Summer 6-2018

NDIKIMI I KRIMEVE KIBERNETIKE DHE PRIVATËSIA NË INTERNET

Besarta Pllana

Kolegji UBT
Fakulteti i Sistemeve të Informacionit

NDIKIMI I KRIMEVE KIBERNETIKE DHE PRIVATËSIA NË INTERNET

Shkalla Bachelor

Besarta Pllana

Qershor, 2018
Prishtinë

Kolegji UBT
Fakulteti i Sistemeve të Informacionit

Punim Diplome
Viti akademik 2015-2016

Besarta Pllana

NDIKIMI I KRIMEVE KIBERNETIKE DHE PRIVATËSIA NË INTERNET

Mentori: PhD Cand. Blerton Abazi

Qershor, 2018

Ky punim është përpiluar dhe dorëzuar në përmbushjen e kërkesave të pjesëshme për Shkallën Bachelor.

ABSTRAKT

Dita ditës avancimi i teknologjisë dhe përdorimi i internetit ka kufizuar privatësinë tonë. Ndarja e shumë informatave në internet është bërë e pashmangshme dhe në masë te madhe heq barrierat mes asaj se çka duhet të jetë private dhe çka publike. Pikërisht për këtë arsye kjo tematikë do të jetë si një lloj thirrjeje dhe përkujtimi i gjendjes aktuale të privatësisë në internet, si dhe rreziqet që mund të vijnë për shkak të kësaj gjendjeje.Si rezultat i internetit të dhënat tona private nuk janë më private. Ironikisht përdoruesit vazhdojnë të japin të dhënat e tyre personale kudo që ju kërkohen gjë që është mjaftë shqetësuese.Privatësia në internet është një e drejtë themelore e njeriut.

Pra në këtë kohë kur sfida e shumicës së njerëzve është të fitojnë sa më shumë para dhe të arrijnë majat më të larta të suksesit, ka te atillë që këtë e bëjnë me pandershmëri të plotë. Janë të shumtë ata të cilët marrin pa të drejtë identitetin online të të tjerëve dhe që manipulojnë me të dhënat e tyre.

Kjo temë është e rëndësishme për shumë arsye. Fillimisht, të kuptuarit e rëndësisë së privatësisë në internet dhe krimeve kibernetike dhe ndërlidhjen mes tyre , pastaj të kuptuarit e nivelit të saj dhe se sa ekziston një gjë e tillë janë pikat kyçe që do trajtohen në këtë temë. Kjo do të na ndihmojë që në të ardhmen të dijmë si të ruajmë privatësinë tonë në internet dhe si të mbrohemi nga krimet kibernetike dhe se çfarë duhet të bëjmë për këtë.

Qëllimi i këtij punimi është të hulumtojmë lidhur me sigurinë dhe privatësinë e të dhënave tona për sigurinë kibernetike, se sa ruhet privatësia jonë se sa ne duhet të kemi kujdes me të dhënat tona, se si duhet t'i mbrojmë të dhënat tona personale në internet, se a mbrohen të dhënat tona personale me ligje në vendin tonë e shumë aspekte të tjera që tregojnë rëndësinë e privatësisë.

MIRËNJOHJE/FALËNDERIME

Falënderimet më të mëdha për familjen time cila ka qenë me mua që nga fillimi i këtij rrugëtimi duke e bërë më të lehtë çdo hap timin.

Falenderimi gjithashtu shkon edhe për shoqërinë për bashkëpunimin, përkrahjen dhe kujtimet e mira gjatë kohës së studimeve.

Një falënderim të posaçëm kam për Profesorin Blerton Abazin për ndihmën e pakursyer që më ka dhënë gjatë studimeve si dhe për mbështjetjen morale dhe gatishmërinë që më ofroi gjatë gjithë punës sime drejt përfundimit të temës së diplomës. Profesori ishte gjithmonë i gatshëm për konsultime, këshilla profesionale dhe përkrahje.

Falënderoj gjithashtu gjithë profesorët dhe asistentët për përkrahjen e tyre të vazhdueshme.

Ju falënderoj të gjithëve.

PËRMBAJTJA

LISTA E FIGURAVE

FJALORI I TERMEVE

PII – Personally Identifiable Information

ISP – Internet Service Provider

PIPL – People Search

HTTPS – Hypertext

IRS – Internal Privat Network

GDPR – General Data Protection Regulation

Wi-Fi – Wireless Fidelity

CIA – Confidentiality, Integrity , Availability

DOS - Denial-of-Service

TCP- Transmission Control Protocol

IP – IP Address

ICMP – Internet Control Message Protocol

MitM – Man-in-the-Middle

URL – Uniform Resource Locator

PHP – Hypertext Pre Processor

PE – Provider Edge Router

SQL – Structured Query Language

ASP – Application Service provider

XSS – Cross-site Scripting

IT – Internet Technology

SSL – Transport Layer Security

1 HYRJA

Sot, interneti është më i madh se çka dikush parashikoi se do të bëhej ndonjëherë. Që herët interneti i të 90-tave ka pasur një ndikim në shoqëri në përgjithësi dhe më e rëndësishmja në biznese. Ajo që ishte dikur një mënyrë e thjeshtë e shkëmbimit të informacionit është bërë në njëfarë mënyre, një databazë që përmban një pasuri shumë të ndryshme të informacionit. Ka blogje, faqe të rrjeteve sociale, forume diskutimi dhe një sërë faqesh e blerjeve online. Organizatat e korporatave përdorin internetin në një shumëllojshmëri të mënyrave për të promovuar biznesin e tyre dhe individët përdorin faqet e rrjeteve sociale dhe bloget për të praktikuar në mënyrë të dukshme jetën e tyre.

Privatësia përcaktohet si e drejtë për t'u çliruar nga mbikëqyrja dhe për të përcaktuar nëse kur dhe për të cilin duhet zbuluar informacioni personal apo organizativ i tij. Kompani të tilla si Facebook kanë politika të privatësisë dhe mund të mbrojnë të dhënat tuaja private nga ndërhyrës të jashtëm, por çfarë po bëjnë ata me informacionin tuaj dhe me kë po e ndajnë? Në të njëjtën mënyrë, korporatat e mëdha mund të kenë rrjete të sigurta për t'u mbrojtur nga hakerët dhe kriminelët e tjerë në internet, por çfarë po bëjnë ata me informacionin tuaj dhe me kë po e ndajnë?

Fusha problematike që drejton hulumtimin për këtë tezë është madhësia në të cilën informatat personale momentalisht ndahen në internet dhe siguria ose mungesa e saj.

Krimi kibernetik është tani një nga sfidat më të mëdha ligjore. Që nga viti 2000 deri në vitin 2014 interneti është zgjeruar me një normë mesatare prej 741.0% në nivel global dhe aktualisht rreth 3 miliardë njerëz janë online. Hapësira kibernetike sot është një nga sfidat më të mëdha ligjore e cila ka nxitur një formë tjetër të krimit, duke krijuar një mjedis për metodat e reja të krimit. Tani pothuajse të gjitha krimet mund të kryhen me përdorimin e kompjuterëve.

2 SHQYRTIMI I LITERATURËS

2.1 Privatësia në internet

Shqyrtimi i literaturës ofroi disa përkufizime interesante për termin ‘privatësi’. Në një nga përkufizimet e tij më të vjetra, q ë përshkruan privatësinë si 'të drejtën për t'u larguar'. Ndërsa kjo është një përkufizim i thjeshtë i privatësisë. *(Warren dhe Brandeis, 1890*) .

Një përkufizim më të hollësishëm duke vënë në dukje se privatësia ishte një formë e kontrollit individual mbi zbulimin dhe përdorimet pasuese të informacionit personal të dikujt. Privatësia e internetit është niveli i privatësisë dhe sigurisë së të dhënave personale të publikuara nëpërmjet internetit. Është një term i gjerë që i referohet një sërë faktorësh, teknikash dhe teknologjish të përdorura për të mbrojtur të dhëna të ndjeshme dhe private, komunikime dhe preferenca.

Privatësia dhe anonimiteti i internetit janë shumë të rëndësishme për përdoruesit, veçanërisht pasi e-commerce vazhdon të fitojë tërheqje. Shkeljet e privatësisë dhe rreziqet e kërcënimit janë konsiderata standarde për çdo faqe interneti në zhvillim. *(Westin,1967)*

Privatësia e internetit gjithashtu njihet si privatësia në internet.
Privatësia e internetit është shkak për shqetësim për çdo përdorues që planifikon të bëjë një blerje në internet, të vizitojë një faqe të rrjeteve sociale, të marrë pjesë në lojëra online ose të ndjekë forume. Nëse një fjalëkalim kompromentohet dhe zbulohet, identiteti i viktimës mund të përdoret ose të vjedhet me mashtrim. *(Assets.mozilla.net, 2018)*
Privatësia në internet, është e drejtë themelore e njeriut. Ajo i referohet privatësisë personale që njerëzit kanë të drejtë ta kenë kur ofrojnë, shfaqin ose ruajnë informacione rreth vetes në internet
Privatësia në internet po bëhet një shqetësim në rritje për këto ditë për njerëzit e të gjitha mo-shave. Kompanitë ndjekin sjelljen tuaj nëpër faqet e internetit për t'ju shërbyer reklama shumë relevante. Qeveritë monitorojnë çdo lëvizje që bëni për të parashikuar sjelljen tuaj dhe për të kontrolluar më mirë. Dhe kriminelët kibernetikë vjedhin të dhënat tuaja për qëllimet e tyre të poshtëra!

Intimiteti i internetit, gjithashtu i referuar si privatësia në internet, është nëngrup i privatësisë së të dhënave dhe një e drejtë themelore e njeriut. Në thelb, ajo i referohet privatësisë personale që ju keni të drejtë kur shfaqni, ruani ose jepni informacion në lidhje me veten tuaj në internet.

Kjo mund të përfshijë informacionin personal identifikues (PII), si dhe informacione që nuk identifikojnë personalisht, të tilla si sjellja juaj në një faqe interneti. Pa fshehtësinë e Internetit, të gjitha aktivitetet tuaja i nënshtrohen mbledhjes dhe analizës nga palët e interesuara *(Shahid and Shahid, 2018).*

Po ashtu përsëritin studimin e njëtë të vitit 2002 me qëllim të hulumtimit nëse gjatë kësaj periudhe kohore ka ndryshuar diçka në lidhje me privatësinë e përdoruesve të internetit, mirëpo rezultatet tregojnë që shqetësimet e tyre mbesin të njëjta dhe vetëm sa janë rritur, dhe ironikisht përdoruesit vazhdojnë të japin të dhënat e tyre personale kudo që ju kërkohen. (*Anton dhe Earp, 2010)*

Si shumë hulumtime të tjera rreth privatësisë, u hulumtuan perceptimet e rrezikut në lidhje me pazaret online dhe vuri në dukje se shqetësimi më i madh në mesin e përdoruesve ishte me të vërtetë privatësia e tyre.*(Miyazaki & Fernandez,2001)*

Po ashtu shpjegohet se privatësia individuale është kryesisht një tërësi dhe se në botën online, njerëzit, organizatat dhe qeveritë dëgjojnë jo vetëm atë që është publike, por edhe atë që duhet të mbetet private. U theksua se për të trajtuar çështjet që kanë të bëjnë me privatësinë individuale, do të duhej një qasje multidisiplinare që bashkon njohuritë nga shkencat shoqërore dhe shkencat humane me shkenca kompjuterike. *(Almeida, 2012)*

Dy autror e definojnë si "paradoksi i privatësisë". Pra, pavarësisht faktit që janë të brengosur për të dhënat e tyre prapë nuk ndërmarrin asgjë për t'i mbrojtur ato.

Njerëzit përdorin mediat sociale për ndërveprime të rëndësishme sociale si mbajtja e kontakteve me miqtë dhe familjen dhe kthimin e kontakteve me miqtë e vjetër. Veçanërisht adoleshentët raportojnë se mediat sociale janë të rëndësishme për miqësitë e tyre dhe, ndonjëherë, për lidhjet e tyre romantike. *(Barnes, 2006 dhe Norberg, 2007)*

Përveç kësaj,studimet dokumentojnë se mediat sociale luajnë një rol në mënyrën se si njerëzit marrin pjesë në aktivitete qytetare dhe politike, nisjen dhe mbajtjen e protestave, marrjen dhe shpërndarjen e informacionit shëndetësor, mbledhjen e informacionit shkenëcor, angazhimin

në çështjet familjare, kryerjen e aktiviteteve të punës dhe marrjen e lajmeve. Autorët Barnes (Përderisa ka dëshmi se mediat sociale punojnë në disa mënyra të rëndësishme për njerëzit, studimet e Qendrës Kërkimore Pew kanë treguar se njerëzit janë të shqetësuar për gjithë informacionin personal që mblidhet dhe ndahet dhe sigurinë e të dhënave të tyre.

Në përgjithësi, një sondazh i vitit 2014 zbuloi se 91% e amerikanëve "pajtohen" ose "pajtohen plotësisht" se njerëzit kanë humbur kontrollin informacioneve personale se si grumbullohen dhe përdoren nga të gjitha llojet e entiteteve. Rreth 80% e përdoruesve të mediave sociale thanë se ishin të shqetësuar për reklamuesit dhe bizneset që u qasen të dhënave që ata ndajnë në platformat e mediave sociale dhe 64% thanë se qeveria duhet të bëjë më shumë për të rregulluar reklamuesit. Një tjetër sondazh i vitit të kaluar zbuloi se vetëm 9% e përdoruesve të mediave sociale ishin "shumë të sigurt" që kompanitë e mediave sociale do t'i mbronin të dhënat e tyre. Rreth gjysma e përdoruesve nuk ishin fare ose nuk ishin shumë të sigurtë se të dhënat e tyre ishin në duar të sigurta.

Për më tepër, njerëzit e kanë vështirë ta kuptojnë natyrën dhe shtrirjen e të dhënave të mbledhura mbi ta. Vetëm 9% besojnë se kanë "shumë kontroll" mbi informacionin që mblidhet rreth tyre, edhe pse shumica dërrmuese (74%) thonë se është shumë e rëndësishme për ta që ta kenë në kontroll se kush mund të marr informacione rreth tyre. Gjashtë në dhjetë amerikanë (61%) kanë thënë se do të donin të bënin më shumë për të mbrojtur privatësinë e tyre. Përveç kësaj, dy të tretat kanë thënë se ligjet aktuale nuk janë mjaft të mira për mbrojtjen e privatësisë së njerëzve, dhe 64% mbështesin më shumë rregullimin e reklamuesve *(Rainie, 2018).*

Figure 1:Privatësia në internet

(Shahid and Shahid, 2018)

2.2 Shqetësim për privatësinë

Janë bërë shumë studime duke shqyrtuar shqetësimet e njerëzve në lidhje me privatësinë në internet, veçanërisht në lidhje me informacionin personal. Për shembull, një hulumtim zbuloi se konsumatorët në internet janë të shqetësuar nëse ofruesit e internetit i shesin të dhënat e tyre personale palëve të treta pa pëlqimin apo njohurinë e tyre. Mbi 80 për qind e konsumatorëve thjesht nuk dëshironin që informacioni i tyre të ribotohej në biznese të tjera *(Hoffman et.al, 1999).*

Në mënyrë të ngjashme, në vitin 2002, një sondazh Interactive zbuloi se shumica e konsumatorëve janë të shqetësuar për humbjen e kontrollit mbi mbledhjen e informacionit personal dhe të përdorura nga kompanitë. Rreth 75 përqind e të anketuarve ishin të shqetësuar për kërcënimin e të dhënat e tyre personale bien në duart e palëve të treta (individë ose kompani) *(Harris, 2002).*

Interesante, një studim izbuloi se konsumatorët ishin të gatshëm dhe të ndjerë të rehatshme në sigurimin e informacionit në një faqe interneti, por vetëm nëse faqja ka dhënë njoftim për mënyrën se si do të përdoret informacioni i mbledhur para publikimit. *(Westin, 1997)*

Autorët sugjerojnë se shumica e konsumatorëve nuk kanë informacion të mjaftueshëm për të marrë vendime të ndjeshme ndaj privatësisë dhe madje edhe kur ata kanë informacion, ata ka

të ngjarë të injorojnë shqetësimet afatgjata të privatësisë për përfitime afatshkurtra. *(Acquisti dhe Grosslags, 2005).*

Po ashtu është kryer një studim për të përcaktuar nëse besimi në përdorimin e teknologjisë kompjuterike në lidhje me katër komponentët e privatësisë së informacionit. Të dy më të rëndësishme për këtë hulumtimet janë përdorimi i paautorizuar dytësor dhe qasja e pahijshme. Gjetjet e këtij studimi mbështesin idenë se përdoruesit e internetit mund të largohen nëse kërkohet informacion i papërshtatshëm dhe megjithëse ata janë më të shqetësuar për aksesin e paautorizuar dhe përdorimin dytësor të informacionit personal, gjykimi i tyre për aftësinë e tyre për të kontrolluar kompjuterin nuk është konsideratë. Kjo do të thotë se edhe pse privatësia është një çështje për ne, ne nuk e kuptojmë se ne jemi me të vërtetë nën kontrollin e të dhënave që ne i ndajmë dhe, nëse diçka duket e mirë tani, ne jemi ka më shumë gjasa të dëshirojë të shijojë lëvizjen e tanishme sesa të shqetësohet për implikimet e ardhshme të informacionit tonë personal. *(White et. al , 2008)*

Për më tepër, një studim i kryer zbuloi se shqetësimet e privatësisë nuk luajtën drejtpërdrejtë një rol kuptimplotë në udhëheqjen e sjelljes së informacionit të përdoruesve. Ata zbuluan se ndërveprimi mes njohurisë, shqetësimit dhe shpërblimit luajti një rol të rëndësishëm në përcaktimin sjellje informacioni. *(Park et al, 2012)*

Pra, ndërsa White et.al argumentojnë se ne jemi në fakt në kontrollin e informacionit që ndajnë, Park et. al nënkuptojnë se kompanitë mund të menaxhojnë sjelljen e njerëzve duke u ofruar atyre një formë shpërblimi dhe duke i bërë ata më të gatshëm për të ndarë informata personale.

E argumentuan se intimiteti, si një e drejtë kushtetuese, është subjekt i ndryshimit të normave si rezultat i ardhjes së shoqërisë së informacionit. Duke marrë parasysh të gjitha gjetjet e mësipërme të hulumtimit, mund të argumentohet se praktika më e mirë për të siguruar kontrollin mbi informacionet personale të tyre është leximi i njoftimeve të privatësisë ose i politikave të faqeve të internetit dhe të mësuar rreth praktikave të informacionit të organizatës. (*Kleve & Mulder ,2008)*

Studimet e bëra pohuan se ky informacion mund të ndihmojë konsumatorin të vendosë nëse do të zbulojë ose jo informacione personale në faqen e internetit. Kjo gjithashtu mund të zvogëlojë rrezikun e shkëmbimit të informacionit tek një palë e tretë. (*Culnan & Milberg , 1998)*

Për më tepër, në një studim të kohëve të fundit u konkludua se politikat e privatësisë duhet të hartohen me këndvështrimin e përdoruesit.

Është e drejtë të thuhet se shumica e politikave të privatësisë zakonisht kanë interesat e përdoruesve në zemër thjesht duke siguruar që të dhënat personale të mbeten të sigurta dhe jashtë fushës publike. pjesa tjetër e politikës është në të vërtetë për të mbështetur kompaninë në vend të përdoruesit. Në fakt, disa faqe të rrjeteve sociale do t'ju lejojnë të bashkoheni vetëm nëse jeni dakord që ata të ndajnë së paku disa nga të dhënat tuaja personale me palët e treta, p.sh. Facebook. (*Lin, 2012)*

2.3 Çështjet më të zakonshme që rrethojnë privatësinë në internet në ditët e sotme

Tani që ju e kuptoni se çfarë është privatësia e internetit dhe rëndësia e saj, le të diskutojmë çështjet më të zakonshme që rrethojnë privatësinë tënde në internet sot:

2.3.1 Ndjekja

Kur shfletoni internetin, mund të keni vërejtur ato reklama bezdisëshme që vijnë pas jush, ku shkoni, që bazohen në kërkimet tuaja më të herëshme në internet ose në vizita në faqet e internetit. E pra, kjo është për shkak se lëvizjet tuaja janë gjurmuar nga faqet e internetit, reklamuesit,

Profilimi i cookit dhe teknika të tjera përdoren për të gjurmuar aktivitetet e përgjithshme në internet dhe për të krijuar një profil të detajuar të shprehive tuaja të shfletimit. Disa njerëz mund të mos kenë mendje që reklamat relevante t'u shërbejnë atyre, por për të tjerët kjo është një pushtim serioz i privatësisë.

2.3.2 Mbikëqyrja

Disa qeveri spiunojnë qytetarët e tyre online për të ndihmuar gjoja agjencitë e zbatimit të ligjit. Merrni, për shembull, Aktin e Fuqive Hetuese të Britanisë së Madhe që autorizon vëzhgimin masiv dhe i lejon qeverisë që të mbikëqyrë ligjërisht përdorimin e internetit të

qytetarëve të saj.
Kompanive të internetit (ISP), telcos, si dhe ofruesit e tjerë të shërbimeve të komunikimit kërkohet të mbajnë të dhënat e konsumatorëve për lidhje interneti për një vit, të cilat mund të merren nga autoritetet qeveritare dhe të përdoren në hetime - edhe nëse nuk jeni të lidhur me to në në asnjë mënyrë!

