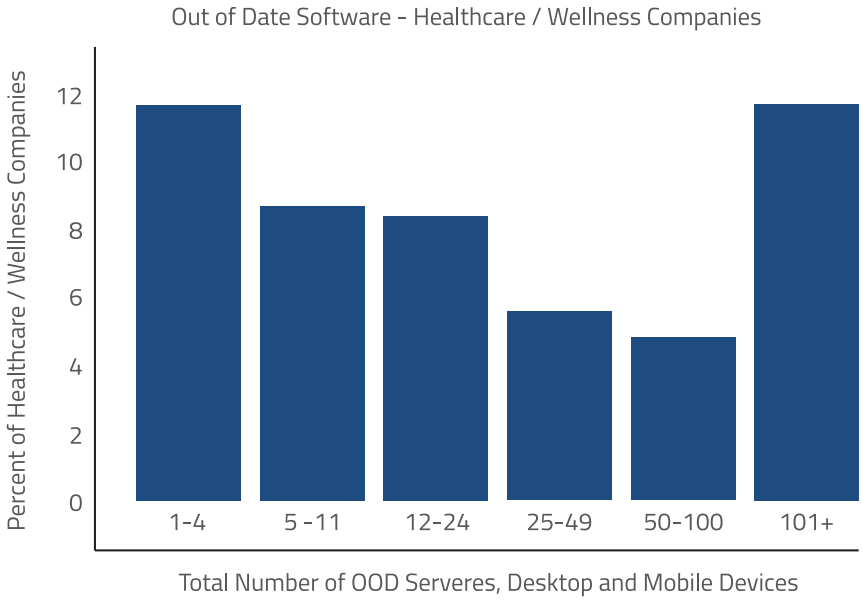

Figura 2 Pajisjet e papërditësuara, Bitsight

Grafiku i mëposhtëm tregon se 39% të kompanive të kujdesit shëndetësor i kanë portat në thelb të pasigurta ose të prekshme nga sulmet kibernetike. Kjo tregon se disa prej këtyre organizatave lënë hapësira që hakerat të shfrytëzojnë sistemet e tyre, të tilla si pajisje mjekësore me softuer të papërditësuar.

