ASDO
ALBANIA SUSTAINABLE DEVELOPMENT ORGANIZATION

CYBER SECURITY & DATA PROTECTION

# VLERËSIMI I NIVELIT TË NDËRGJEGJËSIMIT PËR SIGURINË E INFORMACIONIT, MBROJTJEN E TË DHËNAVE DHE SIGURINË KIBERNETIKE NË SHQIPËRI

Supported by:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

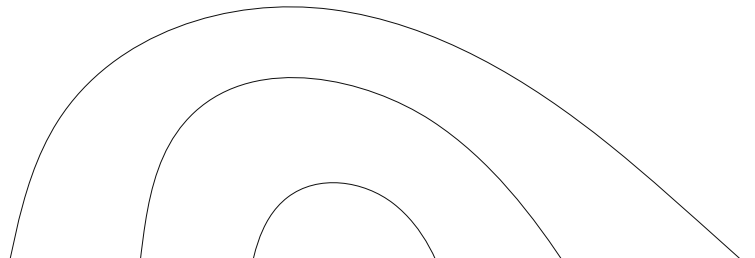
**Ambasada e Zvicrës në Shqipëri**

# 01

## HYRJE

Studimi "Vlerësimi i nivelit të ndërgjegjësimit për sigurinë e informacionit, mbrojtjen e të dhënave dhe sigurinë kibernetike në Shqipëri" është realizuar në kuadër të projektit "Cyber Security and Personal Data Protection in Albania" i drejtuar nga Albania Sustainable Development Organization (A.S.D.O) në bashkëpunim me Komisionerin për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, Fakultetin e Shkencave të Natyrës dhe me mbështetjen bujare të Ambasadës Zviceriane në Shqipëri.

Qëllimi i këtij studimi është të analizojë të dhënat e mbledhura mbi ndërgjegjësimin dhe mbrojtjen kibernetike në organizatat dhe kompanitë në Shqipëri si dhe të identifikojë nevojat dhe fushat në të cilat duhen rritur informacioni, trainimet dhe mjetet për të fuqizuar mbrojtjen kibernetike.



02

# METODOLOGJIA

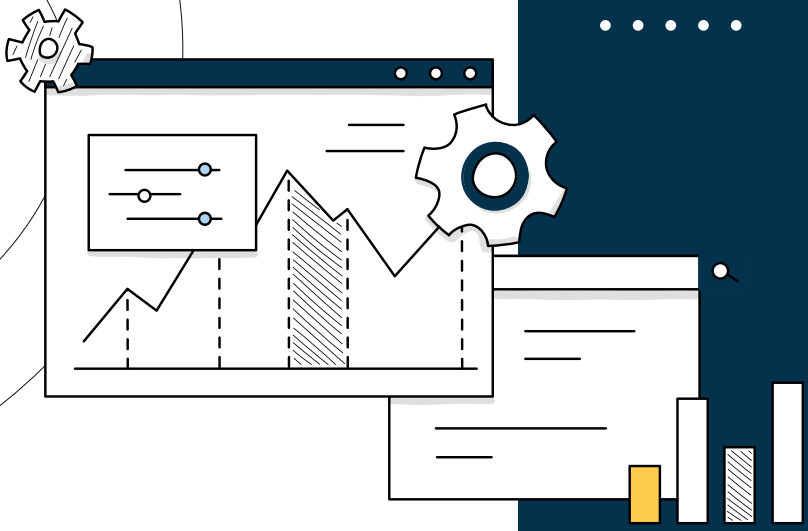
Në këtë studim u  përdor një kombinim i metodave kualitative dhe kuantitative.

Përdorimi i Pyetësorit: Në fillim të studimit u krijua një pyetësor me qëllim mbledhjen e informacionit rreth kërcënimeve kibernetike, strategjive të mbrojtjes, dhe ndërgjegjësimit në lidhje me këto çështje. Pyetësori u realizua me 165 kompani të sektorëve të ndryshëm, duke përfshirë sektorët kyç të shërbimeve që procesojnë të dhëna personale dhe janë të rrezikuara nga sulmet kibernetike. Pyetesorët janë plotësuar përmes bisedave të drejtpërdrejta (face-to-face) me përfaqësuesit e kompanive ose organizatave. Disa prej pyetesoreve janë plotësuar online.
Strukturimi i Pyetësorit: Pyetësori është strukturuar në 18 seksione, secili me tema specifike të sigurisë kibernetike dhe ndërgjegjësimit. Ky strukturim është bërë për të lejuar një analizë të hollësishme të çështjeve të ndryshme të sigurisë kibernetike.

Përdorimi i Intervistave: Përfaqësues të studimit kanë bërë intervista me përfaqësuesit e kompanive për të siguruar që pyetësorët të plotësohen në mënyrë korrekte dhe për të siguruar që të dhënat të interpretohen saktë.
Kombinimi i Përgjigjeve Onsite dhe Online: Disa prej pyetësoreve janë plotësuar me intervistat e drejtpërdrejta (onsite), ndërsa disa të tjera janë plotësuar në mënyrë online. Kjo ka mundësuar një shtrirje të gjerë të studimit dhe përfshirjen e një spektri të madh të kompanive.

Analiza e të Dhënave: Pas mbledhjes së të dhënave, është bërë një analizë e thellë e të dhënave për të identifikuar trendet, nevojat dhe fushat ku duhet rritur ndërgjegjësimi dhe mjetet për mbrojtjen kibernetike.

Kjo metodologji është përdorur për të siguruar një pamje të qartë të sigurisë kibernetike në organizatat dhe kompanitë në studim dhe për të identifikuar sfidat dhe mundësitë në këtë fushë. Kombinimi i pyetësorëve dhe intervistave ka ndihmuar në krijimin e një analize të pasur dhe të saktë të situatës aktuale të sigurisë kibernetike.



# 03

## GJETJET

Organizimi i pyetësorit u bë në disa seksione të cilat na japin informacion mbi nivelin e ndërgjegjësimit mbi sigurinë e informacionit, mbrojtjes së të dhënave dhe sigurisë kibernetike në organizatat dhe kompanitë në Shqipëri.

## SEKSIONI "PASQYRA E PËRGJITHSHME E BIZNESIT"

Seksioni "Pasqyra e përgjithshme e Biznesit" ka si qëllim të japë një panoramë të përgjithshme mbi kontekstin dhe nevojat e organizatave apo kompanive që morën pjesë në studim. Sektori i biznesit është një kontekst i rëndësishëm për sigurinë e informacionit. Njohja e sektorit, madhësisë, natyrës së aktiviteteve dhe strukturës së organizatës ndihmon në identifikimin e rreziqeve specifike të sigurisë dhe nevojave të mbrojtjes së të dhënave. Një analizë e përgjigjeve të marra në këtë seksion jepet në aneksin e studimit.

## SEKSIONI "NATYRA E INFRASTRUKTURËS TË TEKNOLOGJISË SË INFORMACIONIT PRANË ORGANIZATËS/KOMPANISË TUAJ"

Infrastruktura e teknologjisë së informacionit konsiston në komponente që janë të nevojshme për operimin  dhe menaxhimin e ambientit të teknologjisë së informacionit të një kompanie biznesi të cilat shërbejnë për të mbështetur dhe shpërndarë procese të sistemeve informatike si: harduerë, softuerë, sisteme operimi, rrjete dhe magazinimin e të dhënave.

Në kohën e sotme, biznesi po mbështetet gjithmonë e më tepër tek teknologjia dhe tek të dhënat për të ndërmarrë vendime kritike biznesi. Mbrojtja e burimeve që bëjmë të mundur realizimin e këtyre aktiviteteve është mjaft e rëndësishme.

Nëse infrastruktura e teknologjisë së informacionit është fleksibël, e besueshme dhe e sigurt, ajo mund të ndihmojë një kompani të realizojë qëllimet e saj dhe të jetë konkurruese në treg duke u bërë një faktor i rëndësishëm që kompania të jetë e suksesshme ose jo.

Për këtë arsye pyetësori ka një seksion të veçantë që lidhet me njohjen e infrastrukturës së teknologjisë së informacionit që përdorin organizatat apo kompanitë në Shqipëri si: harduerи, llojet e aplikacioneve që përdorin, portalet e avancuara të tregtisë elektronike, shkëmbimin e të dhënave etj.

Ndër pyetjet e këtij seksioni janë edhe pyetjet **"A përdorin punonjësit nga telefoni sisteme informacioni të kompanisë?" dhe "A përdoret emaili i kompanisë si ID digjitale  (emërpërdoruesi) për t'u autentifikuar apo regjistruar në platforma, rrjete sociale?"**

Pothuajse **48% e** kompanive janë përgjur "**po" pyetjes** "A përdorin punonjësit nga telefoni sisteme informacioni të kompanisë?" Përdorimi i sistemeve të informacionit të kompanisë nga telefoni personal i punonjësve të saj, mund të ketë ndikim të rëndësishëm në aspekte të ndryshme të sigurisë kibernetike dhe menaxhimit të riskut për kete kompani. Si p.sh:

**Rreziqet e Sigurisë Kibernetike**: Përdorimi i pajisjeve personale, si telefoni celular, për të aksesuar sistemet e kompanisë mund të rrisë rreziqet e shkeljeve të sigurisë kibernetike. Pajisjet personale mund të jenë më të ndjeshme ndaj sulmeve të hakerave dhe viruseve.

**Mbrojtja e të Dhënave të Kompanisë**: Përdorimi i pajisjeve personale mund të rezultojë në rrezikun e humbjes së të dhënave të kompanisë nëse pajisjet humbasin ose vidhen. Siguria e të dhënave dhe informacionit të kompanisë është një prioritet kritik.

**Ndërgjegjësimi**: Nëse punonjësit janë të informuar dhe të ndërgjegjshëm për rreziqet kibernetike që lidhen me përdorimin e telefonave për qasje në sistemet e kompanisë, ata mund të jenë në gjendje më të mirë për të zbatuar praktika të sigurisë kibernetike dhe të ndihmojnë në zvogëlimin e rreziqeve.

**Politikat dhe Rregulloret**: Kompania duhet të ketë politika të qarta dhe rregullore të përcaktuara për përdorimin e pajisjeve personale për qasje në sistemet e saj. Kjo përfshin rregulla për aksesin, autentifikimin, enkriptimin dhe menaxhimin e pajisjeve personale.

**Trajnime dhe Edukim**: Nëse punonjësit përdorin telefonat për qasje në sistemet e kompanisë, është e rëndësishme që ata të trajnohen rregullisht rreth sigurisë kibernetike dhe praktikave të duhura. Trajnimi duhet të adresojë rreziqet potenciale dhe t'i informojë për mënyrën e duhur të përdorimit të pajisjeve personale në kontekstin e sigurisë kibernetike.

**Menaxhimi i Përdorimit të Pajisjeve Personale**: Kompania mund të ketë nevojë të vendosë politika që rregullojnë aksesin dhe përdorimin e pajisjeve personale. Kjo përfshin rregulla për aplikacionet e instaluar, aksesin në rrjet, përdorimin e email-ave, dhe shfrytëzimin e aplikimeve të tjera.

Për të përmirësuar mbrojtjen kibernetike, këto kompani duhet zhvillojnë strategji të përshtatshme të sigurisë kibernetike, të investojë në trajnime për punonjësit dhe të përdorin teknologji të avancuara për të minimizuar rreziqet e mundshme të shkeljeve të sigurisë.

Nga përgjigjet vihet re se **39 %** e kompanive i janë përgjigjur po pyetjes "**A përdoret emaili i kompanisë si ID digjitale (emërpërdoruesi) për t'u autentifikuar apo regjistruar në platforma, rrjete sociale?"**

Nëse kompania lejon punonjësit të përdorin adresën e emailit të saj si ID digjitale për autentifikim ose regjistrim në platforma të ndryshme dhe rrjete sociale, është e rëndësishme që kompania të hartojë një politikë të qartë dhe gjithëpërfshirëse për ta bërë këtë proces sa më të sigurt dhe të përgjegjshëm që të jetë e mundur. Në përgjithësi, është e rëndësishme që politika të jetë fleksibël dhe e përshtatshme me zhvillimet e sigurisë kibernetike dhe praktikat e mira në industrinë e IT. Është mirë që kompania të bëjë një vlerësim dhe të vendosë nëse politika e përdorimit të adresës së emailit të kompanisë është e përshtatshme, ose nëse është më mirë të ndryshohet për të adresuar rreziqet dhe nevojat e kompanisë në mënyrë më të mirë.

Në aneksin e studimit jepen informacione shtesë në lidhje me përgjigjet e marra në këtë seksion.

## SEKSIONI “POLITIKAT E SIGURISË”

Një seksion tjetër i pyetësorit është seksioni “Politikat e Sigurisë” i cili ka si qëllim të vlerësojë se sa efektive janë politikat dhe procedurat e sigurisë në organizatë dhe të identifikojë nevojat për përmirësim. Një politikë e mirë e sigurisë së informacionit dhe një staf i informuar dhe i trajnuar ndihmojnë një organizatë ose kompani të jetë më e përgatitur dhe të mbrojë të dhënat e saj nga kërcënimet e mundshme. Nëse organizata ose kompania ka një politikë të hartuar për sigurinë e informacionit, kjo tregon se ajo ka një qëndrim të përgjegjshëm ndaj sigurisë dhe ka ndërmarrë hapa për të garantuar integritetin, konfidencialitetin dhe disponueshmërinë e të dhënave. Kjo politikë mund të përcaktojë rolet dhe përgjegjësitë e ndryshme për sigurinë e informacionit. Duke dhënë edukimin dhe trajnimin e duhur për stafin mbi sigurinë e informacionit dhe duke i informuar ata për politikën dhe praktikat e pranueshme, organizata ose kompania ndihmon në rritjen e ndërgjegjësimit të stafit për këtë çështje të rëndësishme. Përgjegjësia për të garantuar sigurinë e informacionit dhe mbrojtjen e të dhënave është e rëndësishme për të parandaluar incidente të sigurisë dhe sulmet kibernetike. Një politikë e mirë e sigurisë së informacionit dhe një staf i informuar dhe i trajnuar ndihmojnë organizatën ose kompaninë të jetë më e përgatitur dhe të mbrojë të dhënat e saj nga kërcënimet e mundshme.

**Ndër pyetjet që përfshihen në këtë seksion janë:**

**1.** Rolet dhe përgjegjësitë për sigurinë e informacionit në organizatën/kompaninë tuaj janë të përcaktuara mirë, p.sh. dikush është përgjegjës për ruajtjen e të dhënave (back-upet), regjistrimin e përdoruesve në sistem, planifikimin kundër një ngjarje katastrofe, sigurimin e ndërlidhjes me ofruesit e shërbimeve.

Një pjesë e kompanive i është përgjigjur **"Jo nuk eshte e nevojshme"** kësaj pyetjeje. Për këto kompani, te cilat nuk e shohin të nevojshme përcaktimin e roleve dhe përgjegjësive për sigurinë e informacionit, mund të paraqiten sfida në sigurinë e tyre kibernetike. Është i nevojshëm ndërgjegjësimi i këtyre kompanive se:

Kërcënimet janë reale: asnjë kompani nuk është e paprekshme nga kërcënimi kibernetik, dhe përdorimi i roleve dhe përgjegjësive të përcaktuara mund të ndihmojë në parandalimin e këtyre incidenteve.

Ndryshimet janë të vazhdueshme: Teknologjia dhe taktikat e sulmeve kibernetike zhvillohen shpejt. Një strategji statike nuk është e mjaftueshme, dhe është e nevojshme të përditësohen rregullisht politikat dhe praktikat e sigurisë.

Rregulloret dhe standardet e industrisë: shumë industri kanë standarde dhe rregullore për sigurinë e informacionit që kërkohen për tu përputhur me legjislacionin dhe për të fituar besim të klientëve dhe partnerëve. Përfshirja në këto standarde mund të ndihmojë në rritjen e përformancës së kompanisë dhe në zbulimin e mënyrave për përmirësim.

**2.** Organizata/kompania juaj ka politika të hartuara për sigurinë e informacionit.

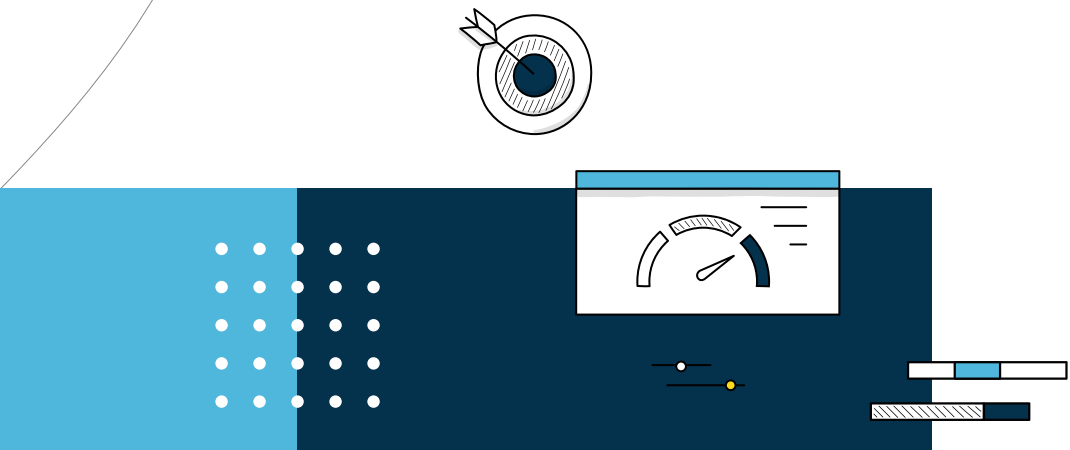
Vihet re se **9.1%** e kompanive janë përgjigjur se nuk është e nevojshme që organizata apo kompania të ketë politika të hartuara për sigurinë e informacionit. Është e rëndësishme që këto kompani të ndërgjegjësohen se vendosja e politikave të sigurisë kibernetike dhe mbrojtjes së të dhënave personale është një hap i rëndësishëm për të siguruar që kompania të jetë e përgatitur dhe e mbrojtur në një mjedis kibernetik gjithnjë e më kompleks dhe të rrezikshëm. Për këto kompani dhe kompanitë që janë përgjigjur **"Jo, por do t'i përcaktojmë në të ardhmen" dhe "Po, ka iniciativa por jo të formalizuara",** të cilat në përqindje janë respektivisht **13.9%** dhe **18.2%,** është shume e rëndësishme të zhvillohen fushata ndërgjegjësuese dhe trajnime për komponentët që përbëjnë një plan të sigurisë së informacionit cilësor, si dhe për hapat që duhet të ndiqen për të zbatuar atë me një përpikmëri maksimale.