2.3.3 Vjedhja

Mbi 17 milionë amerikanë tronditëse janë prekur nga vjedhjet e identitetit në vitin 2017, sipas Javelin Strategy. Kriminelët kibernetikë përdorin teknika malware, spyware dhe phishing për t'u futur në llogaritë ose pajisjen tuaj online dhe vjedhin të dhënat tuaja personale për t'u angazhuar në aktivitete si vjedhjet e identitetit.
Viktimat natyrisht përfundojnë duke humbur shumicën ose të gjitha paratë e tyre të fituara, vetëm për shkak se nuk kanë pasur kujdes kur janë në lidhje me hapjen e bashkëngjitjeve, mesazheve të menjëhershme ose emaileve nga burime të panjohura.. (Shahid and Shahid, 2018)

2.4 Sjelljet në internet që ndikojnë në privatësinë tuaj

Ju keni dëgjuar herë pas here se privatësia dhe siguria në internet janë të rëndësishme, por a keni bere në të vërtetë diçka në lidhje me të? Shumica prej nesh e praktikojnë higjienën e keqe të Internetit dhe as nuk e kuptojnë atë, prandaj mos harroni të shmangni bërjen e mëposhtme:

2.4.1 Përdorimi i të njëjtave kredenciale për llogaritë e shumëfishta

Sigurisht, është e lehtë të mbani mend dhe të bëni gjërat në internet kur përdorni të njëjtat kredenciale në llogaritë tuaja. Por në qoftë se një kriminel kibernetik është në gjendje të fitojë akses në llogaritë tuaja , ata do të marrin më shumë mundësi edhe në ato të tjera.

2.4.2 Qëndrimi i regjistruar në uebfaqe

Mos kyqja nga faqet e internetit dhe duke pasur mundsin per ti mbajtur ne mend te dhenat eshte me te vertet e papershtatshme.
Megjithate ajo gjithashtu I le llogrite dhe informatat personale te prekshme ndaj kudo qe e perdor apo hakon ne paisjet e tuaja.

2.4.3 Përdorimi i Shërbimeve pa Lexuar Termat dhe Kushtet e tyre

Asnjëherë mos kliko "agree" derisa të kuptoni se ne çfarë po e futni veten tuaj. Ju nuk do të doni të jepni ligjërisht kompanive dhe ofruesve të shërbimeve qasje në të gjitha llojet e të dhënave. Më pas shitni këtë informacion te ofertuesi më i lartë!

2.4.4 Hapja e bashkëngjitjeve të dyshimta ose shkarkimi i skedarëve keqdashës

Duhet të jeni të kujdesshëm kur hapni ndonje bashkëngjitjet apo shtese në email ose në mediat sociale, pasi ato mund të përmbajnë malware dhe viruse. Ngjashëm, gjithmonë kur shkarkoni skedarë nga burime të besuara, sepse mund të rezultojë në një infeksion të virusit. *(Shahid and Shahid, 2018)*

2.5 Mënyrat e thjeshta për të mbrojtur privatësinë tuaj

Ndërkohë që mund të mendoni se informacioni juaj personal është personalisht, do të habiteni sa shumë informata rreth jush përfundojnë në internet. Vetëm bëni një kërkim për veten në Pipl, një direktori për kërkimin e njerëzve, për të parë detajet personale atje. (Shko, ne do të presim.) Shanset janë kërkimi që erdhi me emrin tuaj, profilet e mediave sociale dhe ndoshta edhe emrat e prindërve tuaj, adresën dhe numrin e telefonit.
Pipl nuk është një bazë e dhënash sekrete e hakerëve. Është vetëm një depo e të dhënave publike në dispozicion në internet për individë, të cilat bizneset dhe reklamuesit janë të etur për të marrë në duart e tyre. Kjo është e drejtë: ky lloj i grumbullimit të të dhënave është

krejtësisht legjitim, dhe shumë prej tij është tërhequr nga informacionet që vendosni në internet.

Nëse jeni i shqetësuar për vjedhjet e identitetit ose thjesht nuk i pëlqeni ideja e njerëzve të tjerë që ndjekin çdo lëvizje, ka hapa që mund të ndërmarrni për të mbajtur të dhënat tuaja private private. *(Harper, 2018)*

2.5.1 Fjalëkalimi – mbron gjithçka

Ju nuk mund të mendoni se është e domosdoshme për të mbrojtur me fjalëkalimin kompjuterin tuaj në shtëpi, por të gjitha pajisjet tuaja digjitale duhet të jenë të mbrojtura me fjalëkalim. Kjo përfshin kompjuterat, tabletët, smartphone-et tuaja dhe çdo pajisje të tjera me të dhëna personale mbi to. Nëse është e pasiguruar me një fjalëkalim, një vegël e humbur ose e vjedhur është një burim informacioni personal për këdo që e ka, gjë që mund të çojë në vjedhje të identitetit dhe më keq.

E njëjta këshillë shkon për llogaritë në internet. Meqenëse shumica e tyre kanë nevojë për një fjalëkalim për të ngritur, sfida është duke bërë fjalëkalime të forta. Përdorni këshilla për fjalëkalime të forta për t'u siguruar që juaji është i mirë. Mos përdorni të njëjtin fjalëkalim për më shumë se një vend, sepse një llogari e hackuar mund të rezultojë në kompromet imin e të gjitha llogarive tuaja. Për t'ju ndihmuar të mbani mend të gjitha këto fjalëkalime, përdorni një menaxher fjalëkalimi.

Aktivizo legalizimin me dy faktorë për çdo vend që e mbështet atë, gjë që mbron llogarinë tënde edhe nëse një haker merr fjalëkalimin tënd. Dhe ato pyetje të sigurisë të dizajnuara për t'ju ndihmuar të shënohni një fjalëkalim të humbur ose një përdorues të harruar? Ata nuk janë shumë të sigurt, sepse disa prej tyre janë shumë të lehta për hakerët që të gjejnë. Ne rekomandojmë që të bëheni përgjigje dhe ta mbani atë informacion në menaxherin e fjalëkalimeve.

Ndryshoni fjalëkalimet e paracaktuara për çdo gjë të lidhur me rrjetin tuaj në shtëpi. Ruteri juaj është pajisja më e rëndësishme për t'u siguruar, sepse router juaj mund t'i japë një hacker qasje të plotë në rrjetin tuaj në shtëpi. Mos harroni pajisje të tjera të lidhura si monitorët e foshnjave. *(Harper, 2018)*

2.5.2 Mbani kompjuterinë tuaj me antiviruse

Siguria dixhitale ka shumë të bëjë me privatësinë digjitale. Nëse kompjuteri juaj është i infektuar nga një virus ose malware, jo vetëm që hakerat mund të gërmojnë të dhënat tuaja për të vjedhur identitetin tuaj, por mund të mbyllin skedarët tuaj dhe të kërkojnë një shpërblim për t'i kthyer ato. Zgjidhja? Drejtoni një program antivirus për të parë për viruset dhe mbani përditësimin e softuerit tjetër për të mbyllur vrimat e sigurisë. Kjo vlen jo vetëm për kompjuterin tuaj, por edhe për pajisjet tuaja të lëvizshme. *(Harper, 2018)*

Antivirus jonë e preferuar është Kaspersky, e cila ofron mbrojtje për pajisjet Windows, Apple dhe Android. Ju mund të blini një licencë për tre pajisje ose të mbroheni me pajisje me vlerë të një familje me një licencë për pesë pajisje .Nëse dëshironi të përdorni një aplikacion falas, provoni Avast. Ajo nuk ka aq shumë karakteristika si Kaspersky, por është një skaner i fortë antivirus, dhe çmimi sigurisht që është i drejtë.

Sigurohuni që sistemi juaj operativ të jetë i përditësuar me patch-et më të fundit të sigurisë. Për të bërë më të lehtë këtë proces, ne rekomandojmë të aktivizoni funksionin e përditësimit automatik.

Ja se si:

- Aktivizo përditësimet automatike për Windows.
- MacOS automatikisht kontrollon përditësimet sipas parazgjedhjes, por ju mund të kontrolloni manualisht me këto udhëzime.
- Android zakonisht ju njofton për përditësime, por do t'ju duhet t'i instaloni manualisht. Udhëzimet do të ndryshojnë në varësi të pajisjes suaj dhe versionit të Android që po aktivizoni; kontrolloni me prodhuesin e pajisjes tuaj për detaje.
- iOS do të ju bezdisni vazhdimisht për përditësime, kështu që nuk ka shanse t'i humbisni ato. *(Harper, 2018)*

2.5.3 Siguroni shfletuesin tuaj

Shfletuesi juaj është mënyra se si bashkëveproni me botën dixhitale dhe nëse nuk jeni të kujdesshëm, mund të lini një gjurmë gjurmësh gjurmimi pas jush gjatë shfletimit. Nëse janë faqet e internetit dhe marketers ndjekja ju ose një hacker spiunuar në atë që ju jeni duke bërë, ka mënyra për të mbajtur zakonet tuaja të shfletimit privat.

Hapi i parë për mbajtjen e reklamuesit nga shfletuesi juaj është çaktivizimi i cookies të palëve të treta. Reklamuesit përdorin cookie-t për të parë se ku keni qenë dhe përshtate reklamat që ju tregojnë në mënyrë të përshtatshme. Ja se si të bllokoni cookies në Chrome, Edge, Internet Explorer, Firefox dhe Safari.

Për të shkuar një hap më larg, mund të çaktivizosh JavaScript. Kjo ndërpret një tjetër reklamues të zakonshëm (ose hacker), por ju mund të bëni disa faqe interneti jofunksionale. Nëse dëshironi të aktivizoni JavaScript, gjithsesi, si mund ta bëni atë në Chrome, Edge, Internet Explorer, Firefox dhe Safari. A nuk duan të shqetësohen për ndonjë nga këto?

Provoni shfletuesin e shfletuesit "Privacy Badger" për Chrome, Firefox dhe Opera, i cili mbyll automatikisht shumë ndjekës të mundshëm. HTTPS Everywhere është një tjetër shfletues i mirë i cili e detyron shfletuesin tënd të përdorë faqe të sigurta dhe të koduara kur të jenë në dispozicion, gjë që ndihmon në mbajtjen e snoopëve nga të dhënat tuaja.

Modaliteti i shfletimit privat fshin cookies tuaj, historinë e shfletimit dhe skedarët e tjerë të përkohshëm sa herë që mbyllni dritaren. Ja se si të përdorësh regjimin privat të shfletimit në Chrome, Edge, Internet Explorer, Firefox dhe Safari. Nëse jeni serioz në lidhje me shfletimin diskrete, megjithatë lexoni artikullin tonë mbi shfletimin e internetit në mënyrë anonime. *(Harper, 2018)*

2.5.4 Ndërroni motorët e kërkimit

Shumica e motorëve të kërkimit mbajnë skedat në atë që kërkoni, në mënyrë që të mund të synojnë reklamat në shijet tuaja. Nëse nuk ju pëlqen ideja e historisë së kërkimit që përdoret për të shitur gjërat, DuckDuckGo është motor kërkimi për ju. Site nuk ndjek ndonjë nga të

dhënat tuaja personale, kështu që ju mund të kërkoni pa shikuar dikush mbi supe tuaj. *(Harper, 2018)*

2.5.5 Keni kujdes se çfarë ndani në mediat sociale

Mediat sociale mund të ndjehen si një bisedë me miqtë tuaj më të afërt - përveç se mund të jetë një bisedë e gjithë bota mund të shohë. Nëse postoni mjaftueshëm në mediat sociale, informacioni mund të përdoret për të gjetur se ku jeni dhe çfarë jeni duke bërë. Linja e parë e mbrojtjes është mbyllja e llogarive të mediave tuaja sociale. Ndani vetëm me njerëzit që dëshironi të shihni informacionin që po ndani, si miqtë dhe familjen tuaj. Në Twitter, llogaria jote është tërësisht e hapur ose e mbyllur për njerëzit që ju ftojnë për t'ju ndjekur; duke ndryshuar atë cilësim është aq e lehtë sa duke klikuar një kutizë. Facebook lejon kontroll më të madh se kush sheh atë që postoni. Lexoni udhëzuesin tonë në parametrat e privatësisë së Facebook për të konfiguruar profilin tuaj.

A nuk doni të bllokohet llogaria juaj? Pastaj bëhuni të zgjedhur për atë që ndani. Kini kujdes të veçantë me informacionin personal që mund të përdoret për t'ju identifikuar ose për të gjetur vendndodhjen tuaj. Mos e plotësoni profilin tuaj të plotë në mënyrë që të mos lejoni identifikimin e lehtë ose t'i jepni dikujt detaje të mjaftueshme personale për të vjedhur identitetin tuaj. Merrni parasysh uljen poshtë të asaj që ndani. A duhet me të vërtetë të kontrolloni në çdo biznes që vizitoni, duke e bërë veten të lehtë për të gjetur? Ndoshta jo. *(Harper, 2018)*

2.5.6 Pyesni pse të tjerët kanë nevojë për informacionin tuaj

Sa herë që ju kërkohet të jepni informacion personal, qoftë personalisht, në telefon ose në internet, merrni në konsideratë nëse keni nevojë të jepni atë. Ndonjëherë informacioni si adresa juaj e postës elektronike dhe Kodi ZIP përdoret thjesht për qëllime marketingu; në atë rast, prisni që kuti postare tuaja reale dhe virtuale të jenë të mbushura me junk mail.

Për të ruajtur privatësinë tuaj, mos jepni kurrë më shumë informacion se sa duhet. Kjo është dyfish e vërtetë për informacionin e ndjeshëm personal si numri juaj i sigurimit social - madje

vetëm katër shifrat e fundit. Nëse nuk është banka juaj, një zyrë krediti, një kompani që dëshiron të bëjë një kontroll sfondi mbi ju ose ndonjë subjekt tjetër që duhet të raportojë në IRS, shanset janë që ata nuk kanë nevojë për të. *(Harper, 2018)*

2.5.7 Mos bjerë pre e mashtrimeve

Kujdes nga faqet e internetit, thirrjet telefonike dhe emailet që përpiqen të ndajnë ju nga të dhënat tuaja personale. Përhershme po bëhen më të mirë në imitimin e bizneseve të ligjshme, prandaj ruajini. Një taktikë e zakonshme me të përhershme është që të presësh që të heqësh dorë nga të dhënat personale duke paraqitur pasoja të tmerrshme nëse nuk e bën. Për shembull, një scammer mund të ju tregojë se ju jeni duke u audituar nga IRS ose se kompjuteri juaj ka një virus të rrezikshëm që ata mund të rregullojnë nëse dorëzoni informacionin tuaj personal.

Këto taktika të presionit të lartë mund t'ju spërkasin në dhënien e shumë detajeve personale, por mos u mashtroni. Bizneset legjitime nuk bëjnë thirrje të kërkuara për të kërkuar numrin tuaj të sigurimeve shoqërore ose fjalëkalimin e kompjuterit. Nëse keni marrë një telefonatë ose email si kjo, mendoni se mund të jetë legjitim, bashkë

ntact biznesin që pretendon të jetë nga. Mos përdorni lidhjen ose numrin e telefonit të siguruar nga kushdo që ju ka kontaktuar; në vend të kësaj, kontaktoni direkt me kompaninë duke përdorur informacionin e kontaktit që personalisht kërkoni në faqen e internetit të kompanisë. Nëse çështja është e ligjshme, kompania do ta konfirmojë këtë dhe do t'ju ndihmojë të zgjidhni problemin, duke siguruar që të dhënat tuaja personale të jenë të sigurta. *(Harper, 2018)*

2.5.8 Përdorni vetëm softuerin që ju i besoni

Nëse jeni duke instaluar softuer të ri në telefonin tuaj ose në kompjuterin tuaj, sigurohuni që jeni duke e marrë atë nga një burim që ju besoni. Softueri me pamje legjitime nganjëherë mund të jetë një mashtrim i plotë, si skandali mbi aplikacionin fotografik Meitu, i cili mbledh një sërë të dhënash mbi përdoruesit e tij. Sigurohuni që çdo gjë që shkarkoni vjen nga një

zhvillues i besuar dhe një burim i besueshëm. Nëse nuk e dini se nga vjen programi juaj, nuk e dini se çfarë po bën vërtet - dhe kjo do të thotë që nuk ka të dhëna se ku po shkon informacioni yt. *(Harper, 2018)*

2.5.9 Përdorni vetëm lidhjet e sigurta Wi-Fi

Sigurisht, është e përshtatshme të përdorni shërbimin falas Wi-Fi në Starbucks tuaj lokal, por nuk ka thënë se kush po e sheh këtë trafik interneti. Nëse përdorni Wi-Fi publik, mos e përdorni për të transmetuar informacion privat. Shfletimi i faqes suaj të preferuar është e mirë, por merrni masa shtesë të sigurisë nëse jeni duke hyrë në një llogari. Përdorni një shërbim VPN për të enkriptuar të gjitha të dhënat që dërgoni. Ka shumë shërbime që mund ta bëjnë këtë, përfshirë NordVPN (lidhje shoqëruese) dhe VPN me buffer. Shërbimet e VPN paguajnë një tarifë për t'u përdorur, që nga dita kalon në mbrojtjen gjatë gjithë vitit. *(Harper, 2018)*

2.6 Virtual private network VPN

Një VPN ose Rrjet privat privat ju lejon të krijoni një lidhje të sigurt në një rrjet tjetër në internet. VPN-të mund të përdoren për të hyrë në faqet e internetit të kufizuara nga rajoni, mbrojnë aktivitetin tuaj të shfletimit nga sytë e çmuar në Wi-Fi publik dhe më shumë. Këto ditë VPN-të janë shumë të njohura, por jo për arsyet që u krijuan fillimisht. Ata fillimisht ishin vetëm një mënyrë për të lidhur rrjetet e biznesit së bashku në mënyrë të sigurtë në internet ose t'ju lejojnë të hyni në një rrjet biznesi nga shtëpia.

VPN-të në thelb përcjellin të gjithë trafikun e rrjetit tuaj në rrjet, ku përfitojnë të gjitha - si qasja në burimet e rrjetit lokal në distancë dhe anashkalimi i censurës së internetit. Shumica e sistemeve operative kanë mbështetje të integruar VPN. *(How-To Geek, 2018)*

Figure 2:Virtual Private Network

("How to Choose a Good VPN", 2019)

2.6.1 Çfarë është VPN dhe si më ndihmon?

Në terma shumë të thjeshtë, një VPN lidh kompjuterin, smartphoneun ose tabletin tuaj në një kompjuter tjetër (i quajtur një server) diku në internet dhe ju lejon të shfletoni internetin duke përdorur lidhjen e internetit të kompjuterit. Pra, nëse ai server është në një vend tjetër, do të duket sikur po vjen nga ai vend dhe mund të hyni në gjëra që normalisht nuk mund të keni. Pra, si e ndihmon kjo? Pyetje e mirë! Ju mund të përdorni një VPN për:

- Heqja e kufizimeve gjeografike në faqet e internetit ose audio dhe video streaming.
- Shikoni streaming media si Netflix dhe Hulu.
- Mbroni veten nga snooping në pikat e nxehta Wi-Fi të pasigurta.
- Shtoni të paktën disa anonime online duke fshehur vendndodhjen tuaj të vërtetë.
- Mbroni veten nga të qenit i regjistruar kur jeni duke kërcyer.

Shumica dërrmuese e njerëzve këto ditë po përdorin VPN për përhapjen ose anashkalimin e kufizimeve gjeografike për të parë përmbajtjen në një vend tjetër. Ata janë ende shumë të dobishme për të mbrojtur veten gjatë punës në një dyqan kafeje, por kjo nuk është përdorimi kryesor. *(How-To Geek, 2018)*

2.6.2 Si mund të merrni një VPN dhe cilën duhet të zgjedhni?

Në varësi të nevojave tuaja, mund të përdorësh një VPN nga vendi i punës, të krijosh një server VPN ose ndonjëherë të mbash një nga shtëpitë e tua - por realisht shumica dërrmuese e njerëzve po kërkojnë diçka për t'i mbrojtur ato, shikoni disa media në internet që ata nuk mund të duken të kenë qasje nga vendi i tyre. Gjëja më e lehtë për të bërë është thjesht kreu në një nga këto vende, regjistrohuni dhe shkarkoni klientin VPN për Windows PC, Mac, Android, iPhone ose iPad. Është aq e lehtë.

- ExpressVPN - Ky server VPN ka kombinimin më të mirë të serverëve me lehtësi përdorimi, me të vërtetë të shpejtë dhe mbështet mediat dhe transmetimet rrjedhëse, të gjitha për një çmim të lirë.
- Tunnelbear - Kjo VPN është me të vërtetë e lehtë për t'u përdorur, është e madhe për përdorim në kafenetë, dhe ka një nivel të kufizuar. Kjo nuk është e mirë për torrenting ose streaming media .
- StrongVPN - jo aq e lehtë sa të përdoret si të tjerat, por mund t'i përdorni ato për mediat që transmetojnë dhe transmetojnë. *(How-To Geek, 2018)*

2.6.3 Si funksionon një VPN?

Kur lidhni kompjuterin (ose një pajisje tjetër, si një smartphone ose tabletë) në një VPN, kompjuteri vepron sikur të jetë në të njëjtin rrjet lokal si VPN. I gjithë trafiku i rrjetit tënd është dërguar në një lidhje të sigurt me VPN. Për shkak se kompjuteri yt sillet sikur është në rrjet, kjo ju lejon të siguroni qasje në burimet e rrjetit lokal edhe kur jeni në anën tjetër të botës. Ju gjithashtu do të jeni në gjendje të përdorni internetin sikur të ishit të pranishëm në vendndodhjen e VPN-së, e cila ka disa përfitime nëse po përdorni Wi-Fi publik ose dëshironi të përdorni faqet e internetit të bllokuara.