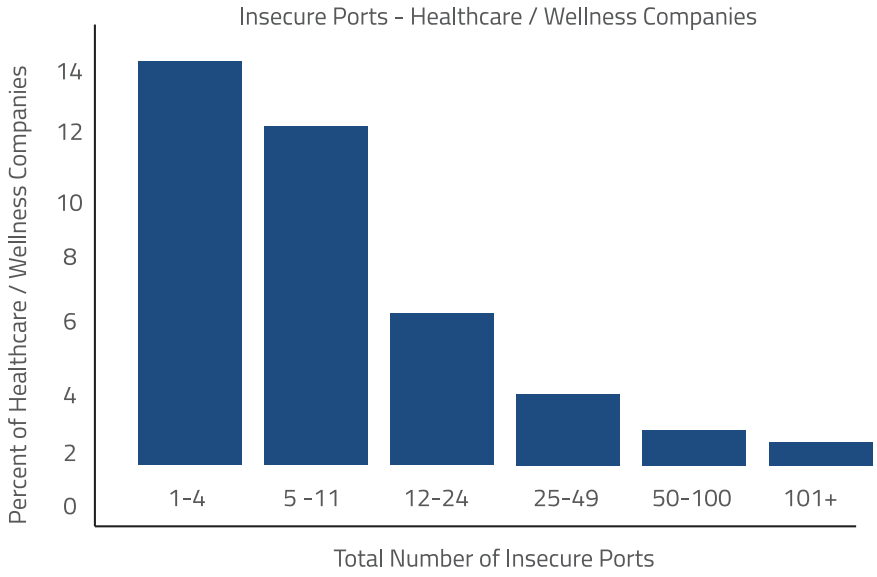

Figura 3 Portat e pasigurta, Bitsight

Përfundimet tregojnë se 7% e kompanive të kujdesit shëndetësor kishin një ose më shumë sulme botnet brenda tre muajve të fundit. Ky numër mund të duket relativisht i ulët, por përkufizimi i "botnet" tregon se këto sulme shtrihen përtej një makine të vetme - qoftë në rrjetin e tyre apo jo. Hulumtimi i BitSight ka identifikuar një korrelacion të fortë midis sulmeve botnet dhe shkeljeve të të dhënave. Më konkretisht, kompanitë me një vlerësim botnet B të BitSight ose më të ulët kishin dy herë më shumë mundësi të përjetojnë një shkelje të të dhënave.

