Ndikimi i Rregullores së Përgjithshme të Mbrojtjes së të Dhënave (GDPR) në sigurinë kibernetike

Abstrakt
Përdorimi i teknologjive të informacionit synon rritjen e standardit të jetesës dhe përmirësimin e cilësisë së shërbimeve. Krahas përfitimeve të përdorimit të teknologjive të reja dixhitale, përdorimi i internetit sjell problemet e veta që lidhen me sigurinë kibernetike. Futja e teknologjive të reja, shpesh herë, bëhet pa një vlerësim të duhur paraprak të ndikimit të tyre në mbrojtjen e të dhënave dhe privatësinë. Rregullorja e Përgjithshme Evropiane për Mbrojtjen e të Dhënave ("GDPR") po çon në një fazë ndryshimi, i cili do të rrisë jo vetëm mbrojtjen e të dhënave personale, por edhe ndërgjegjësimin e sigurisë në organizatat që përpunojnë këto të dhëna. Megjithëse kjo rregullore nuk është krijuar për qëllime të sigurisë kibernetike, GDPR është një udhëzues i mirë për të adresuar siç duhet sigurinë (dhe mbrojtjen e të dhënave) në një fazë të hershme. Ai vendos parimin e llogaridhënies, ku çdo kompani është përgjegjëse për zbatimin e saj dhe përgjegjësinë ligjore. Në këtë punim kemi treguar disa elementë se si GDPR ndikon në rritjen e nivelit të sigurisë së informacionit. Duke pasur parasysh legjislacionin përkatës në Shqipëri, propozojmë që në kuadër të harmonizimit me legjislacionin e BE-së, adresimi i udhëzimeve GDPR të bëhet në kuadër të përmirësimeve të legjislacionit të sigurisë kibernetike.

1. Hyrje

GDPR është rregullorja për mbrojtjen e të dhënave personale brenda Bashkimit Evropian (BE) dhe Zonës Ekonomike Evropiane dhe synon të përmirësojë më tej kontrollin mbi të dhënat personale të individëve. Ky grup i gjerë rregullash për mënyrën se si mblidhen, përpunohen dhe ruhen të dhënat personale po shkakton ndryshime thelbësore në mënyrën se si organizatat i qasen të dhënave personale. Masat e detyrueshme për moszbatimin e GDPR nga organizatat janë të rëndësishme: 4% e xhiros globale vjetore ose 20 milionë euro. [3]

Rregullorja e Përgjithshme Evropiane për Mbrojtjen e të Dhënave ("GDPR") po çon në një etapë ndryshimi, e cila do të rrisë jo vetëm mbrojtjen e të dhënave personale, por edhe ndërgjegjësimin për sigurinë në organizatat që përpunojnë këto të dhena. Deri më sot, është bërë shumë për ndërgjegjësimin për sigurinë kibernetike (në internet/online) në përgjithësi, dhe pak për sigurinë kibernetike për mbrojtjen e të dhënave personale. Digjitalizimi dhe kalimi i të gjitha informacioneve personale, shërbimeve publike e private nga formati leter në publikim online, po shton rrezikun e humbjes së privatësisë, vjedhjes së të dhënave private apo tjetersimin e tyre duke rritur kështu mundësinë për kryerjen e krimeve kibernetike.

Zhvillimi i teknologjive 5G dhe IoT ka rritur domosdoshmërinë për garantimin e një niveli të lartë të sigurisë së të dhënave personale në përputhje me kërkesat e GDPR-së. Këto pajisje zakonisht mbledhin dhe transmetojnë informacione të cilat mund të klasifikohen si të dhëna personale, prandaj kërkesat e GDPR-së kanë ndikim tek zhvilluesit dhe certifikuesit e këtyre pajisjeve. [1]

Problematika me sigurine kibernetike nuk sjell vetem teknologjia por dhe "Faktori njerëzor". Për shembull, një punonjës i shpërqëndruar thjesht duke lënë një kompjuter të shkyçur ose duke hapur emaile phishing, mund të shkaktojë një rrjedhje të të të dhënave sipas GDPR. Adresimi i faktorit njerëzor sipas GDPR, kërkon që organizatat të sigurojnë që punonjësit e tyre të jenë të trajnuar në mënyrën e duhur. Trajnimet e punonjësve në lidhje me GDPR do të ndihmojë në adresimin e kërcënimit më të madh kibernetik: mosvetëdijes për sigurinë (dhe mbrojtjen e të dhënave).