**3.** Nëse keni një politikë për sigurinë e informacionit, stafi është në dijeni të saj?

Në këtë pyetje, **8.8%** e kompanive është përgjigjur **"Jo nuk është e nevojshme"** dhe **20.8%** është përgjigjur "Jo, vetëm një pjesë e stafit". Duke qënë se siguria e informacionit është një aspekt shumë i rëndësishëm për secilën kompani, të kesh të gjithë stafin në dijeni të politikës për sigurinë e informacionit sjell përfitime për kompaninë si p.sh: Ndërgjegjësim mbi Rreziqet dhe Rregullat; Mbrojtje e Të Dhënave Personale; Përgjegjësi Kolektive; Parandalimi i Incidenteve të Sigurisë; Përmirësimi i Kulturës së Sigurisë; Rritje e Nivelit të Përgjegjësisë; Zhvillimi Personal dhe Profesional; Respektimi i Ligjeve dhe Rregulloreve. Për të arritur këto përfitime, është e rëndësishme që kompania të ketë një strategji për komunikimin dhe edukimin e stafit në lidhje me politikën e sigurisë së informacionit. Kjo mund të përfshijë trajnime periodike, mbledhje informuese, dhe materiale të ndryshme edukative.

**4.** Të gjithë stafit i jepet edukimi dhe trajnimi i duhur dhe i përshtatshëm për sigurinë e informacionit.

Rreth **17%** e kompanive janë përgjigjur që stafi nuk trajnohet dhe **8.5%** e kompanive që nuk është i nevojshëm trajnimi. Edukimi dhe trajnimi i të gjithë stafit për sigurinë e informacionit ka efekte pozitive të shumta për kompaninë, siç janë mbrojtja e të dhënave, minimizimi i rreziqeve, ruajtja e besimit të klientëve, dhe përmirësimi i kulturës së sigurisë. Ndaj është shumë e rëndësishme të zhvillohen fushata ndërgjegjësuese për kompanitë të cilat nuk e trajnojnë stafin mbi sigurinë e informacionit.
Një analizë më e detajuar e përgjigjeve të marra në këtë seksion dhe lidhja midis variablave në seksion dhe nivelit të ndërgjegjësimit për seksionin



## SEKSIONI “SIGURIA ORGANIZATIVE”

Duke qënë se siguria organizative është një aspekt i rëndësishëm i sigurisë së informacionit dhe mbrojtjes së të dhënave në organizata dhe kompani në pyetësor është përfshirë një seksion në lidhje me sigurinë organizative. Nëse një anëtar i stafit ka përgjegjësi për sigurinë e informacionit, atëherë ky person është i detyruar të monitorojë dhe të sigurojë që politikat dhe procedurat e krijuara për sigurinë të zbatohen në mënyrë efikase. Ekspertiza për sigurinë e informacionit është gjithashtu një element kryesor. Nëse një organizatë ka profesionistë të trajnuar dhe të aftë për të vlerësuar dhe zbatuar masat e sigurisë, kjo ndikon në nivelin e ndërgjegjësimit dhe në aftësinë e organizatës për të përballuar rreziqet dhe kërcënimet e mundshme kibernetike. Masa e kontrollit të aksesit nga palët e treta në sistemet e informacionit është një tjetër aspekt i rëndësishëm i sigurisë organizative. Përdorimi i politikave dhe procedurave të sigurisë për kontratat me palët e treta siguron që aksesi në informacionin e kompanisë të jetë i limituar dhe i kontrolluar në mënyrë të rregullt.  Në këtë kontekst, ndërgjegjësimi i stafit dhe vlerësimi rregullisht i masave të marra për sigurinë e informacionit dhe mbrojtjen e të dhënave janë të lidhura ngushtë dhe përbëjnë një pjesë të rëndësishme të ndërhyrjes për të përmbushur standardet e sigurisë dhe kufizuar rreziqet potenciale.

Ndër pyetjet që përfshihen në këtë seksion janë.

**1.** Një anëtar i stafit tuaj ka përgjegjësi për sigurinë e informacionit.

Nga përgjigjet vihet re se **23.6%** e kompanive nuk ka një anëtar të stafit përgjegjës për sigurinë e informacionit. Të kesh një anëtar të stafit me përgjegjësi për sigurinë e informacionit është e domosdoshme. Kjo është një nga gjërat bazë për të garantuar që kompania të ketë një qasje të koordinuar dhe efektive ndaj sfidave të sigurisë kibernetike. Ky anëtar i stafit duhet të ketë për detyrë të udhëheqë dhe të implementojë politikat dhe praktikat e sigurisë së informacionit në të gjitha nivelet e organizatës. Ky person duhet të jetë përgjegjës  për të identifikuar rreziqet potenciale të sigurisë, të hartojë planin e sigurisë së informacionit, të monitorojë incidentet e mundshme të sigurisë, dhe të koordinojë trajnimet për stafin për të promovuar ndërgjegjësimin dhe shtuar njohuritë e tyre në lidhje me sigurinë kibernetike. Përmes përfshirjes aktive dhe mbikëqyrjes së masave të sigurisë, ky anëtar i stafit mund të ndihmojë në parandalimin e shkeljeve të sigurisë dhe në zvogëlimin e ndikimit të incidenteve.

Në një ambjent ku sulmet kibernetike janë shtuar dhe ka ndërlikime të mëdha të mjeteve teknologjike, një anëtar i stafit me përgjegjësi për sigurinë e informacionit përfaqëson një investim të vlefshëm që ndihmon kompaninë të rrisë nivelin e përgatitjes dhe aftësive të veta në këtë fushë të ndjeshme. Ai ndihmon në mbrojtjen e të dhënave të kompanisë, privatësisë së klientëve, dhe reputacionit të saj. Gjithashtu, ai përcjell një mesazh të përkushtimit ndaj sigurisë dhe integritetit të informacionit në të gjitha aspektet e funksionimit të organizatës.

**2.** Ekspertiza për sigurinë e informacionit garantohet brenda organizatës/kompanisë, ose kërkohet këshillim nga jashtë.

Në këtë pyetje **17.6%** e kompanive janë përgjigjur se ekspertiza nuk është e nevojshme. Për një kompani ekspertiza për sigurinë e informacionit ka rëndësi të jashtëzakonshme. Ky element ka ndikim të thellë në mënyrën se si një kompani mund të adresojë sfidat e sigurisë kibernetike dhe të përgatitet për të mbrojtur të dhënat dhe mjetet e saj nga rreziqet e mundshme. Ndaj është shumë e rëndësishme  të zhvillohen fushata ndërgjegjësuese për kompanitë të cilat nuk garantojnë ekspertizë te brendshme apo të jashtme për sigurinë kibernetike.

**3.** Aksesi nga palët e treta (të jashtme) në sistemet tuaja të informacionit kërkon miratimin nga një menaxher i lartë.

Nga përgjigjet vihet re se **12.1%** e kompanive shprehen që nuk është i nevojshëm miratimi nga një menaxher i lartë per akses nga palët e treta (të jashtme) në sistemet e informacionit te kompanise. Miratimi nga një menaxher i lartë për aksesin nga palet e treta në sistemet e informacionit të kompanisë kontribuon në ndërtimin e kulturës së sigurisë dhe në forcimin e mbrojtjes kibernetike në kompani.

**4.** Ekziston një politikë, procedurë sigurie që ndiqet për kontratat me palët e treta.

Vihet re se **9.1%** e kompanive jane përgjigjur që nuk është e nevojshme një politikë, procedurë sigurie për kontratat me palët e treta dhe **12.1%** e kompanive jane përgjigjur se nuk ekziston një politikë, procedurë sigurie për kontratat me palët e treta. Mungesa e një politike apo procedure të strukturuar për kontratat me palët e treta hap dyert për sfidat e mundshme dhe rreziqet në lidhje me të dhënat dhe mjetet e kompanisë që përdoren nga partnerët e tretë. Pa një udhëzim të strukturuar për trajtimin dhe mbikëqyrjen e kontratave me palët e treta, kompanitë rrezikojnë të ekspozohen ndaj shkeljeve të sigurisë, ndërhyrjeve të papërshtatshme dhe humbjes së integritetit të të dhënave. Në fushën e zhvillimit të marrëdhënieve me partnerët e tretë, një politikë e rregulluar e sigurisë, siguron një bazë të fortë për përzgjedhjen, monitorimin dhe vlerësimin e partnerëve potencialë. Kjo jo vetëm që do të ndihmonte në minimizimin e rreziqeve, por gjithashtu do të rriste ndërgjegjësimin e të gjithë pjesëmarrësve në procesin e kontratave.

Një analizë më e detajuar e përgjigjeve të marra në këtë seksion dhe lidhja midis variablave në seksion dhe nivelit të ndërgjegjësimit për seksionin siguria organizative jepet në aneksin e këtij studimi.

## SEKSIONI KLASIFIKIMI I ASETEVE DHE KONTROLLI

Duke qënë se klasifikimi i aseteve dhe kontrolli është një pjesë e rëndësishme e strategjisë së sigurisë së informacionit dhe mbrojtjes së të dhënave në organizata dhe kompani, në pyetësor u vendos një seksion në lidhje me të. Nëse organizata ose kompania mund të identifikojë, gjurmojë dhe lokalizojë të gjitha asetet e tyre, duke përfshirë softuerin, harduerin, stafin dhe sherbimet e përdorura për trajtimin e informacionit, kjo do të thotë se ata kanë një perceptim të qartë të aseteve të tyre të informacionit dhe mund të përmirësojnë kontrollin dhe sigurinë e tyre. Kontrolli i aksesit në asetet e informacionit, si brenda ashtu edhe në distancë, është një masë e rëndësishme për të parandaluar aksesin e palëve të paautorizuara dhe për të mbrojtur të dhënat e kompanisë. Njohja e stafit për procedurat dhe politikat e ruajtjes, arkivimit të të dhënave dhe shkatërrimit të informacionit është gjithashtu e rëndësishme për të siguruar përdorimin e duhur dhe të sigurt të të dhënave. Krijimi dhe zbatimi i një politike ose procedure për menaxhimin e aseteve dhe kontrollin e konfigurimit të tyre ndihmon në përmirësimin e sigurisë së aseteve të informacionit dhe ndërgjegjësimin e stafit për rëndësinë e mbrojtjes së tyre.

Ndër pyetjet që përfshihen në këtë seksion janë:

**1.** Organizata ose Kompania juaj mund të identifikojë, gjurmojë dhe lokalizojë të gjitha asetet (përfshirë softuerin, harduerin, stafin dhe shërbimet) e përdorura për trajtimin e informacionit.

Nga përgjigjet vihet re se **17.6%** e organizatave/kompanive nuk mund të identifikojnë, gjurmojnë dhe lokalizojnë të gjitha asetet (përfshirë softuerin, harduerin, stafin dhe shërbimet) e përdorura për trajtimin e informacionit. Identifikimi, gjurmimi dhe lokalizimi i të gjitha aseteve të përdorura për trajtimin e informacionit ndihmojnë në përmirësimin e sigurisë kibernetike, reduktimin e rreziqeve dhe ndërgjegjësimin e të gjithëve në organizatë. Kjo nxit krijimin e një mjedisi më të sigurt në fushën e sigurisë kibernetike. Nëse organizatat dhe kompanitë nuk kanë një strategji për të gjurmuar dhe lokalizuar asetet e tyre, përfshirë softuerin, harduerin, stafin dhe shërbimet, ato rrezikojnë të kenë ndërhyrje të papërballueshme, ndërprerje të veprimtarive dhe humbje të të dhënave.

**2.** Organizata ose Kompania juaj kontrollon në mënyrë të përshtatshme aksesin brenda dhe në distancë të aseteve të informacionit.

Nga përgjigjet vihet re se vetëm **42.2%** e kompanive kontrollojnë në mënyrë të përshtatshme aksesin brenda dhe në distancë të aseteve të informacionit. Kontrolli i aksesit të aseteve të informacionit është një masë kritike për të siguruar që organizata të mbrojë të dhënat e saj, të parandalojë shkelje dhe të funksionojë në mënyrë të sigurt dhe efikase në një mjedis ku sulmet kibernetike po bëhen gjithnjë e më te sofistikuara dhe të ndërlikuara. Është shqetësuese që një pjesë e konsiderueshme e kompanive dhe organizatave ka mungesë të një kontrolli të përshtatshëm të aksesit ndaj aseteve të informacionit. Ky boshllëk në kontrollin e aksesit, qoftë brenda strukturave fizike ose nëpërmjet rrjetave të lidhur me internetin, krijon një situatë të rrezikshme për mbrojtjen e të dhënave sensitive dhe për sigurinë kibernetike në përgjithësi. Me një kontroll të dobët të aksesit, mundësia për qasje të paautorizuar në të dhënat dhe burimet e informacionit rritet ndjeshëm. Kjo mund të rezultojë në ndërhyrje të padëshiruara, shkelje të sigurisë dhe përdorim të paautorizuar të të dhënave. Mungesa e kontrollit të aksesit gjithashtu lejon ndërhyrjet e jashtme dhe të brendshme të paligjshme që mund të ndikojnë në integritetin e sistemeve të kompanisë dhe qëndrueshmërinë e operacioneve të saj.

Duke qene se, sulmet kibernetike po bëhen gjithnjë e më te sofistikuara dhe të ndërlikuara, mungesa e një kontrolli të rreptë të aksesit mund të çojë në pasoja serioze për organizatat dhe kompanitë. Duke mos arritur të identifikojnë dhe të parandalojnë shkeljet e mundshme të sigurisë, ato rrezikojnë të përballen me humbje financiare, dëmtim të imazhit dhe ndërprerje të shërbimeve të tyre. Për këtë arsye, për këto kompani, një fokus i rëndësishëm duhet të jetë ndryshimi i situatës aktuale duke vendosur një kontroll të fortë dhe efikas të aksesit ndaj aseteve të informacionit. Kjo do të ndihmonte në përmirësimin e sigurisë kibernetike, minimizimin e rreziqeve dhe ruajtjen e integritetit të të dhënave të organizatave dhe kompanive.

**3.** Stafi juaj e di se çfarë të bëjë referuar ruajtjes, arkivimit të të dhënave (back-upit) dhe shkatërrimit të informacionit.

Vihet re se vetëm **39.4%** e kompanive janë përgjigjur që i gjithe stafi është i informuar se çfarë të bëjë referuar ruajtjes, arkivimit të të dhënave, back-upit dhe shkatërrimit të informacionit. Njohuria e stafit për procedurat e ruajtjes, arkivimit, back-upit dhe shkatërrimit të të dhënave ka një ndikim të drejtpërdrejtë në sigurinë kibernetike, efikasitetin operacional dhe përmbushjen e detyrimeve ligjore. Në një mjedis kibernetik të ndryshuar dhe të kërcënuar, i gjithë stafi në organizatë duhet të jetë i përgatitur për të trajtuar të dhënat në mënyrë të sigurt dhe të përgjegjshme.

**4.** Organizata/Kompania juaj ka krijuar dhe zbaton një politikë/procedurë për menaxhimin e aseteve dhe kontrollin e konfigurimit të tyre.

Politikat dhe procedurat për menaxhimin e aseteve dhe kontrollin e konfigurimit të tyre ndihmojnë në mbrojtjen e të dhënave, minimizimin e rreziqeve dhe përmirësimin e performancës, ndërsa janë të domosdoshme për të përshtatur organizatën me standardet aktuale të sigurisë dhe standardet ligjore. Vihet re se një **11.5%** e kompanive u përgjigjën që nuk ekziston një politikë apo procedurë për menaxhimin e aseteve dhe kontrollin e konfigurimit të tyre dhe **4.8%** e kompanive u përgjigjën se nuk është e nevojshme. Duke qënë se politika dhe procedurat për menaxhimin e aseteve dhe kontrollin e konfigurimit të tyre janë thelbësore për sigurinë, qëndrueshmërinë dhe efikasitetin e një kompanie apo organizate, për këto kompani një fokus i rëndësishëm duhet të jetë ndryshimi i situatës aktuale duke hartuar dhe zbatuar politika dhe procedura për menaxhimin e aseteve dhe kontrollin e konfigurimit tyre.

## SEKSIONI SIGURIA E PERSONELIT

Duke qënë se masat që organizata apo kompania ka ndërmarrë për të përmirësuar sigurinë dhe ndërgjegjësimin e personelit në lidhje me informacionin dhe të dhënat e tyre të punës janë një pjesë e rëndësishme e sigurisë së informacionit dhe mbrojtjes së të dhënave në organizata dhe kompani, në pyetësor u vendos një seksion në lidhje me të. Nëse stafi është i vetëdijshëm për rëndësinë e raportimit të incidenteve të sigurisë, është i trajnuar për të siguruar kompjuterat e tyre në momentet e largimit nga postet e punës, dhe ekziston një proces i formalizuar disiplinor për shkelësit e politikave të sigurisë, kjo tregon se organizata apo kompania i kushton një vëmendje të veçantë sigurisë së personelit dhe informacionit të tyre. Duke siguruar që stafi është i informuar dhe i trajnuar për masat e sigurisë, organizata mund të reduktojë rreziqet potenciale dhe të forcojë ndërgjegjësimin e tyre për ndjekjen e politikave të sigurisë. Përveç kësaj, zbatimi i politikave dhe procedurave për revokimin e drejtës së aksesit në rast të ndryshimeve të personelit ndihmon në mbrojtjen e informacionit nga akseset e paligjshme ose të panevojshme. Këto masa ndihmojnë në përmirësimin e sigurisë së informacionit dhe mbrojtjen e të dhënave në organizata ose kompani.