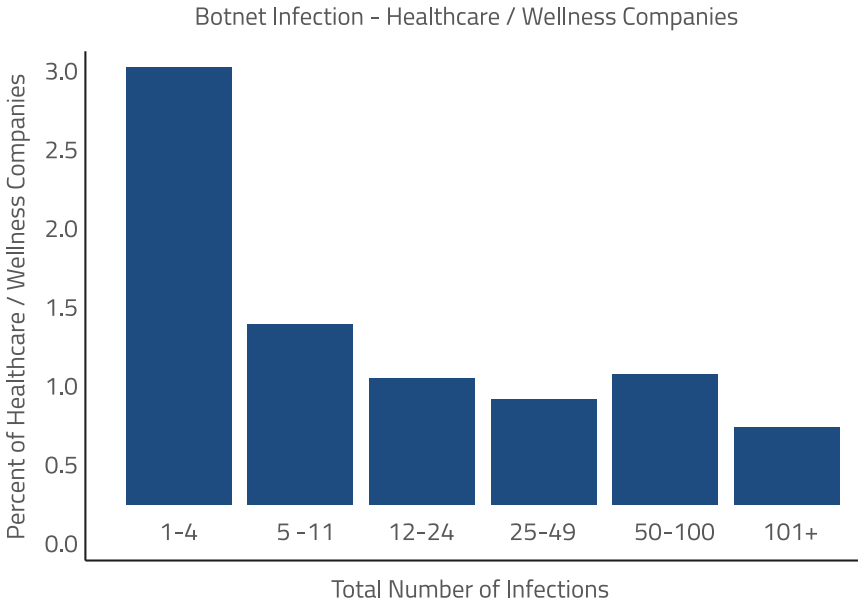

Figura 4 Infektimet botnet, Bitsight

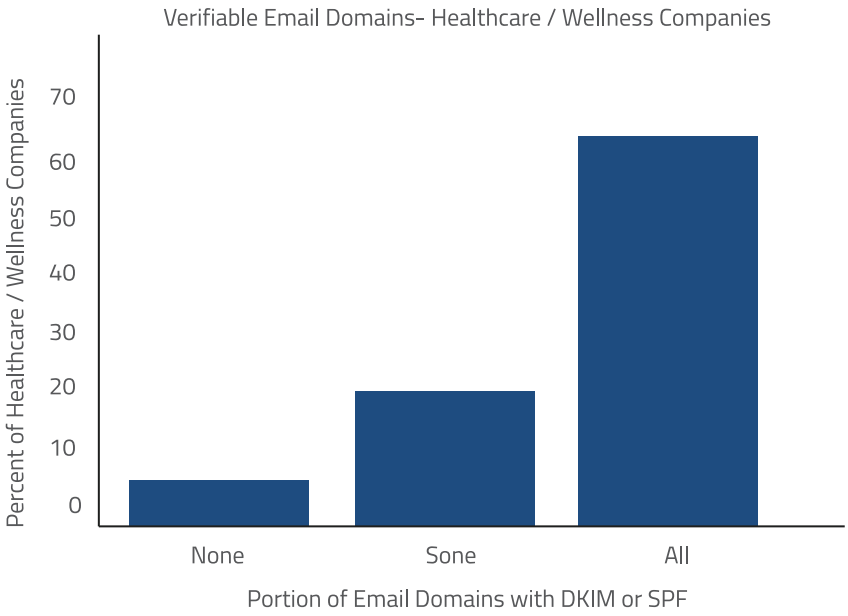

Figura 5 Domain të infektuar, Bitsight

Nga ana tjetër, sektori i kujdesit shëndetësor është më efektiv ndaj mbrojtjes nga SPAM dhe phishing i postës elektronike, me gati 70% të sektorit duke përdorur DKIM ose SPF.

III. Situata në Shqipëri me referenca statistikore

Gjigandi rumun i sigurisë kibernetike Bitdefender ka raportuar se sulmet që lidhen me COVID-19 janë rritur 475% në muajin Mars të vitit 2020 krahasuar me një muaj më parë. Pothuajse një e treat e sulmeve që lidhen me COVID-19 targetojnë autoritetet publike dhe institucionet e kujdesit shëndetësor.

Duke iu referuar praktikave më të mira Evropiane e ndërkombëtare, edhe Shqipëria ka realizuar hapa pozitivë përsa i përket identifikimit të sektorit shëndetësor në listen 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 listuar për herë të parë edhe spitalet private që ushtrojnë veprimtarinë e tyre në Republikën e Shqipërisë. Në këtë VKM janë listuar 4 operatorë dhe rreth 10 sisteme kritike dhe të rëndësishme të informacionit.

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 shëndetësor arrin në nivelin 790. Vlerësimi i sigurisë paraqet një mesatarizim të vlerësimit të sistemeve të kompromentuara, Diligjenca dhe sjellja e përdoruesve të operatorëve të sektorit shëndetësor. 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.

Sipas një studiuesi të sigurisë, organizatat e kujdesit shëndetësor duhet të jenë të përgatitura për një rritje prej 10% -15% të numrit të thyerjeve të të dhënave, ku ofruesit e tyre të shërbimeve do të jenë objektivi kryesor. Bazuar në rezultatet e 6 muajve të parë të vitit 2019, pritet që numri i thyerjeve të të dhënave do të rritet me një shpejtësi alarmante, pavarësisht nga përpjekjet që po bëjnë shumë organizata për të siguruar të dhënat e tyre. Në këtë platformë, për sektorin shëndetësor 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
CVE- 2014 - 3398	50.0 %	50.0 %	-
CVE- 2020 - 3452	50.0 %	50.0 %	-
POODLE	100.0 %	50.0 %	-50.0 %

Figura 6 Vulnerabilitetet kryesore, Bitsight

Në 30 ditët e fundit vulnerabiliteti më i shpeshtë është CVE-2014-3398, lejon sulmuesit në distancë të marrin informacione sensitive të softuerit duke lexuar të dhënat e përgjigjes që gjenerohen nga URL specifike.

Në nivel rajonal, Shqipëria renditet në nivelet më të larta të sigurisë së sektorit shëndetësor, duke lënë pas Serbinë, Maqedoninë e Veriut dhe Bosnjë Hercegovinën.