Privatësia dhe siguria e të dhënave, të konsideruara prej kohësh gjëra të veçanta, po ndërthuren falë kësaj rregullore. Prandaj, në këtë artikull do të trajtohet ndikimi i GDPR në sigurine kibernetike, masat dhe teknikat që duhen implementuar nga organet që preken.

2. Metodologjia

Për shkrimin e këtij artikulli është ndjekur metoda e ´literature review´, duke kërkuar në disa baza të dhënash në internet duke përfshirë Google; Google Scholar; Journal of Cybersecurity; dhe International Journal of Law and Information Technology.
Janë përdorur termat e mëposhtëm të kërkimit këtë: 'impact of GDPR', 'changes to practices and behaviors', 'investment in cyber security'. Secili nderlidhej me Cybersecurity` dhe 'GDPR'.
Për shkak të zbatimève relativisht të fundit të rregullores të GDPR, nuk kishte shume literaturë akademike, të rishikuar nga kolegët. Prandaj u morren informacione shtesë nga përfshirë artikujt në internet në lidhje me ndikimin e GDPR në sigurinë kibernetike.

3. GDPR dhe siguria kibernetike

Siguria kibernetike adreson mbrojtjen e sistemeve kritike dhe informacioneve sensitive nga sulmet kibernetike, ndërsa GDPR adreson ceshtjet për mbrojtjen e të dhënave. Megjithëse nuk është krijuar për qëllime të sigurisë kibernetike, GDPR është një orjentues i mirë për të adresuar siç duhet sigurinë (dhe mbrojtjen e të dhënave) në një fazë me të hershme. Ajo vendos parimin e llogaridhënies, ku çdo kompani është përgjegjëse për implementimin dhe përgjegjësinë ligjore te saj. Përgjegjësi të tilla përfshijnë masat e duhura të sigurisë, të cilat duhet të marrin në çdo kohë parasysh natyrën, kontekstin dhe qëllimet e përpunimit të të dhënave dhe rreziqet e lidhura me to. Përmes parimit të llogaridhënies pothuajse të gjitha dispozitat e GDPR bëhen të rëndësishme nga këndvështrimi i sigurisë kibernetike. Sipas GDPR, organizatat duhet të marrin parasysh rrezikun e privatësisë, gjatë gjithë procesit të projektimit të një produkti ose shërbimi të ri, dhe të miratojnë mekanizma për të siguruar se të dhënat personale që do të mblidhen, përdoren dhe ruhen të jenë minimale. [2] Për të arritur pajtueshmërinë me kërkesat e GDPR mund të përdoret një mekanizëm certifikimi i miratuar per organizatat qe përpunojnë të dhënat personale.

Për shembull, vlerësimi i ndikimit në privatësi (PIA) të GDPR duhet të bëhet një mjet i vlefshëm për mbrojtjen kibernetike. PIA duhet të jetë një parakusht i detyrueshëm përpara përpunimit të të dhënave për subjektet e të dhënave që paraqesin rreziqe më të larta të privatësisë. E njëjta gjë vlen edhe me të drejtën e transferimit të të dhenave së GDPR, sipas së cilës subjektet e të dhënave mund të kërkojnë që skedarët e të dhënave të transferohen nga një ofrues shërbimi në tjetrin. Siç thuhet te Nenit 29, organizatat duhet të kenë përgjegjësi për të siguruar që të mos ketë rreziqe për rrjedhjen e të dhënave gjatë transferimit, duke vlerësuar gjithashtu që të dhënat të arrijnë destinacionin e duhur.[3] Rreziqet e mësipërme mund të shmangen, për shembull, përmes enkriptimit dhe masave të forta të autentitkimit.

Organizatat që duhet të jenë në përputhje me GDPR duhet të fillojne me dy kategori të ndryshme të kornizave ekzistuese per sigurine e informacionit:

1. Kornizat e sigurisë kibernetike si ISO 27001/27002, Korniza e Sigurisë Kibernetike e NIST.

2. Kornizat e privatësisë ose seksionet specifike të privatësisë që gjenden në shembuj si ISO 29100, ISO 27018.

GDPR është shtytësi kryesor për sigurinë kibernetike per organizatat e të dhenave personale. Ai ka rritur ndjeshëm nivelin e ndërgjegjësimit midis organizatave për rrjedhjen e të dhënave që vijnë nga krimi kibernetik dhe nevojën për mbrojtje.