Ndër pyetjet që përfshihen në këtë seksion janë:

**1.** Stafi është trajnuar për të siguruar kompjuterat e tyre në çdo kohë, kur largohen nga postet e tyre të punës. p.sh. mbylljen ose shkëputjen e kompjuterave të tyre kur shkojnë për një pushim kafeje ose për drekë.

Trajnimi i stafit për të siguruar kompjuterat e tyre në çdo kohë është një hap i rëndësishëm për sigurinë kibernetike dhe mbrojtjen e të dhënave në organizatë. Kjo praktikë ndihmon në parandalimin e incidenteve të padëshiruara dhe në ruajtjen e integritetit të të dhënave. Vihet re se **13.9%** e kompanive u përgjigjën që një pjesë e stafit është e trajnuar, **15.2%** e kompanive u përgjigjën se stafi nuk është i trajnuar dhe 6.1% se trajnimi i stafit nuk është i nevojshëm. Është e rëndësishme të përfshihet trajnimi dhe ndërgjegjësimi i stafit në politikat dhe praktikat e sigurisë kibernetike, përfshirë mbylljen ose shkeputjen e kompjuterave kur largohen nga postet e tyre të punës. Ky trajnim ndihmon në zvogëlimin e rreziqeve dhe në rritjen e sigurisë kibernetike të organizatës.

**2.** Ndiqet dhe ekziston një proces i formalizuar disiplinor për punonjësit që kanë shkelur politikat dhe proceset tuaja të sigurisë.

Vihet re se **33.3%** e kompanive janë përgjigjur që nuk ekziston dhe ndiqet një proces i formalizuar disiplinor për punonjësit që kanë shkelur politikat dhe proceset e sigurisë se organizatës. Procesi disiplinor për shkeljet e politikave dhe proceseve të sigurisë së organizatës është i rëndësishëm për të mbrojtur organizatën nga rreziqet kibernetike dhe për të ruajtur integritetin e të dhënave. Ai ndihmon në kultivimin e ndërgjegjësimit dhe përgjegjësisë në lidhje me sigurinë në organizatë. Kur një punonjës ndëshkohet për shkelje të sigurisë, ky mesazh mund të ndikojë te të tjerët për të respektuar politikat dhe praktikat e sigurisë. Kjo është një mënyrë për të ndikuar në sjelljen e të gjithë stafit në lidhje me sigurinë kibernetike. Procesi disiplinor ka ndikim në kulturën e sigurisë të organizatës. Punonjësit e dinë se shkeljet e sigurisë nuk tolerohen dhe kjo krijon një mjedis më të sigurt për të gjithë.

**3.** Organizata/Kompania në rast të ndryshimit të personelit zbaton politika/procedura të revokimit të së drejtës së aksesit (badge, aksesit në pajisje, sisteme etj.).

Vihet re se vetëm **47.3%** e kompanive u përgjigjën se zbatojnë politika/procedura të revokimit të së drejtës së aksesit në rast të ndryshimit të personelit, menjëherë sapo dikush largohet. Mungesa e zbatimit të politikave dhe procedurave të revokimit të së drejtës së aksesit në rast të ndryshimit të personelit mund të sjellë disa pasoja:

- Kur një person largohet nga organizata ose ndryshon pozicionin e tij, është e rëndësishme që aksesi i tij të revokohet menjëherë për të parandaluar aksesimin e padëshiruar të informacionit. Mungesa e revokimit të aksesit mund të çojë në shkelje të sigurisë kibernetike, grabitje të të dhënave dhe dëmtim të reputacionit.
- Për shkak të mungesës së revokimit të aksesit, personi që largohet nga organizata ose ndryshon pozicion mund të mbajë privilegje të paautorizuara për të aksesuar të dhëna ose burime të ndryshme. Kjo rrit rreziqet e shfrytëzimit të këtyre privilegjeve në mënyra të dëmshme.
- Mungesa e revokimit të aksesit ndaj hapësirave fizike (p.sh., ndërtesa, dhomat e serverave) mund të ndikojë në sigurinë fizike të organizatës. Personi që largohet mund të ketë ende akses fizik në mjedisin e organizatës.
- Shkelja e sigurisë kibernetike mund të dëmtojë rëndë reputacionin e organizatës dhe të çojë në ndeshkim ligjor, veçanërisht nëse është e dokumentuar që politikat dhe procedurat e revokimit të aksesit nuk janë ndjekur.
- Organizatat që janë të detyruara të përmbushin standarde të sigurisë, siç është ISO 27001, janë të detyruara të demonstrojnë se ata kanë procese të qarta dhe efektive për menaxhimin e të drejtave të aksesit. Mungesa e zbatimit të këtyre proceseve mund të krijojë vështirësi në çertifikim dhe auditime.

Për këto arsye, është e rëndësishme që organizatat të zbatojnë dhe të ndjekin politika dhe procedura të qarta të revokimit të së drejtës së aksesit në rast të ndryshimit të personelit. Kjo ndihmon organizatat të kenë një ambient më të sigurt kibernetik dhe në parandalimin e rreziqeve të mundshme të sigurisë.

Një analizë më e detajuar e përgjigjeve të marra në këtë seksion dhe lidhja midis variablave në seksion dhe nivelit të ndërgjegjësimit për seksionin "Siguria e Personelit" jepet në aneksin e këtij studimi.

## SEKSIONI SIGURIA FIZIKE DHE MJEDISORE

Duke qënë se siguria fizike dhe mjedisore është shumë e rëndësishme për sigurinë e informacionit, mbrojtjen e të dhënave dhe sigurinë kibernetike në pyetësor ka një seksion në lidhje me të. Politikat dhe procedurat e sigurisë fizike dhe mjedisore në një organizatë ose kompani janë thelbësore për të siguruar mbrojtjen e mallrave me vlerë të lartë, për të parandaluar ndërhyrjet e paligjshme në mjediset e biznesit dhe sistemet e informacionit, si dhe për të reduktuar rreziqet e kompromentimit të të dhënave. Ndërveprimi i stafit me mjedisin fizik dhe teknologjinë e informacionit është një aspekt kritik për sigurinë. Trajnimi dhe ndërgjegjësimi i stafit për rreziqet e vjedhjes së laptopëve dhe ndërveprimin e kujdesshëm me vizitorët tregon përkujdesje për sigurinë fizike. Përveç kësaj, aplikimi i sistemeve të kontrollit të aksesit fizik tek asetet kryesore, ruajtja e serverave në ambiente të sigurta, ruajtja e kopjeve rezervë të të dhënave në ambiente të tjera të sigurta dhe gjurmimi i aksesit të autorizuar në sistemet e teknologjisë së informacionit janë masa të rëndësishme për të mbrojtur të dhënat personale dhe të siguruar funksionimin e vazhdueshëm të organizatës ose kompanisë në rast emergjencash. Shkatërrimi i pajisjeve fizike që mbajnë të dhëna personale dhe informacione të rëndësishme, pasi ato kanë përfunduar qëllimin e tyre, gjithashtu ndihmon në parandalimin e rrezikut të kompromentimit të të dhënave. Këto masa përbëjnë një sistem të integruar sigurie për një organizatë ose kompani dhe ndihmojnë në ngritjen e nivelit të ndërgjegjësimit mbi sigurinë e informacionit, mbrojtjen e të dhënave dhe sigurinë kibernetike.

Ndër pyetjet që përfshihen në këtë seksion janë:

**1.** Organizata ose Kompania juaj ka procedura të përshtatshme të sigurisë fizike dhe mjedisore për të parandaluar ndërhyrjen tek mjediset e biznesit dhe sistemet e informacionit.

Vetëm **45.5%** e kompanive u përgjigjën se kanë procedura të përshtatshme të sigurisë fizike dhe mjedisore për të parandaluar ndërhyrjen tek mjediset e biznesit dhe sistemet e informacionit. Mungesa e procedurave të përshtatshme të sigurisë fizike dhe mjedisore ka ndikim të madh në sigurinë kibernetike dhe integritetin e të dhënave dhe çon në disa sfida:

- Mungesa e sigurisë fizike dhe mjedisore hap rrugën për ndërhyrje të padëshiruara në mjediset e biznesit dhe sistemet e informacionit. Kjo përfshin aksesin e paautorizuar në pajisje, servera, dhe infrastrukturë të rëndësishme, që mund të çojë në shkelje të sigurisë kibernetike.
- Kur nuk ekzistojnë procedura të përshtatshme për sigurinë fizike dhe mjedisore, organizata humbet kontrollin dhe mundësinë për të monitoruar këto aspekte. Kjo e bën organizatën më të prekshme ndaj rreziqeve dhe sulmeve.
- Siguria fizike është thelbësore për mbrojtjen e pajisjeve të rëndësishme, serverave, dhe të dhënave fizike. Mungesa e procedurave për sigurinë fizike mund të çojë në vjedhje të pajisjeve dhe humbje të të dhënave.
- Në rast të ndërhyrjeve në mjediset e biznesit dhe sistemet e informacionit, integriteti i të dhënave rrezikon të preket. Kjo mund të përfshijë modifikimin e të dhënave ose shkatërrimin e tyre.
- Shkelja e sigurisë fizike dhe mjedisore mund të ndikojë në disponueshmërinë e sistemeve të informacionit dhe shërbimeve të organizatës, duke shkaktuar ndërprerje të operacioneve.
- Shkeljet e sigurisë fizike dhe mjedisore mund të dëmtojnë rëndë reputacionin e organizatës, veçanërisht nëse ato bëhen publike.

Për të adresuar këto sfida, është e rëndësishme që organizatat të zhvillojnë dhe të zbatojnë procedura të përshtatshme për sigurinë fizike dhe mjedisore. Kjo përfshin politika dhe praktika të qarta për aksesin fizik në mjediset e biznesit, monitorimin e tyre, dhe masat për të parandaluar ndërhyrje të padëshiruara. Trajnimi dhe ndërgjegjësimi i stafit për këto procedura janë po ashtu të rëndësishëm për të rritur sigurinë kibernetike dhe integritetin e të dhënave.

**2.** Vizitorët tuaj shoqërohen gjithmonë nëpër ndërtesë/zyra dhe nuk lihen kurrë të lëvizin vetë.

Nga përgjigjet vihet re se vetëm **47.9%** e kompanive shoqërojnë gjithmonë vizitorët nëpër ndërtesë ose zyra. Mungesa e shoqërimit të vizitorëve nëpër ndërtesë ose zyra sjell disa problematika:

Për shkak të mungesës së shoqërimit të vizitorëve, organizata humbet kontrollin mbi aksesin e tyre në mjediset e saj. Kjo mund të çojë në akses të padëshiruar në ambiente të ndryshme, duke përfshirë zonat sensitive dhe sistemet e informacionit. Vizitorët që lëvizin lirshëm nëpër ndërtesë ose zyra pa shoqërim dhe kontroll të duhur mund të shpërdorojnë, grabisin pajisje, ose të përdorin rrjetin e organizatës në mënyrë të paautorizuar. Mungesa e shoqërimit të vizitorëve mund të ndikojë në sigurinë kibernetike, pasi ata mund të lidhen me rrjetin e organizatës. Organizatat duhet të dinë kush ndodhet në ambientet e tyre për siguri dhe monitorim të efektshëm. Mungesa e shoqërimit të vizitorëve vështirëson identifikimin dhe verifikimin e tyre. Incidentet e sigurisë që shkaktohen nga mungesa e shoqërimit të vizitorëve mund të dëmtojnë reputacionin e organizatës para klientëve, partnerëve, dhe opinionit publik.

Për të adresuar këto sfida, është e rëndësishme që organizatat të zhvillojnë dhe të zbatojnë politika dhe procedura të qarta për shoqërimin e vizitorëve në mënyrë që të kufizohet aksesi i tyre në zona sensitive dhe të monitorohet aktiviteti i tyre. Përveç kësaj, trajnimet e stafit mbi praktikat e sigurisë në lidhje me vizitorët janë të rëndësishme për të përmirësuar ndërgjegjësimin dhe implementimin e këtyre politikave. Këto masa do të ndihmonin në zvogëlimin e rreziqeve të sigurisë fizike dhe kibernetike të lidhura me vizitorët.

**3.** Serverët tuaj mbahen në ambiente të sigurta, me ajër të kondicionuar, në ambiente rezistente ndaj zjarrit dhe mund të punojnë pa ndërprerje në rast shkëputje të energjisë.

Nga përgjigjet vihet re se vetëm **53.3%** e kompanive u përgjigjën **"Po, i plotësojnë të gjitha kriteret"** kësaj pyetjeje. Mungesa e mbajtjes së serverave në ambiente të sigurta dhe të përshtatshme sjell një gamë të gjerë të problematikave dhe rreziqeve në organizatën ose kompaninë e cila nuk i ka implementuar këto praktika të rëndësishme për mbrojtjen kibernetike dhe qëndrueshmërinë e operacioneve të tyre. Disa nga këto problematika dhe rreziqe përfshijnë:

- Serverat janë shpesh burime të rëndësishme të të dhënave dhe informacionit sensitiv. Kur ato nuk mbahen në ambiente të sigurta, ata bëhen më të prekshëm për sulmet kibernetike. Një server i ekspozuar mund të jetë më i prekshëm nga sulmet e hakerave dhe malware-ve.
- Në raste të mundshme të zjarrit ose ndërprerjeve të energjisë, serverat që nuk janë mbajtur në ambiente të përshtatshme mund të përballen me humbje të të dhënave të rëndësishme. Mungesa e sistemeve të kondicionimit të ajrit mund të rrisë temperaturën në server dhe të dëmtojë pajisjet.
- Serverat që nuk janë të mbajtur në ambiente të sigurta dhe të kondicionuara mund të ndërpresin funksionimin kur ndodhin ngjarje si shkëputja e energjisë. Kjo mund të çojë në ndërprerje të veprimtarisë së organizatës dhe humbje financiare.
- Serverat që nuk janë të vendosur në ambiente rezistente ndaj zjarrit mund të rrezikojnë të dëmtohen ose shkatërrohen në raste zjarri. Ky dëmtim mund të çojë në humbje të të dhënave dhe të pajisjeve të vlefshme.
- Në rast shkeputje të energjisë, serverat duhet të kenë burime rezervë energjie për të vazhduar të funksionojnë. Mungesa e këtyre burimeve mund të çojë në ndërprerje të papritur të shërbimeve.

Për të adresuar këto problematika dhe rreziqe, organizatat dhe kompanitë duhet të kryejnë një vlerësim të hollësishëm të mjedisit të serverave dhe të investojnë në ambientet e sigurta, sistemet e kondicionimit të ajrit, dhe burimet rezervë për energjinë. Kjo është e rëndësishme për mbrojtjen e të dhënave të organizatës dhe për sigurinë kibernetike.

**4.** Sistemet e përpunimit të informacionit, programet ose pajisjet ku mbahet një databazë, aksesohen me fjalëkalim dhe bëhet backup-i (një kopje) e të dhënave personale dhe databaza ruhet në një ambient tjetër të sigurt.

Kësaj pyetjeje **22.4%** e kompanive j'u përgjigjën **"Po, për disa të dhëna personale"** dhe **9.1%** e kompanive j'u përgjigjën **"Jo, nuk është e nevojshme"**. Mungesa e aksesimit me fjalëkalim i sistemeve të perpunimit të informacionit, programeve, ose pajisjeve ku ruhet një databazë dhe mungesa e procesit të bërjes së backup-it dhe ruajtjes së një kopjeje të të dhënave personale dhe databazës në një ambient tjetër të sigurt sjell një gamë të gjerë problematikash dhe rreziqesh në organizatën ose kompaninë që nuk i ka implementuar këto praktika të rëndësishme për mbrojtjen kibernetike. Disa nga këto problematika dhe rreziqe përfshijnë:

- Kur aksesimi në sisteme, programe dhe pajisje që mbajnë informacionin është pa fjalëkalim, ekziston rreziku i aksesit të paligjshëm dhe shpërdorimit të të dhënave.
- Në raste kur nuk ka një proces të përditësimit të rregullt të backup-eve dhe ruajtjes së kopjeve të të dhënave në ambiente të sigurta, organizata është më e prekshme nga humbja e integritetit të të dhënave. Kjo përfshin humbjen e të dhënave në raste të ndërprerjes së energjisë, sulmeve kibernetike ose dështimeve të pajisjeve.
- Mungesa e sigurisë së të dhënave personale dhe kopjeve të ruajtura në ambiente të sigurta rrit rrezikun e humbjes së të dhënave personale të klientëve, punonjësve ose partnereve të biznesit. Kjo lloj humbjeje mund të rezultojë në dëme të serioze financiare dhe dëmtim të imazhit të organizatës.
- Në disa raste, mosrespektimi i kërkesave ligjore për mbrojtjen e të dhënave personale mund të çojë në pasojat ligjore serioze për organizatën.
- Humbja e të dhënave ose aksesimi i paligjshëm mund të çojë në ndërprerje të veprimtarisë së organizatës dhe dëme financiare serioze. Përdoruesit mund të humbasin besimin në organizatën nëse ata vënë re humbje të të dhënave personale.
- Mungesa e kopjeve të sigurta të të dhënave mund të çojë në dëmtim të pakthyeshëm të tyre në raste të ndërprerjes së energjisë, ngjarjeve natyrore ose dështimeve të pajisjeve. Kjo do të thotë që të dhënat mund të humbasin përgjithmonë.

Për të adresuar këto problematika dhe rreziqe, organizatat dhe kompanitë duhet të investojnë në sigurinë e aksesimit me fjalekalim të fortë dhe politika të qarta të sigurisë. Ato gjithashtu duhet të zhvillojnë dhe të zbatojnë procese të rregullta të backup-it dhe ruajtjes së kopjeve të të dhënave personale dhe databazës në ambiente të sigurta, për të siguruar që të dhënat të jenë të sigurta dhe të arritshme në raste emergjente. Kjo është e rëndësishme për mbrojtjen e të dhënave të organizatës dhe për sigurinë kibernetike.