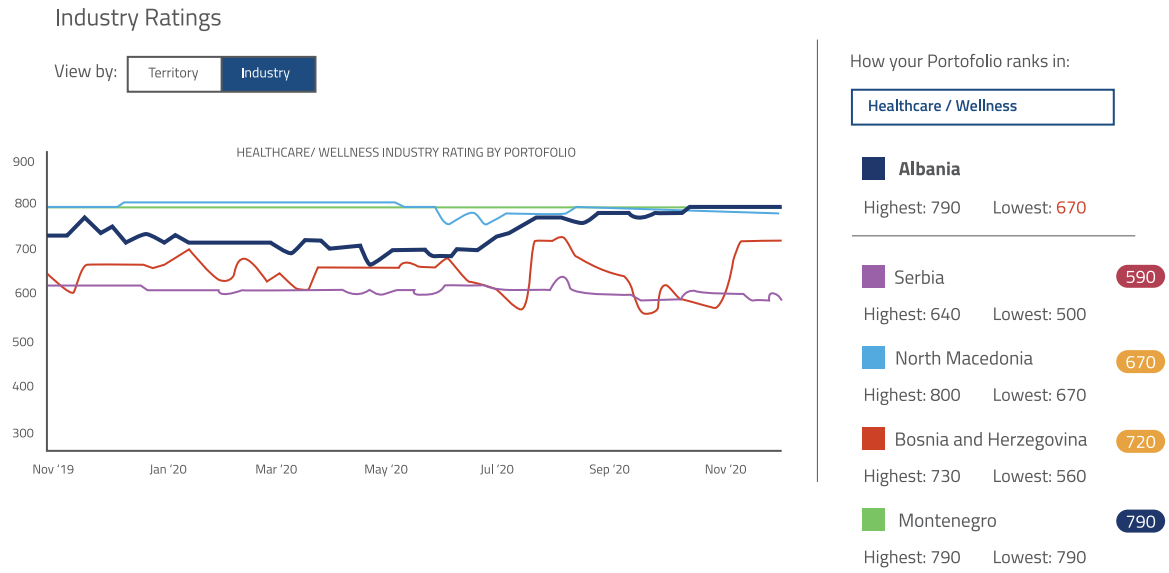

Figura 7 Rankimi rajonal

Sektori i kujdesit shëndetësor ka qenë prej kohësh një shënjestër e kriminelëve kibernetikë. Por së fundmi, ndërsa të gjithë sytë ishin përqendruar në pandeminë e koronavirusit që shtrihet në të gjithë globin, kërcënime të tjera ishin në pritje për të përfituar nga sistemi i mbingarkuar i kujdesit shëndetësor. Këto kërcënime ishin të larmishme, duke synuar teknologjitë në të cilat mbështeten sistemet dhe ofruesit e kujdesit shëndetësor. Në vendin tonë, ashtu si në shtetet e tjera të krahasueshme me zhvillimin digjital dhe të sigurisë kibernetike me Shqipërinë, pasojat e sulmeve kibernetike gjatë pandemisë ishin thuajse të papërfillshme.

IV. Benefitet e investimit në sigurinë kibernetike sektorin e shëndetësisë

Jo shumë kohë më parë, mjekëve u duhej të kufizonin kohën e tyre me pacientët për shkak të shumë dokumentave të komplikuara. Revolucioni digjital ka ndihmuar në zgjidhjen e këtij problemi. Me më pak shënime të shkruara me dorë dhe aksesim të dosjeve elektronike të pacientëve, dokumentet dhe sasia e kohës që i kushtohet plotësimit të tyre kanë rënë në mënyrë të ndjeshme. Ky është një zhvillim i rëndësishëm ndërkohë që popullsia rritet dhe numri i të dhënave të kujdesit shëndetësor bëhet më i vështirë për t'u siguruar. Siguria kibernetike në kujdesin shëndetësor duhet të sigurojë rrjetin dhe bazën e të dhënave pa ngadalësuar procesin e sigurimit të kujdesit efikas.

1. Siguria kibernetike kursen miliona dollarë në industrinë e kujdesit shëndetësor.
Industria është rritur me shpejtësi në dy dekadat e fundit. Me ruajtjen e të dhënave në cloud, ofruesit mund të aksesojnë informacionin e pacientëve, kolegëve dhe departamenteve të tjera në mënyrë të shpejtë. Njëkohësisht, ruajtja dhe aksesi në të dhënat e pacientëve është shumë më e lehtë për t'u siguruar.