Frika nga ndëshkimet financiare ka ndryshuar mënyrën se si organizatat po mendojnë për mbrojtjen dhe sigurinë e të dhënave. Shumë biznese kanë rishikuar mënyrën e mbrojtjes së të dhënave dhe kontrollet e privatësisë së të dhënave dhe kanë bërë një investim në mbrojtjen e aseteve të të dhënave. Në Angli, 62% e bizneseve investuan më shumë në sigurinë kibernetike per tu pergatitur per permbushjen e udhezimeve te GDPR, 49% nuk besojnë se GDPR e ka bërë biznesin e tyre më të sigurt dhe 26% nuk besojnë se një vit pas afatit të përmbushjes se GDPR, biznesi i tyre është plotësisht në përputhje me të. [7]

2. GDPR dhe legjislacioni shqiptar

Në Shqipëri, AKCESK është Autoriteti përgjegjës për implementimin dhe mbikqyrjen e zbatimit të legjislacionit në fushën e sigurisë kibernetike. Gjithashtu, AKCESK, përcakton standardet minimale teknike për sigurinë e të dhënave dhe rrjeteve/sistemeve kompjuterike të shoqërisë së informacionit, në përputhje me standardet ndërkombëtare në këtë fushë, me qëllim krijimin e një mjedisi të sigurtë. Misioni i Autoritetit është arritja e një niveli të lartë të sigurisë kibernetike, duke përcaktuar masat e sigurisë, të drejtat, detyrimet, si dhe bashkëpunimin e ndërsjellë ndërmjet subjekteve që operojnë në fushën e sigurisë kibernetike. [2] Udhëzimet e GDPR dhe ligji i sigurise kibernetike detyrojnë organet e të dhënave personale të plotësojnë kërkesat e njoftimit në rast incidenti. Megjithatë, ato mbrojnë interesa të veçanta dhe zbatohen për lloje të ndryshme incidentesh.

Së pari, ligji i sigurisë kibernetike dhe udhëzimet e GDPR zbatohet nga instanca të ndryshme. GDPR zbatohet për çdo person ose subjekt që përpunon të dhënat personale të shtetasve për ofrimin e mallrave dhe shërbimeve ose për të monitoruar sjelljen e tyre. Ligji i sigurise kibernetike zbatohet për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit. Kështu, mbivendosja ndodh vetëm në lidhje me ata operatorë që përpunojnë të dhëna personale.

Së dyti, qëllimi i GDPR është të ruajë të dhënat personale, ligji i sigurisë kibernetike ka si qëllim sigurinë e rrjetit dhe sistemeve. Kështu, GDPR kërkon që kontrollorët të miratojnë masa që sigurojnë të dhënat personale, ndërsa ligji i sigurisë kibernetike kërkon që operatorët të sigurojnë siç duhet rrjetet e tyre për të mbrojtur ofrimin e shërbimit. Mund të ndodh që kur këto qellime te mbivendosen, qëllimi i njërit prej tyre nuk mund të plotësohet. Për shembull, kriptimi mbron të dhënat personale sipas GDPR pa mbrojtur rrjetin nga dobësitë siç kërkon ligji i sigurisë kibernetike.

Për njoftimin për rrjedhjen e të dhënave, GDPR kërkon që kontrollorët të njoftojnë autoritetin kompetent për kete rrjedhje “pa vonesë dhe, kur është e mundur, jo më vonë se 72 orë pasi të kenë marrë dijeni për këtë, nëse shkelja e të dhënave personale nuk perben rrezik për të drejtat dhe liritë e individëve.” [3] Pra, GDPR kërkon njoftimin e rrjedhjes së të dhënave vetëm kur të dhënat personale janë në rrezik. Ligji i sigurisë kibernetike, detyron njoftimin për rrjedhjen e të dhënave nëse ka një ndërprerje të konsiderueshme në ofrimin e shërbimit. Nuk ka sanksione për kompromentimin e informacionit specifik, siç ka sipas GDPR kur nuk janë mbrojtur të dhënat personale. Në vend të kësaj, ligji penalizon operatorët që nuk zbatojnë masat e duhura të sigurisë ose nuk njoftojnë autoritetet kompetente për një incident.

Së fundi, sipas ligjit të sigurisë kibernetike, operatorët duhet të njoftojnë vetëm autoritetet kompetente. GDPR, kërkon që kontrollorët të njoftojnë subjektet e të dhënave, individët, nëse shkelja paraqet një “rrezik të lartë” për të drejtat dhe liritë e tyre. GDPR u siguron këtyre individëve përveç mjeteve juridike administrative dhe një të drejtë veprimi, për të mbrojtur të drejtat e tyre. Ligji i sigurisë kibernetike parashikon vetëm gjoba administrative.