Kur shfletoni uebin gjatë lidhjes me një VPN, kompjuteri juaj kontakton faqen e internetit përmes lidhjes së VPN të koduar. VPN dërgon kërkesën për ju dhe dërgon përgjigjen nga faqja e internetit përsëri përmes lidhjes së sigurt. Nëse jeni duke përdorur një VPN me bazë

në SHBA për të hyrë në Netflix, Netflix do ta shohë lidhjen tuaj si të ardhur nga brenda SHBA. *(How-To Geek, 2018)*

2.6.4 Shembuj të tjerë per përdorimin e VPN-së

VPN-të janë një mjet mjaft i thjeshtë, por ato mund të përdoren për të bërë një shumëllojshmëri të gjerë të gjërave:

- Qasja në një rrjet biznesi gjatë udhëtimit: VPN-të përdoren shpesh nga udhëtarët e biznesit për të hyrë në rrjetin e biznesit të tyre, duke përfshirë të gjitha burimet e rrjetit lokal, ndërsa në rrugë. Burimet lokale nuk duhet të ekspozohen direkt në internet, gjë që rrit sigurinë
- Qasja në rrjetin tuaj në shtëpi gjatë udhëtimit: Ju gjithashtu mund të krijoni VPN tuaj për të hyrë në rrjetin tuaj gjatë udhëtimit. Kjo do t'ju lejojë të hyni në një Desktop Remote të Windows në Internet, të përdorni aksione të skedarëve lokal dhe të luani lojëra në Internet sikur të ishit në LAN të njëjtë (rrjet lokal).
- Fshih aktivitetin tuaj të shfletimit nga rrjeti juaj lokal dhe ISP: Nëse po përdorni një lidhje publike Wi-Fi, aktiviteti juaj në shfletim në faqet e internetit jo-HTTPS është i dukshëm për të gjithë ata që janë në gjendje të mirë, nëse ata dinë të shikojnë. Nëse dëshironi të fshehni aktivitetin tuaj të shfletimit për një pak më shumë privatësi, mund të lidheni me një VPN. Rrjeti lokal do të shohë vetëm një lidhje VPN të vetme dhe të sigurt. I gjithë trafiku tjetër do të udhëtojë gjatë lidhjes VPN. Ndërsa kjo mund të përdoret për të anashkaluar monitorimin e lidhjeve nga ofruesi i shërbimit të Internetit, mbani në mend se ofruesit e VPN mund të zgjedhin të identifikojnë trafikun në skajet e tyre.
- Censura e anashkalimit të internetit: Shumë njerëz kinezë përdorin VPN-të për të marrë rreth Zjarrit të Madh të Kinës dhe për të fituar qasje në të gjithë Internetin. (Megjithatë, Firewall i Madh duket se ka filluar të ndërhyjë me VPN-të kohët e fundit.)
- Shkarkimi i skedarëve: Po, le të jemi të sinqertë - shumë njerëz përdorin lidhje VPN për të shkarkuar skedarë nëpërmjet BitTorrent. Kjo në të vërtetë mund të jetë e

dobishme edhe nëse jeni duke shkarkuar torrente krejtësisht ligjore - nëse ISP-ja juaj është duke shtypur BitTorrent dhe duke e bërë atë jashtëzakonisht të ngadaltë, ju mund të përdorni BitTorrent në një VPN për të marrë shpejtësi më të larta. E njëjta gjë vlen edhe për llojet e tjera të trafikut që ISP-ja juaj mund të ndërhyjë (nëse nuk ndërhyjnë me trafikun VPN.) *(How-To Geek, 2018)*

2.6.5 Përdorimi i një VPN të Korporatës në Windows

Lidhja me një VPN është mjaft e thjeshtë. Në Windows, shtypni butonin e Windows, shkruani VPN dhe klikoni në konfigurimin e lidhjes së rrjetit privat virtual (VPN). (Nëse përdorni Windows 8, duhet të klikoni në kategorinë Cilësimet pas kërkimit.) Përdorni magjistarin për të futur adresën dhe identifikimin e kredencialeve të shërbimit VPN që dëshironi të përdorni. Ju pastaj mund të lidheni dhe shkëputeni nga VPN-të duke përdorur ikonën e rrjetit në tabelëne sistemit - e njëjta gjë ku menaxhoni rrjetet Wi-Fi me të cilat jeni lidhur. *(How-ToGeek, 2018)*

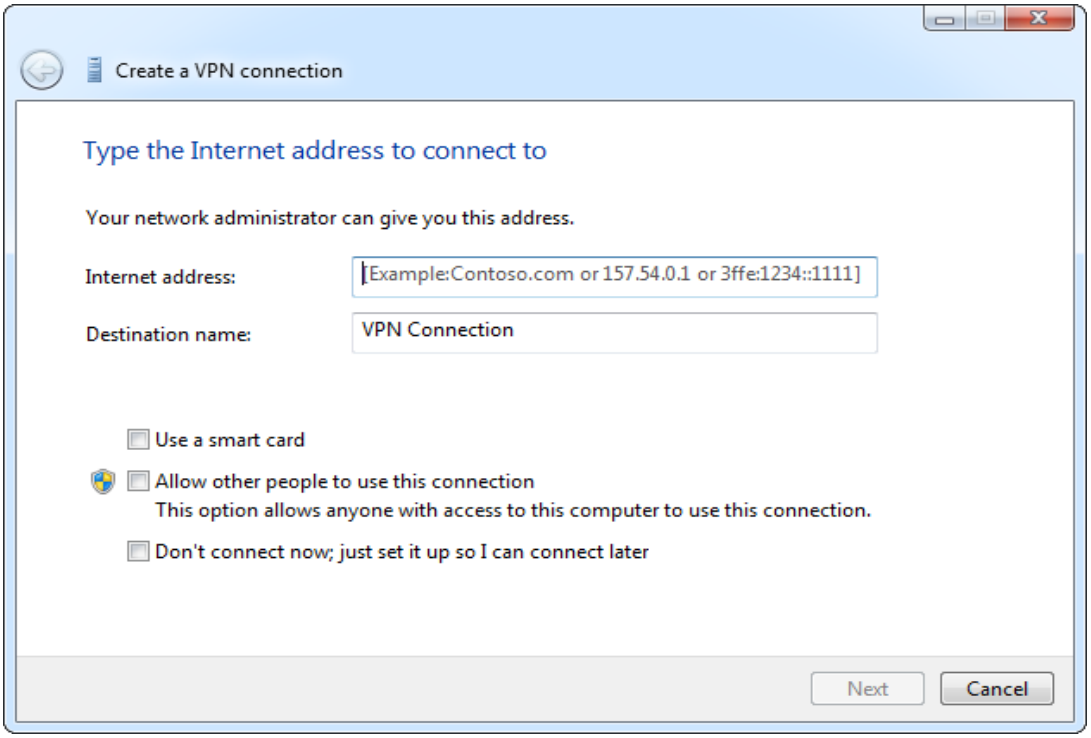

Figure 3:Përdorimi i një VPN të Korporatës në Windows

(HowToGeek, 2018)

2.7 Statistikat e thelluara të privatësisë në Internet

86% e njerëzve që përdorin internetin në mënyrë aktive po ndërmarrin hapa aktivë për të përmirësuar privatësinë e tyre në internet.

Shumica e njerëzve akoma duan të mbeten anonim gjatë kohës që janë në internet, por vetëm sot nuk është një mundësi. Ka shumë mënyra, madje edhe një histori skanimi në fshehtësi ose private mund të arrihet nga distanca. Gjithçka që duhet është një shkarkim pa dashje, një fjalëkalim hakuar ose një portofol i vjedhur për një person që të humbasë identitetin e tyre. Ndërsa bota bëhet më e lidhur, privatësia e internetit do të vazhdojë të rritet.

11% e njerëzve që janë vazhdimisht online kanë pasur informacione personale të vjedhura në internet. Kjo përfshin numrat e kartës së kreditit, informacionin e llogarisë bankare ose një numër personal identifikimi si patentë shoferi ose SSN.

1 në 4 përdorues të rrjeteve sociale të regjistruar kishin postuar të dhëna personale të ndjeshme për veten në profilet e tyre.

12% e përdoruesve të internetit thonë se i kanë pasur njerëz që i ngacmojnë ata gjatë kohës që janë në internet ose kanë pasur njerëz që i ndjekin ato.

Përqindja e njerëzve që thonë se kanë humbur një mundësi pune ose një shans për të ndjekur kolegjin për shkak të mungesës së privatësisë në internet: 1%.

6%. Kjo është përqindja e njerëzve që pranojnë se humbën paratë për shkak të një scam online që erdhi në rrugën e tyre.

1 në 5 njerëz që përdorin rregullisht internetin thonë se kanë pasur rrjetet e tyre sociale ose emailin e komprometuar nga hakerat ose dikush që njihnin të paktën një herë pa leje.

Më shumë se gjysma e përdoruesve të internetit [55%] po ndërmarrin hapa për të shmangur vëzhgimin nga dikush ose diçka specifike.

84% e përdoruesve të internetit amerikanë thonë se nuk e dinë se ku dhe si mund të sigurojnë informacionin që gjendet në emailin e tyre.

41% e fëmijëve të moshës 8-17 vjeç që kishin një profil të dukshëm kishin profilin e tyre në mënyrë që të ishte e dukshme për këdo.

17% e përdoruesve të rritur thanë se biseduan me njerëzit në faqet e rrjeteve sociale që nuk dinin dhe 35% u foli njerëzve që ishin "miq të shokëve".

68% besojnë se ligjet e tanishme nuk janë mjaft të mira për mbrojtjen e të drejtave të përdoruesve të internetit.

Më shumë se gjysma e të gjithë përdoruesve të internetit thonë se është e pamundur të jetë 100% anonim online dhe ata ndoshta janë të sakta. Shumica e njerëzve përdorin emrin e tyre ligjor për një llogari të rrjeteve sociale dhe rregullisht kanë të njëjtat fjalëkalime për emailin e tyre, llogaritë e tyre bankare dhe llogaritë e tjera në internet. Pasi dikush të ketë një fjalëkalim, ata kanë qasje në gjithçka që personi bën në internet. Megjithëse personi mesatar nuk do t'i nënshtrohet shumicës së problemeve të privatësisë në internet, rreziku është gjithmonë i pranishëm dhe duhet të trajtohet në një farë mënyre *("29 Profound Internet Privacy Statistics - BrandonGaille.com", 2019)*

2.7.1 Sa jemi të shqetësuar rreth Internet Privacy?

3 nga 4 njerëz që dërgojnë email rregullisht janë të shqetësuar se informacioni i tyre personal do të kompromentohet nga dikush tjetër përveç palës së synuar.

56%. Kjo është përqindja e njerëzve që janë të shqetësuar në një farë mënyre me Google dhe kompani të ngjashme që përdorin informacion në mesazhet private kundër tyre në një farë mënyre. 68% e përdoruesve të internetit besojnë se ligjet e tanishme nuk janë mjaft të mira për mbrojtjen e të drejtave të përdoruesve të internetit.

Më shumë se gjysma e prindërve nuk i kanë lexuar politikat e privatësisë në internet të faqeve që fëmijët e tyre po vizitojnë rregullisht. Vetëm 1 në 3 persona kanë filluar të përdorin encryption, një shfletues të sigurt, ose një ofrues të sigurt email për nevojat e tyre në internet.

15% e amerikanëve asnjëherë nuk kanë kontrolluar rregullat e privatësisë për rrjetet e tyre të preferuar sociale. Edhe pse 88% e adoleshentëve kanë përjetuar ngacmime online 68% e adoleshentëve thonë se njerëzit në përgjithësi janë mirëdashës me njëri-tjetrin në internet.

41% e adoleshentëve që përdorin mediat sociale kanë përjetuar të paktën një rezultat negativ si rezultat i përdorimit të një rrjeti social.

1 në 5 adoleshencë në SHBA ka ndarë numrin e tyre të vërtetë personal të telefonit celular në rrjetin e tyre të preferuar social.

Këtu duhet të trajtohen dy çështje. E para është me mbingarkesë. Kur njerëzit ndajnë gjithçka që po bëjnë, atëherë modelet fillojnë të vërehen. Të tjerët do të dinë kur dikush është larg shtëpisë. Ata mund të jenë në gjendje të përcaktojnë se ku jeton dikush në bazë të fotografive të një shtëpie. Fotot e brendshme i bëjnë njerëzit të dinë se çfarë lloj sendesh ka dikush. Cilësimet e intimitetit të Internetit që janë vendosur në publik ose global, e bëjnë atë në mënyrë që të gjithë të kenë qasje në këtë informacion. Pastaj së dyti, kur ky informacion bëhet publik, mund të abuzohet. Kjo është arsyeja pse privatësia në internet duhet të bëhet përparësi kryesore për të gjithë ata që janë në internet. *("29 Profound Internet Privacy Statistics - BrandonGaille.com", 2019)*

2.8 Siguria Kibernetike

Siguria kibernetike është shumë e afërt me sigurinë tradicionale të informacionit, sipas definicionit. I vetmi ndryshim është se siguria kibernetike fokusohet në hapësirën kibernetike në vend që të përfshijë sigurinë fizike. IT Governance Ltd përcakton sigurinë kibernetike si mbrojtje e rrjeteve, sistemeve dhe informacionit në hapësirën kibernetike. *(IT Governance Ltd 2014).*

Siguria kibernetike përbëhet nga teknologji, procese dhe kontrolle që janë të dizajnuara për të mbrojtur sistemet, rrjetet dhe të dhënat nga sulmet kibernetike. Siguria efektive në internet zvogëlon rrezikun e sulmeve kibernetike dhe mbron organizatat dhe individët nga shfrytëzimi i paautorizuar i sistemeve, rrjeteve dhe teknologjive.

Siguria e fuqishme kibernetike përfshin zbatimin e kontrolleve që bazohen në tre shtylla: njerëzit, proceset dhe teknologjia. Kjo qasje e trefishtë i ndihmon organizatat të mbrojnë veten nga sulmet shumë të organizuara dhe kërcënimet e përbashkëta të brendshme, siç janë shkeljet aksidentale dhe gabimet njerëzore. *(Itgovernance.co.uk, 2018)*

Cyberspace, sipas Limnéll, Majewski dhe Salminen (2014, 29) do të thotë bota artificiale e krijuar nga njerëzit që përmban internetin, mediat sociale, rrjetet kompjuterike dhe sistemet dhe madje edhe softuerin Smartphone. Lidhur me përkufizimin e sigurisë kibernetike, Limnéll et al. (2014, 30-31) gjithashtu theksojnë se fjala "cyber" është bërë për të përfaqësuar mbrojtjen e informacionit edhe gjatë tranzitit dhe jo vetëm një term për mbrojtjen e informacionit të ruajtur siç ishte rasti me sigurinë e informacionit. Ata gjithashtu e

konsiderojnë fjalën "cyber" për të përshkruar më mirë hapësirën kibernetike në botën e sotme kur krahasohen me kushtet e tjera Limnéll et al.(2014, 30-31). Kjo lidhet me konfuzionin e përgjithshëm mbi atë se siguria kibernetike është në lidhje me termat e tjerë si siguria e informacionit.

Siguria Kibernetike është një tentim i vazhdueshëm për mbrojtjen e këtyre sistemeve të lidhura në rrjetë dhe të gjitha informacioneve, nga përdorimi i pa autorizuar apo përdorimi i dëmshëm i tyre, improvizuar tek figura 2. Në një nivel personal, ju duhet të mbroni identitetin tuaj, të dhënat tuaja, si dhe pajisjet e juaja teknologjike. Në një nivel korporatash, mbrojtja e reputacionit, të dhënave dhe konsumatorëve të organizatës, është përgjegjësi e të gjithë pjesëmarrësve në atë organizatë. Në nivel shteti, siguria nacionale, siguria e qytetarëve, si dhe mirëqenia e tyre janë në rrezik

2.8.1 Tri shtyllat e sigurisë kibernetike

Njerëzit

Çdo punonjës duhet të jetë i vetëdijshëm për rolin e tyre në parandalimin dhe reduktimin e kërcënimeve kibernetike, dhe personeli i specializuar teknik i sigurisë kibernetike duhet të jetë plotësisht i azhurnuar me aftësitë dhe kualifikimet e fundit për të zbutur dhe për t'iu përgjigjur sulmeve kibernetike.

Proceset

Proceset janë vendimtare në përcaktimin se si aktivitetet, rolet dhe dokumentacioni i organizatës përdoren për të zbutur rreziqet ndaj informacionit të organizatës. Kërcënimet kibernetike ndryshojnë shpejt, kështu që proceset duhet të rishikohen vazhdimisht për t'u përshtatur me to.

Teknologjia

Duke identifikuar rreziqet kibernetike me të cilat ballafaqohet organizata juaj, atëherë mund të filloni të shikoni se cilat kontrolle do të vendosni dhe çfarë teknologjish do t'ju nevojitet për ta bërë këtë. Teknologjia mund të vendoset për të parandaluar ose zvogëluar ndikimin e rreziqeve kibernetike, në varësi të vlerësimit të rrezikut dhe asaj që konsideron një nivel të pranueshëm rreziku. *(Itgovernance.co.uk, 2018)*

2.9 Pse është e rëndësishme siguria kibernetike?

Shpenzimet e shkeljeve të të dhënave janë të larta:

Me Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave të BE (GDPR) të BE-së, organizatat mund të ballafaqohen me gjoba deri në 20 milionë euro ose 4% të qarkullimit vjetor global për shkelje të caktuara. Ekzistojnë edhe kostot jofinanciare, siç janë dëmtimi i reputacionit dhe humbja e besimit të klientit. *(Itgovernance.co.uk, 2018)*

Sulmet kibernetike po bëhen gjithnjë e më të sofistikuara:

Sulmet kibernetike janë bërë më të sofistikuara me sulmuesit duke përdorur një shumëllojshmëri të taktikave gjithnjë në rritje për të shfrytëzuar dobësitë, siç janë inxhinieri sociale, malware dhe ransomware.

Siguria kibernetike është një çështje kritike e bordit:

Rregulloret e reja dhe kërkesat e raportimit bëjnë që mbikëqyrja e rrezikut të sigurisë kibernetike të jetë një sfidë. Bordi do të vazhdojë të kërkojë garanci nga menaxhmenti se strategjitë e tyre të rrezikut në internet do të zvogëlojnë rrezikun e sulmeve dhe do të kufizojnë ndikimet financiare dhe operacionale.

Një qëndrim i fuqishëm për sigurinë kibernetike është një mbrojtje kyçe kundër dështimeve dhe gabimeve të lidhura me kibernetike dhe sulme kibernetike me qëllim të keq, prandaj është jetësore që të keni masat e duhura të sigurisë kibernetike për të mbrojtur organizatën tuaj. *(Itgovernance.co.uk, 2018)*

2.10 Të dhënat tuaja

Çdo informacion rreth jush mund të konsiderohet si një e dhënë e juaj(ang. Data). Ky informacion personal mund të ju identifikoj juve në mënyrë unike si një individ. Këto të dhëna përfshijnë fotografitë dhe mesazhet që ju i shkëmbeni me familjen dhe shoqërinë tuaj online. Të tjera informacione, si emri, numri identifikues, data dhe vendi i lindjes, apo mbiemri vajzëror i nënës suaj, janë të ditura nga ti, dhe mund të përdoren për identifikimin tuaj. Informa-

ta tjera si mjekësore, arsimore, financiare apo informata punësimi, po ashtu mund të përdoren për identifikimin tuaj online.

2.10.1 Ku ndodhen të dhënat e juaja?

Të gjitha këto informata janë informata rreth jush. Ekzistojnë ligje të ndryshme për mbrojtjen e privatësisë dhe të dhënave tuaja në vendin tonë. Mirëpo, a e dini se ku ndodhen të dhënat tuaja? Kur ju jeni në klinikë, biseda që ju bëni me doktorin ruhet në të dhënat e juaja mjekësore. Për qëllim të vërtetësisë së çmimeve, këto informata i jepen kompanisë së sigurimit shëndetësor. Me këtë rast, një pjesë e të dhënave tuaja mjekësore rreth asaj vizite mjekësore është po ashtu edhe te kompania e sigurimeve shëndetësore.

Figure 4:Përhapja e të dhënave

(Zuckerberg, 2013)

Kur ju shkëmbeni fotografitë tuaja online me shokët tuaj, a e dini se kush ka mundësi të ketë kopje të këtyre fotografive? Kopje të këtyre fotografive janë në pajisjen tuaj. Po ashtu edhe shokët tuaj mund të kenë kopje të tyre pas shkarkimit të tyre në pajisjet e tyre. Nëse fotografitë shpërndahen publikisht, njerëz të huaj mund gjithashtu të kenë kopje të tyre. Ata mund

të shkarkojnë ato fotografi apo të marrin "screenshot" te atyre fotografive. Për arsye se fotografitë janë shpërndarë në rrjetë, apo thënë më mirë janë postuar online, ato po ashtu ruhen në serverë të gjendur në pjesë të ndryshme të botës. Tanimë fotografitë nuk gjenden vetëm në pajisjen tuaj të mençur.