**5.** Vetëm personave të autorizuar u lejohet aksesi në pajisjet dhe sistemet e teknologjisë së informacionit për përpunimin e të dhënave personale dhe gjurmohet lehtësisht kush e ka aksesuar.

Nga përgjigjet vihet re se **21.8%** e kompanive u përgjigjën që të gjithë mund të aksesojnë pajisjet dhe sistemet e teknologjisë së informacionit për perpunimin e të dhënave personale dhe **3.6%** e kompanive u përgjigjën se **"Aksesi në sisteme nuk mund të gjurmohet".**

Aksesi në pajisjet dhe sistemet e teknologjisë së informacionit për përpunimin e të dhënave personale nga të gjithë dhe mungesa e një sistemi të efektshëm të gjurmimit të personave që kanë aksesuar këto të dhëna sjell një numër të madh problematikash dhe rreziqesh në organizatë ose kompani. Disa nga këto problematika dhe rreziqe janë:

- Kur persona të paautorizuar kanë mundësi të aksesojnë të dhënat personale të individëve, kjo shkel privatësinë dhe mund të çojë në dëme serioze për personat e përfshirë. Lejimi i aksesit të gjithëve në të dhënat personale pa autorizim shkel privatësinë dhe është një shkelje e rëndë e rregullave të mbrojtjes së të dhënave personale. Kjo mund të rezultojë në humbje të besimit të klientëve dhe pasojat ligjore të shkeljes së privatësisë.
- Personat e paautorizuar që kanë akses në të dhënat personale mund t'i shfrytëzojnë ato për qëllime të këqija, përfshirë vjedhjen e identitetit, mashtrimin financiar, ose dëmtimin e reputacionit të individëve. Kjo mund të shkaktojë dëme serioze.
- Për shumë organizata, ka rregulla ligjore që kërkojnë mbrojtjen dhe sigurinë e të dhënave personale. Mosrespektimi i këtyre rregullave mund të çojë në gjoba të rënda dhe pasojat ligjore të tjera.
- Në raste të shkeljeve të sigurisë dhe shpërdorimit të të dhënave personale, besimi i konsumatorëve në organizatë ose kompani mund të humbasë. Kjo mund të sjellë humbje të klientëve dhe imazh të keq në treg.
- Nëse nuk ka një sistem të efektshëm të gjurmimit të personave që kanë aksesuar të dhënat personale, organizata nuk është në gjendje të identifikojë shpërdorimet ose shkeljet e sigurisë në kohë reale. Kjo lejon incidentet të qëndrojnë të paidentifikuara dhe të shkaktojnë më shumë dëme para se të zbulohen.
- Lejimi i të gjithëve të kenë akses të papërcaktuar në të dhënat personale mund të rezultojë në humbje të kontrollit mbi to. Kjo humbje e kontrollit mund të rrisë rreziqet e shkeljes së sigurisë dhe shpërdorimit të të dhënave.

Për të adresuar këto problematika dhe rreziqe, organizatat dhe kompanitë duhet të krijojnë dhe të zbatojnë politika të rrepta të sigurisë së informacionit dhe të kontrollimit të aksesit. Kjo përfshin:

- Identifikimin dhe Autentifikimin: Ato duhet të sigurohen që vetëm personat e autorizuar kanë akses dhe që ata identifikohen dhe autentifikohen me mënyrat e duhura përpara se të kenë qasje në të dhënat personale.
- Sistemet e Gjurmimit: Ndërtimin dhe përdorimin e sistemeve të gjurmimit që ndjekin veprimet e personave në sistemet e teknologjisë së informacionit.
- Kufizimet e Aksesit: Përcaktimi dhe zbatimi i kufizimeve të aksesit, duke lejuar qasje vetëm për personat dhe departamentet që kanë nevojë për të dhënat për punën e tyre.
- Marrjen e Autorizimeve: Ato duhet të sigurohen që kërkohet marrja e autorizimeve për aksesin në të dhënat personale dhe që ndërmerren veprimet e nevojshme për sigurimin e tyre.

Përmes këtyre masave, organizatat mund të përmirësojnë sigurinë e të dhënave personale dhe të mbrojnë integritetin dhe privatësinë e tyre.

**6.** Organizata ose Kompania shkatërron perfundimisht të gjitha pajisjet fizike që mbajne të dhëna personale, kur ato e kanë përmbushur qëllimin për të grumbulluar ose përpunuar informacionin (letrat e printuara, fotokopjet, fotografite, formulare, regjistra fizik, CD ROM, DVD ROM, USB, kaseta regjistruese dhe hard disqe).

Mungesa e shkatërrimit perfundimisht të pajisjeve fizike që mbajnë të dhëna personale, pasi ato kanë përmbushur qëllimin për të grumbulluar ose përpunuar informacionin, paraqet një problem të rëndësishëm për organizatën ose kompaninë. Ky problem sjell disa sfida dhe rreziqe:

- Pajisjet dhe mediat fizike që përmbajnë të dhëna personale janë potencialisht të rrezikshme nëse ato nuk shkatërrohen në mënyrë të sigurt dhe të përhershme pasi nuk janë më të nevojshme. Kjo mund të çojë në humbjen ose keqpërdorimin e të dhënave personale nga palë të paautorizuara.
- Mungesa e shkatërrimit të duhur të të dhënave personale pasi ato nuk janë më të nevojshme mund të çojë në shkelje të ligjit dhe në ndëshkime ligjore për organizatën ose kompaninë.

- Lënia e pajisjeve dhe mediave të informacionit të paasgjesuara jashtë kontrollit hap rrugën për rreziqe kibernetike. Mund të ketë përpjekje për të grumbulluar ose rikuperuar të dhëna nga pajisjet që janë hedhur pasi nuk janë më funksionale. Kjo është një hapësirë potenciale për sulmet dhe grabitjet kibernetike.
- Nëse të dhënat personale të klientëve, punonjësve, ose palëve të treta përfshihen në këto pajisje dhe ato pastaj bien në duar të palëve të paautorizuara, organizata ose kompania mund të hasë një dëm të rëndë në reputacionin e tyre.
- Në disa industri dhe sektorë, ka kërkesa të veçanta për shkatërrimin e të dhënave personale për të përmbushur standardet e sigurisë dhe për të respektuar rregulloret. Mungesa e shkatërrimit të duhur mund të sjellë mos-përmbushjen e këtyre kërkesave dhe pasoja ligjore që mund të vijojnë prej tyre.

Për të zgjidhur këtë problematikë, organizatat dhe kompanitë duhet të zhvillojnë dhe të zbatojnë politika dhe procedura të qarta për shkatërrimin e pajisjeve dhe mediave fizike që mbajnë të dhëna personale. Kjo përfshin procedura të sigurta dhe të dokumentuara për shkatërrimin dhe fshirjen e të dhënave, duke përfshirë faza të ndryshme të shkatërrimit dhe metoda të sigurta të asgjesimit së pajisjeve pasi nuk janë më funksionale.

Një analizë më e detajuar e përgjigjeve të marra në këtë seksion dhe lidhja midis variablave në seksion dhe nivelit të ndërgjegjësimit për seksionin "Siguria fizike dhe mjdisore" jepet në aneksin e këtij studimi.

## SEKSIONI MENAXHIMI I KOMUNIKIMEVE DHE I OPERACIONEVE

Duke qënë se menaxhimi i komunikimeve dhe operacioneve të një organizate ose kompanie është një aspekt kritik i sigurisë së informacionit dhe mbrojtjes së të dhënave në pyetësor është shtuar një seksion në lidhje me të. Kopjet rezervë dhe ruajtja e të dhënave janë thelbësore për të siguruar rifitimin e informacionit në rast të keqfunksionimit të pajisjeve, vjedhjes ose katastrofave. Duke pasur mekanizma të duhura për kopjet rezerve dhe ruajtjen e të dhënave, një organizate ose kompani mund të sigurojë që puna të vazhdojë me sa më pak ndërprerje në rast emergjencash. Përditësimet dhe përmiresimet e sistemeve sipas një plani të strukturuar tregojnë përkushtim ndaj sigurisë dhe ndihmojnë në zvogëlimin e rreziqeve të sigurisë kibernetike. Procedurat e përcaktuara për menaxhimin e incidenteve të sigurisë, si dhe identifikimi i personave të përgjegjshëm për të vepruar në rast krizash, sigurojnë që reagimi ndaj incidenteve të sigurisë të jetë efikas dhe i koordinuar. Sistemet antivirus të përditësuara dhe mekanizmat e verifikimit të identitetit të përdoruesve ndihmojnë në mbrojtjen e sistemeve të informacionit nga sulmet e mundshme. Këto masa përbëjnë një pjesë të rëndësishme të strategjisë së sigurisë së organizatës ose kompanisë, duke ndikuar në nivelin e ndërgjegjësimit mbi sigurinë e informacionit, mbrojtjen e të dhënave dhe sigurinë kibernetike.

**1.** Jeni të bindur se në rast të keqfunksionimit në pajisje, vjedhjes ose një katastrofe, kopjet rezervë dhe ruajtja e të dhënave tuaja do t'ju mundësojnë të rifitoni informacionin tuaj me ndërprerje minimale të punës.

Nga përgjigjet vihet re se vetëm **42.4%** e kompanive mund të rifillojnë menjëherë aktivitetin në rast të keqfunksionimit në pajisje, vjedhjes ose një katastrofe. Problematika që organizatat dhe kompanitë përballen në lidhje me mosrifitimin e informacionit me ndërprerje minimale të punës është një sfidë serioze për sigurinë kibernetike dhe qëndrueshmërinë e operacioneve të tyre. Disa nga këto probleme përfshijnë: Humbje e të dhënave të rëndësishme; Pasojat financiare; Rënie e efikasitetit dhe produktivitetit; Dëmtim i imazhit dhe reputacionit; Mosrespektimi i kërkesave ligjore. Për të adresuar këto probleme dhe rreziqe, organizatat dhe kompanitë duhet të zhvillojnë dhe të zbatojnë strategji të qëndrueshme për mbrojtjen e të dhënave dhe sigurinë kibernetike. Kjo përfshin hartimin e planeve të detajuara të sigurisë, vendosjne e kopjeve rezervë të të dhënave në ambiente të sigurta, zhvillimin e procedurave të ndërhyrjes në raste emergjencash, dhe trajnimin e stafit për të vepruar në mënyrë efikase në situata të tilla. Gjithashtu, është e rëndësishme të përdoren teknologjitë dhe mjetet e duhura për të bërë backup të të dhënave dhe për të siguruar që informacioni të jetë i arritshëm edhe pas incidenteve. Një qasje e përgjegjshme ndaj mbrojtjes kibernetike dhe qëndrueshmërisë është thelbësore për të parandaluar dhe përballuar sfidat e mundshme.

**2.** Sistemet tuaja përditësohen ose përmirësohen sipas një plani të strukturuar.

Vetëm **39.4%** e kompanive u përgjigjën që sistemet e kompanisë përditësohen apo përmirësohen sipas një plani të strukturuar. Mungesa e përditësimit dhe përmirësimit të sistemeve të një organizate ose kompanie sipas një plani të strukturuar ka pasoja të rënda për sigurinë kibernetike të organizatës. Disa prej tyre janë:

- Një numër i madh i incidenteve kibernetike ndodhin për shkak të mungesës së përditësimeve periodike të sistemeve dhe aplikacioneve. Organizatat duhet të kenë një plan të strukturuar për monitorimin dhe implementimin e përditësimeve të sigurisë.
- Mungesa e trajnimeve për stafin: Përdoruesit e brendshëm janë pika e dobët më e madhe në sigurinë kibernetike. Trajnimet ndihmojnë që këta përdorues të jenë të vetëdijshëm për rreziqet dhe praktikat e sigurisë.

- Përdorimi i pajisjeve të vjetra: Pajisjet dhe sistemet e vjetra janë më të prekshme nga rreziqet kibernetike. Organizatat duhet të planifikojnë përmirësimin ose zëvendësimin e pajisjeve të vjetra me pajisje të sigurisë më të përparuara.
- Mungesa e një plani të strukturuar të sigurisë kibernetike: Në shumë raste, organizatat nuk kanë një plan të strukturuar për të menaxhuar rreziqet dhe për të reaguar ndaj incidenteve kibernetike. Ky është një problem serioz që kërkon një përmirësim të menjëhershëm.
- Njohuritë teknike të papërdorura: Në disa raste, organizatat kanë teknologji të përparuara për sigurinë kibernetike, por nuk i përdorin ato në mënyrë efikase ose nuk kanë njohuri për t'i përdorur ato në maksimumin e tyre.

Për të adresuar këto problematika kompanitë duhet të sigurohen që të kenë një proces të strukturuar për monitorimin dhe implementimin e përditësimeve të sistemeve dhe aplikacioneve. Përditësimet e rregullta të sigurisë janë të domosdoshme për parandalimin e incidenteve kibernetike. Ato duhet të sigurohen që të ofrojnë trajnime të rregullta dhe të përshtatshme për stafin në lidhje me sigurinë kibernetike. të identifikojnë pajisjet dhe sistemet e vjetra që janë të prekshme nga rreziqet kibernetike dhe të planifikojnë përmirësimin ose zëvendësimin e tyre me teknologji më të përparuara dhe të sigurta.

**3.** Sistemet tuaja antivirus janë të përditësuara dhe në rast të një sulmi, ju jeni në gjendje t'i mbroni sistemet tuaja sa më mirë që të jetë e mundur.

Vetëm **40%** e kompanive u përgjigjën që sistemet të tyre përditësohen gjithmonë. Mungesa e përditësimit të sistemeve antivirus në një organizatë ose kompani mund të çojë në incidente të rënda kibernetike:

- Rreziku i infektimit me malware: Sistemet antivirus janë mbrojtja e parë kundër softuerëve të rrezikshëm si viruset, trojanët, dhe malware të tjerë. Kur këto sisteme nuk përditësohen, ata nuk mund të njihen dhe të ndalohen në mënyrë efikase. Kjo e rrezikon sigurinë e të dhënave dhe sistemeve.
- Dobësitë e reja të zbuluara: Nëse një dobësi është zbuluar në një version të vjetër të programit antivirus, kjo mund të përdoret për hyrje të paligjshme në sistemin tuaj.
- Rreziqet e zero-day: Sulmuesit shpesh shfrytëzojnë rreziqe të njohura si "zero-day" - ato që nuk janë ende të njohura ose të riparuara nga prodhuesit e softuerit. Përditësimet e sistemeve antivirus ndihmojnë në zbulimin e këtyre rreziqeve.

- Mosfunksionimi i sistemeve: Nëse një sistemi antivirus nuk përditësohet, ai mund të fillojë të japë sinjale të rreme pozitive ose të neglizhojë rreziqe reale. Kjo mund të shkaktojë ndërprerje të panevojshme në operacionet e organizatës.
- Mungesa e mbështetjes së teknikës: Për prodhuesit e softwareve antivirus, të përditësuarit e versioneve të vjetra zakonisht ndodhin pas një periudhe të caktuar kohore. Mungesa e përditësimeve do të thotë që organizata nuk do të ketë më mbështetje teknike nga prodhuesi.

Për të adresuar këtë problematikë organizatat dhe kompanitë duhet të: Sigurohen që sistemet antivirus të përditësohen automatikisht kur janë në dispozicion përmes konfigurimeve të zgjedhura paraprakisht. Kjo do të minimizojë rrezikun e harresës ose neglizhencës njerëzore për përditësimet. Testojnë çdo përditësim të sistemit antivirus përpara se t'i zbatojnë në realitet për të parë nëse ka ndonjë ndikim negativ në sistemin e tyre. Përmirësojnë ndërgjegjësimin e personelit: Edukojnë stafin mbi rreziqet e mungesës së përditësimeve të sigurisë, dhe inkurajojnë ata të raportojnë menjëherë për çdo problem që mund të kenë. Përdorin mjete për monitorimin e ngjarjeve që mund të identifikojnë probleme me sistemin antivirus dhe ngjarje të tjera të sigurisë kibernetike.  Këto do të ndihmojnë organizatat apo kompanitë të mbrohen në mënyrë efikase kundër rreziqeve të sigurisë kibernetike që janë të lidhura me përditësimet e sistemeve antivirus.

Një analizë më e detajuar e përgjigjeve të marra në këtë seksion dhe lidhja midis variablave në seksion dhe nivelit të ndërgjegjësimit për seksionin "Menaxhimi i komunikimeve dhe i operacioneve" jepet në aneksin e këtij studimi.

## SEKSIONI KONTROLLI AKSESIT

Duke qënë se kontrolli i aksesit është një aspekt shumë i rëndësishëm i sigurisë së informacionit, mbrojtjes së të dhënave dhe sigurisë kibernetike në organizata dhe kompani në pyetësor u krijua një seksion në lidhje me të. Nëse në një organizatë ose kompani, është përcaktuar se perdoruesit nuk mund të kenë akses në sistemet e saj pa qenë të regjistruar fillimisht me llogaritë e tyre të përdoruesit, është bërë një nga hapat parandalues shumë kritik për të shmangur hyrjen e paligjshme në sistemet e kompanisë. Nëse ekziston një sistem i menaxhimit të fjalekalimeve, që kërkon shpeshtësinë e ndryshimeve të fjalekalimeve dhe kompleksitetin minimal të tyre forcohet e siguria duke e bërë më të vështirë për personat e paautorizuar të kenë akses në llogaritë e përdoruesve. Politika e kontrollit të aksesit përcakton se cilët përdorues kanë akses në cilat të dhëna, duke siguruar që të dhënat e ndjeshme janë të mbrojtura dhe të aksesueshme vetëm nga personat e autorizuar. Pajisjet e perpunimit të informacionit përdoren vetëm për qëllime të autorizuara, duke siguruar që ndryshimet ose përdorimi i tyre nuk i rrezikojnë të dhënat e kompanisë. Përveç kësaj, kontrolli i aksesit ndaj paleve te treta është një masë e rëndësishme për të mbrojtur asetet kryesore të rrjeteve dhe sistemeve të informacionit nga personat e paautorizuar. Vlerësimi periodik i politikave dhe mekanizmave të kontrollit të aksesit ndihmon në identifikimin e vështirësive dhe përmirësimeve të nevojshme për të rritur efektivitetin e sigurisë së informacionit dhe mbrojtjes së të dhënave.