2. Sensitiviteti i të dhënave të pacientëve.
Sektori i kujdesit shëndetësor duhet të ruajë të dhënat e pacientëve, pasi në rast se aksesohen nga një haker, mund të shpërndahen dhe të përdoren për qëllime dashakeqëse dhe manipulime. Siguria kibernetike ndihmon në ruajtjen e informacioneve konfidenciale dhe parandalon sulmet kibernetike.

Teknologjia ka një numër të madh benefitesh të cilat janë avantazh jo vetëm për spitalet por edhe për trajtimet. Investimi në siguri kibernetike ndihmon në ruajtjen e biznesit per spitalet private, ne dhënien e shërbimit më të mirë kundrejt pacientëve dhe shkëmbimin e të dhënave të pacientëve në departamente të tjera lehtësisht.
Më poshtë është paraqitur një model biznesi për një organizatë që vepron në sektorin shëndetësor 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.

ZËRAT	EUR
Shpenzimet aktuale mesatare per nje sulm kibernetik	27.000
Numri i sulmeve per nje vit	0,5
Totali i shpenzimeve per nje vit	13.500
Investimi fillestar	
Servera	3.000
Infrastruktura e rrjetit	200
Ndertimi i Telefonise VOIP	15.000
Routers dhe switches	10.000
Firewall	2.000
Software te ndryshem	1.000
Totali	**31.200**
Mirembajtja	624
Kosto te tjera jo te drejtperdrejta	
Demtim Imazhi	3000

Figura 8 Supozimet e kostove

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 50%.

Kthimi nga projekti - SHËNDETËSI	*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	13.500	13.811	14.252	14.680	15.135	15.604	16.088	16.587	17.101	17.631	18.178
Investimi fillestar	(44.000)										
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	(3.000)	(3.069)	(3.167)	(3.262)	(3.363)	(3.468)	(3.575)	(3.686)	(3.800)	(3.918)	(4.039)
Fluksi I lire I parase	**(35.500)**	**8.696**	**8.974**	**9.243**	**9.530**	**9.825**	**10.129**	**10.444**	**10.767**	**11.101**	**11.445**
Kosto e kapitalit te projektit *12,0%*											
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	0,84	0,75	0,67	0,60	0,54	0,48	0,43	0,38	0,34
Vlera e skontuar e fluksit te lire te parase	**(35.500)**	**8.216**	**7.571**	**6.963**	**6.409**	**5.900**	**5.431**	**5.000**	**4.602**	**4.237**	**3.900**
Tregues kryesore financiare											
Vlera aktuale neto (NPV)	22.728										
Norma e brendshme e kthimit (IRR)	*24%*										
Periudha e shlyerjes (PBP) ne vite	7										
Flukset e akumuluara	(35.500)	(27.284)	(19.713)	(12.750)	(6.341)	(441)	4.990				
Viti i shlyerjes se investimit	-	-	-	-	-	-	7				

Figura 9 Modeli financiar

Kthimi nga projekti - SHËNDETËSI	*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		13.500	13.811	14.252	14.680	15.135	15.604	16.088	16.587	17.101	17.631	18.178
Kosto e sherbimit		(12.000)	(12.276)	(12.669)	(13.049)	(13.453)	(13.870)	(14.300)	(14.744)	(15.201)	(15.672)	(16.158)
Fluksi I lire I parase		**1.500**	**1.535**	**1.584**	**1.631**	**1.682**	**1.734**	**1.788**	**1.843**	**1.900**	**1.959**	**2.020**
Kosto e kapitalit te projektit	*12,0%*											
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	0,84	0,75	0,67	0,60	0,54	0,48	0,43	0,38	0,34
Vlera e skontuar e fluksit te lire te parase		**1.500**	**1.450**	**1.336**	**1.229**	**1.131**	**1.041**	**958**	**882**	**812**	**748**	**688**
Tregues kryesore financiare												
Vlera aktuale neto (NPV)		11.776										

Figura 10 Modeli financiar, 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.