2.11 Pajisja juaj e mençur

Pajisjet e juaja të mençura nuk bëjnë vetëm ruajtjen e të dhënave tuaja. Tani këto pajisje janë bërë portal i të dhënave tuaja dhe gjenerojnë informata rreth jush. Përveç se nëse keni zgjedhur që të pranoni deklarata në formë letre për të gjitha llogaritë tuaja, ju përdorni këto pajisje për qasje në të dhëna. Nëse ju dëshironi një kopje digjitale të deklaratës së fundit ' qasur në ueb-faqen e lëshuesit të kartelës suaj të kreditit. Nëse ju dëshironi të paguani faturën e kartës së kreditit online, ju i qaseni uebfaqes së bankës suaj për të transferuar fondet duke përdorur pajisjen e mençur. Pajisja e mençur, përveç që ju lejon qasjen në të dhënat e juaja, po ashtu mund të gjenerojë informacione rreth jush. Me gjithë këto informacione rreth jush online, të dhënat e juaja personale janë bërë të leverdishme për hakerët.

2.12 Çfarë duan hakerët nga ju?

Nëse ju keni diçka të vlefshme, kriminelët e duan atë. Kredencialet tuaja online janë të vlefshme. Këto kredenciale i japin hajdutëve qasje në llogaritë tuaja. Ju mund të mendoni se kilometrat që ju keni grumbulluar si një fluturues frekuent nuk janë të vlefshme për kriminelët kibernetikë. Mendo prapë. Pasi përafërsisht 10.000 llogari u hakuan të agjencive "American Airlines "dhe "United " kriminelet rezervuan flutrime pa pagese dhe ngritjete klases se uleseve duke përdorur ato kredenciale të vjedhura. Edhe pse ato kilometra të fluturuesve frekuent iu kthyen konsumatorëve nga agjencitë e lartë përmendura, kjo demonstron vlerën e kredencialeve të qasjes. Një kriminel mund po ashtu të përdorë edhe lidhjet e juaja. Ata mund të iu qasen llogarive tuaja online dhe reputacionit tuaj për të ju trukuar në dërgimin e parave te shokët e juaj apo te familjarët. Krimineli mund të dërgoj mesazhe duke pretenduar se familja juaj apo shokët kanë nevojë që ju të i dërgoni para në mënyrë që ata të mund të kthehen në

shtëpi nga jashtë, pasi kuletat iu kanë humbur. Kriminelët janë shumë imagjinativ kur mundohen që të ju trukojnë në dërgimin e parave te ta. Ata nuk plaçkitin vetëm paratë e juaja, por ata mund të marrin edhe identitetin tuaj dhe ta shkatërrojnë jetën tuaj.

Përveç vjedhës së parave për një fitim afat-shkurtët monetar, kriminelët dëshirojnë profite afat-gjate duke vjedhur identitetin tuaj. Me rritjen e shpenzimeve mjekësore, edhe vjedhja e identitetit mjekësor është në rritje. Hajdutët e identitetit mund të vjedhin sigurimin tuaj mjekësor dhe mund të përdorin benefitet tuaja për vete, dhe ato procedura medicinale, tani do të jenë në historinë tuaj mjekësore

Procedura për pagesat e taksave vjetore mund të ndryshojnë nga shteti në shtet, mirëpo, kriminelët kibernetikë shohin këtë kohë si mundësi. Për shembull, njerëzit e Shteteve të Bashkuara duhet të kryejnë këtë procedurë deri më 15 Prill, çdo vjet. Shërbimi i Përfitimeve të Brendshme(IRS) nuk i kontrollon taksat se a po përputhen me ato të punëdhënësit deri në Korrik. Një hajdut identiteti mund të aplikoj me një aplikim fals për ato taksa, dhe të marrë rimbursimin e parave për vete. Aplikuesit legjitim do të vërejnë këtë kur rimbursimi i refuzohet nga IRS-ja. Me identitetin e vjedhur, ata po ashtu mund të hapin llogari për kredi kartela dhe të marrin borxhe në emrin tuaj. Kjo do të shkaktojë dëm në vlerësimin e bankave për ju si konsumator dhe do të bëjë më të vështirë për ju që të merrni kredi. ("5 Things Hackers Don't Want You to Know", 2018).

2.13 Besueshmëria, Integriteti dhe Disponueshmëria

Besueshmëria, integriteti dhe disponueshmëria, e njohur si trekëndëshi CIA(inicialet ang.), është një direktivë për informacione rreth sigurisë për një organizatë. Besueshmëria siguron privatësinë e të dhënave duke kufizuar qasjen përmes autentifikimit të enkriptuar. Integriteti siguron që informacioni është i saktë dhe nga burimi i besueshëm. Disponueshmëria siguron që informacioni është i qasshëm për personat e autorizuar. *(Checkmarx, 2018)*

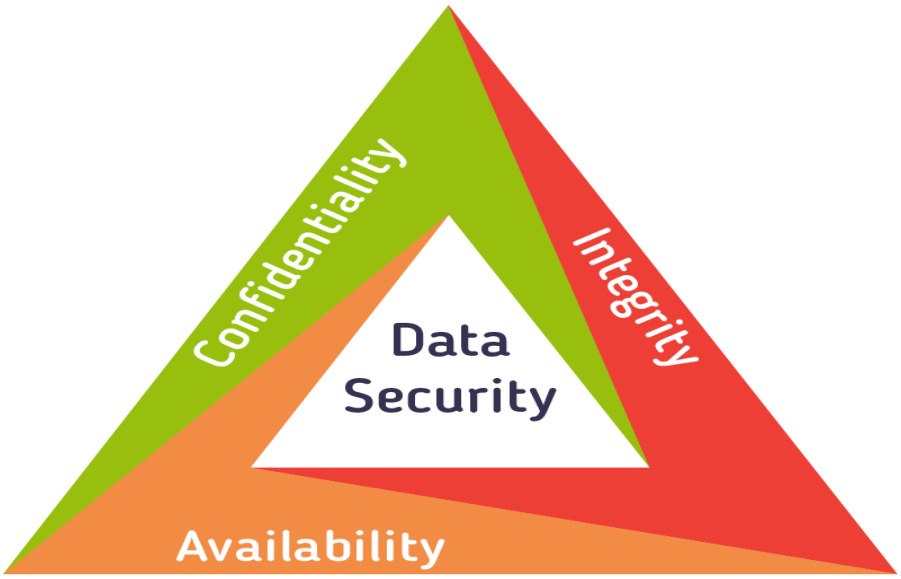

Figure 5:Trekëndëshi i CIA-së

(Checkmarx, 2018)

Besueshmëria

Një tjetër term për besueshmërinë mund të jetë privatësia. Rregullat e kompanisë do duhej të limitojnë qasjen në informacione vetëm për personelin e autorizuar dhe të sigurojnë që vetëm ata individë të autorizuar të hapin këto të dhëna. Të dhënat mund të jenë të fragmentuara në akordancë me sigurinë ose nivelin e ndjeshmërisë së informacioneve. Për shembull, një zhvillues programi nuk do duhej të ju qaset informacioneve personale të të gjithë punonjësve. Për më shumë, punonjësit do duhej të marrin trajnime për të kuptuar praktikën më të mirë për mbrojtjen e informacioneve të ndjeshme, që të mbrojnë veten dhe kompaninë e tyre nga sulmet. Metodat që sigurojnë besueshmëri përfshijnë enkriptimin e të dhënave, ID të përdoruesit dhe fjalëkalim, autentifikim me dy faktorë, dhe ekspozim minimal të informacioneve të ndjeshme. *(Checkmarx, 2018)*

Integriteti

Integriteti është saktësi, konsistencë, dhe burim i besueshëm i të dhënave gjatë jetës së tyre. Të dhënat duhet të jenë të pandryshuara gjatë kalimit nga një resurs në tjetrin dhe të

pandryshuara nga entitete të pa autorizuara. Lejet për fajlla, dhe kontrolli i qasjes së shfrytëzueseve mund të preventojnë qasjen e pa autorizuar. Kontrollimi i versionit mund të përdoret për parandalimin e ndryshimeve të rastësishme nga shfrytëzues të autorizuar. Backup-ët duhet të jenë të disponueshëm për rikthimin e ndonjë të "checksum hashing " munde te perdoret per te identifikuar identitetin e te dhënave gjatë transferimit. Një checksum përdoret për të verifikuar integritetin e fajllave, stringjeve të karaktereve, pasi ato janë transferuar nga një pajisje në tjetrën përmes një rrjete lokale apo përmes Internetit. Këto checksum-a llogariten duke përdorur HASH funksionet. Disa nga to janë: MD5, SHA-1, SHA-256, dhe SHA-512. Një HASH funksion përdorë një algoritëm matematik për të transformuar të dhënat në një vlerë me një vlerë fikse të gjatësisë, që reprezanton të dhënat. Vlera e hashuar është thjeshtë për krahasim. Nga vlera e hashuar, të dhënat origjinale nuk mund të ri-projektohen direkt. Për shembull, nëse keni harruar fjalëkalimin tuaj, fjalëkalimi juaj nuk mund të kthehet vetëm me vlerën e hashuar. Fjalëkalimi duhet të resetohet. Pasi një fajll shkarkohet, ju mund të verifikoni integritetin e tij duke verifikuar vlerat e hashuara nga burimi me atë që ju keni gjeneruar duke përdorur ndonjë llogaritës së vlerës së hashuar. Duke krahasuar vlerat e hashuara, ju mund të siguroni që fajlli nuk është ndryshuar apo korruptuar gjatë transferimit. *(Checkmarx, 2018)*

Disponueshmëria

Mirëmbajtja e pajisjeve, riparimi i harduerit, përditësimi i sistemeve operative dhe softuerit, dhe krijimi i backup-ëve siguron disponueshmërinë e rrjetës dhe të të dhënave për shfrytëzuesit e autorizuar. Duhet të ekzistojnë plane për rikuperim të shpejtë nga shkatërrime natyrale apo nga njerëzit si pajisjet e sigurisë në formë softueri, si firewall-i, ruajtja nga sulmet për të shkaktuar rrëzim të sistemit, si sulmet DoS(Mohimi i shërbimit). Mohimi i shërbimit ndodh kur një sulmues mundohet "lodh " resurset ne menyre qe resuret te mos jene te disponueshme per perdoruesit e tjere *(Checkmarx, 2018)*

2.14 Llojet më të zakonshme të sulmeve kibernetike

Një sulm në internet është çdo lloj veprimi sulmues që synon sistemet informatike

kompjuterike, infrastrukturat, rrjetet kompjuterike ose pajisjet kompjuterike personale, duke përdorur metoda të ndryshme për të vjedhur, ndryshuar ose shkatërruar të dhëna ose sisteme informacioni. Llojet më të zakonshme të sulmit kibernetik:

2.14.1 Denial-of-service (DoS) dhe shperndarja e sulmeve denial-of-service (DDoS)

Një sulm denial-of-service sulmon burimet e një sistemi në mënyrë që të mos i përgjigjet kërkesave të shërbimit. Një sulm DDoS është gjithashtu një sulm ndaj burimeve të sistemit, por është nisur nga një numër i madh i makinave të tjera pritëse që janë të infektuar nga softuerë me qëllim të keq të kontrolluar nga sulmuesi.

Ndryshe nga sulmet që janë të dizajnuara për t'i mundësuar sulmuesit të fitojnë ose rrisin aksesin, mohimi i shërbimit nuk ofron përfitime të drejtpërdrejta për sulmuesit. Për disa prej tyre, mjafton të kesh kënaqësinë e mohimit të shërbimit. Megjithatë, nëse burimi i sulmuar i përket një konkurrenti biznesi, atëherë përfitimi i sulmuesit mund të jetë mjaft i vërtetë. Një tjetër qëllim i një sulmi DoS mund të jetë marrja e një sistemi offline në mënyrë që të nisë një lloj tjetër sulmesh. Një shembull i zakonshëm është rrëmbimi i seancave, të cilat unë do të përshkruaj më vonë.

Përmbajtja e sulmit TCP SYN

Në këtë sulm, një sulmues shfrytëzon përdorimin e hapësirës tampon gjatë një shtyrje dore të inicializimit të sesionit të Protokollit të Transmisionit (TCP). Pajisja e sulmuesit përmbyt sistemin e synuar të vogël të procesit në radhë me kërkesat e lidhjes, por nuk përgjigjet kur sistemi i synuar i përgjigjet atyre kërkesave. Kjo shkakton që sistemi i synuar të kalojë kohën duke pritur përgjigjen nga pajisja e sulmuesit, gjë që e bën rrëzimin e sistemit ose të bëhet i papërdorshëm kur radhitja e radhës së lidhjes plotësohet.

Ka disa kundërveprime ndaj një sulmi TCP SYN :

Vendosni serverat prapa një firewall të konfiguruar për të ndaluar paketat SYN përbrenda. Rritja e madhësisë së radhës së lidhjes dhe zvogëlimi i kohës për lidhjet e hapura.

Sulmi teardrop

Ky sulm shkakton fushat e kompensimit të gjatësisë dhe copëzimit në paketat vijues të Internet Protocol (IP) për të mbivendosur njëra-tjetrën në hostin e sulmuar; sistemi i sulmuar përpiqet të rindërtojë pako gjatë procesit, por dështon. Sistemi i synuar pastaj bëhet i hutuar dhe rrëzon. Nëse përdoruesit nuk kanë arna për të mbrojtur kundër këtij sulmi DoS, çaktivizoni SMBv2 dhe bllokoni portet 139 dhe 445.

Sulmi i Smurf

Ky sulm përfshin përdorimin e spoofing IP dhe ICMP për të mbushur një rrjet të synuar me trafikun. Kjo metodë e sulmit përdor kërkesa të ICMP-së për shënjestër në adresat IP të transmetimit. Këto kërkesa të ICMP kanë origjinën nga një adresë "viktimë" e mashtruar. Për shembull, nëse adresa e viktimës është 10.0.0.10, sulmuesi do të prishë një kërkesë ICMP echo nga 10.0.0.10 në adresën 10.255.255.255 të transmetimit. Kjo kërkesë do të shkonte në të gjitha IP-të në rang, me të gjitha përgjigjet që kthehen në 10.0.0.10, duke e mbingarkuar rrjetin. Ky proces është i përsëritshëm dhe mund të automatizohet për të gjeneruar sasi të mëdha të bllokimeve të rrjetit.

Për të mbrojtur pajisjet tuaja nga ky sulm, duhet të çaktivizoni transmetimet e drejtuara nga IP në routerët. Kjo do të parandalojë që ICMP të kërkojë emetimin e transmetimit në pajisjet e rrjetit. Një tjetër mundësi do të ishte konfigurimi i sistemeve fundore për t'i mbajtur ata nga përgjigjja ndaj paketave ICMP nga adresat e transmetimit.

Ping of death attack

Ky lloj sulmi përdor pako IP për të 'pinguar një sistem të synuar me një madhësi IP mbi maksimumin prej 65,535 bytes. Paketat IP të kësaj madhësie nuk lejohen, kështu që sulmuesi fragmenton paketën IP. Sapo sistemi i synuar të ripunon paketën, mund të përjetojë përplotje tamponash dhe rrëzime të tjera.

Ping-i i sulmeve me vdekje mund të bllokohet duke përdorur një firewall që do të kontrollojë paketat IP të fragmentuara për madhësinë maksimale *(Blog.netwrix.com, 2018)*

2.14.2 Sulmi Man-in-the-middle (MitM)

Një sulm MitM ndodh kur një hacker futet në mes të komunikimit të një klienti dhe një serveri. Këtu janë disa lloje të zakonshme të sulmeve Man-in-the-middle :

Session hijacking:

Në këtë lloj sulmi MitM, një sulmues rrëmben një sesion në mes të një klienti të besuar dhe serverit të rrjetit. Kompjuteri sulmues zëvendëson adresën e tij IP për klientin e besuar, ndërsa serveri vazhdon sesionin, duke besuar se po komunikon me klientin. Për shembull, sulmi mund të shpaloset kështu:

1) Një klient lidhet me një server.
2) Kompjuteri i sulmuesit fiton kontrollin e klientit.
3) Kompjuteri i sulmuesit shkencon klientin nga serveri.
4) Kompjuteri i sulmuesit zëvendëson adresën IP të klientit me adresën e vet IP dhe spoofs numrat e rendit të klientit.
5) Kompjuteri i sulmuesit vazhdon dialogun me serverin dhe serveri beson se është ende duke komunikuar me klientin.

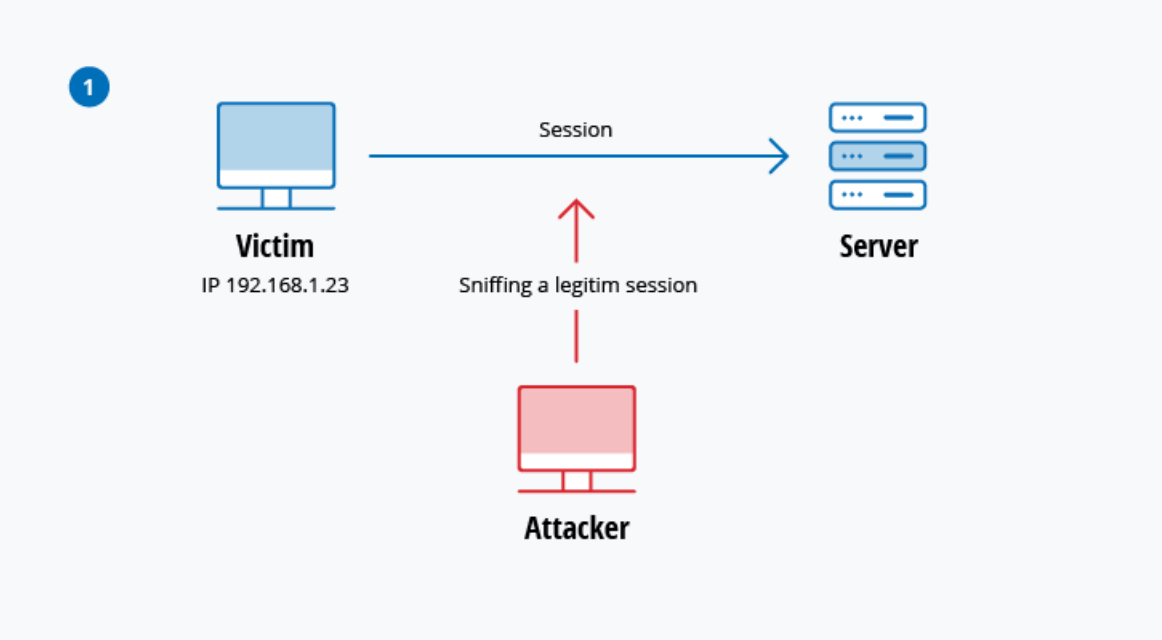

Figure 6:Sulmi në mes të një klienti dhe një serveri të rrjetit

(Blog.netwrix.com, 2018)

IP Spoofing

Spoofing IP është përdorur nga një sulmues për të bindur një sistem që ajo është duke komunikuar me një njësi të njohur, të besuar dhe të sigurojë sulmuesit me qasje në sistem. Sulmuesi dërgon një pako me adresën e burimit IP të një host të njohur, të besuar në vend të adresës së vet të burimit IP në një host të synuar. Pritësi i synuar mund të pranojë paketën dhe të veprojë sipas tij.*(Blog.netwrix.com, 2018)*

2.14. 3 Phishing and spear phishing attacks

Sulmi Phishing është praktika e dërgimit të postës elektronike që duket të jetë nga burime të besueshme me qëllim të fitimit të informacionit personal ose ndikimit të përdoruesve për të bërë diçka. Ajo kombinon inxhinierinë sociale dhe mashtrimet teknike. Kjo mund të përfshijë një shtojcë në një email që ngarkon malware në kompjuterin tuaj. Mund të jetë gjithashtu një lidhje me një faqe të paligjshme që mund t'ju mashtrojë në shkarkimin e malware ose dorëzimin e informacionit tuaj personal.

Shfletimi i phishing është një tip shumë i synuar i aktivitetit phishing. Sulmuesit marrin kohë për të kryer hulumtime në objektiva dhe për të krijuar mesazhe që janë personale dhe relevante. Për shkak të kësaj, vjedhja me fjalëkalim mund të jetë shumë e vështirë për t'u identifikuar dhe madje edhe më e vështirë për t'u mbrojtur. Një nga mënyrat më të thjeshta që një haker mund të kryejë një sulm phishing në shtizën është spoofing me email, që është kur informacioni në seksionin "Nga" është falsifikuar, duke e bërë atë të duket sikur po vjen nga dikush që njeh, siç është menaxhimin tuaj ose kompaninë tuaj partnere. Një tjetër teknikë që përdori përdoruesit për të shtuar kredibilitetin në historinë e tyre është klonimi i internetit - ata kopjojnë faqet e internetit të ligjshme për t'ju mashtruar në futjen e informacioneve personalisht të identifikueshme (PII) ose kredencialet e identifikimit.