GDPR është një rregullore për mbrojtjen e të drejtave të individëve për përdorimin e të dhënave të tyre personale. Si një model rregullator, GDPR merret veçanërisht me parimet dhe të drejtat që çdo organizate duhet të ndjekë në menaxhimin dhe mbrojtjen e të dhënave personale. Megjithatë, GDPR shmang identifikimin e mjeteve më të përshtatshme që një organizate duhet të zgjedhë për të zbatuar keto rregulla. Pasi çdo kompani ose organizatë është e ndryshme nga të tjerat dhe i njëjti përpunim i të dhënave, i cili mund të jetë një rrezik i lartë për të drejtat dhe liritë e personave për një kompani, mund të jete një rrezik me i ulët për një kompani tjetër që ushtron biznesin në një fushë tjetër.

Megjithate, GDPR rekomandon që organizata të vendosë masa sigurie për të garantuar një nivel të duhur sigurie mbi çdo përpunim të të dhënave, sidomost në rastet e përpunimit që mund të rezultojë në një rrezik të lartë për të drejtat dhe liritë e personave fizik. Nese të dhënat e një ogani janë në përputhje me GDPR nuk do të thotë që të dhënat janë të sigurta. Mbrojtja e të dhënave është vetëm

një pjesë për përmbushjen e sigurisë, që nënkupton zbatimin e masave, politikave dhe procedurave në lidhje me sigurinë brenda një organizate.

3. Rishikimi dhe përmirësimi i kornizës ligjore

Një qasje gjithëpërfshirëse kombëtare e sigurisë kibernetike, nuk mund të bëhet duke përdorur vetëm teknologjitë dhe shërbimet, por duhet të shoqërohet me një kornizë ligjore të mirë dhe aktuale, me fokus në natyrën dinamike të mjedisit të TIK-ut dhe natyrën evoluese të kërcënimeve kibernetike. Aktualisht, autoritetet e sigurisë në vend, kanë krijuar bazën ligjore mbi të cilën të ushtrojnë veprimtarinë e tyre. Pavarësisht hartimit të ligjeve e akteve nënligjore, rregulloreve dhe standardeve nga analiza e kryer, si dhe nga vlerësimi i nivelit të maturimit të sigurisë kibernetike në vend, është evidentuar nevoja për rishikim të të gjithë kuadrit ligjor e rregullator, me qëllim harmonizimin e plotë me direktivat e Bashkimit Evropian, si dhe koordinimin e brendshëm institucional. [4] Realizimi i këtij objektivi specifik synon të kryejë harmonizimin e legjislacionit shqiptar mbi sigurinë kibernetike me atë të BE-së. Në këtë kontekst, përmirësimi i legjislacionit kombëtar shqiptar për sigurinë kibernetike duhet të konsiderojë edhe adresimin e udhëzimeve të GDPR 2016/679 për sigurinë kibernetike për organet e mbrojtjes së të dhënave personale. Ne propozojmë që adresimi i udhëzimeve të GDPR-së të bëhet në konteksin e përmirësimeve të legjislacionit për sigurinë kibernetike bazuar në argumentat e mëposhtëm.

Kur mbrojtja e të dhënave dhe siguria kibernetike kanë të bëjnë me mbrojtjen e të dhënave sensitive nga kërcënime të ndryshme dixhitale, ato duhen të ndërlidhen. Në rast shkeljesh, në vend të përgjigjeve të ndara, është më efikase një qasje të integruar e trajtimit të incidentit.

Një arsye tjetër është se aktualisht në Shqipëri për organet e mbrojtjes së të dhënave personale nuk ka asnjë detyrim për të zbatuar standardet kombëtare të sigurisë së TIK-ut. Megjithatë, disa sektore psh, sektori i financave si bankat, ndjekin standardet që zbatohen në vendet e tjera evropiane, si Rregullorja e Përgjithshme për Mbrojtjen e të Dhënave (GDPR) ose standardet ISO (Organizata Ndërkombëtare për Standardizim) edhe pse nuk janë të certifikuara.