V. Rreziqet në sigurinë kibernetike në sektorin e shëndetësisë

Institucionet shëndetësore përpiqen të implementojnë praktika sa më efektive për sigurinë kibernetike pasi mund të riskojnë disa faktorë. Së pari, të dhënat mjekësore dhe personale te pacientëve po integrohen në botën digjitale, duke u lënë të hapur mundësinë për ekspozim të tyre. Së dyti, krimet kibernetike dhe rreziqet e sigurisë kibernetike në shëndetësi po bëhen çdo ditë e më komplekse dhe të dhënat mund të vidhen ose organizata detyrohet të paguajë një shumë të konsiderueshme për t'i riaksesuar të dhënat.

Për të shmangur vjedhjen e të dhënave të pacientëve duhen konsideruar 4 rreziqe të sigurisë kibernetike me të cilat përballen organizatat:

1. Pajisje IT të papërditësuara

Ofruesit e shërbimit shëndetësor punojnë me një gamë të gjerë subjektesh, nga burimet njerëzore e deri te ofruesit e pajisjeve mjekësore. Me këtë ekosistem të larmishëm, është e rëndësishme të konsiderohet se disa nga palët e treta mund të kenë akses në rrjetin tuaj dhe në të dhënat konfidenciale nëpërmjet pajisjeve fundore të papërditësuara (si psh. kompjuterë, laptopë, tableta, etj). Nëse personave të paautorizuar, u jepen të drejta aksesi me rrjetin dhe ata përdorin pajisje të papërditësuara, bëhen shkak për ekspozim të të dhënave të organizatës shëndetësore.

2. Pajisje mjekësore të papërditësuara

Pajisjet mjekësore mund të mos jenë shqetësimi kryesor i sigurisë kibernetike, por siguria e tyre është e rëndësishme për sigurinë e organizatës në tërësi. Për shembull, edhe nëse nuk përdoret më një sistem operativ i vjetër, si pajisja e Rrezeve X, mund të ketë ende gjurmë të atij sistemi. Nëse mbi atë sistem injektohet një worm, ai ka potencial të vendosë në rrezik të gjithë rrjetin.
Në ditët e sotme prodhuesit e pajisjeve mjekësore po e përdorin kriterin e sigurisë si një mënyrë për të diferencuar veten në treg dhe duke sinjalizuar një ndryshim në mënyrën se si palët e treta po konsiderojnë për sigurinë kibernetike në kujdesin shëndetësor.

3. Ransomware

Ransomware përbën një nga rreziqet më potenciale të sigurisë për organizatat e kujdesit shëndetësor. Ky është një problem i zakonshëm në industrinë e kujdesit shëndetësor, ndoshta për shkak të natyrës sensitive të të dhënave të përdorura në këtë sektor. Suksesi i një sulmi ransomware varet pothuajse vetëm nga sa dëshpërimisht nevojiten të dhënat. Pra, nëse një spital sulmohet dhe të dhënat nuk janë të aksesueshme në një mënyrë tjetër, disa janë të gatshëm të paguajnë për të fituar akses. Si rezultat, është e rëndësishme për organizatat e kujdesit shëndetësor që të monitorojnë vazhdimisht palët e tyre të treta dhe të vlerësojnë nëse hyrja në rrjetin e tyre mund të sjellë dobësi (të cilat, nga ana tjetër, mund të çojnë në ransomware dhe sulme të tjera kibernetike). Zakonisht shpërblimi për të marrë të dhënat kërkohet minimalisht nga 300$.