Ndër pyetjet që përfshihen në këtë seksion janë:

**1.** Ekziston një sistem i menaxhimit të fjalëkalimit i cili specifikon shpeshtësinë e ndryshimeve të fjalëkalimit si dhe kompleksitetin minimal të fjalëkalimit, p.sh. fjalëkalimi duhet të ndryshohet çdo dy javë dhe të jetë i gjatë të paktën X karaktere.

Vetëm **45.5%** e kompanive u përgjigjën se **"Po, fjalëkalimet janë komplekse dhe përditësohen vazhdimisht sipas një sistemi menaxhimi".**

Fjalëkalimet luajnë një rol të rëndësishëm në skenën e sigurisë pasi janë një mjet për autentifikimin e përdoruesave dhë parandalimin e aksesit të paautorizuar. Përdorimi i tyre është shtuar mjaft kohët e fundit me shtimin e shërbimeve online duke qenë se janë me kosto të ulët dhe implementohen lehtësisht. Shumë administratorë forcojnë përdoruesit që të ndryshojnë fjalëkalimet e tyre në intervale të rregullta kohe duke përcaktuar dhe rregulla që fjalëkalimet të jenë sa më të forta. Gjithsesi kjo kërkesë vendos një barrë mbi punonjësin i cili në përgjithësi zgjedh fjalëkalime që janë lehtësisht të ndryshëm nga të parat. Sulmuesit përdorin mjaft mjete për të zbuluar fjalëkalimet që nga gjetja manual duke përdorur të dhënat personale deri tek mjetë të fuqishme të automatizuara.

Për këtë arsye kompanitë duhet të përdorin dhe mjete të tjera përvec kërkesave për ndryshimin e fjalëkalimeve nga punonjësit si:

- Monitorimi i login-eve jo të zakonshme
- Njoftimi i përdoruesave me detaje të logineve
- Mbrojtja nga mënyra e gjetjes së fjalëkalimeve duke përdorur një nga mënyrat e mëposhtme:
  - Kycja e llogarive pas jo më shumë se 10 përpjekjeve të pasusksesshme
  - Limitimi I numrit të hamendësimeve të lejuara në një periudhë kohore për jo më shumë se 10 përpjekjeve Brenda 5 minutave
  - Vendosja e një gjatësie fjalëkalimesh me së paku 8 karaktere
  - Mos vendosja e një gjatësie fjalëkalimi maksimale
  - Ndryshimi i menjëhershëm i fjalëkalimit kur aplikanti din ose dyshon që ato janë kompromentuar
  - Kanë një politikë fjalëkalimesh që i tregon përdoruesit:
  - Si të evitojë të zgjedhë fjalëkalime evidente ose fjalëkalime të zakonshme
  - Të mos përdorë të njëjtin fjalëkalim diku tjetër si për shembull në shtëpi
  - Ku dhe si të rregjistrojë dhe të ruajë fjalëkalimet në mënyrë të sigurtë
  - Nëse përdorin softuerë menaxhimi të fjalëkalimeve të përcaktohet lloji dhe mënyra e përdorimit të këtyre aplikacioneve.

**2.** Organizata/Kompania juaj kontrollon aksesin në informacion nëpërmjet një politike të kontrollit të aksesit e cila specifikon se cilët përdorues kanë akses në cilat të dhëna.

**42.4%** e kompanive u përgjigjën **"Po, organizata ka një politikë kontrolli".**

Aksesi i kontrollit konsiderohet si një nga aspektet më të rëndësishme të sigurisë së informacionit. Ajo ka dy komponente kryesore: autentifikimin dhe autorizimin. Autentifikimi është verifikimi i identitetit të përdoruesit që akseson sistemin. Qëllimi i autentifikimit është gjithashtu përcaktimi i vendit dhe kohës së aksesit, nëse sistemi aksesohet nga një kompjuter privat ose jo etj. Autorizimi është lejimi ose kufizimi i aksesit tek informacioni bazuar në tipin e përdoruesave dhe rolit të tyre: punonjës, administrator ose menaxher.

Çdo kompani duhet të specifikojë në mënyrë të qartë kontrollin e aksesit të aktiviteteve. Kompania ka nevojë të implememtojë politika efektive dhe praktika për menaxhimin se kush mund të aksesojë të dhënat, si dhe nën cila kushte. Sipas ISO 27002:2022(Standarti për sigurinë e kontrolleve të informacionit ), Control 5.18 – Access Rights kompanitë duhet të përfshijnë rregullat dhe kontrollet në proceset për vendosjen dhe revokimin e të drejtave të aksesit për autentifikimin individual:

- Pronari i asetit të informacionit duhet të sigurojë autorizimin e tij për aksesin dhe përdorimin e aseteve të rëndësishme të informacionit. Kompanitë duhet të konsiderojnë gjithashtu të kërkojnë aprovim të ndarë nga menaxhimi për të dhënë të drejta aksesi.
- Nevojat e biznesit të kompanisë dhe politika e saj mbi kontrollin e aksesit duhet të merret parasysh.
- Organizatat duhet të konsiderojnë detyra të ndara. Për shembull aprovimi i një detyre dhe implementimi i të drejtave të aksesit mund të kryhen nga individë të ndryshëm.
- Kur një individ nuk ka më nevojë të aksesojë asetin e informacionit, veçanërisht kur nuk janë më pjesë e kompanisë, të drejtat e aksesit të tyre duhet të anullohen menjëherë.
- Personelit që punon për organizatën me kohë të pjesshme mund ti sigurohet të drejta aksesi të përkohshme. Këto të drejta duhet të anulohen nëse ata nuk punojnë më për organizatën.
- Niveli i aksesit që sigurohet për një individ duhet të jetë në linjë me politikën e kontrollit të aksesit dhe duhet të rishikohet dhe verifikohet në mënyrë të rregullt.

- Kompanitë duhet të sigurojnë se të drejtat e aksesit nuk janë aktivizuar derisa një procedurë autorizimi më i përshtatshëm është përfunduar.
- Të drejtat e aksesit të siguruara për secalin identifikues individual, si ID ose fizike, duhet të jetë rregjistruar në një sistem menaxhimi qendror për kontrollin e aksesit dhe ky system duhet mirëmbajtur.
- Nëse roli i një individi ose detyra ndryshojnë niveli i tyre i aksesimit të të drejtave duhet të ndryshohet.
- Heqja ose modifikimi i të drejtave të aksesit fizik ose logjik mund të kryhet nëpërmjet metodave të mëposhtme: Heqja ose zëvendësimi i celësave, kartave ID, ose informacioni i autentifikimit.
- Ndryshimet e të drejtave të aksesit fizik ose logjik të një përdoruesi duhet të rregjistrohen në system dhe duhet të mirëmbahen.

**3.** Pajisjet e përpunimit të informacionit përdoren vetëm për qëllime të autorizuara.

Kësaj pyetjeje **69.7%** e kompanive u përgjigjën **"Po"**

Një parim kyç në siguri është që përdoruesit duhet të kenë akses vetëm në të dhënat dhe funksionalitetin që është i nevojshëm për të mbështetur qëllimet e tyre legjitime. "Qasje" mund të nënkuptojë si qasje fizike në një pajisje, ashtu edhe qasje në distancë në shërbimet dhe funksionet e ofruara nga produkti. Kërcënimet fizike dhe mjedisore ndaj pajisjeve të IT-së si serverët, kompjuterët, disqet e ngurtë dhe mediat e lëvizshme të ruajtjes së të dhënave mund të rrezikojnë gjithashtu disponueshmërinë, konfidencialitetin dhe integritetin e aseteve të informacionit.

Në përputhje me ISO 27002:2022, Control 7.8 – Vendndodhja dhe mbrojtja e pajisjeve përfshihet krijimi e një inventari të pajisjeve që mbajnë asetet e informacionit, vendosjen e të gjitha pajisjeve në zona të sigurta dhe zbatimin e masave të duhura për të parandaluar kërcënimet fizike dhe mjedisore.

- Pajisjet duhet të vendosen në zona të sigurta në mënyrë që personat e paautorizuar të mos kenë akses në pajisje.
- Mjetet e përdorura për përpunimin e informacionit të ndjeshëm si kompjuterët, monitorët dhe printerët duhet të pozicionohen në një mënyrë që personat e paautorizuar të mos shohin informacionin e shfaqur në ekran pa leje.

- Duhet të merren masat e duhura për të eliminuar dhe/ose zbutur rreziqet që lindin nga kërcënimet fizike dhe mjedisore si eksplozivët, ndërhyrjet në komunikim, zjarri, pluhuri dhe rrezatimi elektromagnetik. Për shembull, një shufër rrufeje mund të jetë një kontroll efektiv kundër goditjeve nga rrufeja.
- Udhëzimet për të ngrënë dhe pirë rreth pajisjeve duhet të vendosen dhe t'u komunikohen të gjitha palëve përkatëse.
- Kushtet mjedisore që mund të pengojnë operacionet e përpunimit të informacionit duhet të monitorohen vazhdimisht. Këto mund të përfshijnë nivelet e temperaturës dhe lagështisë.
- Në të gjitha ndërtesat dhe zyrat duhet të zbatohen mekanizmat e mbrojtjes nga rrufetë. Për më tepër, filtrat e mbrojtjes nga rrufetë duhet të ndërtohen në të gjitha linjat e energjisë elektrike në hyrje, duke përfshirë linjat e komunikimit.
- Nëse pajisjet janë të vendosura në një mjedis industrial, duhet të përdoren kontrolle të veçanta mbrojtëse si membranat e tastierës nëse është e nevojshme.
- Rrezatimi elektromagnetik mund të rezultojë në rrjedhjen e informacionit të ndjeshëm. Prandaj, pajisjet që mbajnë asete informacioni të ndjeshme ose kritike duhet të sigurohen për të parandaluar një rrezik të tillë.
- Pajisjet e TI-së në pronësi dhe të kontrolluara nga një organizatë duhet të ndahen qartë nga ato që nuk zotërohen dhe kontrollohen nga organizata.

4. Organizata/Kompania juaj përforcon kontrollet për aksesin në distancë në asetet kryesore të rrjeteve dhe sistemeve të informacionit nga palët e treta.

Vetëm **33.3%** e kompanive u përgjigjën "**Po, kemi sisteme kontrolli që zbatohen gjithmonë"** ndërsa **23.6%** e kompanive u përgjigjën **"Po, kontrollet zbatohen në raste specifike".**

Organizatat mund të përfitojnë shumë nga puna në distancë. Megjithatë ky trend paraqet disa sfida serioze të sigurisë për departamentet e IT. Disa përdorues, veçanërisht ata që nuk janë të aftë për teknologjinë, mund ta marrin të mirëqenë nevojën për t'u lidhur në mënyrë të sigurt me rrjetin e brendshëm nga jashtë zyrës,duke e vënë rrjetin në rrezik me sjellje potencialisht të dëmshme. Nëse një politikë e aksesimit në distancë nuk ekziston në kompani, një sjellje e tillë e rrezikshme mund të vazhdojë e pazbuluar dhe mund të rrezikojë sigurinë e informacionit të kompanisë.

Organizatat duhet të ndërtojë një politikë aksesi në distancë i cili është një dokument i shkruar që përmban udhëzimet për lidhjen me rrjetin e një organizate nga jashtë zyrës. Është një mënyrë për të ndihmuar në sigurimin e të dhënave dhe rrjeteve të korporatës nga aksesi jashtë dhe është veçanërisht e dobishme për organizatat e mëdha me përdorues të shpërndarë gjeografikisht që hyjnë nga vende të pasigurta, si p.sh. rrjetet e tyre shtëpiake. 5. Në mënyrë periodike organizata ose kompania juaj vlerëson efektivitetin e politikës së kontrollit të aksesit dhe të zbatimit të mekanizmave të kontrollit të aksesit.

Kësaj pyetjeje **27.8%** e kompanive u përgjigjën **"Po, në mënyrë periodike vlerësohet efektiviteti"**, ndërsa **26.5%** e kompanive u përgjigjën **"Po, vlerësohet por jo periodikisht".**

Kontrolli i aksesit është një metodë që garanton se përdoruesit janë ata që thonë dhe se kanë akses të përshtatshëm tek të dhënat e kompanisë. Rregullat e aksesit të kontrollit duhet të ndryshojnë sipas faktorit të riskut duke përdorur analiza sigurie të mbështetura në algoritmat e mësimit të makinës dhe inteligjencës artificiale. Ato duhet gjithashtu të identifikojnë kërcënimet në kohë reale dhe të automatizojnë rregullat e kontrollit të aksesit sipas rrethanave. Prandaj është e nevojshme që në mënyrë periodike organizata ose kompania juaj të vlerësojë efektivitetin e politikës së kontrollit të aksesit dhe të zbatimit të mekanizmave të kontrollit të aksesit.

## SEKSIONI ZHVILLIMI DHE MIRËMBAJTJA E SISTEMEVE

Përditësimet e rregullta të sistemeve dhe mirëmbajtja e tyre të vazhdueshme janë kritike për sigurinë e informacionit dhe mbrojtjen e të dhënave. Gjithashtu zhvillimi i sistemeve të sigurta dhe auditimi i tyre i rregullt siguron një mjedis më të sigurt për të përpunuar informacionin dhe të mbrojtur të dhënat. Duke qënë se së bashku kontribuojnë në ngritjen e nivelit të ndërgjegjësimit mbi sigurinë e informacionit, mbrojtjen e të dhënave dhe sigurinë kibernetike në organizatat dhe kompanitë në Shqipëri u krijua një seksion në pyetësor në lidhje me to. Duke mbajtur sistemet të përditësuara dhe duke iu përgjigjur ndryshimeve të rrezikshme të sigurisë, një organizatë zvogëlon rrezikun e ekspozimit ndaj kërcënimeve të sigurisë. Nëse një organizatë sistemet i blen si produkte softuerësh të disponueshëm në treg, është e rëndësishme të ketë parasysh sigurinë e tyre. Prodhuesit e besueshëm të softëare ofrojnë rregullisht përditësime për të adresuar ndonjë shkelje të sigurisë ose ndonjë problem tjetër të identifikuar. Duke përditësuar këto produkte me rregullsi, kompanitë mund të minimizoni rreziqet e sigurisë dhe të mbroheni nga kërcënimet e reja. Nëse kompanitë zhvillojnë sisteme të personalizuara ose të kontraktuara nga zhvilluesit, duhet të sigurohen që zhvilluesit respektojnë standardet e sigurisë gjatë procesit të zhvillimit. Përdorimi i praktikave të mira të sigurisë dhe testeve të sigurisë gjatë fazës së zhvillimit është thelbësor për të minimizuar kërcënimet potenciale. Siguria e informacionit dhe mbrojtja e të dhënave kërkojnë një gjurmim të rregullt të aktivitetit të sistemeve. Gjurmimi i auditimit lejon identifikimin e ndryshimeve të te dhenave, hyrjeve dhe daljeve të përdoruesve, dhe veprimtarisë së sistemit në përgjithësi. Kjo ndihmon në zbulimin e veprimtarisë të dyshimtë dhe potencialisht të paautorizuar.

Disa nga pyetjet në këtë seksion janë:

**1.** Sistemet tuaj i blini si produkte softuerësh të disponueshëm në treg ose si sisteme të personalizuara, të kontraktuara nga zhvilluesit.
Kësaj pyetjeje **44.2%** e kompanive u përgjigjën **"Blejmë sisteme të disponueshme në treg"**, ndërsa **31.5%** e kompanive u përgjigjën **"Blejmë sisteme të personalizuara"**.

Kur është e nevojshme një zgjidhje të re softuerike për kompaninë, dy janë opsionet kryesore: të blihet një produkt i disponueshëm që tashmë ekziston, ose të ndërtohet një i personalizuar që plotëson kërkesat specifike të kompanisë. Të dyja opsionet kanë të mirat dhe të këqijat e tyre, dhe zgjedhja e asaj të duhurit varet nga disa faktorë.

Nëse konsiderojmë sigurinë dhe mbrojtjen e të dhënave në biznes zhvillimi i personalizuar i softuerit mund të konsiderohet si zgjidhje për disa arsye si më poshtë:

- Masat e përshtatura të sigurisë: zgjidhjet softuerike të disponueshme shpesh kanë veçori gjenerike të sigurisë që mund të mos adresojnë plotësisht nevojat specifike dhe dobësitë e një biznesi të caktuar. Zhvillimi i personalizuar i softuerit i lejon bizneset të zbatojnë masa të personalizuara sigurie bazuar në kërkesat e tyre unike, duke siguruar një nivel më të lartë mbrojtjeje për të dhënat e ndjeshme.
- Zbutja e dobësive: zhvillimi i personalizuar i softuerit u mundëson bizneseve të inkorporojnë protokolle të fuqishme sigurie që në fazat fillestare të zhvillimit. Kjo qasje proaktive lejon identifikimin dhe zbutjen e dobësive përpara se softueri të svendoset, duke reduktuar rrezikun e shkeljeve të sigurisë dhe rrjedhjeve të të dhënave.
- Sipërfaqja e sulmit të limituar: softueri i personalizuar është ndërtuar për të përmbushur nevojat specifike të një biznesi, që do të thotë se veçoritë dhe funksionalitetet e panevojshme mund të eliminohen. Duke reduktuar sipërfaqen e sulmit - pikat e mundshme të hyrjes për sulme me qëllim të keq - bizneset mund të minimizojnë rrezikun e aksesit të paautorizuar dhe shkeljeve të të dhënave.
- Kriptimi i përmirësuar i të dhënave: zhvillimi i personalizuar i softuerit i lejon bizneset të zbatojnë teknika të forta enkriptimi për të mbrojtur të dhënat e tyre. Zhvilluesit mund të integrojnë algoritme kriptimi standarde të industrisë dhe të personalizojnë protokollet e kriptimit për të mbrojtur informacionin e ndjeshëm, duke e bërë dukshëm më të vështirë për individët e paautorizuar deshifrimin ose aksesin e të dhënave.