Për të zvogëluar rrezikun , mund t'i përdorni këto teknika:

- Critical thinking - Mos e pranoni se një email është marrëveshja e vërtetë vetëm për shkak se jeni i zënë ose i theksuar ose keni 150 mesazhe të tjera të palexuara në kutinë tuaj. Ndaluni për një minutë dhe analizoni emailin.

- Hovering over links - Leviz miun mbi linkun, por mos kliko! Vetëm le kursorin e miut h mbi mbi lidhjen dhe të shohim se ku do të marrë në të vërtetë ju. Aplikoni të menduarit kritik për të deshifruar URL-në.
- Analyzing email headers - Headers Email përcaktojnë se si një email mori në adresën tuaj. Parametrat "Përgjigje-përgjigje" dhe "Kthim-Path" duhet të çojnë në të njëjtën fushë siç është thënë në email.
- Sandboxing - Mund të provoni përmbajtjen e email-it në një mjedis sandbox, aktivitetin e prerjes nga hapja e shtojcës ose klikimi i lidhjeve brenda emailit. *(Blog.netwrix.com, 2018)*

2.14.4 Drive-by attack

Sulmet me anë të shkarkimit janë një metodë e zakonshme e përhapjes së malware. Hakerët kërkojnë faqet e internetit të pasigurtë dhe mbajnë një skriptë me qëllim të keq në kodin HTTP ose PHP në një nga faqet. Ky dorëshkrim mund ta instalojë malware direkt në kompjuterin e dikujt që viziton faqen, ose mund të ri-drejtojë viktimën në një vend të kontrolluar nga hakerat. Shkarkimet nga disku mund të ndodhin kur vizitoni një faqe interneti ose shikoni një mesazh PE ose një dritare pop-up. Ndryshe nga shumë lloje të tjera të sulmeve të sigurisë kibernetike, një makinë nuk mbështetet në një përdorues që të bëjë asgjë për të aktivizuar aktivisht sulmin - nuk duhet të klikosh butonin e shkarkimit ose të hapësh një shtojcë të dëmshme me email për t'u infektuar. Një shkarkim nga "drive-by" mund të përfitojë nga një aplikacion, sistem operativ ose shfletues web që përmban të meta të sigurisë për shkak të përditësimeve të pasuksesshme ose mungesës së përditësimeve.

Për të mbrojtur veten nga drive by attack, ju duhet të mbani shfletuesit dhe sistemet operative të përditësuara dhe të shmangni faqet e internetit që mund të përmbajnë kod me qëllim të keq. Rrini në vendet që zakonisht i përdorni - megjithëse mbani në mend se edhe këto vende mund të jenë të hackuara. Mos mbani shumë programe dhe aplikacione të panevojshme në pajisjen tuaj. Sa më shumë plug-ins që keni, aq më shumë dobësi ekzistojnë që mund të shfrytëzohen nga drive by attack *(Blog.netwrix.com, 2018)*

2.14. 5 Password attack

Meqenëse fjalëkalimet janë mekanizmi më i zakonshëm për të autentikuar përdoruesit në një sistem informacioni, marrja e fjalëkalimeve është një qasje e zakonshme dhe efektive e sulmit. Qasja në fjalëkalimin e një personi mund të merret duke shikuar rreth tavolinës së personit, duke " nuhatur " lidhjen në rrjet për të marrë fjalëkalime të paskrupulluara, duke përdorur inxhinierinë sociale, duke fituar qasje në bazën e të dhënave të fjalëkalimit ose në mënyrë të drejtpërdrejtë. Qasja e fundit mund të bëhet në mënyrë të rastësishme ose sistematike:

- Fjalëkalimi bruto-force guessing do të thotë duke përdorur një qasje të rastit duke provuar fjalëkalime të ndryshme dhe duke shpresuar që një punë Disa logjikë mund të zbatohen duke provuar fjalëkalimet që lidhen me emrin e personit, titullin e punës, hobi apo sende të ngjashme.
- Në një sulm fjalor, një fjalor i fjalëkalimeve të zakonshme përdoret për të tentuar të fitojë akses në kompjuterin dhe rrjetin e një përdoruesi. Një qasje është të kopjoni një skedar të koduar që përmban fjalëkalimet, të zbatojë të njëjtën enkriptim në një fjalor të fjalëkalimeve të përdorura zakonisht dhe të krahasoni rezultatet

Në mënyrë që të mbroheni nga sulmet me fjalor ose me brutalitet, duhet të implementoni një politikë të mbylljes së llogarisë që do të mbyllë llogarinë pas disa përpjekjeve të pavlefshme të fjalëkalimit. Ju mund të ndiqni këto praktika më të mira për mbylljen e llogarisë në mënyrë që të vendosni atë në mënyrë korrekte. *(Blog.netwrix.com, 2018)*

2.14.6 SQL injection attack

Injektimi SQL është bërë një çështje e zakonshme me faqet e internetit të bazuara në bazën e të dhënave. Kjo ndodh kur një keqtrajtues ekzekuton një query SQL në bazën e të dhënave nëpërmjet të dhënave të dhëna nga klienti në server. Komandat SQL futen në të dhënat e hyrjes në aeroplan (për shembull, në vend të identifikimit ose fjalëkalimit) në mënyrë që të ekzekutohen komandat SQL të paracaktuara. Një shfrytëzim i suksesshëm i SQL injektimit mund të lexojë të dhëna të ndjeshme nga baza e të dhënave, të modifikojë (fut, përditësojë ose fshijë) të dhënat e bazës së të dhënave, të ekzekutojë operacionet e administratës (si mbyllja) në

bazën e të dhënave, të rikuperojë përmbajtjen e një skedari të caktuar dhe në disa raste, lëshoni komandat në sistemin operativ.
Për shembull, një formë web në një faqe mund të kërkojë emrin e një llogarie të përdoruesit dhe pastaj ta dërgojë atë në bazën e të dhënave në mënyrë që të tërheqë informacionin e llogarisë së lidhur duke përdorur SQL dinamike si kjo:

*"SELECT * FROM users WHERE account = '" + userProvidedAccountNumber +"';"*

Ndërsa kjo funksionon për përdoruesit që hyjnë siç duhet në numrin e tyre të llogarisë, ajo lë një vrimë për sulmuesit. Për shembull, nëse dikush ka vendosur të japë një numër llogarie prej "'ose' 1 '=' 1 '", që do të rezultonte në një varg query:

*"SELECT * FROM users WHERE account = '' or '1' = '1';"*
Për shkak se '1' = '1' gjithmonë vlerëson TRUE, baza e të dhënave do t'i kthejë të dhënat për të gjithë përdoruesit në vend të vetëm një përdoruesi të vetëm.
Dobësia ndaj këtij lloji të sulmit të sigurisë kibernetike varet nga fakti se SQL nuk bën dallim të vërtetë midis kontrollit dhe planeve të të dhënave. Prandaj, injektimet SQL punojnë kryesisht nëse një faqe interneti përdor SQL dinamike. Përveç kësaj, injektimi SQL është shumë i zakonshëm me aplikacionet PHP dhe ASP për shkak të prevalencës së ndërfaqeve funksionale më të vjetra. Aplikacionet J2EE dhe ASP.NET kanë më pak gjasa që të kenë shfrytëzuar lehtë injektimet SQL për shkak të natyrës së ndërfaqeve programore në dispozicion.
Për të mbrojtur veten nga sulmet me injeksion SQL, aplikoni modelin e privilegjeve më të ulëta të lejeve në databazën tuaj. Rrini në procedurat e ruajtura (sigurohuni që këto procedura të mos përfshijnë ndonjë SQL dinamike) dhe deklarata të përgatitura (pyetje me parametra). Kodi që ekzekutohet kundër bazës së të dhënave duhet të jetë mjaft i fortë për të parandaluar sulmet e injektimit. Përveç kësaj, vërtetoni të dhënat e hyrjes kundër një liste të bardhë në nivelin e aplikimit. *(Blog.netwrix.com, 2018)*

2.14. 7 Cross-site scripting (XSS) attack

Sulmet e XSS përdorin burime të palëve të treta të internetit për të drejtuar skriptat në shfletuesin e internetit të viktimës ose në aplikacionin e shkrimit. Në mënyrë të veçantë, sulmuesi fut një ngarkesë me JavaScript me qëllim të keq në bazën e të dhënave të një faqe interneti. Kur viktima kërkon një faqe nga faqja e internetit, faqja e internetit transmeton faqen, me ngarkesën e sulmuesit si pjesë të trupit HTML, tek shfletuesi i viktimës, i cili ekzekuton skriptën me qëllim të keq. Për shembull, mund të dërgojë cookie të viktimës në serverin e sulmuesit dhe sulmuesi mund ta nxjerrë atë dhe ta përdorë atë për rrëmbimin e seancave. Pasojat më të rrezikshme ndodhin kur XSS përdoret për të shfrytëzuar dobësi shtesë. Këto dobësi mund t'i mundësojnë një sulmuesi që jo vetëm të vjedhë cookies, por edhe të hyjë në shënjestër, të kapë screenshotet, të zbulojë dhe të mbledhë informacionin e rrjetit dhe të aksesojë dhe kontrollojë në mënyrë të largët makinën e viktimës.

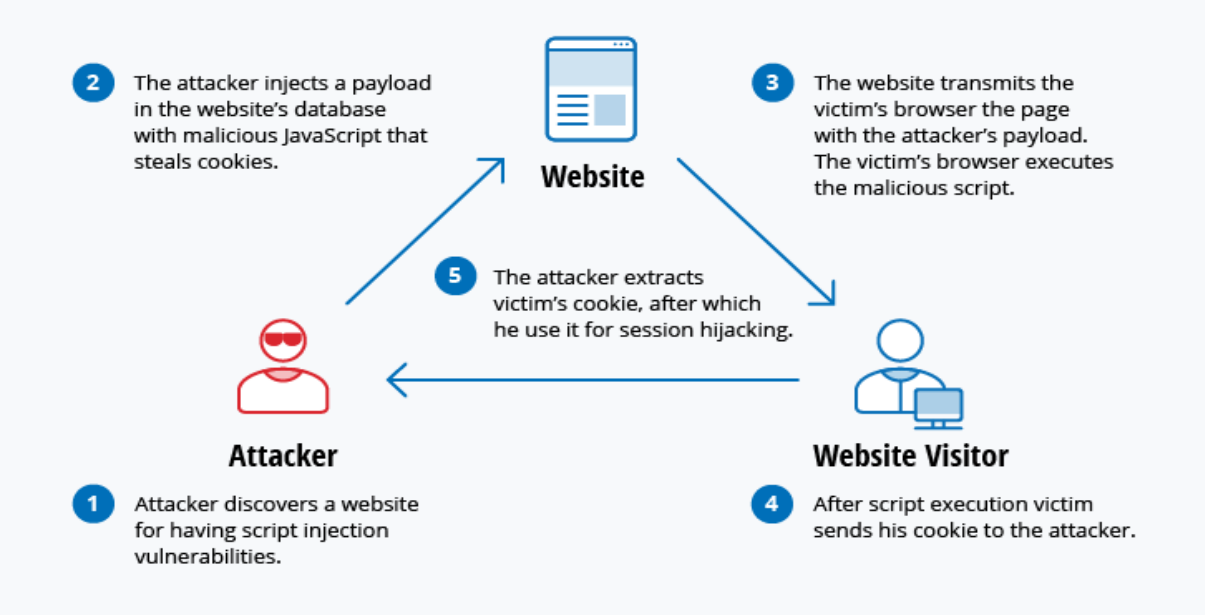

Figure 7:Sulmi Cross-site scripting (XSS)

(Blog.netwrix.com, 2018)

Ndërsa XSS mund të përfitohet nga brenda VBScript, ActiveX dhe Flash, më gjerësisht abuzuar është JavaScript - kryesisht sepse JavaScript është mbështetur gjerësisht në internet.
Për të mbrojtur kundër sulmeve të XSS, sigurohuni që të gjitha të dhënat të jenë të vlefshme, të filtruara ose të ikin para se t'i bëjnë jehonë çdo gjë mbrapa përdoruesit, siç janë vlerat e parametrave të kërkimeve gjatë kërkimeve. Konvertimi i karaktereve të veçanta të tilla si?, &, /, <,> Dhe hapësira në HTML ose URL ekuivalent të koduar përkatës. Jepni përdoruesve mundësinë për të çaktivizuar skriptet në anën e klientit. *(Blog.netwrix.com, 2018)*

2.14. 8 Eavesdropping attack

Sulmet e përgjimit ndodhin përmes përgjimit të trafikut të rrjetit. Duke përgjuar, një sulmues mund të marrë fjalëkalime, numra të kartave të kreditit dhe informacione të tjera konfidenciale që një përdorues mund të dërgojë në rrjet. Përgjimi mund të jetë pasiv ose aktiv:

- Mbyllja pasive - Një haker zbulon informacionin duke dëgjuar transmetimin e mesazhit në rrjet.
- Mbyllja aktive - Një haker në mënyrë aktive grumbullon informacionin duke e maskuar veten si njësi miqësore dhe duke dërguar pyetje tek transmetuesit. Kjo quhet hetim, skanim ose manipulim.

Zbulimi i sulmeve të përgjimit pasiv shpesh është më i rëndësishëm sesa zbulimi i atyre aktivë, pasi sulmet aktive kërkojnë që sulmuesi të fitojë njohuri për njësitë miqësore duke kryer përgjimin pasiv para.
Kriptimi i të dhënave është kundërmasa më e mirë për përgjimin. *(Blog.netwrix.com, 2018)*

2.14. 9 Birthday attack

Sulmet e ditëlindjes bëhen kundër algoritmave të hash që përdoren për të verifikuar integritetin e një mesazhi, softueri ose nënshkrimi dixhital. Një mesazh i përpunuar nga një funksion hash prodhon një mesazh digest (MD) me gjatësi fikse, pavarësisht nga kohëzgjatja e mesazhit të hyrjes; ky MD në mënyrë unike e karakterizon mesazhin. Sulmi ditëlindje i

referohet probabilitetit të gjetjes së dy mesazheve të rastit që krijojnë të njëjtin MD kur përpunohen nga një funksion hash. Nëse një sulmues llogarit MD të njëjtë për mesazhin e tij si përdorues, ai mund të zëvendësojë me siguri mesazhin e përdoruesit me të, dhe marrësi nuk do të jetë në gjendje të zbulojë zëvendësimin edhe nëse krahason MD. *(Blog.netwrix.com, 2018)*

2.14. 10 Malware attack

Programet keqdashëse mund të përshkruhen si softuer të padëshiruar që është instaluar në sistemin tuaj pa pëlqimin tuaj. Ajo mund të bashkangjitet në kod legjitim dhe të përhapet; ai mund të rri në aplikacione të dobishme ose të përsëritet në të gjithë Internetin. Këtu janë disa nga llojet më të zakonshme të malware:

- Viruset makro - Këto viruse infektojnë aplikacione të tilla si Microsoft Word ose Excel. Viruset makro të bashkëngjiten në sekuencën e inicializimit të një aplikacioni. Kur aplikacioni të hapet, virusi ekzekuton udhëzimet përpara se të transferojë kontrollin në aplikacion. Virusi përsëritet dhe i bashkëngjitet kodit tjetër në sistemin kompjuterik. Infektuesit e skedarëve - Viruset e infektimit të skedarëve zakonisht bashkëngjiten me kodin ekzekutues, siç janë skedarët .exe. Virusi është instaluar kur kodi është i ngarkuar. Një version tjetër i një infektuesi fotografi bashkohet me një skedar duke krijuar një skedar virusi me të njëjtin emër, por një shtrirje .exe. Prandaj, kur hapet skeda, kodi i virusit do të ekzekutohet.
- Viruset polimorfike - Këto viruse fshehin veten përmes cikleve të ndryshme të enkriptimit dhe dekriptimit. Virusi i koduar dhe një motor i lidhur mutacion fillimisht decrypted nga një program decryption. Virusi vazhdon të infektojë një zonë të kodit. Motori i mutacioneve pastaj zhvillon një rutinë të re decryption dhe virusi kripton motorin e mutacionit dhe një kopje të virusit me një algoritëm që korrespondon me rutinën e re të decryption. Paketa e koduar e motorit dhe virusit të mutacionit është e bashkangjitur me kodin e ri dhe procesi përsëritet. Këto viruse janë të vështira për t'u zbuluar, por kanë një nivel të lartë të entropisë për shkak të modifikimeve të shumta të

kodit të tyre burimor. Anti-virus software ose mjete të lirë si Hacker Procesi mund të përdorin këtë funksion për t'i zbuluar ato.

- Virusët e vjedhura - Virusët e vjedhura marrin përsipër funksionet e sistemit për të fshehur vetveten. Ata e bëjnë këtë duke kompromentuar softuerin e zbulimit të malware, në mënyrë që softueri të raportojë një zonë të infektuar si të padëmtuar. Këto viruse fshehin çdo rritje në madhësinë e një skedari të infektuar ose ndryshime në datën dhe kohën e modifikimit të fundit të skedarit.
- Trojans - Një trojan apo një kalë trojan është një program që fsheh në një program të dobishëm dhe zakonisht ka një funksion me qëllim të keq. Një dallim i madh midis viruseve dhe Trojans është se Trojans nuk vetë-përsëriten. Përveç sulmeve në një sistem, një trojan mund të krijojë një derë të pasme që mund të shfrytëzohen nga sulmuesit. Për shembull, një trojan mund të programohet për të hapur një port me numër të lartë, kështu që hakerja mund ta përdorë atë për të dëgjuar dhe pastaj të kryejë një sulm.
- Bomba logjike - Një bombë logjike është një lloj softueri me qëllim të keq që është i bashkangjitur në një aplikacion dhe është shkaktuar nga një dukuri specifike, si një kusht logjik ose një datë dhe kohë specifike.
- Worms - Worms ndryshojnë nga viruset në atë që ata nuk i bashkëngjitni një skedari pritës, por janë programe të pavarura që propagandojnë nëpër rrjetet dhe kompjuterët. Worms janë të përhapur zakonisht përmes attachments email; hapja e bashkëngjitjes aktivizon programin krimb. Një shfrytëzues tipik i krimbave përfshin krimbin duke dërguar një kopje të vetvetes në çdo kontakt në adresën e emailit të kompjuterit të infektuar Përveç kryerjes së aktiviteteve me qëllim të keq, një krimb që përhapet në internet dhe mbingarkesa e serverëve të postës elektronike mund të rezultojë në sulme të mohimit të shërbimit kundër nyjeve në rrjetit.
- Droppers - Një pikatore është një program i përdorur për instalimin e viruseve në kompjuterë. Në shumë raste, kapaku nuk është i infektuar me kod me qëllim të keq dhe prandaj nuk mund të zbulohet nga softueri për skanimin e viruseve. Një kapsulë gjithashtu mund të lidhet me internetin dhe të shkarkoni përditësime për softuerin virus që është rezident në një sistem të komprometuar.

- Ransomware - Ransomware është një lloj malware që bllokon hyrjen në të dhënat e viktimës dhe kërcënon të publikojë ose fshijë atë nëse nuk paguhet një shpërblim. Ndërsa disa ransomware të thjeshta kompjuterike mund të bllokohet sistemi në një mënyrë që nuk është e vështirë për një person të ditur për të ndryshuar, malware më të përparuara përdor një teknikë të quajtur zhvatje kriptovirale, e cila krijon skedarët e viktimës në një mënyrë që i bën ata pothuajse të pamundur të shërohen pa celes kyç
- Adware - Adware është një aplikacion softuerik i përdorur nga kompanitë për qëllime marketingu; banderolat e reklamave shfaqen kurdo që programi ekzekutohet. Adware mund të shkarkohet automatikisht në sistemin tuaj duke shfletuar ndonjë faqe interneti dhe mund të shikohet përmes dritareve pop-up ose përmes një shirit që shfaqet automatikisht në ekranin e kompjuterit.
- Spyware - Spyware është një lloj programi që është instaluar për të mbledhur informacion rreth përdoruesve, kompjuterëve të tyre ose zakoneve të tyre të shfletimit. Ai gjurmon gjithçka që bëni pa njohuritë tuaja dhe i dërgon të dhënat një përdoruesi të largët. Gjithashtu mund të shkarkojë dhe instalojë programe të tjera me qëllim të keq nga interneti. Spyware punon si adware, por zakonisht është një program i veçantë që instalohet pa dijeninë kur instaloni një aplikacion tjetër freeware. *(Blog.netwrix.com, 2018)*

2.15 Hapat që duhet të bëni nëse ju keni qenë i hakuar

Një shkelje e të dhënave mund të jetë një skenar shkatërrimtar për një biznes të vogël apo të mesëm dhe madje edhe më i madhi i korporatave mund të kthehet në muajt e tjerë ose të shpenzojë miliona nga një kollë e thatë. Minimizimi i rrezikut dhe parandalimi i sulmit të rrjetit në vendin e parë duhet të jetë një nga prioritetet kryesore të çdo kompanie, për të mbajtur të dhënat e punonjësve dhe klientëve të sigurt dhe për të mbrojtur reputacionin e organizatës.