4. Dëmtim të reputacionit

Duhet konsideruar se: Si spital, nëse dërgon mostra të pacientëve në një laborator për analiza dhe nëse laboratori përjeton një thyerje të sigurisë, të dhënat e pacientëve tuaj - përfshirë emrat e tyre, numrat e regjistrave mjekësorë, rezultatet e analizave dhe informacione të tjera të identifikueshme personalisht (PII) - mund të jenë në rrezik. Nëse organizata juaj nuk po monitoron në mënyrë aktive për t'u siguruar që po merren masat e duhura të sigurisë, të dhënat e pacientëve tuaj vendosen në një situatë të pasigurt duke rrezikuar dëmtimin e reputacionit të spitalit. Kjo do të shkaktojë dhe humbje biznesi për spitalin. Katër rreziqet e renditura më sipër janë vetëm disa nga arsyet pse menaxhimi i rrezikut që vjen nga ofruesit e shërbimeve zë vendin kryesor në diskutimet në lidhje me sigurinë kibernetike në kujdesin shëndetësor.

VI. Masat mbrojtëse që duhet të aplikojnë institucionet shëndetësore

1. Sigurimi i pikave të hyrjes

Pikat hyrëse janë burim potencial sulmesh kibernetike. Duke shfrytëzuar dobësitë e tyre, hakerat përhapin një virus për të ngadalësuar rrjetin, për të aksesuar informacione kritike shëndetësore ose për ta bërë sistemin më të cënueshëm në të ardhmen. Malware mund të hyjë nga çdo vend i prekshëm në rrjet ose sistemin operativ.

Një punonjës mund të klikojë pa e ditur një skedar, të shkarkojë softuer të paautorizuar ose të ngarkojë një dokument të kontaminuar. Gjithashtu, kur nuk përdoren fjalëkalime të forta të sigurta, krijohet një pikë e lehtë hyrëse për hakerat. Për më tepër, softueri mjekësor dhe aplikacionet në internet të përdorura për ruajtjen e të dhënave të pacientëve u zbuluan se përmbajnë dobësi të shumta. Statistikat e sigurisë kibernetike të sektorit shëndetësor nga "Kaspersky Security Bulletin" zbuluan vulnerabilitete në pikat hyrëse të rreth 1500 pajisjeve pajisje që profesionistët e kujdesit shëndetësor përdorin për të përpunuar imazhet e pacientëve. [5]

2. Përvetësimi i njohurive për ransomware

Një sulm ransomware është një lloj specifik i malware që kërcënon të bllokojë një kompjuter ose një rrjet të tërë nëse nuk paguhet një shumë e caktuar parash. Shpërblimi nuk është domosdoshmërisht një shifër e lartë. Edhe të kërkosh disa qindra dollarë nga një biznes mund të jetë easy money për një haker, dhe më e menaxhueshme për individët ose kompanitë për të marrë përsëri akses në kompjuterët e tyre. Për këtë është e nevojshme të rriten njohuritë e stafit dhe përdoruesve të pajisjeve për të identifikuar ransomware e për të mësuar si të veprojnë nëse janë target i një sulmi të tillë.

[5]Kaspersky security bulletin, 2019

3. Krijimi i një politike mbi ransomware

Një kompjuter me akses të kufizuar nuk sjell domosdoshmërisht dëm. Sidoqoftë, rreziku për të mos qenë në gjendje të aksesoni skedarët ku ruhen të dhënat mund të jetë i rrezikshëm për trajtimin e pacientit. Kur ndodh një incident i tillë, punonjësit duhet të kontaktojnë menjëherë IT. Kjo duhet të jetë pjesë e trajnimit të tyre të sigurisë. Ata duhet të ndjekin procedurat e organizatës së kujdesit shëndetësor kur shohin një mesazh ransomware, në vend që të përpiqen ta zgjidhin vetë çështjen.

4. Trajnimi i punonjësve

Për të minimizuar gabimet njerëzore, administratorët e sistemit duhet të trajnojnë vazhdimisht të gjithë stafin për sjelljet e rrezikshme. Kjo përfshin element të ndryshëm, nga shkarkimi i software-it të paautorizuar dhe krijimi i fjalëkalimeve të dobëta deri te vizita në faqet e internetit me përmbajtje të dëmshme ose përdorimi i pajisjeve të infektuara. Duhet të edukohen punonjësit se si të njohin një email dashakeq, kërcënime dhe faqe të paligjshme e të dyshimta në mënyrë që të shmangin sulmet. (Ngjyrat e pazakonta në logo ose fjalor i ndryshueshëm përgjatë faqes janë dy shenja paralajmëruese). Trajnimi duhet të zhvillohet rregullisht ose të personalizohet për grupe të ndryshme të punonjësve.