- Përditësimet e rregullta të sigurisë: softueri i personalizuar siguron kontroll më të madh mbi procesin e zhvillimit, duke i lejuar bizneset të monitorojnë dhe përditësojnë vazhdimisht masat e sigurisë. Kjo siguron që softueri të qëndrojë i përditësuar me arnimet, rregullimet dhe avancimet më të fundit të sigurisë, duke luftuar në mënyrë efektive kërcënimet dhe dobësitë e reja.
- Pajtueshmëria me rregulloret: Industri dhe rajone të ndryshme kanë rregullore specifike për mbrojtjen e të dhënave dhe kërkesa të pajtueshmërisë. Zhvillimi i personalizuar i softuerit u mundëson bizneseve të përshtatin sistemet e tyre për t'iu përmbajtur këtyre rregulloreve, duke siguruar përputhjen ligjore dhe duke minimizuar rrezikun e ndëshkimeve ose pasojave ligjore.

**2.** Sistemet tuaj ofrojnë gjurmë auditimi në mënyrë që përdorimi i sistemit dhe futja/ndryshimet e të dhënave të mund të auditohen.

Vetëm **46.3%** e kompanive u përgjigjën **"Po, sistemet tona sigurojnë gjurmim"**. Një gjurme auditimi është një sekuencë ngjarjesh kompjuterike të regjistruara që përfshin çdo aktivitet rreth sistemit operativ, aplikacioneve ose veprimeve të përdoruesit. Një kompjuter mund të ketë disa gjurmë auditimi që secila i shërben një qëllimi të ndryshëm. Qëllimi i një gjurme auditimi është të reduktojë gabimet, aktivitetet mashtruese dhe aksesin e paautorizuar të sistemit, të përmirësojë kontrollet e brendshme dhe të verifikojë saktësinë e transaksioneve themelore të kontabilitetit që rrjedhin në pasqyrat financiare.

Gjurmët e auditimit janë thelbësore për të zbuluar dhe kuptuar se çfarë shkoi keq kur një kompani ose organizatë pëson një shkelje të sigurisë, humbje të të dhënave ose sjellje të pahijshme. Duke pasur një regjistër të detajuar se kush ka akses në çfarë dhe kur, mund ta bëjë kërkimin për atë që shkoi keq shpejt dhe lehtë

## SEKSIONI MENAXHIMI I VAZHDIMËSISË SË BIZNESIT

Menaxhimit të vazhdimësisë së biznesit është i lidhur ngushtë me sigurinë e informacionit, mbrojtjen e të dhënave dhe sigurinë kibernetike në organizatat dhe kompanitë në Shqipëri. Ndaj në pyetësor eshte shtuar një seksion në lidhje me të. Një plan i vazhdimësisë së biznesit është i rëndësishëm për të siguruar që një organizatë ose kompani mund të vazhdojë të funksionojë në rast të ndodhjes së një fatkeqësie, siç mund të jetë një zjarr, një përmbytje, një katastrofë e siguruar nga njeriu ose pakujdesia etj. Ky plan specifikon hapat dhe veprimet që duhet të ndërmerren, si dhe personat përgjegjës për të minimizuar ndërprerjen dhe humbjet e mundshme të informacionit dhe të dhënave. Rishikimi i masave të sigurisë gjatë vitit të fundit është një proces i rëndësishëm për të identifikuar çdo ndryshim në mjedisin e rreziqeve dhe kërcënimeve. Duke e rishikuar rregullisht planin e sigurisë dhe masat për të parandaluar dhe trajtuar incidentet e sigurisë, një organizatë ose kompani siguron që të jetë e përgatitur për ndonjë situatë emergjente.

Disa nga pyetjet në këtë seksion janë:

**1.** Kompania ose organizata juaj ka një plan të vazhdimësisë së biznesit, i cili specifikon se kush duhet të ndërmarrë çfarë veprimi dhe çfarë duhet bërë për të siguruar që organizata ose kompania mund të vazhdojë të funksionojë në rast të një fatkeqësie të tillë si një zjarri, përmbytjesh apo katastrofe të siguruar nga njeriu ose pakujdesia etj.

Vetëm **51.5%** e kompanive u përgjigjën **"Po, kemi një plan vazhdimësie"**. Planifikimi i Vazhdimësisë së Biznesit fokusohet në ruajtjen e funksioneve të biznesit ose rifillimin efikas të tyre në rast të një fatkeqësie të madhe. Një fatkeqësi e madhe mund të jetë çdo gjë nga një përmbytje, zjarr, kriminel keqdashës kibernetik deri në një pandemi. Një plan i vazhdimësisë së biznesit (BCP) përshkruan procedurat që organizata juaj do të ndjekë përballë fatkeqësive të tilla. Ai mbulon strategjinë e komunikimit të krizës, asetet, partnerët e biznesit, burimet njerëzore dhe më shumë.

Si pjesë e këtij dokumentacioni, një biznes vlerëson rreziqet unike për operacionet e tij. Këto rreziqe mund të përfshijnë gjithçka, nga ndërprerjet e TI-së, si humbja e të dhënave, deri te dëmtimet fizike nga fatkeqësitë natyrore. Dokumenti gjithashtu identifikon ndikimin operacional dhe financiar të secilit prej këtyre kërcënimeve, në mënyrë që biznesi të mund të prioritizojë planifikimin e tij të vazhdimësisë në mënyrë të përshtatshme. Dokumenti identifikon sistemet dhe teknologjitë e zbatuara në biznes për të ndihmuar në ruajtjen e vazhdimësisë, të tilla si zgjidhjet rezervë të të dhënave. Në mënyrë thelbësore, ky dokument përshkruan hapat specifikë që duhet të ndërmerren pas çdo lloj fatkeqësie, siç janë procedurat për t'iu përgjigjur një sulmi "ransomware".

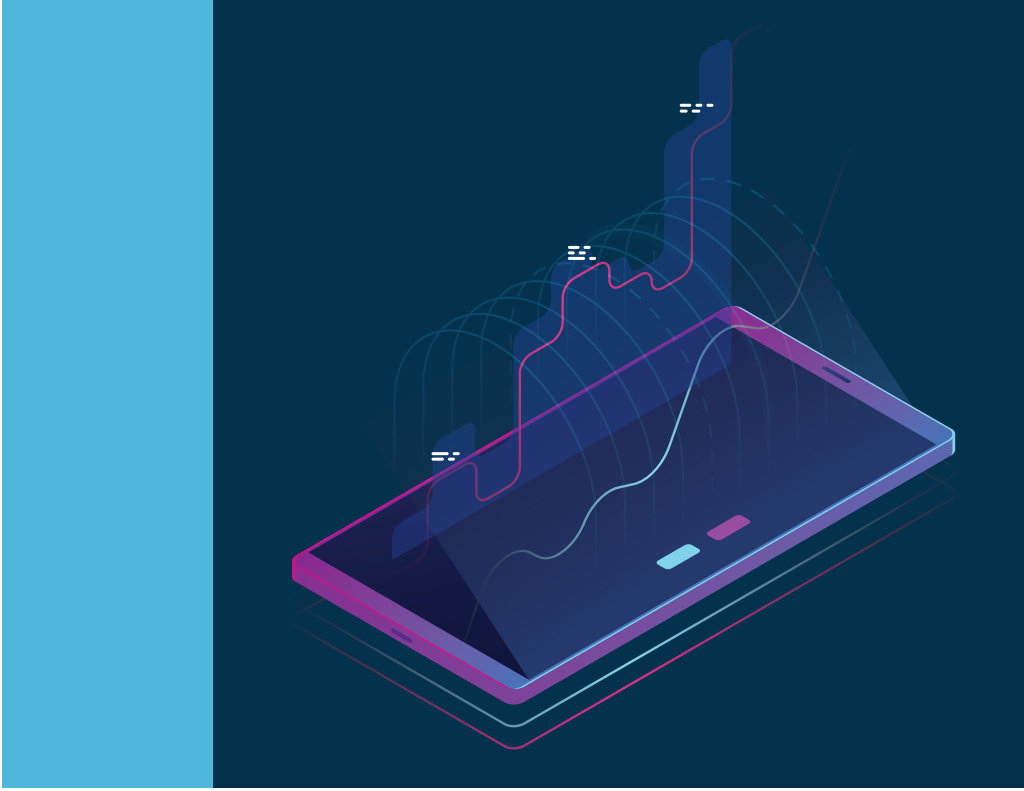
**2.** Masat tuaja të sigurisë janë rishikuar gjatë vitit të fundit.

Vetëm **52.1%** e kompanive u përgjigjën **"Po"**.

Politikat dhe procedurat e sigurisë së informacionit punojnë për të siguruar që organizata po mbron të dhënat e saj në mënyrë efektive. Pa rishikuar politikat e kompanisë, është e pamundur të dalloni nëse po punohet për të minimizuar rrezikun e shkeljeve, për të identifikuar kërcënimet e mundshme, për të dalluar aktivitete të dyshimta dhe për të ofruar një plan veprimi nëse diçka ndodh.

Të paktën një herë në vit duhen rishikuar dhe forcuar politika e sigurisë së informacionit të kompanisë dhe të analizohet efektiviteti i saj në mënyrë që të siguroheni që masat e sigurisë së biznesit po funksionojnë kur nevojitet dhe janë në përputhje me praktikat më të mira të industrisë.

Për industritë me rrezik të lartë si kujdesi shëndetësor, siguria publike dhe shërbimet financiare mund të jetë e nevojshme të rishikohen politikat dhe procedurat e organizatës dy herë në vit.



## SEKSIONI ANALIZA E RRISKUT

Analiza e rreziqeve është një proces i rëndësishëm për identifikimin dhe vlerësimin e rreziqeve të mundshme për një organizatë apo kompani. Në këtë analizë përfshihet identifikimi i potencialit të rreziqeve të sigurisë së informacionit, mbrojtjes së të dhënave dhe sigurisë kibernetike. Duke zhvilluar analiza të rreziqeve në mënyrë periodike dhe dokumentimin e tyre në një mënyrë të kuptueshme, një organizatë mund të marrë masa për eliminimin ose minimizimin e këtyre rreziqeve. Ndaj në pyetësor është një seksion për analizën e rreziqeve.

Disa nga pyetjet në këtë seksion janë:

**1.** Pranë organizatës/kompanisë tuaj realizohen analiza rreziku dhe propozohen masa për eliminimin apo minimizimin e rreziqeve të identifikuara. Kësaj pyetjeje **28.5%** e kompanive u përgjigjën **"Po, gjithmonë"**, ndërsa **24.8%** e kompanive u përgjigjën **"Po, ndonjëherë"**.

Menaxhimi i rrezikut është faza më e rëndësishme në fillimin e çdo projekti të sigurisë së informacionit, pasi ai hedh bazat për sigurinë e informacionit në kompani. Ai përfshin njohjen, analizimin dhe përgjigjen ndaj kërcënimeve ndaj konfidencialitetit, integritetit dhe disponueshmërisë së aseteve të një kompanie.

Vlerësimi i rrezikut (i njohur edhe si analiza e rrezikut) dhe trajtimi i rrezikut janë dy komponentët themelorë të menaxhimit të rrezikut.
Analiza e rrezikut të sigurisë gjen, vlerëson dhe zbaton masa të rëndësishme sigurie. Ai gjithashtu fokusohet në parandalimin e të metave dhe dobësive të sigurisë në aplikacione. Ai ndihmon menaxherët në marrjen e vendimeve të mirëinformuara në lidhje me shpërndarjen e burimeve, mjetet dhe zbatimin e kontrollit të sigurisë. Si rezultat, përfundimi i një vlerësimi është një aspekt i rëndësishëm i strategjisë së menaxhimit të rrezikut të një organizate. Në përgjithësi, analizat e rrezikut kryhen në të gjithë organizatën. Pasi të jetë kryer vlerësimi i rrezikut, kompania duhet të vendosë se si të menaxhojë rreziqet, bazuar në burimet dhe buxhetin e alokuar.

**2.** Analiza e rreziqeve kryhet në mënyrë periodike, dhe dokumentohet në mënyrë të kuptueshme.

Kësaj pyetjeje **33.3%** e kompanive u përgjigjën **"Po, kryhet në mënyrë periodike dhe hartohen raporte"**, ndërsa **13.9%** e kompanive u përgjigjën "Po, kryhet në rast sulmesh kibernetike por nuk raportohet"

Për të garantuar që keni llogaritur ndryshimet në mënyrën se si funksionon organizata juaj, si dhe mjedisin në zhvillim të kërcënimit, do t'ju duhet të përsërisni procesin e vlerësimit çdo vit. Teknikat e zbutjes, përgjegjësitë, buxheti dhe afati kohor duhet të përfshihen të gjitha në strategjinë e vlerësimit të rrezikut.

ISO 27001 detyron kompanitë të regjistrojnë të gjithë procesin e vlerësimit të rrezikut, i cili plotësohet në dokumentin e Metodologjisë së Vlerësimit të Riskut.

## SEKSIONI MENAXHIMI I RREZIKUT KIBERNETIK

Në pyetësor është vendsour dhe një seksion mbi menaxhimin e rrezikut kibernetik duke qënë se pasja e një liste të rreziqeve kryesore kibernetike, trajnimi i stafit, përdorimi i metodologjisë dhe mjeteve për menaxhimin e rreziqeve, si dhe rishikimi i tyre në mënyrë të vazhdueshme, kontribuojnë në ngritjen e nivelit të ndërgjegjësimit mbi sigurinë e informacionit, mbrojtjen e të dhënave dhe sigurisë kibernetike në organizatat dhe kompanitë në Shqipëri. Ekzistenca e një liste të rreziqeve kryesore kibernetike është e rëndësishme për të identifikuar dhe vlerësuar rreziqet e mundshme që një organizatë ose kompani mund të përballet në lidhje me sigurinë e rrjeteve dhe sistemeve të informacionit. Kjo listë ndihmon në identifikimin e kërcënimeve potenciale dhe ndikimin e tyre në sigurinë e informacionit. Për të minimizuar rreziqet kibernetike, personeli kryesor duhet të jetë i ndërgjegjshëm dhe i trajnuar mbi këto rreziqe dhe mënyrat e mbrojtjes. Trajnimi dhe ndërgjegjësimi i stafit ndihmon në identifikimin dhe parandalimin e sulmeve të mundshme dhe sjelljeve rrezikuese. Ekzistenca e një metodologjie dhe mjeteve të specializuara për menaxhimin e rreziqeve kibernetike bazuar në standarde të njohura ndërkombëtare është thelbësore për sigurinë e informacionit. Këto metodologji dhe mjete ndihmojnë në identifikimin, vlerësimin, trajtimin dhe monitorimin e rreziqeve kibernetike për të siguruar që një organizatë ose kompani është e përgatitur për të trajtuar incidente të mundshme. Menaxhimi i rreziqeve kibernetike duhet të jetë një proces i vazhdueshëm. Është e rëndësishme që një organizatë ose kompani të rishikojë në mënyrë të vazhdueshme metodologjinë dhe mjete për menaxhimin e rreziqeve kibernetike për të përshtatur ndaj ndryshimeve të mundshme në mjedisin kibernetik dhe për të forcuar masat e sigurisë.

Disa nga pyetjet në këtë seksion janë:

**1.** Ekziston në organizatën ose kompaninë tuaj një listë e rreziqeve kryesore kibernetike, ndikimit të tyre për sigurinë e rrjeteve dhe sistemeve të informacionit.

Kësaj pyetjeje **34.5%** e kompanive u përgjigjën **"Po, ekziston një listë"**, ndërsa **10.9%** e kompanive u përgjigjën **"Po, ekziston një listë por nuk është përditësuar"**.

Siguria kibernetike është bërë një domosdoshmëri për bizneset e të gjitha madhësive pasi sistemet dhe rrjetet e tyre përmbajnë të dhëna të ndjeshme dhe të vlefshme dhe këto të dhëna mund të vihen në shënjestër nga sulmues keqdashës. Ajo është krijuar për të mbrojtur të gjitha kategoritë e të dhënave nga vjedhja dhe dëmtimi. Krimi kibernetik është një kërcënim në zhvillim për të cilin bizneset moderne duhet të planifikojnë, duke krijuar një qasje dhe procese të krimit kibernetik për të luftuar sulmet si ransomëare, malëare dhe phishing.

Çdo lloj biznesi i vogël apo i madh, pavarësisht nga industria, duhet të jetë i vetëdijshëm për rreziqet e kërcënimeve të sigurisë kibernetike. Kriminelët kibernetikë po modifikojnë vazhdimisht teknikat e tyre, që do të thotë se është e rëndësishme të kesh një plan të sigurisë kibernetike dhe gjithashtu të sigurohuni që punonjësit të jenë të vetëdijshëm për kërcënimet e sigurisë kibernetike dhe të marrin masa paraprake për të mbrojtur veten dhe biznesin. Duhen bërë analiza për të kuptuar dhe përcaktuar kërcënimet kryesore kibernetike që lidhen me aktivitetet e përditshme të kompanisë dhe hartuar programe ndërgjegjësimi trajnimi për punonjësit për tu njohur me etiketën e duhur kibernetike dhe rreziqet e sigurisë.

**2.** Personeli kryesor është i ndërgjegjësuar dhe i trajnuar mbi rreziqet kryesore kibernetike dhe mënyrën se si ato mund të minimizohen.

Vetëm **35.2%** e kompanive u përgjigjën **"Po, trajnohet vazhdimisht"**.

Trajnimi për sigurinë kibernetike është një teknikë e dobishme e ekzekutuar nga ekspertët e IT dhe sigurisë së organizatave moderne për të kontrolluar dhe zbutur rrezikun kibernetik. Këto sesione trajnimi janë krijuar posaçërisht për të qartësuar funksionet dhe detyrat e tyre në ruajtjen e sigurisë së të dhënave.