Për fat të keq, jo të gjitha hackat janë të parandalueshme, madje edhe sistemet më të mira të sigurisë mund të kapërcehen duke përdorur truket dhe metodat që hakerët nuk e kanë provuar më parë. Metodat e reja të sulmeve hulumtohen çdo ditë, dhe pavarësisht nga përpjekjet më të

mira të profesionistëve, ata thjesht nuk mund të jenë të mjaftueshëm. Bizneset do të sulmohen ende, por ekziston një mënyrë e duhur për t'u përgjigjur. Dëmtimi mund të minimizohet në kohë dhe një katastrofë e mundshme mund të shndërrohet në një përplasje me shpejtësi në rrugën drejt rritjes së biznesit.

Nëse rrjeti yt hakohet, këtu janë hapat që duhet të merrni menjëherë.

Hapi 1. Gjeni burimin e problemit dhe rregulloje ate

Vetëm për shkak se ka ndodhur një shkelje e të dhënave dhe është zbuluar një incident i sigurisë kibernetike, kjo nuk do të thotë se kërcënimi ka kaluar ose që sistemet tuaja tani janë të sigurta. Sa më shpejt të jetë e mundur, profesionistët e TI (dhe ndoshta një ekspert i angazhuar, në varësi të stafit që punojnë në biznesin tuaj) duhet të jenë në gjendje të gjejnë burimin e problemit. Kjo është më pak për tu fajësuar në rast të gabimit njerëzor (i cili ka të ngjarë të ishte i përfshirë), dhe më shumë për të prerë shkeljet dhe për të parandaluar shfrytëzimin përsëri në të ardhmen.

Sapo të gjendet problemi, profesionistët duhet ta rregullojnë atë sa më shpejt që të jetë e mundur, ose duke e zbukuruar atë ose duke e hequr (në varësi të problemit). Përveç kësaj, biznesi duhet të bëjë përpjekje për të siguruar që probleme të ngjashme nuk ekzistojnë në sistemet ose proceset e tjera të biznesit. *("4 Steps You Should Take If You Have Been Hacked", 2018)*

Hapi # 2. Kryeni një Kontroll të Sigurisë në Cybersecurity dhe Mbani Inventarin

Pas lëshimit të menjëhershëm, është e rëndësishme që bizneset të marrin një inventar të të dhënave të tyre dhe të kryejnë një "auditim të sigurisë kibernetike". Ky është një term i vështirë për t'u zbatuar me saktësi për të gjitha bizneset, por biznesi juaj mund të dëshirojë të bëjë sa vijon, :

- Shqyrto të gjitha të dhënat në të gjithë kompaninë dhe mbani gjurmët se ku janë skedarët dhe ku kanë qenë, nëse është e mundur. Kontrolloni se si janë përdorur shërbimet dhe ku ka udhëtuar informacioni më i ndjeshëm (dhe nëse ato lëvizje kanë qenë brenda politikave të kompanisë). Kjo mund të jetë e vështirë për t'u ndjekur, por më shumë informacion, aq më mirë.

- Kontrollo për të parë nëse ndonjë skedar mungon. Përderisa kjo nuk ka gjasa që hakerët dhe kriminelët kibernetikë të kenë më shumë mundësi të kopjojnë vetëm skedarët, ia vlen të përmenden edhe shenja të sabotimit të mundshëm.
- Përcaktoni nëse ndonjë fotografi është lëshuar për publikun ose nëse ekziston një gjurmë që mund të përcaktojë se ku ndodheshin skedat e rrjedhura. Ndërsa mund të mos jeni në gjendje t'i hiqni ose t'i merrni ato, kjo do t'ju lejojë të përcaktoni motivin potencial dhe ndikimin e mundshëm të sulmeve, duke ju lejuar të reagoni më mirë tani dhe në të ardhmen.

Këto hapa mund të ndryshojnë në mënyrë të egër dhe mund të keni nevojë të shtoni hapa shtesë, por pika kryesore që duhet bërë është që ju duhet të hetoni gjërësisht problemin dhe të merrni inventarin e të dhënave që keni dhe ku është zhdukur. Ky informacion do të jetë i paçmuar në përpjekjet tuaja për të mbajtur problemin. *("4 Steps You Should Take If You Have Been Hacked", 2018)*

Hapi # 3. Kryen kontrollin e dëmeve

Ky është një hap tjetër që varet shumë nga lloji i incidentit të sigurisë kibernetike që ka ndodhur dhe nga lloji i biznesit me të cilin jeni përfshirë. Ka probleme të ndryshme që mund të lindin kur ndodh një shkelje e të dhënave, dhe këtu është se si të merrni përpara shumicën e tyre:

- Merrni përpara problemin përpara se të bëhet njohja publike, nëse kompania juaj është e përfshirë me publikun ose ka investitorë. Nën asnjë rrethanë nuk duhet të fshihet një shkelje e të dhënave nën qilim, pasi që ka të ngjarë të zbulohet dhe duke u përpjekur ta fsheh vetëm do t'i bëjë gjërat shumë më keq për biznesin tuaj. Shpjegoni se problemi është zbuluar, se është duke u menaxhuar dhe se të gjitha hapat e nevojshëm janë duke u ndërmarrë në mënyrë që të mos ndodhë kurrë më.
- Ndryshoni fjalëkalimet dhe metodat e verifikimit menjëherë pasi që të dyja janë një masë për të siguruar punonjësit si dhe për të forcuar sigurinë.
- Merrni masa proaktive për të mbrojtur ata që preken nga një thyerje ose vjedhje identiteti si një mjet për të ndrequr dhe mbrojtur ato lidhje. Sigurimi i shërbimeve të monitorimit të kredive është në përgjithësi një fillim i mirë.

- Vendosni mënjanë burimet për të trajtuar komplikime të mëtejshme nga problemi, ndoshta edhe lënë mënjanë kohën IT të IT për t'u përgjigjur pyetjeve nga punonjësit dhe klientët / klientët
- Dokumentoni gjithçka. Është mjaft e mundshme beteja ligjore ose çështje mund të lindin si rezultat i shkeljes së të dhënave, dhe ju do të dëshironi të siguroheni që çdo gjë të jetë në rregull në mënyrë që ju të bëni një argument të fortë në favorin tuaj.
- Kthehu në rutinë e përditshme të kompanisë. Jashtë theksit të mëposhtëm mbi trajnimin, ju do të dëshironi të mbani mesazhin me markën tuaj dhe ju do të dëshironi të siguroni një shërbim spektakolar për të ruajtur kredibilitetin e biznesit tuaj. Askush nuk dëshiron të shohë një kompani në panik. *("4 Steps You Should Take If You Have Been Hacked", 2018).*

Hapi # 4. Retrain dhe Refocus

Sapo pluhuri të zgjidhet dhe biznesi juaj ka plane për t'u përballur me problemin dhe për të parandaluar që ajo të ndodhë përsëri në të ardhmen, është një kohë e mirë për të rishikuar protokollet tuaja të sigurisë kibernetike në përgjithësi dhe për të ofruar trajnime efikase për punonjësit brenda organizatës suaj . Ka gjasa të përmirësojë moralin e të punësuarve, të cilët do të ndjehen më të sigurt se një gjë e tillë nuk do të ndodhë më, dhe duke pasur parasysh kërcënimin, ata do të jenë më të hapur ndaj reagimeve dhe trajnimit mbi temat e sigurisë në kibernetikë. Ju mund të dëshironi të përmirësoni ose rifokusoni trajnimin në varësi të natyrës së saktë të shkeljes së të dhënave dhe veprimeve të kompanisë suaj, dhe biznesi juaj duhet të mbështetet në sigurinë kibernetike ose në IT profesionistët për këto konsiderata. *("4 Steps You Should Take If You Have Been Hacked", 2018)*

2.16 Mbrojtja nga sulmet kibernetike

Kërcënimi i sulmeve kibernetike po zgjerohet me shpejtësi dhe po transformohet. Ndërsa njerëzit bëhen gjithnjë e më shumë të lidhur me teknologjinë, mundësia për ekspozim rritet. Por vetëm për shkak se këto incidente po ndodhin më shpesh, kjo nuk do të thotë që ne duhet vetëm të mësohemi me to. Në fakt, është më e rëndësishme se kurrë që ne vazhdojmë të mësojmë rreth mashtrimeve të fundit dhe tendencave të hacking dhe si të mbrohemi kundër

tyre. Ndërsa një "buton i lehtë" nuk ekziston për të mbrojtur veten, ka një grusht gjëra që mund të bëni tani për të rritur mbrojtjen tuaj personale kundër sulmeve kibernetike. (Matis and Matis, 2018).

Sulmet kibernetike po bëhen gjithnjë e më të përhapura, pasi viruset, malware dhe hakerat rriten gjithnjë e më shumë në zgjuarsi.

Ne shpjegojmë se si të mbrohemi nga sulmet kibernetike. Këtu janë 11 mënyra për t'ju ndihmuar të mbroheni nga sulmet kibernetike, ose të minimizoni kërcënimin nëse jeni kompromet uar. *("11 Ways to Protect Yourself from Cyber Attacks - Nexus", 2018)*

1. Përmirësoni sistemin tuaj operativ

Mbani sistemin tuaj operativ të përditësuar me versionin më të fundit. Sistemet operative të vjetra dhe të vjetruara shpesh janë më të lehta për t'u krehur ose për të infektuar. *("11 Ways to Protect Yourself from Cyber Attacks - Nexus", 2018)*

2. Aktivizo përditësimet automatike

Aktivizimi i përditësimeve automatike merr supozimin nga përditësimi i softuerit në mënyrë që të mos harroni. Shumica e programeve kanë një listë të thjeshtë të kontrollit që mund ta përdorni për ta aktivizuar këtë. ("11 Ways to Protect Yourself from Cyber Attacks - Nexus", 2018)

Më shumë pajisje sesa ti e kupton janë të lidhura me internetin. Telefoni, ruteri, printeri, madje edhe disa frigoriferë mund të paraqesin kërcënim. Një nga mënyrat më të thjeshta për të shmangur hakmarrjen është përditësimi i vazhdueshëm i këtyre pajisjeve. Duke qëndruar up-to-date mbi softuerin më të fundit dhe lajmet që rrethojnë pajisjet tuaja, ju jo vetëm që do të shmangni gabimet dhe gabimet e padëshiruara, por gjithashtu do të rrisni sigurinë e tyre. Programuesit dhe zhvilluesit e pajisjeve shpesh krijojnë ndërprerje shtesë të sigurisë në përditësime të reja. Nëse jeni gjithmonë duke përdorur versionet më të fundit të softuerit, gjasat që një nga këto pajisje të kompromet ohen zvogëlohen. *(Matis and Matis, 2018).*

3. Anti-Virus Software

Pasi të keni paguar anti-virus të instaluar në të gjitha pajisjet tuaja është vendimtare. Disa kompjuterë vijnë me anti-virus software të para-instaluar, por vlen të përmendet paguar anti-virus siguron siguri dhe mbrojtje shumë më të fortë. Siç shkon duke thënë, ju merrni atë që ju paguani për! *("11 Ways to Protect Yourself from Cyber Attacks - Nexus", 2018)*

4. Ktheni mbrapa të dhënat tuaja

Mbështetja e të dhënave tuaja është thelbësore. Rezervoni rregullisht të dhënat tuaja më të rëndësishme rregullisht, të paktën një herë në javë. Për ta bërë më të lehtë detyrën, mund të vendosni rezerva automatike duke përdorur një aplikacion të tillë si OneDrive ose Google Drive. *("11 Ways to Protect Yourself from Cyber Attacks - Nexus", 2018)*

5. Krijo fjalëkalime të sigurta

Përdorni fjalëkalime të sigurta që janë të vështira për t'u menduar. Fjalëkalimet më të mira do të kenë një kombinim letrash, numrash dhe simbole. Nëse keni probleme që vijnë me ide, ju mund të përdorni një gjenerator me fjalëkalim të sigurt online. Gjithashtu gjithmonë përdorni një fjalëkalim tjetër për çdo llogari. Përdorni 1Password i cili është një aplikacion i koduar i sigurt që mund të përdorni për të regjistruar të gjitha fjalëkalimet tuaja në mënyrë që të mos harroni kurrë ato! *("11 Ways to Protect Yourself from Cyber Attacks - Nexus", 2018)*

Fjalëkalime të forta dhe të sigurta janë mënyra të thjeshta dhe efektive për të kufizuar rreziqet tuaja. Fjalëkalimet e gjata, të rastësishme dhe komplekse e bëjnë shumë më të vështirë për këdo që nuk dëshiron të ketë qasje në të dhënat tuaja. Përdorni një menaxher fjalëkalimi. Ka programe të shumta atje që mbajnë gjurmët e fjalëkalimeve tuaja të gjata dhe komplekse për ju, dhe madje gjenerojnë ato të sigurta për faqet e reja që ju regjistroheni. Kjo është një mënyrë e shkëlqyeshme për të siguruar që cenueshmëria e llogarive tuaja të jetë e kufizuar dhe madje edhe nëse një vend është i kompromet uar, duke siguruar që nuk ka të ngjarë që të tjerët të jenë me të.

Ndërsa një "buton i lehtë" nuk ekziston për të mbrojtur veten, ka një grusht gjëra që mund të bëni tani për të rritur mbrojtjen tuaj personale. Duke përditësuar vazhdimisht të gjitha pajisjet e lidhura, ngrirjen e kredisë, edukimin e vetes dhe të tjerëve për mashtrimet e zakonshme dhe mbylljen e llogarive tuaja me fjalëkalime hiper-të sigurta, kufizoni shanset që informacioni juaj të kompromentohet. Pavarësisht se bëhet gjithnjë e më i zakonshëm për llogaritë, kredinë, të dhënat dhe informacionin për t'u vjedhur, mund të bëni pjesën tuaj për të siguruar që kjo të mos ndodhë me ju ose me njerëzit që njihni(*Matis and Matis, 2018).*

6. Vendosni një firewall

Gjithmonë sigurohuni që firewall juaj të jetë aktiv në mënyrë që t'ju njoftoheni me kërcënime të mundshme. Një firewall mund të identifikojë dhe të bllokojë përpjekjet e sulmit kibernetik përpara se të ndodhë. *("11 Ways to Protect Yourself from Cyber Attacks - Nexus", 2018)*

7. Beni valide Certifikaten SSL

Vendosni shfletuesin tuaj për të përcaktuar vlefshmërinë e certifikatave SSL nga faqet e internetit që vizitoni. Kjo do t'ju ndihmojë të njihni nëse një faqe interneti është siguruar ose jo, dhe të sigurt për t'u përdorur me informacione private si kartat e kreditit. *("11 Ways to Protect Yourself from Cyber Attacks - Nexus", 2018)*

8. Shmangni instalimin e frekuencave të paketuara

Merrni kujdes - shumë softuer të lirë mund të kenë paketa të paketuara me të! Para se të instaloni ndonjë gjë bëni detyrat e shtëpisë tuaj të parë. Lexoni komente përdoruesish dhe shikoni për kutitë e zgjedhjes ose butonat që instalojnë objekte të tjera gjatë procesit të instalimit. *("11 Ways to Protect Yourself from Cyber Attacks - Nexus", 2018)*

9. Kini kujdes se çfarë shkarkoni

Para se të vendosni të shkarkoni atë pjesë të softuerit, filmit ose muzikës, sigurohuni që të dini nëse ajo që shkarkoni është e sigurt ose ligjore. Nganjëherë viruset mund të fshihen në skedarë ndryshe të pafajshëm. *("11 Ways to Protect Yourself from Cyber Attacks - Nexus", 2018)*

10. Çfarë duhet të bëni nëse ju merrni hacked

Në një situatë ku merrni hacked merrni menjëherë veprime për të ndryshuar të gjitha fjalëkalimet tuaja dhe shikoni për njoftimet me email të adresave të reja IP që hyni në ndonjë nga llogaritë tuaja. Gjithashtu mbani një sy në bankat dhe kartat e kreditit për aktivitete të paautorizuara dhe nëse është e nevojshme kontaktoni bankën tuaj për të marrë kartat tuaja të anuluara. *("11 Ways to Protect Yourself from Cyber Attacks - Nexus", 2018)*

11. Asnjëherë mos paguani hakerat

Nëse llogaria juaj kompromentohet dhe ju merrni një ofertë nga hakerat për të rivendosur skedarët tuaj për një çmim, të drejtuar! Nuk ka asnjë mënyrë që të jeni të sigurtë se ata do të rikthenin skedarët tuaj të çmuar nëse paguani, dhe në të dyja mënyrat që ju keni të bëni me kriminelët kibernetikë!

Secila nga këto gjëra mund të bëjë një rrugë të gjatë për t'ju ndihmuar të shmangni viktimizimin e një sulmi kibernetik. Siguria juaj është e vlefshme! *("11 Ways to Protect Yourself from Cyber Attacks - Nexus", 2018)*

2.17 Online Privacy vs Cyber Security

Termat privacy në internet dhe siguria kibernetike janë dy subjekte të ndryshme që janë të qetë shpesh të ndërthurura me njëri-tjetrin. Sidoqoftë, është e rëndësishme të theksohet se privatësia ka të bëjë me mbajtjen e informacionit personal privat dhe larg syve të vështira, ndërsa siguria kibernetike ka të bëjë me mbajtjen e sistemeve në të cilat informacioni mbahet i sigurt dhe i mbrojtur. Ku është theksuar mirë se megjithëse është i ndërlidhur, privatësia dhe siguria. *(Rombel, 2001).*

Janë çështje me të vërtetë të ndara me hollësitë e ndryshme dinamike. Në mënyrë të ngjashme, është përmend se privatësia dhe siguria mund dhe duhet të trajtohen si çështje të ndryshme.*(Bambauer, 2013)*

Megjithëse ka shumë informata në lidhje me privatësinë në internet dhe veçmas për sigurinë kibernetike, një hulumtim i vogël është në dispozicion në lidhje me lidhjen ndërmjet privatësisë dhe sigurisë.

Sidoqoftë, është gjetur se ka një mbivendosje të konsiderueshme në hulumtimin për privatësinë dhe atë të sigurisë. Ndoshta kjo nuk është e habitshme duke pasur parasysh se mekanizmat e sigurisë janë në vend për të mbrojtur sistemet që përmbajnë informacionin që duam të mbajmë private. Si e tillë, është vështirë të studiohet ai pa përmendur tjetrën.

Autori thekson se siguria është një ndërfaqe midis informacionit dhe privatësisë. Ndërsa privatësia, siç u përmend më herët, ka të bëjë me mbajtjen e informacionit larg syve të vështira, siguria ndihmon ndërmjetësimin e këtyre të drejtave në privatësi dhe ndihmon që ato të ndikohen. *(Bambauer, 2013)*

Në një studim u zhvillua një instrumet dhe u testua për të matur nevojën e perceptuar të një individi për sigurinë dhe nevojën e perceptuar për privatësi. Instrumenti u gjet të jetë shumë i besueshëm dhe u gjet një marrëdhënie e rëndësishme mes nevojës së perceptuar për privatësi dhe nevojës së perceptuar për konstruksione të sigurisë. Pra, edhe pse është e qartë se njerëzit kërkojnë si intimitet dhe sigurinë, nuk përmendet shumë në lidhje me lidhjen midis privatësisë dhe sigurisë. A po jep më shumë informacion do të thotë siguri më e mirë apo siguria më e mirë do të thotë të japësh më pak informacion? *(Pirim et al, (2008).*

Një zbulim interesant në këtë hulumtim ishte puna e dy autoreve. Ku shqyrtuan marrëdhëniet midis sigurisë dhe privatësisë dhe vunë re se privatësia dhe siguria nuk duhet të jenë të

kundërta në vetvete dhe se ai mund të ndikojë me të vërtetë në tjetrin. Për më tepër, ata argumentojnë se siguria nuk është në kundërshtim me privatësinë, por një aspekt i tij. Kjo do të thotë që ndërsa privatësia dhe siguria janë dy nocione të ndryshme, siguria ndihmon në atë që është privatësia. Ndërsa siguria ruan informacionin personal privat, privatësia në internet nuk mund të arrihet pa siguri adekuate. (*Kleve dhe Mulder,2008)*

Një shembull i mirë i asaj se si ndihmon një tjetër është rasti i shkeljes së të dhënave Acxiom që u zhvillua në mes të viteve 2002 dhe 2003. Në këtë shkelje të të dhënave, Acxiom ekspozuar ndaj ndjeshme të dhënat e konsumatorit tri herë. Shkelja e parë u krye nga kontraktuesi që ishte duke punuar me Acxiom dhe dy të tjera nga kërcënimet e jashtme. Këtu, siguria ishte e papërshtatshme, dhe si rezultat i kësaj u arritën të dhënat personale të klientëve. Pra, ndërsa siguria mund të jetë një entitet i pavarur, privatësia nuk mund të arrihet pa siguri të mjaftueshme.

2.18 Mbrojtja me ligj e të dhënave personale në Republikën e Kosovës

Te dhënat personale mbrohen me ligje në tërë botën po ashtu edhe në Republikën e Kosovës

Në mbështetje të nenit 65 (1) të Kushtetutës së Republikës së Kosovës, Miraton LIGJIN PËR MBROJTJEN E TË DHËNAVE PERSONALE.