Në një studim të Qendres per Inovacioni Protik në bashkëpunim me RisiAlbania per vitin 2021, ku ishin mbledhur të dhëna nga 180 kompani shqiptare nga sektori i TIK-ut, prodhimit, mikpritjes dhe turizmit, rezultoi se legjislacioni, rregulloret dhe aktet kanë një ndikim të drejtpërdrejtë në dixhitalizimin e sektorëve ekonomikë duke u fokusuar kryesisht në mbrojtjen e të dhënave, transaksionet dixhitale, mbrojtjen e konsumatorëve dhe tregtinë elektronike. [5] Kompanitë janë të ndjeshme në zbatimin e kuadrit ligjor për dixhitalizim dhe mbrojtjen e të dhënave personale.

Së fundmi, shumica e rrjedhjeve të të dhënave janë pasojë e sulmeve dashakeqe. Studimi i Institutit Ponemon paraqet një përmbledhje të tre kategorive kryesore për shkaqet kryesore të rrjedhjes së të dhënave. 52% e incidenteve përfshinin një sulm dashakeq, krahasuar me 25% të shkaktuar nga defektet e sistemit dhe 23% të shkaktuar nga gabimet njerëzore. [6]

4. Konkluzionet

Siguria kibernetike adreson mbrojtjen e sistemeve kritike dhe informacioneve sensitive nga sulmet kibernetike, ndërsa GDPR adreson ceshtjet që mbrojtjen e të dhënave. Megjithëse nuk është krijuar për qëllime të sigurisë kibernetike, GDPR është një orjentues i mirë për të adresuar siç duhet sigurinë (dhe mbrojtjen e të dhënave) në një fazë të hershme. Nga ana tjetër, shmangia e penaliteteve financiare që shoqërojnë mos zbatimin e GDPR janë kthyer në një shtytës kryesor për sigurinë kibernetike.

Në Shqipëri, AKCESK është Autoriteti përgjegjës për implementimin dhe mbikqyrjen e zbatimit të legjislacionit në fushën e sigurisë kibernetike[2] duke përcaktuar standardet minimale teknike për sigurinë e të dhënave dhe rrjeteve/sistemeve kompjuterike të shoqërisë së informacionit, në përputhje

me standardet ndërkombëtare në këtë fushë. Megjithëse udhëzimet e GDPR dhe ligji i sigurisë kibernetike detyrojnë organet e të dhënave personale të plotësojnë kërkesat e njoftimit në rast incidenti, ato mbrojnë interesa të veçanta dhe zbatohen për lloje të ndryshme incidentesh.

Aktualisht, autoritetet e sigurisë në vend, kanë krijuar bazën ligjore mbi të cilën të ushtrojnë veprimtarinë e tyre, megjithatë është i nevojshëm rishikimi i të gjithë kuadrit ligjor e rregullator me qëllim harmonizimin e plotë me direktivat e Bashkimit Evropian dhe koordinimin e brendshëm institucional. Në këtë konteks, përmirësimi i legjislacionit kombëtar shqiptar për sigurinë kibernetike duhet të konsiderojë edhe adresimin e udhëzimeve të GDPR 2016/679 për sigurinë kibernetike për organet e mbrojtjes së të dhënave personale.

Në këtë punim ne propozojmë që adresimi i udhëzimeve të GDPR-së të bëhet ne konteksin e përmirësimeve të legjislacionit për sigurisë kibernetike sepse në këtë mënyrë do të rritet efikasiteti i përgjigjes në rast incidentesh, do të rritet më shumë ndjeshmëria në mbrojtjen e të dhënave personale dhe nxitet një komunitet më i madh biznesesh për ti kushtuar vëmendjen e duhur sigurisë kibernetike dhe mbrojtjes së të dhënave.

References

[1] GDPR will Help Enhance Cyber Security, [Online]. Available: https://innovationatwork.ieee.org/gdpr-cyber-security/ [Accessed: May. 07, 2022].

[2] Law No.2 . 2017, "On Cyber Security", [Online]. Available: https://cesk.gov.al/publicAnglisht_html/legjislacioni/index.html. [Accessed: May. 07, 2022].

[3] GDPR, General Data Protection Regulation, [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed: May. 02, 2022].

[4] ITU, Global Cybersecurity Index 2020, 2021.

[5] Protik Innovation Centers, RisiAlbania, Market Assessment of Digital Solution Opportunities in the Albanian Economy, 2021.

[6] Cost of a Data Breach Report 2020, IBM Corporation.

[7] Impact Of The GDPR On Cyber Security Outcomes, Final Report, August 2020.