Një nga përfitimet kryesore të trajnimit të punonjësve për sigurinë kibernetike është rritja e ndërgjegjësimit për kërcënimet e sigurisë kibernetike. Duke edukuar punonjësit mbi kërcënimet më të fundit dhe praktikat më të mira për ruajtjen e informacionit të ndjeshëm, bizneset mund t'i fuqizojnë punonjësit e tyre për të njohur dhe për t'iu përgjigjur sulmeve të mundshme kibernetike. Trajnimi për sigurinë kibernetike gjithashtu mund t'i ndihmojë punonjësit të kuptojnë rëndësinë e fjalëkalimeve të forta, përdorimin e duhur të emailit dhe internetit dhe mbajtjen e softuerit të përditësuar.

3. Pranë organizatës/kompanisë tuaj ka metodologji dhe mjete për menaxhimin e rrezikut kibernetik bazuar në standarde të njohura ndërkombëtare.

Vetëm **30.3%** e kompanive u përgjigjën **"Po, kemi metodologji bazuar në standarde ndërkombëtare"**.

Menaxhimi i rrezikut kibernetik është një proces i domosdoshëm për ruajtjen e sigurisë së informacionit në çdo kompani. Ekzistojnë disa metodologji të disponueshme për menaxhimin e rrezikut, secila me qasjen dhe karakteristikat e veta unike. Zbatimi i kornizave të sigurisë kibernetike kërkon identifikimin e aseteve, vlerësimin e rreziqeve dhe vendosjen e kontrolleve të përshtatshme të sigurisë për të mbrojtur asetet për të siguruar mbrojtjen e mjaftueshme të pajisjeve dhe të dhënave që ato trajtojnë dhe transmetojnë.

ISO/IEC 27001:2022 përqendrohet në menaxhimin e sigurisë së informacionit dhe i jep përparësi identifikimit të aseteve të informacionit, vlerësimit të rreziqeve që lidhen me to dhe zbatimit të masave përkatëse të kontrollit. Një nga avantazhet e ISO/IEC 27001:2022 është qasja e tij e strukturuar dhe e orientuar drejt procesit, e cila lehtëson menaxhimin efektiv dhe efikas të sigurisë së informacionit.

4. Nëse keni metodologji dhe mjete për menaxhimin e rreziqeve a rishikohen ato në mënyrë të vazhdueshme.

Kësaj pyetjeje **26.4%** e kompanive u përgjigjën "**Po, rishikohen vazhdimisht"**, ndërsa **23.9%** e kompanive u përgjigjën **"Po, rishikohen por sipas rastit"**.

Rishikimi dhe përditësimi i vlerësimit dhe menaxhimit të rrezikut është thelbësor për tu siguruar që ai pasqyron me saktësi realitetetin aktual dhe të ardhshëm të mjedisit të biznesit, si dhe përafrimin me qëllimet dhe strategjitë e tij.

Rishikimi në mënyrë të vazhdueshme e metodologjive dhe mjeteve për menaxhimin e rrezikut  mund të ndihmojë kompaninë të monitorojë efektivitetin e kontrolleve  të rrezikut dhe veprimeve zbutëse, të identifikojë rreziqe të reja, të vlerësojë ndikimin e faktorëve të brendshëm dhe të jashtëm në profilin e rrezikut sipas fushës së veprimit, të përmirësojë ndërgjegjësimin dhe kulturën e punonjësve për rrezikun dhe të përmirësojë vendimmarrjen dhe planifikimin duke rritur elasticitetin dhe konkurrencën e kompanisë.

# A#$3A%!@D

## SEKSIONI PËRDORIMI I ENKRIPTIMIT

Përdorimi i enkriptimit për të dhënat gjatë ruajtjes dhe transmetimit tregon gjithashtu kujdesin e organizatës ose kompanisë për të siguruar të dhënat nga aksesi i paautorizuar.

Duke qënë se  një politike  enkriptimi e përshtatshme, përdorimi i enkriptimit gjatë ruajtjes dhe transmetimit të të dhënave, si dhe rishikimi i politikës së enkriptimit në mënyrë të vazhdueshme, ndihmojnë në ngritjen e nivelit të ndërgjegjësimit mbi sigurinë e informacionit, mbrojtjen e të dhënave dhe sigurisë kibernetike në organizatat dhe kompanitë në Shqipëri ne pyetësor u krijua një seksion në lidhje me politikën e enkriptimit. Përdorimi i enkriptimit është një masë e rëndësishme për të siguruar që të dhënat janë të mbrojtura dhe të padëshifrueshme nëse ato vidhen. Një politikë e enkriptimit e hartuar dhe zbatuar pranë një organizatës ose kompanie tregon që ka një përkushtim ndaj sigurisë së informacionit dhe mbrojtjes së të dhënave. Enkriptimi i të dhënave gjatë ruajtjes së tyre nëpër sistemet e organizatës dhe gjatë transmetimit nëpër rrjete të ndryshme ndihmon në parandalimin e aksesit të paautorizuar dhe shpërndarjen e informacionit të padëshifruar nëse ndodh ndonjë incident sigurie. Përditësimi dhe rishikimi i politikës së enkriptimit në mënyrë të vazhdueshme tregon që një organizata është e përgatitur për të përballuar ndryshimet në mjedisin e sigurisë kibernetike dhe për të përshtatur masat e sigurisë sipas nevojave të reja.

Disa nga pyetjet në këtë seksion janë:

**1.** Organizata Ose Kompania juaj zbaton një politikë enkriptimi

Vetëm **39.4%** e kompanive u përgjigjën **"Po"**.

Enkriptimi ka shumë përfitime për shpërndarjen e të dhënave në internet, veçanërisht informacione të ndjeshme. Enkriptimi i të dhënave ndihmon në reduktimin e rrezikut të vjedhjes së identitetit ose mashtrimit. Ai gjithashtu parandalon kriminelët kibernetikë që të vjedhin informacione të ndjeshme personale që u dërgohen në mënyrë elektronike organizatave të tilla si banka ose shitës me pakicë në internet. Uebsajtet e koduara që përdorin HTTPS sigurojnë që njerëzit nuk mund të kenë qasje në informacion kur ato dërgohen nga pajisja juaj në faqen e internetit dhe kthehen përsëri.

Është e rëndësishme që kompania të ketë dhe zbatojë politika enkriptimi, duke i përshtatur sipas fushës së veprimit dhe të dhënave që ka. Nëse kompania mbledh informacione të dhënash personale si: emrat, datat e lindjes ose informacione financiare nga klientët ose klientët, ai informacion duhet të sigurohet pasi nëse ky informacion vidhet ose informacioni rrjedh, kompania mund të mbajë përgjegjësi. Për këto arsye është një praktikë e mirë që të kriptohen të dhënat e ndjeshme.

**2.** Të dhënat enkriptohen gjatë ruajtjes së tyre dhe/ose transmetimit nëpërmjet rrjeteve.

Vetëm **38.7%** e kompanive u përgjigjën **"Po"**.

Të dhënat e gjetura në pajisjet e punës janë shpesh më të prekshmet ndaj shkeljeve që bëhen me të dhënat. Pavarësisht nëse ruhet në laptopë, pajisje të lëvizshme ose telefona celularë, nëse një pajisje vidhet ose humbet, kjo do të thotë që të dhënat mund të aksesohen lehtësisht. Kredencialet e hyrjes në vetvete nuk i mbrojnë të dhënat në kompjuterët e kompanisë nga aksesi pasi ato mund të anashkalohen lehtësisht duke nisur një pajisje duke përdorur një disk USB. Enkriptimi ofron një mënyrë efektive për të mbrojtur të dhënat. Duke koduar hard disqet e kompjuterëve të punës, kompanitë sigurojnë që pavarësisht se si ruhet një pajisje, të huajt nuk do të kenë akses në të dhënat e ruajtura në të pa një çelës deshifrimi.Ka disa mënyra se si enkriptimi ndihmon informacionin që transmetohet online.

- Navigimi në internet: Për të shfletuar internetin në mënyrë të sigurt, sigurohuni që faqet e internetit që vizitoni të kenë HTTPS dhe një ikonë në formë  dryri përpara URL-së, që do të thotë se faqja e internetit është e koduar.
- Kur dërgoni email: Përdorni shërbimet e postës elektronike dhe aplikacionet e mesazheve që ofrojnë enkriptim nga skaji në skaj për të mbajtur të koduar informacionin tuaj nga dërgimi në marrjen e mesazhit.
- Kur përdorni Wi-Fi publik: Rrjetet private virtuale (VPN) janë një mënyrë e shkëlqyer për të mbrojtur informacionin tuaj, veçanërisht kur përdorni Wi-Fi publik.
- Kur dërgoni informacione të ndjeshme: Mos harroni të vlerësoni ndjeshmërinë e të dhënave që dëshironi të ndani për të përcaktuar nëse ato duhet të jenë të koduara. Duhet të përdorni gjithmonë një rrjet personal (Wi-Fi në shtëpi), një VPN dhe aplikacione që mbështesin enkriptimin kur trajtoni informacione të ndjeshme si numri juaj i sigurimeve shoqërore (SIN), informacioni i kartës së kreditit ose informacione të tjera personale.

**3.** Politika e enkriptimit pranë organizatës ose kompanisë tuaj rishikohet në mënyrë të vazhdueshme.

Vetëm **29.4%** e kompanive u përgjigjën **"Po"**.

Enkriptimi është i rëndësishëm në shumë rrethana për të siguruar që informacioni të ruhet në një formë që nuk mund të kuptohet lehtësisht nga individë ose subjekte të paautorizuara. Metodat e enkriptimit duhet të rishikohen rregullisht për t'u siguruar që ato të vazhdojnë të jenë relevante dhe efektive dhe të përdoren aty ku është e nevojshme. Kjo përfshin sigurimin që fushëveprimi i enkriptimit të jetë mjaft i gjerë në mënyrë që sulmuesit të mos kenë akses në një kopje tjetër të paenkriptuar të informacionit tuaj të koduar.

Disa pyetje që mund të bëhen gjatë fazës së rishikimit të politikës së enkriptimit mund të jenë:
Cilat metoda të enkriptimit përdorni? A rishikohen rregullisht për t'u siguruar që janë efektive?
A keni menduar nëse duhet të përdorni enkriptimin e:

- Bazat e të dhënave të përdorura për të ruajtur informacionin personal?
- Serverët?
- Informacioni i ruajtur në serverët cloud të palëve të treta?
- Komunikimet e brendshme të rrjetit, të tilla si posta elektronike ose ndarja e skedarëve?
- Pajisjet celulare të përdoruesit fundor, të tilla si telefonat inteligjentë, tabletët dhe laptopët?
- Pajisje portative ruajtëse?
- Të dhënat në tranzit, për shembull të dhënat e transferuara nëpërmjet internetit?
- Si menaxhohen çelësat e deshifrimit?
- A aktivizoni komunikimet e koduara në faqen tuaj të internetit (për shembull, për kryerjen e pagesave)?
- A ka një kopje tjetër të pakriptuar të të dhënave tuaja të koduara?

## SEKSIONI ZBULIMI I NGJARJEVE TË SIGURISË

Duke qënë se ekzistenca e procedurave të avancuara për zbulimin e incidenteve të sigurisë kibernetike tregon një lidhje të fortë me nivelin e ndërgjegjësimit dhe përkushtimit të organizatave dhe kompanive ndaj sigurisë së informacionit. Kjo ndihmon në forcimin e masave të mbrojtjes së të dhënave dhe në përballjen më efikase me kërcënime kibernetike, duke rritur përgatitjen dhe rezistencën e tyre ndaj sulmeve potenciale.

Disa nga pyetjet në këtë seksion janë:

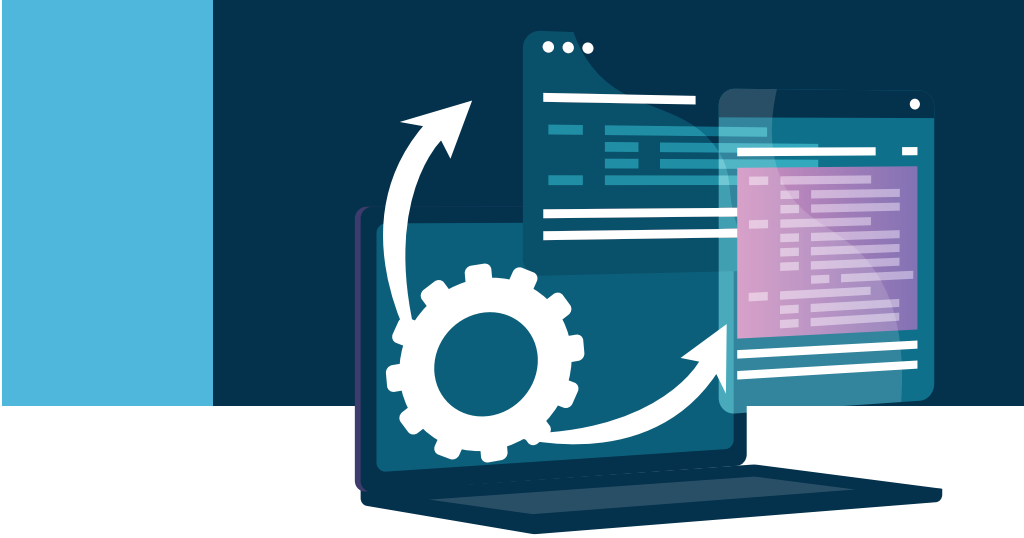
**1.** Organizata ose Kompania juaj ka hartuar dhe zbaton procedura të avancuara për zbulimin e incidenteve të sigurisë kibernetike.

Kësaj pyetjeje **26.1%** e kompanive u përgjigjën **"Po, ekzistojnë procedura të avancuara"**, ndërsa **23%** e kompanive u përgjigjën **"Po, ekzistojnë procedura të thjeshta"**.

Një plan reagimi ndaj incidentit është një grup procedurash të dokumentuara që detajojnë hapat që duhet të ndërmerren në secilën fazë të reagimit ndaj incidentit. Ai duhet të përfshijë udhëzime për rolet dhe përgjegjësitë, planet e komunikimit dhe protokollet e standardizuara të përgjigjes.

Një plan reagimi ndaj incidentit  detajon sa më poshtë:
Çfarë. Cilat kërcënime, shfrytëzime dhe situata kualifikohen si incidente sigurie të zbatueshme dhe çfarë duhet bërë kur ato ndodhin.
Kush. Në rast të një incidenti sigurie, kush është përgjegjës për cilat detyra dhe si mund t'i kontaktojnë të tjerët.

Kur. Në çfarë rrethanash anëtarët e ekipit duhet të kryejnë detyra të caktuara.
Si. Konkretisht se si anëtarët e ekipit duhet t'i kryejnë ato detyra.
Një plan reagimi ndaj incidentit vepron si një hartë e detajuar, autoritative, duke udhëhequr reaguesit nga zbulimi fillestar, vlerësimi dhe klasifikimi i një incidenti deri në kontrollin dhe zgjidhjen e tij.



## SEKSIONI TESTIMI I RRJETEVE DHE SISTEMEVE TË INFORMACIONIT

Testimi i rrjeteve dhe sistemeve të informacionit, rishikimi i politikave dhe procedurave për testimin, dhe ndërgjegjësimi mbi sigurinë e informacionit kontribuojnë në përmirësimin e sigurisë së informacionit dhe mbrojtjen e të dhënave, duke rritur nivelin e ndërgjegjësimit dhe përparimin e organizatave dhe kompanive në Shqipëri përballë kërcënimeve kibernetike  Ndaj në pyetësor u vendos një seksion në lidhje me to. Testimi i rrjeteve dhe sistemeve të informacionit është një praktikë e rëndësishme për të verifikuar se infrastruktura është e sigurt dhe funksionale para se të përdoret në ambientet reale. Siguria e informacionit dhe mbrojtja e të dhënave kërkojnë që politikat dhe procedurat e organizatës të përditësohen rregullisht për të adresuar ndryshimet në kërcënime, teknologji dhe kontekstin e biznesit. Duke rishikuar dhe përditësuar politikat dhe procedurat për testimin, organizata mund të përmirësojë qëndrueshmërinë dhe efikasitetin e masave të sigurisë. Testimi i rrjeteve dhe sistemeve të informacionit, si dhe rishikimi dhe përditësimi i politikave dhe procedurave për testimin, ndihmojnë organizatat dhe kompanitë të jenë më të ndërgjegjshme për rreziqet e mundshme dhe të ndërmarin masa për të rritur sigurinë e informacionit dhe mbrojtjen e të dhënave. Ky ndërgjegjësim mund të jetë thelbësor për të zbatuar një strategji të përshtatshme për sigurinë kibernetike dhe për të minimizuar rreziqet e mundshme të cënimeve të sigurisë.

Disa nga pyetjet në këtë seksion janë:

**1.** Rrjetet dhe sistemet e informacionit përpara përdorimit dhe lidhjes së tyre me sistemet ekzistuese gjithnjë testohen.

Vetëm **57%** e kompanive u përgjigjën **"Po"**.

Përdorimi i sistemeve të informacionit për mbledhjen, ruajtjen dhe referencën e të dhënave personale ka rritur nevojën për të mbrojtur sisteme të tilla nga aksesi dhe përdorimi i paautorizuar. Metodat për mbrojtjen e sistemeve të informacionit përfshijnë verifikimin ose vërtetimin e përdoruesit, kontrollin e aksesit të skedarëve, kontrollet e terminalit dhe monitorimin e rrjetit. Masa të tilla përgjithësisht kontribuojnë si në sigurinë e sistemeve të informacionit ashtu edhe në mbrojtjen e të dhënave personale dhe privatësisë. Testimi i Integrimit të Sistemit, ose SIT, është një proces që përdoret për të siguruar përputhshmërinë e dy ose më shumë sistemeve. Ndihmon për të siguruar që sistemet po punojnë së bashku në mënyrë korrekte dhe se çdo ndërveprim është i përshtatshëm dhe i sigurt. Ky proces mund të përfshijë testimin e softuerit, sistemeve ose rrjeteve. Mund të përfshijë gjithashtu testimin e performancës, integritetit dhe përputhshmërisë së sistemit.