Sipas Nenit 5 përpunimi i ligjshëm i të dhënave personale

1. Të dhënat personale mund të përpunohen vetëm nëse:

1.1. subjekti i të dhënave ka dhënë pëlqimin e tij ose saj;

1.2. përpunimi është i domosdoshëm për përmbushjen e një kontrate në të cilën subjekti i të dhënave është palë kontraktuese ose për të ndërmarrë veprimet lidhur me kërkesën e subjektit të të dhënave para lidhjes së kontratës;

1.3. përpunimi është i domosdoshëm për respektimin e obligimit ligjor të cilit i nënshtrohet kontrolluesi;

1.4. përpunimi është i domosdoshëm për mbrojtjen e interesave jetike të subjektit të të dhënave;

1.5. përpunimi është i domosdoshëm për kryerjen e një detyre me interes publik ose në ushtrimin e autoritetit zyrtar që i është dhënë kontrolluesit apo një pale të tretë të cilës i zbulohen të dhënat;

1.6. përpunimi është i domosdoshëm për qëllime të interesave legjitime të ushtruara nga kontrolluesi ose pala e tretë apo palëve të cilave u janë zbuluar të dhënat, me përjashtim të rasteve kur interesat e tilla janë në kundërshtim me të drejtat dhe liritë themelore të subjektit të të dhënave.*(Agjencia Shtetërore për Mbrojtjen e të Dhënave,2018)*

3 DEKLARIMI I PROBLEMIT

Privatësia në internet dhe krimet kibernetike janë shqetësime aktuale që po shfaqen mjaftë shumë. Privatësia në internet nuk është shumë e sigurtë dhe njerëzt janë mjaftë të shqetësuar për privatësinë e tyre pasi që nuk ndihen të sigurt aspak. Shpesh herë mendojnë se kërkimet qe bëjnë në internet nuk na identifikojnë dhe se mbetemi gjithmonë anonimë pas ekranit të kompjuterit. Ekspertët e privatësisë sugjerojnë që të jeni në dijeni të gjërave para se të filloni t'i përdorni ato. Shumë prej kompanive i bëjnë publike politikat e tyre të privatësisë prandaj duhet t'i lexoni me kujdes.

Krimet kibernetike jane mjaftë aktive në kohën e sotme ku njerzit hakohen me lloje te ndryshme te krimeve kibernetike permes internetit. Krimi kibernetik është një veprim kriminal që zhvillohet në rrjetin e komunikimit, duke keqpërdorur sistemin dhe të dhënat kompjuterike Kompjuterët, telefonet, interneti dhe te gjitha sistemet tjera informative te cilat përdoren nga njerëzit, janë vegla shumë të mira të cilat arrijnë t'i përdorin kriminelët kibernitik. Përmes këtyre teknologjive ata arrijnë të hyjnë në të dhënat tona private, në llogaritë tona bankare, servere, webfaqe, si dhe në të dhënat e institucioneve publike.

Siguria kibernitike ka nevojë për më shumë vëmendje. Duke marrë parasysh kufizimet e njeriut dhe mençurinë e virusëve të kompjuterëve, rrjeti kompjuterik ka nevojë për agjent intelegjent kibernitik, të cilët do te detektojnë, kontrollojnë dhe pergjigjen ndaj sulmeve kibernitike në kohë të shkurtër.

Rrjedhimisht qëllimi i kësaj teme është që të mësojmë më shumë për privatësinë në internet, të dimë çfarë të dhëna të japim në rast se kërkohen, poashtu të mësojmë për krimet kibernetike se çfarë janë këto krime, dhe si të mbrohemi nga ky lloj i krimit.

4 METODOLOGJIA

Ky hulumtim merret me një dukuri që ka të bëjë me privatësinë e të dhënave dhe krimet kibernetike. Për mbledhjen e të dhënave ne kemi përdorur dy metoda shqyrtimin e literaturës si metode per mbledhjen e te dhenave të dhëna që janë në funksion te hulumtimit. Artikujt e ndryshëm dhe punimet apo hulumtimet shkenëcore që të tjerët kanë hulumtuar më parë ne i kemi përpunuar dhe i kemi përdorur si burime të dhënash. Po ashtu kemi përdorur metodën kuantitative përmes një anketimi ku janë pergjigjur disa njerëz.

Fillimisht, qëllimi parësor ka qenë të dijmë më shumë për privatësinë në internet dhe krimet kibernetike për shkak se interneti është një gjë që është bërë pjesë e përditshmërisë se çdo njeriu, pra qëllimi është që të dijmë si ta ruajmë privatësinë sado pak dhe të mbrohemi nga krimet kibernetike. Së pari kemi folur për sigurinë e informacionit se sa janë të sigurta të dhënat tona, se si duhet t'i mbrojmë të dhënat e tona, rëndesinë e te dhënave tona pastaj për krimet kibernetike se cilat janë krimet kibernetike, hapat që duhet t'i ndërmarrim në mënyrë që të mbrohemi nga krime kibernetike .

Pastaj përmes një ankete kemi nxjerrur të dhëna primare nga një pyetësor që është zhvilluar online me anë të Google Forms. Pyetësori përfshin 20 pyetje të formës kuantitative. Pyetësori ka qenë i vetë-administruar dhe është publikuar në mënyrë elektronike duke përdorur internetin.

5 PREZANTIMI DHE ANALIZA E REZULTATEVE

Ky kapitull përfshinë të gjithë rezultatet e fituara nga pytësori i bërë prej 20 pytjesh, ku target kan qenë moshat prej 18-25 vjtë, për të kuptuar se sa din për privatësinë e intenetit dhe krimet kibernetike. Pra pytësori përfshinë 20 pytje të formës kuantitative. Pytësori ka qenë i vetëadministruar dhe është publikuar në mënyrë elektronike duke përdorur internetin. Pytësori është zhvilluar online me anë të Google Forms. Kjo analizë empirike është ralizuar gjatë periudhës Mars-Prill 2019 ku është përfshirë analiza se sa janë të njoftuar njerzit në përgjithësi për privatësin në internet dhe krimet kibernetike.

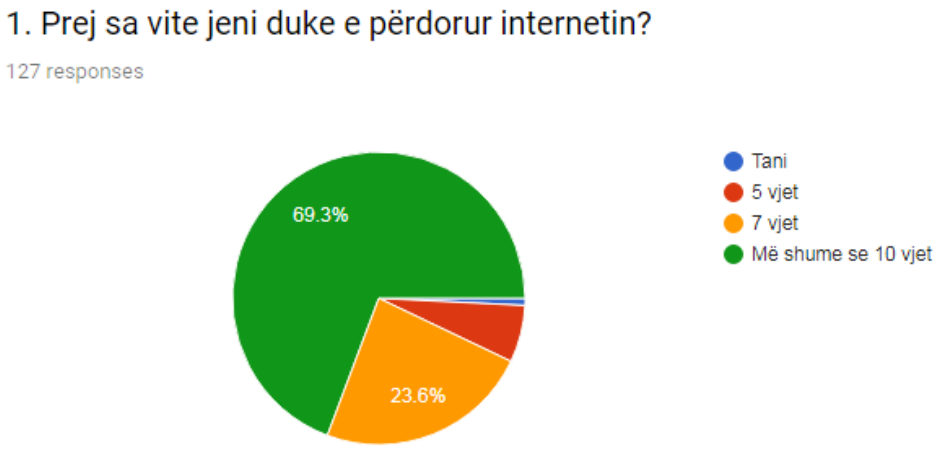

Figure 8: Përdorimi i internetit

Kjo figurë tregon që interneti është bërë i domosdoshëm dhe se 63.3% e përdorin për më shumë se 10 vite.

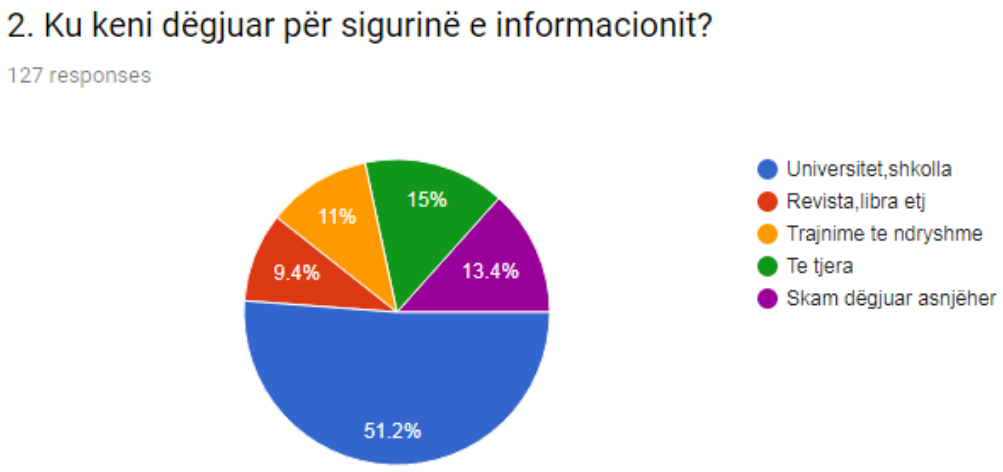

Figure 9: Siguria e Informacionit

Në këtë figurë tregohet që shumica e të anketuarëve për sigurinë e informacionit kanë dëgjuar në universitet dhe shkolla 51.2%, në revista dhe libra 9.4%, në trajnime të ndryshme 11% ndërsa 13.4% nuk kanë dëgjuar asnjëherë.

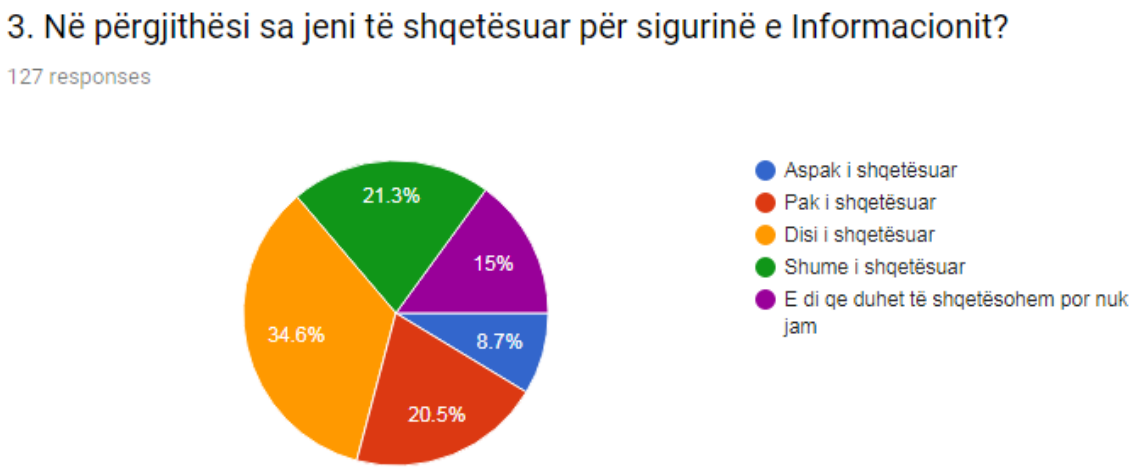

Figure 10: Shqetësime për Sigurinë e Informacionit

Kjo figurë tregon se në përgjithësi njerëzit shqetësohen për privatësinë e të dhënave të tyre.

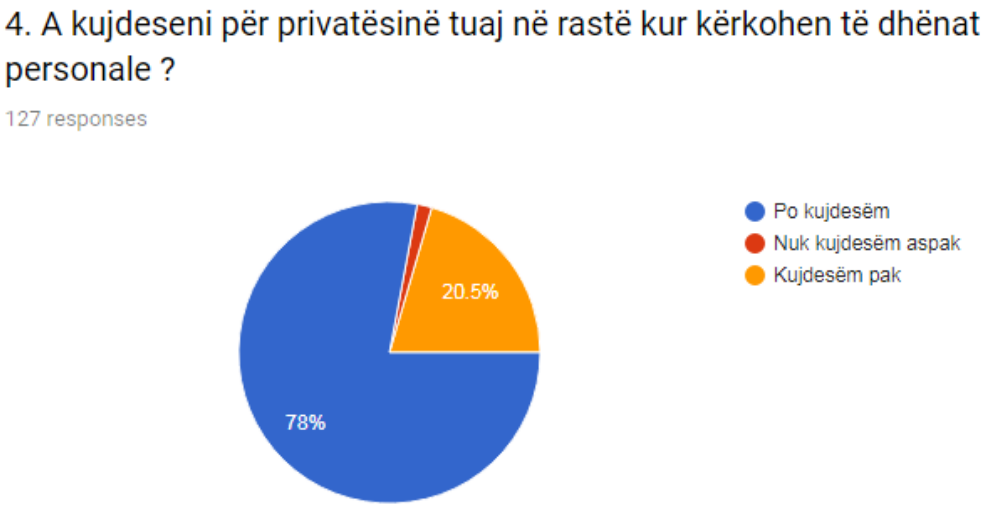

Figure 11: Kujdesi ndaj privatësisë së të dhënave

Kjo figurë tregon se në përgjithësi njerëzit kujdesen për të dhënat e tyre personale kur ju kërkohen në internet.

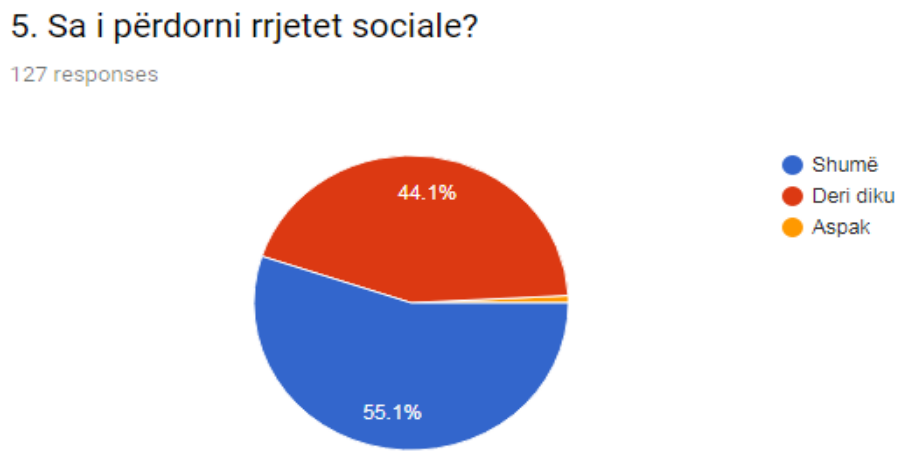

Figure 12: Përdorimi i rrjeteve sociale

Kjo figurë tregon se prej 127 personave që ju përgjigjen pyetësorit online 55.1% përdorin rrjete sociale.

Figure 13: Rrjeti social i përdorur më së shumti

Në këtë figurë është paraqitur se cili rrjete social përdoret më së shumti dhe sipas statistikave rrjeti social që përdoret më së shumti është Instagrami me 57.5% pastaj Snapchat me 17.3% , Viber me 9.4% dhe të tjerat.

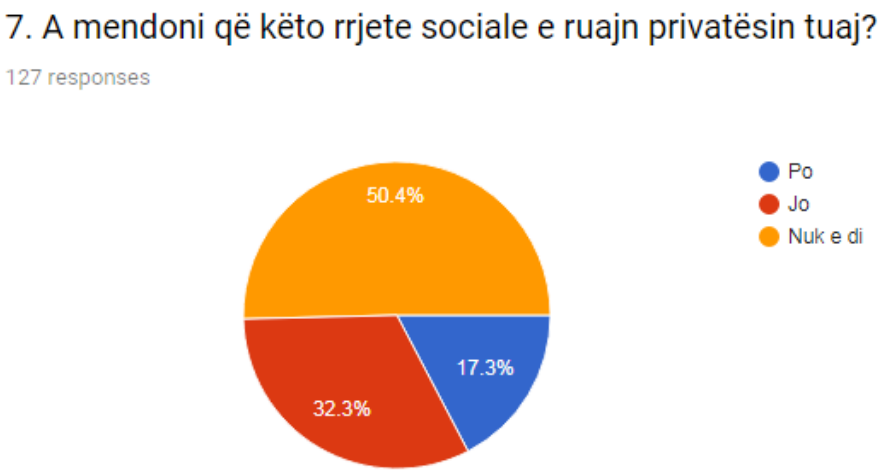

Figure 14: Privatësia në rrjetet sociale

Kjo figurë tregon që shumica e personave nuk e dijnë se sa ruhet privatësia në rrjetet sociale ndërsa (32.3%) mendojnë që privatësia nuk ruhet në rrjetet sociale kurse (17.3%) mendojnë që ruhet privatësia.

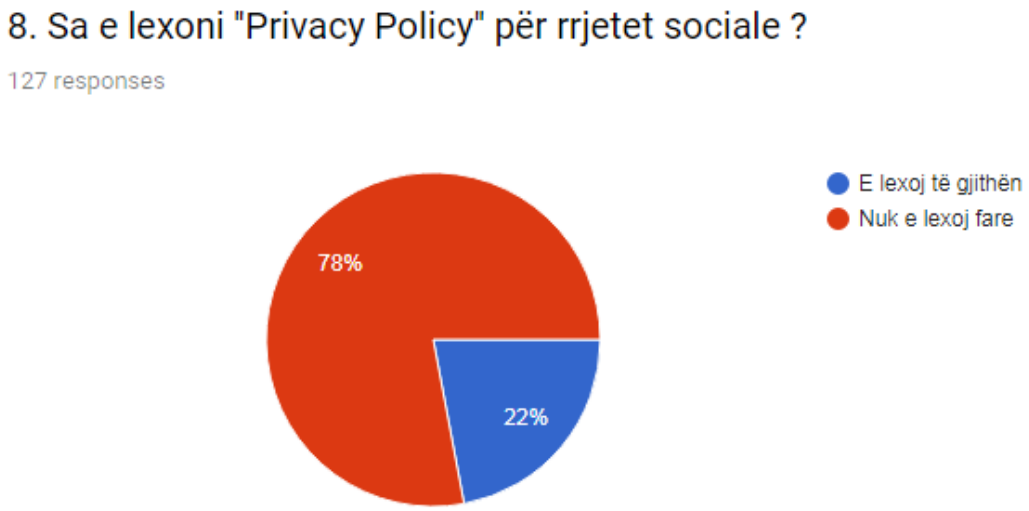

Figure 15:‘’Privacy Policy’’

Kjo figurë tregon se nga shumica e personave nuk lexohet ‘’Privacy Policy’’ aspak.

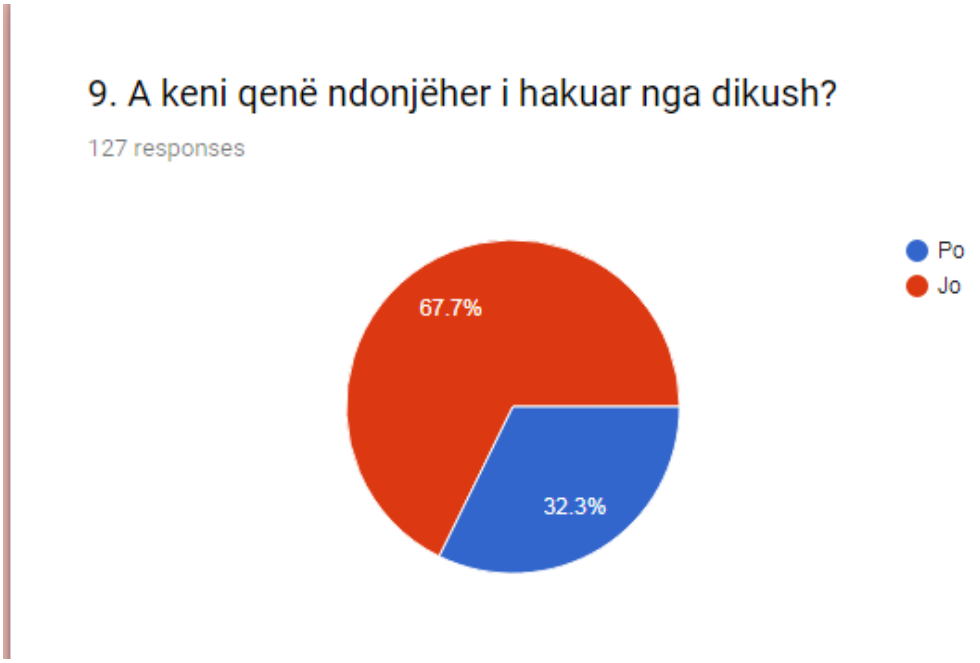

Figure 16: Hakimi

Kjo figurë tregon që 67.7% nuk janë hakuar asnjëherë ndërsa 32.3% janë hakuar.