5. Krijoni ose përditësoni politikat e matjes së nivelit të rrezikut të sigurisë

Punonjësit duhet të pajisen me privilegje të ndryshme të qasjes në rrjet. Në një spital, infermierët mund të kenë nevojë të ndajnë informacione me stafin tjetër në departamentin e tyre, por nuk është e nevojshme që departamentet e tjera ta shohin këtë. Mjekët që vizitojnë mund të marrin akses vetëm në informacionin e pacientit të tyre. Privilegjet e sigurisë duhet të monitorojnë për akses ose përpjekje të paautorizuara në çdo nivel.

Digital Guardian[6] sugjeron fillimisht trajnimin / edukimin, pasuar nga kufizimi i aplikacioneve specifike, zonave dhe të dhënave të kujdesit shëndetësor të pacientëve. Ai gjithashtu rekomandon që të kërkohet autentikimi me shumë faktorë, i cili është një nivel shtesë mbrojtjeje.

6. Siguria kibernetike e industrisë shëndetësore duhet të shkojë përtej aksesit të punonjësve

Shqetësimet e pacientëve në lidhje me sigurinë e të dhënave në kujdesin shëndetësor duhet të konsiderohen kur krijohen sisteme më të sigurta ose kur përmirësohen kornizat e sigurisë kibernetike pasi një spital sulmohet. Pacientët nuk duan të shqetësohen për sigurinë e të dhënave, prandaj administratorët e sistemit duhet të investojnë në iniciativa të sigurisë.

7. Mbroni të dhënat shëndetësore në pajisjet 'inteligjente'

Desktop, laptopë, telefona celularë dhe të gjitha pajisjet mjekësore, veçanërisht ato të lidhura me rrjet, duhet të monitorohen dhe të kenë mbrojtje anti-virus, firewall ose elementë të tjerë të ngjashëm. Në ditët e sotme qendrat mjekësore zotërojnë pajisje të tjera elektronike të lidhura siç janë pajisjet mjekësore si monitorët e insulinës që sinkronizojnë në distancë informacionin e pacientit drejtpërdrejt në tabletën e një mjeku ose një infermiereje. Shumë prej këtyre pajisjeve të ndërlidhura potencialisht mund të hakohen, dëmtohen ose çaktivizohen, e të gjitha këto mund të ndikojnë në shëndetin e pacientit.

[6]Digitalguardian.com

8. Integrimi i të dhënave në Cloud

Cloud ofron një zgjidhje të sigurt dhe fleksibël për ruajtjen dhe rezervimin e të dhënave të kujdesit shëndetësor dhe siguron një mënyrë se si organizatat menaxhojnë të dhënat e tyre. Zgjidhjet e mbështetura në cloud dhe rikuperimin në rast sulmi sigurojnë që regjistrat e pacientëve të jenë të aksesueshëm edhe në rast të shkeljes ose ndërprerjes së punës. Të kombinuara me opsionin për të kontrolluar hyrjen në të dhëna, ofrohet niveli i nevojshëm i sigurisë. Me cloud, një organizatë e kujdesit shëndetësor nuk ka pse të investojë shumë në infrastrukturën kritike për ruajtjen e të dhënave. Ruajtja në Cloud në përputhje me HIPAA lejon ulje të konsiderueshme të kostove të IT, pasi nuk nevojiten investime në pajisje. Clound ofron gjithashtu një nivel të konsiderueshëm fleksibiliteti kur nevojat e ruajtjes së të dhënave të një institucioni ndryshojnë.