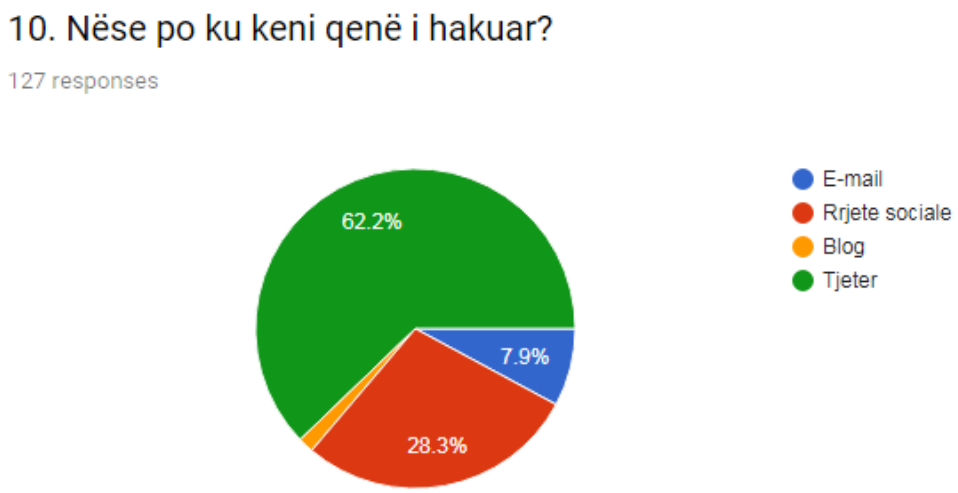

Figure 17:Hakimi në vende te ndryshme

Kjo figurë tregon se përqindja e personave të hakuar në hakuar në rrjete sociale është më e madhe (28.3%) se sa përqindja e njerëzve të hakuar në e-mail (7.9%).

Figure 18:Instalimi i antivirusëve në kompjuter

Në këtë figurë është paraqitur se shumica e njerëzve kanë të instaluar në kompjuterin e tyre antivirusë (63%) ndërsa (37%) nuk kanë të instaluar antivirusë.

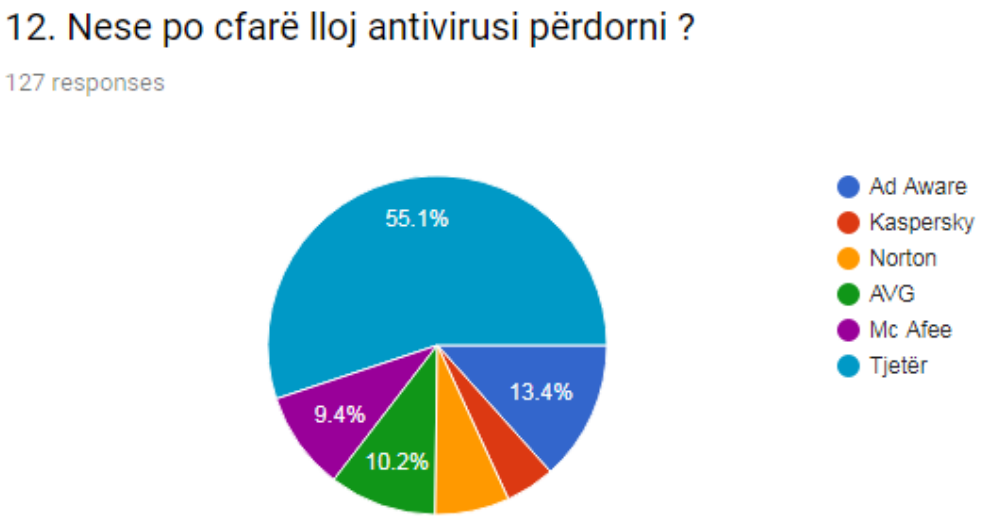

Figure 19:Përdorimi i llojeve të antivirusëve

Kjo figurë tregon se në përgjithësi përdoren antivirusë të ndryshëm (Ad Aware 13.4%), AVG përdoret (10.2%) Mc Afee (9.4%) dhe të tjerë antivirusë me (51.1%).

Figure 20: Siguria për të dhënat e shpërndara në internet

Në këtë figurë tregohet se shumica e personave nuk ndihen të sigurte për të dhënat që i japin në internet (50.4%) ndërsa (29.1%) ndihen të sigurtë.

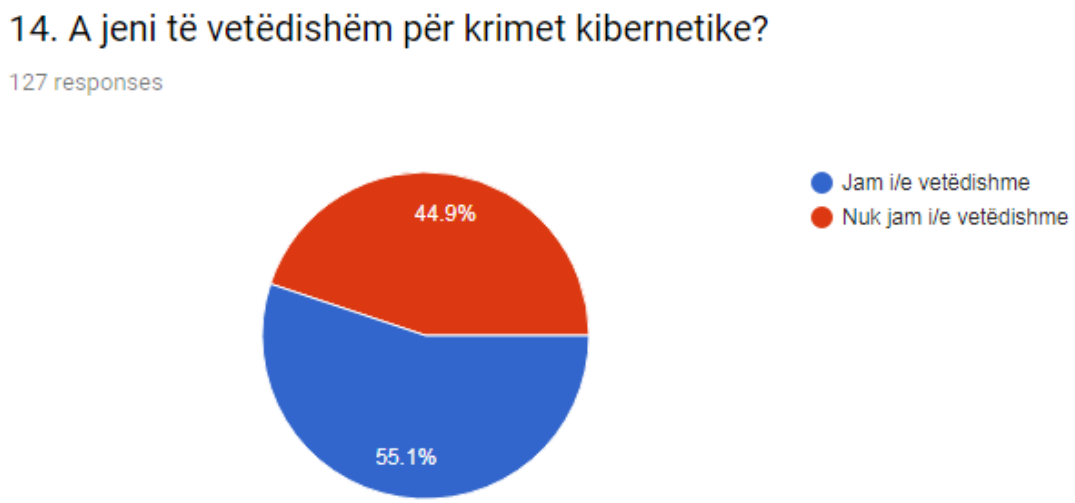

Figure 21:Krimet kibernetike

Kjo figurë tregon se sa janë të vetëdijshëm njerëzit për krimet kibernetike ku 55.1% janë të vetëdijshëm ndërsa pothuajse gjysma tjetër nuk janë të vetëdijshëm me (44.9%).

Figure 22:Viktimet nga krimet kibernetike

Sipas kësaj figure vetëm (7.9%) janë viktimë e krimeve kibernetike ndërsa (92.1) nuk janë viktimë e krimeve kibernetike.

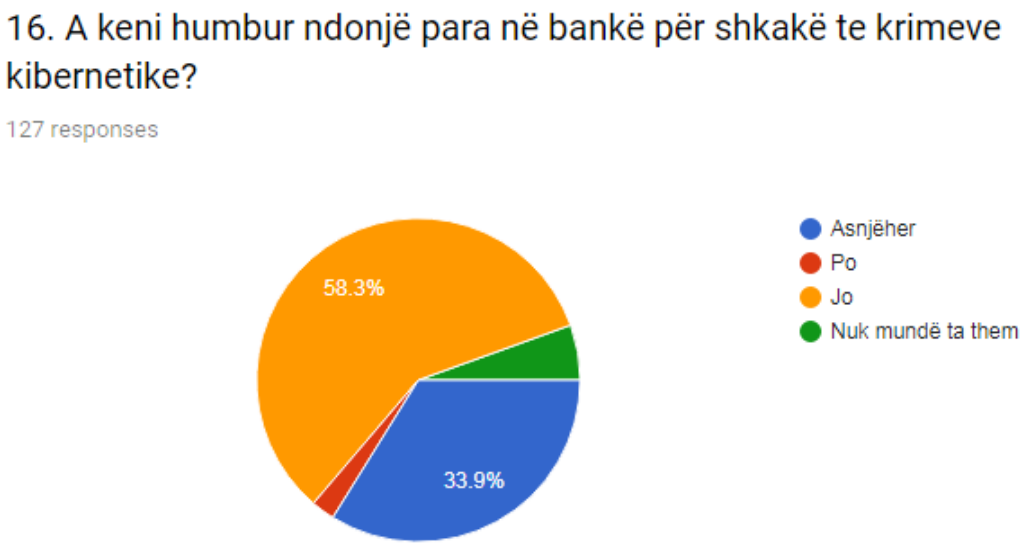

Figure 23:Krimet kibernetike ne banke

Në këtë figurë shihet që personat në përgjithësi nuk kanë humbur para në bankë për shkak të krimeve kibernetike.

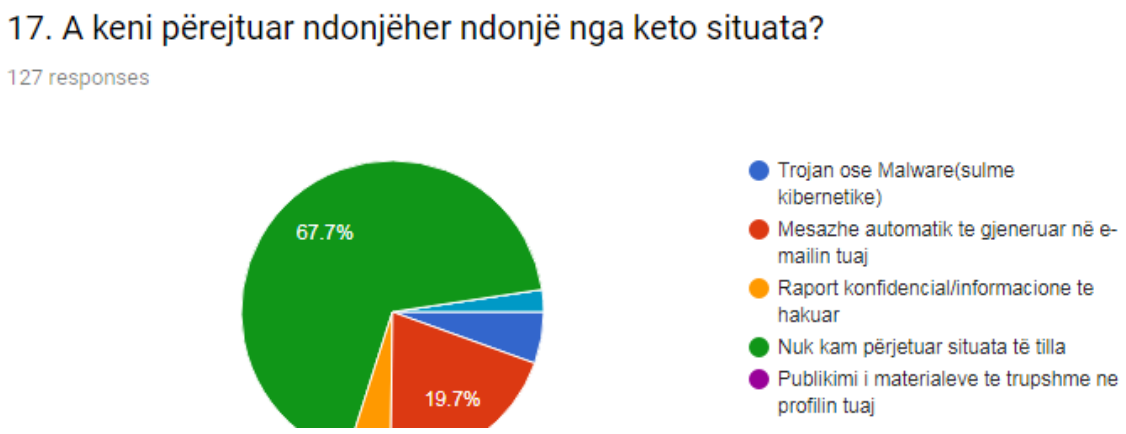

Figure 24:Situata te ndryshme nga krimet kibernetike

Kjo figurë tregon se në përgjithësi personat nuk kanë përjetuar ndonjërën nga situatat e përmendura në pyetsor.

Figure 25:Ndalimi i shopping-ut online per shkake te krimeve kibernetike

Në këtë figurë tregohet se personat nuk bëjnë shumë blerje online ndërsa ata që bëjnë blerje e bëjnë në ndonjë faqe që është e sigurt dhe nuk mund të hakohet.

Figure 26:Mbrojtja nga krimet kibernetike

Kjo figurë tregon se personat që i janë pergjigjur pytësorit mbrohen nga krimet kibernetike deri diku me (63%) ndërsa (29.6%) nuk mbrohen fare kurse (7.1%) mbrohen nga krimet kibernetike.

Figure 27:Ligjet në Kosovë për krimet kibernetike

Në këtë figurë shihet se (55.9%) nuk pajtohen se ligjet në fuqi në Kosove janë në gjendje të mbrojnë nga krimet kibernetike.

6 KONKLUZIONE DHE REKOMANDIME

Në këtë punim diplome janë shpjeguar konceptet dhe rëndësia e sigurisë, si dhe sulmet më të rrezikëshme të kohës moderne te cilat vijnë nga interneti.

Përdoruesit e ueb aplikacioneve shpesh herë nuk janë të vetëdijshëm për veprimet e tyre, dhe me ane të inxhinierisë sociale, sulmuesi mashtron përdoruesin që në mënyrë indirekte ai t'i dorëzojë sulmuesit të gjitha të dhënat personale. Prandaj është e pamundur për t'i ndaluar plotësisht sulmet, mirëpo duhet të paktën të mundohemi t'i minimizojmë ato.

Nga hulumtimi qe kemi bërë ka rezultuar që shumica e njerëzve nuk kujdesen shumë për sigurinë e të dhënave të tyre, japin te dhënat e tyre per çdo gjë që ju kërkohet pa menduar dy herë; përdorin shumë rrjetet sociale pa lexuar ''Privacy Policy '' që është një ligj privatësie që tregon për privatësine, nuk përdorin fjalëkalime të sigurta. Po ashtu nuk dijnë shumë për krimet kibernetike se si te mbrohen nga këto krime kibernetike nuk mbajnë antivirusë në kompjuterët e tyre që sado pak të mbrohen nga krimet kibernetike nuk bëjnë back up të rregulltë dhe shumë të tjera në mënyrë që të mbrohen nga krimet krimet kibernetike dhe mos të jenë viktimë e këtyre krimeve.

Ndërsa te rekomandimet masat për të zbutur këto kërcënime ndryshojnë, por bazat e sigurisë mbeten të njëjta: Mbani sistemet dhe bazat e të dhënave antivirusë të përditësuara, trajnoni punonjësit tuaj, konfiguroni firewall-in tuaj për të bllokuar vetëm portet specifike dhe pritësit që ju nevojiten, mbani fjalëkalimet tuaja të forta, një model me pak privilegj në mjedisin tuaj të IT-së, bëni backup të rregullt dhe kontrolloni vazhdimisht sistemet tuaja të TI-së për veprimtari të dyshimtë.Po ashtu të kujdesen për privatësinë e tyre të shikojnë mirë se çfarë të dhëna po japin në mënyrë që të mos të kenë probleme më vonë, të përdorin fjalëkalime të sigurta ne menyre që të mos vijë deri të hakimi i fjalëkalimit, të lexojnë mirë '' Privacy Policy'' në mënyrë që të dijnë për politikat e çdo rrjeti social. Pasi që me zgjerimin e teknologjisë dhe mundësive që na ofron ajo, rritet edhe përdorimi i internetit, ka shumë gjasa që krimet kompjuterike të zgjerohen edhe më shumë, prandaj duhet t'i luftojmë këto krime duke marrë informata sa më shumë për to, dhe t'i njoftojmë të tjerët që të mbrohen nga këto krime.

7 REFERENCAT

Shahid, H. (2018, agust). *What Is Internet Privacy & Why It Matters so much in 2018?* Gjetur December 14, 2018, nga PureVPN: https://www.purevpn.com/blog/what-is-internet-privacy-scty/

Miyazaki, A., Fernandez, A. (2001) 'Consumer perceptions of privacy and security risks for online shopping', The Journal of Consumer Affairs, Vol. 35 (1), pp. 27-44.

5 Things Hackers Don't Want You to Know. (2018). Retrieved from https://www.inc.com/yolanda-lu/5-things-hackers-dont-want-you-to-know.html

Almeida, V. (2012) "Privacy Problems in the Online World", IEEE Internet Computing, Vol. 16 (2), pp. 4-6.

Checkmarx. (2018). *The Importance of Database Security and Integrity*. [online] Available at: https://www.checkmarx.com/2016/06/24/20160624the-importance-of-database-security-and-integrity/ [Accessed 18 Dec. 2018].

Harris Interactive, 2002. First major post-9-11 privacy survey finds consumers demanding companies do more to protect privacy; public wants company privacy policies to be independently verified.

How-To Geek. (2018). *What Is a VPN, and Why Would I Need One?*. [online] Available at: https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/ [Accessed 19 Dec. 2018].

IT Governance Ltd 2014. What is Cyber Security? Referenced October 13, 2014 http://www.itgovernance.co.uk/what-is-cybersecurity.aspx

Kleve, P., De Mulder, R. (2008). 'Privacy protection and the right to information: In search of a new balance', Computer Law & Security Review, Vol. 24 (3), pp. 223- 232

Limnéll Jarno & Majewski Klaus & Salminen Mirva 2014. Kyberturvallisuus. Jyväskylä: Docendo Oy

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). 'Affect, cognition and reward: Predictors of privacy protection online', Computers in Human Behavior, Vol, 28(3), pp. 1019-1027

White, G., Shah, J., Cook, J. and Mendez, F. (2008) 'Relationship between Information

Privacy Concerns and Computer Self-Efficacy', International Journal of Technology and Human Interaction, vol.4 (2), pp. 52-62, 64-68, 70-82.

(2018). Retrieved from http://www.amdp-rks.org/repository/docs/ligji-172-alb.pdf

11 Ways to Protect Yourself from Cyber Attacks - Nexus. (2018). Retrieved from https://nexusconsultancy.co.uk/blog/11-ways-to-protect-yourself-from-cyber-attacks/

29 Profound Internet Privacy Statistics - BrandonGaille.com. (2019). Retrieved from https://brandongaille.com/28-profound-internet-privacy-statistics/

4 Steps You Should Take If You Have Been Hacked. (2018). Retrieved from https://blog.netwrix.com/2017/09/20/4-steps-you-should-take-if-you-have-been-hacked/

Anton. A.i. & Earp. J.b. (2010). How internet users' privacy concerns have evolved since 2002

Assets.mozilla.net. (2018). [online] Available at: https://assets.mozilla.net/pdf/IHPbriefs_Online_Privacy_March_2017.pdf [Accessed 14 Dec. 2018].

Bambauer, D., E. (2013), "Privacy versus Security", Arizona Legal Studies, Discussion Paper No. 13-06.

Blog.netwrix.com. (2018). *Top 10 Most Common Types of Cyber Attacks*. [online] Available at: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ [Accessed 20 Dec. 2018].

Harper, E. (2018). *9 Simple Ways to Protect Your Privacy*. [online] Techlicious.com. Available at: https://www.techlicious.com/tip/simple-ways-to-protect-your-privacy/ [Accessed 19 Dec. 2018].

Itgovernance.co.uk. (2018). *What is Cyber Security? | IT Governance UK*. [online] Available at: https://www.itgovernance.co.uk/what-is-cybersecurity [Accessed 17 Dec. 2018].

Kleve, P., De Mulder, R. (2008). 'Privacy protection and the right to information: In search of a new balance', Computer Law & Security Review, Vol. 24 (3), pp. 223- 232.

Matis, B. (2018, August 01). 5 Ways to Protect Yourself from Cyber Attacks. Retrieved from https://frsecure.com/blog/5-ways-to-protect-yourself-from-cyber-attacks/

Rainie, L. (2018). *How Americans feel about social media and privacy*. [online] Pew Research Center. Available at: http://www.pewresearch.org/fact-

tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/ [Accessed 15 Dec. 2018].

Rombel, A. (2001) 'Privacy and security in a wired world', Global Finance, Vol. 15 (1), pp. 26-27.

Shahid, H. and Shahid, H. (2018). *What Is Internet Privacy & Why It Matters so much in 2018?*. [online] PureVPN Blog. Available at: https://www.purevpn.com/blog/what-is-internet-privacy-scty/ [Accessed 13 Dec. 2018].

Young, A. & Quan-Hasse. A. (2013). Privacy Protection Strategy On Facebook. *Information, Communication & Society*.

Young - IEEE Security & Privacy Magazine.

8 SHTOJCAT

1.Prej sa vite jeni duke e përdorur internetin?

- Tani
- 5 vjet
- 7 vjet
- Më shumë se 10 vjet

2.Ku keni dëgjuar për sigurinë e informacionit?

- Shkolla, universitete
- Libra, Revista
- Trajnime të ndryshme
- Të tjera
- Nuk kam dëgjuar asnjëherë

3.Në përgjithësi sa jeni të shqetësuar për sigurinë e informacionit?

- Aspak i shqetësuar
- Pak i shqetësuar
- Disi i shqetësuar
- Shumë i shqetësuar
- E di që duhet të shqetësohem por nuk jam

4.A kujdeseni për privatësinë tuaj në rast që kërkohen të dhënat tuaja personale?

- Po kujdesem
- Nuk kujdesem aspak
- Kujdesem pak

5. Sa i përdorni rrjetet sociale?

- Shumë
- Pak
- Aspak

6.Cilin nga rrjetet sociale e përdorni më shumë?

- Facebook
- Instagram
- Snapchat
- Twitter
- Viber
- Whatsapp
- Tjetër

7. A mendoni që këto rrjete sociale e ruajnë privatësinë tuaj?

- Po
- Jo
- Nuk e di

8. Sa e lexoni ‘’Privacy Policy’’ për rrjetet sociale?

- E lexoj të gjithën
- Nuk e lexoj fare

9. A keni qenë ndonjëherë i hakuar nga dikush?

- Po
- Jo

10. Nëse po, ku keni qenë i hakuar?

- E-mail
- Rrjete sociale
- Blog
- Tjetër

11. A keni ndonjë antivirus të instaluar në kompjuterin tuaj?

- Po
- Jo

12.Nëse po çfarë lloj antivirusi përdorni?

- Ad Aware
- Kaspersky
- Norton
- AVG
- Mc Afee
- Tjetër

13. Në përgjithësi sa ndiheni i/e sigurtë për të dhënat tuaja që i shpërndani në internet?

- Shumë i/e sigurt
- I/e sigurt
- Jo i/e sigurt
- Nuk e di

14. A jeni të vetëdijshëm për krimet kibernetike?

- Jam i/e vetëdijshëm
- Nuk jam i/e vetëdijshëm

15.A keni qenë viktimë e krimeve kibernetike?

- Po
- Jo

16. A keni humbur para në bankë për shkak të krimeve kibernetike?

- Po
- Jo
- Nuk mund ta them

17. A keni përjetuar ndonjëherë ndonjë nga këto situata?

- Trojan ose Malware (sulme kibernetike)
- Mesazh automatik të gjeneruar në e-mailin tuaj
- Raport konfidencial/informacione të hakuar

- Nuk kam përjetuar situata të tilla
- Publikimi i materialeve të turpëshme në profilin tuaj

18.A keni ndaluar shopping–un online për shkak të këtyre cështjeve ?

- Deri në një mase
- Ndalje plotësisht
- E bëjë atë vetëm në një faqe interneti të besuar shumë
- E përdori shoping online shpesh
- Nuk e përdori

19. A mundoheni të mbroheni nga krimet kibernetike ?

- Mbrohem shumë
- Deri diku
- Nuk mbrohem fare

20. A mendoni se ligjet në fuqi në Kosovë janë në gjendje të ju mbrojnë nga krimet kibernetike?

- Pajtohem shumë
- Pajtohem
- Nuk pajtohem
- Neutral