**2.** Rishikohen dhe përditësohen politika ose procedurat për testimin, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.

Vetëm **56.4%** e kompanive u përgjigjën **"Po"**.

Politikat e vjetruara mund ta lënë organizatën në rrezik. Politikat e vjetra mund të dështojnë në përputhje me ligjet dhe rregulloret e reja. Ato mund të mos adresojnë sisteme ose teknologji të reja, gjë që mund të rezultojë në praktika jokonsistente. Prandaj është e nevojshme që të përditësohet politika ose procedurat për testimin duke marrë parasysh jo vetëm ligjet apo teknologjitë e reja por edhe incidentet e mëparshme.

Disa nga pyetjet në këtë seksion janë:

**1.** Cila nga të dhënat e mëposhtëm konsiderohet si e dhënë personale.

Vetëm **64.2%** e kompanive u përgjigjën **"Të gjitha janë të dhëna personale"**.

Sipas Ligjit Nr. 9887, datë 10.03.2008, ndryshuar me ligjin Nr. 48/2012 "PËR MBROJTJEN E TË DHËNAVE PERSONALE" i ndryshuar, neni 3 , pika 1
"Të dhëna personale" është çdo informacion në lidhje me një person fizik, të identifikuar ose të identifikueshëm, direkt ose indirekt, në veçanti duke iu referuar një numri identifikimi ose një a më shumë faktorëve të veçantë për identitetin e tij fizik, fiziologjik, mendor, ekonomik, kulturor apo social."

Për t'u siguruar që të dhënat personale janë të sigurta, është e rëndësishme të dini se cilat të dhëna po përpunohen, pse po përpunohen dhe mbi çfarë bazash. Përveç kësaj, është e rëndësishme të identifikoni se cilat masa sigurie janë në përdorim. E gjithë kjo është e mundur përmes një auditimi të plotë të mbrojtjes së të dhënave, i cili identifikon rrjedhën e të dhënave dhe nëse rregullat për mbrojtjen e të dhënave ndiqen.

**2.** A aplikoni sisteme informacioni për grumbullimin e të dhënave të klientëve.
Vetëm **72.7%** e kompanive u përgjigjën **"Po"**.

Një sistem informacioni për klientët është një aplikacion softuerik që ruan dhe organizon të dhënat e klientit. Përdoret për të gjurmuar ndërveprimet me klientët, për të menaxhuar llogaritë e klientëve dhe për të ruajtur informacionin e klientit. Ky sistem mund të përdoret gjithashtu për të gjeneruar raporte dhe analitika rreth sjelljes dhe tendencave të klientëve. Sistemi i informacionit për klientët është një mjet i vlefshëm për bizneset që duan të përmirësojnë marrëdhëniet me klientët dhe të rrisin shitjet. Mund të ndihmojë bizneset të kuptojnë më mirë klientët e tyre, të identifikojnë nevojat e klientëve dhe të synojnë fushatat e marketingut. Gjithashtu mund të ndihmojë bizneset të gjurmojnë dhe menaxhojnë ankesat dhe reagimet e klientëve.

Të dhënat i ndihmojnë kompanitë të kuptojnë më mirë nevojat dhe dëshirat e klientëve të tyre. Ai shërben si bazë për personalizimin, përmirësimin e shërbimit ndaj klientit dhe krijimin e vlerës së klientit. Ato ndihmojnë për të kuptuar se çfarë funksionon dhe çfarë jo. Ato gjithashtu formojnë bazën për proceset e marketingut të automatizuar dhe të përsëritshëm që ndihmojnë kompanitë të evoluojnë operacionet e tyre.

Kompanitë duhet të kenë mekanizma dhe aplikacione jo vetëm për të mbrojtur informacionin personal, por edhe për të identifikuar, analizuar dhe fshirë ato.

3. Nëse aplikoni sisteme informacioni në grumbullimin e të dhënave, ju lutem specifikoni cilin nga të më poshtimit.

Kësaj pyetjeje kompanitë iu përgjigjën si më poshtë:

- **55.3% e kompanive përdornin MS Excel/Access**
- **34.9% e kompanive përdornin Platforma online fiskalizimi**
- **9.2% e kompanive përdornin Dyqan online, platforma e-commerce**
- **28.3% e kompanive përdornin Sistem menaxhimi Klientësh CRM**
- **9.9% e kompanive përdornin Sisteme menaxhimi të ndërmarrjes ERP**
- **28.9 % e kompanive përdornin Sistemte menaxhimi financiar si psh Financa/Alfa etj.**
- **19.7% e kompanive përdorin Sisteme Cloud**
- **8.4% e kompanive  përdorin sisteme të tjera ose nuk grumbullojnë të dhëna**

Kompanitë  e suksesshme të mëdha dhe të vogla përdorin teknologjitë e disponueshme për të menaxhuar aktivitetet e biznesit dhe për të ndihmuar në marrjen e vendimeve. Ata përdorin sisteme informacioni për të mbledhur të dhëna dhe për t'i përpunuar ato sipas nevojave të analistit, menaxherit ose pronarit të biznesit. Bizneset operojnë në mënyrë më efikase duke përdorur sisteme të ndryshme informacioni për të bashkëvepruar me klientët dhe partnerët, për të ulur kostot dhe për të gjeneruar të ardhura. Ekzistojnë lloje të ndryshme të sistemeve të informacionit, duke përfshirë sistemet e menaxhimit të njohurive, sistemet e mbështetjes ekzekutive, sistemet e ekspertëve, sistemet e kontrollit të procesit dhe sistemet e bashkëpunimit të ndërmarrjeve. Çdo lloj sistemi informacioni ka aplikimet e tij unike dhe mund të ndihmojë në përmirësimin e efikasitetit ose performancës së një organizate.

4. A aplikoni ndonjë standard teknik për mbrojtjen e të dhënave?

Vetëm **57%** e kompanive u përgjigjën **"Po"**.

Standardet e sigurisë janë një grup kriteresh që organizatat mund të ndjekin për të mbrojtur informacionin e ndjeshëm dhe konfidencial. Standarde të ndryshme zhvillohen nga organizata dhe agjenci të ndryshme, si për shembull Organizata Ndërkombëtare për Standardizim (ISO) dhe Instituti Kombëtar i Standardeve dhe Teknologjisë (NIST). Disa nga këto standarde janë të detyrueshme, ndërsa të tjerat janë vullnetare dhe rekomandohen si praktikat më të mira.

Vende dhe rajone të ndryshme kanë grupe të ndryshme ligjesh dhe rregulloresh në lidhje me mbrojtjen e të dhënave, prandaj është e rëndësishme të siguroheni që po i ndiqni ato në përputhje me vendin ku operon biznesi juaj.

5. A keni personel të dedikuar që kujdeset për çështjen e të dhënave personale.

Vetëm **53.3%** e kompanive u përgjigjën **"Po"**.

Gjithnjë e më shumë rregullore sigurie kërkojnë një oficer të përkushtuar sigurie, dhe kjo konsiderohet si një praktikë më e mirë në të gjitha organizatat, përveç organizatave më të vogla. Një ose më shumë persona mund të caktohen si përgjegjës për sigurinë si përgjegjësi kryesore e tyre. Ata punojnë ngushtë me IT-në dhe menaxhimin dhe kanë përgjegjësinë për ndërtimin e një programi të sigurisë së informacionit, si dhe për t'u siguruar që ai të zbatohet.

6. Organizata/Kompania juaj është e regjistruar në regjistrin e subjekteve kontrolluese të cilët kanë njoftuar Komisionerin për Mbrojtjen e të Dhënave personale për përpunimin e të dhënave Personale/sensitive në aktivitetin e saj.

Vetëm **35.2%** e kompanive u përgjigjën **"Po, është e regjistruar"**.

Njoftimi nga subjektet kontrollues është një detyrim ligjor i përcaktuar në nenin 21 të ligjit nr. 9887, datë 10/03/2008, "Për mbrojtjen e të dhënave personale", i ndryshuar. Mospërmbushja e detyrimit për të njoftuar pranë Zyrës së Komisionerit përbën kundërvajtje administrative dhe dënohet me gjobë.

Njoftimi, është një proces me anën e të cilit kontrolluesit e të dhënave personale njoftojnë Zyrën e Komisionerit në lidhje me të dhënat që ata përpunojnë gjatë ushtrimit të veprimtarisë së tyre. Ky informacion i dhënë nga kontrolluesit, i parashtruar gjatë plotësimit të rubrikave të "Formularit të Njoftimit", do të pasqyrohen nga Zyra e Komisionerit në Regjistrin Elektronik të Kontrolluesve i hapur për publikun në faqen zyrtare www.idp.al.

**7.** Organizata/Kompania ka caktuar persona përgjegjës për mbikëqyrjen e zbatimit të ligjit gjatë përpunimit të të dhënave sensitive dhe ka hartuar rregulla të veçanta për të drejtat dhe detyrat e personave të ngarkuar.

Vetëm **47.3%** e kompanive u përgjigjën **"Po"**.

Sipas rregulloreve për mbrojtjen, përpunimin , ruajtjen dhe sigurinë e të dhënave personale të institucioneve të ndryshme të konsideruara si një praktikë më e mirë duhet që në të gjitha organizatat të përcaktohen personat përgjegjës për mbrojtjen e të dhënave të cilët kanë si detyrë të kontrollojnë dhe dokumentojnë aksesin në të dhëna dhe informacione.

## SEKSIONI MBROJTJA E TË DHËNAVE PERSONALE

Nëse organizatat përdorin sisteme informacioni për grumbullimin e të dhënave të klientëve, përdorin standarde teknike për mbrojtjen e të dhënave, kanë personel të dedikuar për të dhenat personale dhe janë të regjistruara në regjistrin e subjekteve kontrolluese, kjo tregon një ndërgjegjësim të mirëfilltë dhe përkujdesje në lidhje me sigurinë e të dhënave personale dhe përmbushjen e detyrimeve ligjore. Ndaj për të vlerësuar nivelin e ndërgjegjësimit mbi sigurinë e informacionit, mbrojtjen e të dhënave dhe sigurinë kibernetike në organizatat dhe kompanitë në Shqipëri, është e rëndësishme të shikohet shtrirja e këtyre praktikave të sigurisë. Seksioni mbrojtja e të dhënave personale është krijuar në pyetësor për këtë arsye.

## Seksioni Compliance

Një ndërgjegjësim i mirëfilltë dhe njohuri të thelluara në fushën e sigurisë kibernetike janë thelbësore për të garantuar sigurinë dhe mbrojtjen e të dhënave dhe infrastrukturës së organizatës ose kompanisë. Ky ndërgjegjësim dhe përvoja mund të ndihmojë organizatën në identifikimin e zonave ku mund të përmirësohet siguria e informacionit dhe mbrojtja e të dhënave personale. Për shembull, nëse është vënë re një rritje e cënimeve të sigurisë, organizata mund të kuptojë se ka nevojë për masat e duhura për të përmirësuar sistemin e sigurisë. Nëse punonjësit janë të vetëdijshëm për kuadrin ligjor kombëtar për mbrojtjen e të dhënave personale, ata do të jenë më të ndërgjegjshëm rreth rregullave dhe detyrimeve për sigurinë e informacionit dhe mbrojtjen e të dhënave personale. Kur stafi merr trajnime në fushën e sigurisë kibernetike dhe merr përgatitje nga Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, ata do të kenë njohuri të përmirësuara dhe të ndërgjegjësuar më shumë rreth praktikave të mira dhe masave të sigurisë. Fakti që siguria e informacionit është një çështje e rëndësishme për të gjitha organizatat, pavarësisht madhësisë, tregon se ndërgjegjësimi për këtë çështje është një prioritet i rëndësishëm për të gjithë.

Disa nga pyetjet në këtë seksion janë:

**1.** Para këtij pyetësori Unë kam qenë i vetëdijshëm ose e vetëdijshme se ka standardet ndërkombëtare të sigurisë së informacionit, në dispozicion për t'u përshtatur nga organizata ose kompania.

Vetëm **64.2%** e kompanive u përgjigjën **"Po"**.

Sektori kibernetik në kohët e sotme është plot me standarde dhe çertifikime të ndryshme që bizneset duhet të arrijnë në lidhje me sigurinë kibernetike dhe sigurinë e informacionit. Këto standarde janë paraqitur për t'u ofruar bizneseve një sërë teknikash, kontrollesh dhe procesesh që ata mund të zbatojnë për të arritur dhe ruajtur një nivel të caktuar sigurie. Zgjedhja për të përdorur një kornizë të caktuar sigurie të IT-së mund të drejtohet nga faktorë të shumtë. Lloji i industrisë ose kërkesat e pajtueshmërisë mund të jenë faktorë vendimtarë.

**2.** Kam dëgjuar për standardet ose direktivat e mëposhtme të sigurisë: Kësaj pyetjeje kompanitë iu përgjigjën si më poshtë:

- **47.3% e kompanive nuk kishin njohuri për asnjë standard**
- **37.6% e kompanive kishin njohuri për standartin GDPR**
- **8.5% e kompanive kishin njohuri për standartin Seria NIST SP 1800**
- **32.1% e kompanive kishin njohuri për standartin ISO/IEC 27000-Series**
- **6.1% e kompanive kishin njohuri për standartin Seria NIST SP 800**
- **8.5% e kompanive kishin njohuri për standartin RFC 2196: Manuali i Sigurisë së Sitit**
- **0.6% e kompanive kishin njohuri për standartin HIPAA**
- **0.6% e kompanive kishin njohuri për mbrojtjen e të dhënave në përgjithësi**

Kompanitë e tregtuara publikisht, për shembull, mund të dëshirojnë të përdorin COBIT për t'u pajtuar me Aktin Sarbanes-Oxley të 2002 i cili është një ligj federal i Shteteve të Bashkuara që mandaton disa praktika në mbajtjen dhe raportimin e të dhënave financiare për korporatat, ndërsa sektori i kujdesit shëndetësor mund të marrë në konsideratë HITRUST. Seria ISO 27000 e kornizave të sigurisë së informacionit, nga ana tjetër, është e zbatueshme në sektorët publikë dhe privatë. Ndërsa standardet ISO shpesh kërkojnë kohë për t'u zbatuar, ato janë të dobishme kur një organizatë duhet të demonstrojë aftësitë e saj të sigurisë së informacionit nëpërmjet certifikimit ISO 27000. NIST Special Publication (SP) 800–53 është standardi i kërkuar nga agjencitë federale të SHBA-së, por ai mund të përdoret nga çdo organizatë për të ndërtuar një plan sigurie informacioni specifik për teknologjinë. GDPR është një kornizë e kërkesave të sigurisë që organizatat globale duhet të zbatojnë për të mbrojtur sigurinë dhe privatësinë e informacionit personal të qytetarëve të BE-së. Akti i Transportueshmërisë dhe Përgjegjshmërisë së Sigurimeve Shëndetësore (HIPAA) përfaqëson standardin për mbrojtjen e të dhënave të pacientëve brenda organizatave të kujdesit shëndetësor, veçanërisht në SHBA. Kërkesa për komente(RFC) është një dokument formal i standardeve i zhvilluar në grupet e punës brenda Task Forcës së Inxhinierisë së Internetit.

**3.** Punonjësit e organizatës/kompanisë përgjegjës për të dhënat personale janë në dijeni të kuadrit ligjor kombëtar për mbrojtjen e të dhënave personale.

Vetëm **67.3%** e kompanive u përgjigjën **"Po"**.

Ligji për mbrojtjen e të dhënave përcakton se çfarë duhet bërë për t'u siguruar që të dhënat e të gjithëve të përdoren siç duhet dhe në mënyrë të drejtë. Prandaj është e rëndësishme që punonjësit e organizatës/kompanisë përgjegjës për të dhënat personale të njihen me kuadrin ligjor në mënyrë që ai të aplikohet sa më mirë.

**4.** Organizata juaj ka pësuar cënimet e mëposhtme të sigurisë në 12 - 18 muajt e fundit.

Pjesa më e madhe e kompanive **73.3%** nuk kanë patur asnjë shkelje te sigurisë të informacionit.

Një shkelje e sigurisë është çdo incident që rezulton në akses të paautorizuar në të dhënat kompjuterike, aplikacionet, rrjetet ose pajisjet. Rezulton në aksesimin e informacionit pa autorizim. Në mënyrë tipike, ndodh kur një ndërhyrës është në gjendje të anashkalojë mekanizmat e sigurisë. Teknikisht, ekziston një dallim midis një shkelje të sigurisë dhe një shkelje të të dhënave. Një shkelje e sigurisë është në mënyrë efektive një depërtim, ndërsa një shkelje e të dhënave përkufizohet si një krim kibernetik që arrin të marrë informacion të paautorizuar.
Disa mënyra për të parandaluar një shkelje të të dhënave:
**1.** Vlerësimet e cenueshmërisë
Organizatat duhet të vlerësojnë rregullisht sistemet e tyre për të identifikuar dobësitë dhe rreziqet që lidhen me to. Këto vlerësime ndihmojnë në përcaktimin nëse politikat e vendosura të sigurisë kërkojnë përditësime, duke forcuar strategjinë e përgjithshme të sigurisë.
**2.** Zbatimi i privilegjit më të vogël
Gjatë zbatimit të një sistemi të menaxhimit të identitetit dhe aksesit (IAM), organizatat duhet të zbatojnë parimin e privilegjit më të vogël për të siguruar që çdo përdorues të ketë vetëm lejet e nevojshme të aksesit. Ruajtja e aksesit me më pak privilegje mund të jetë e ndërlikuar, veçanërisht nëse organizata ka shumë përdorues me role që ndryshojnë vazhdimisht. Megjithatë, ky kontroll sigurie është thelbësor për të siguruar që aktorët me qëllim të keq (të brendshëm ose të jashtëm) nuk mund të kenë akses në të dhënat e ndjeshme.
**3.** Rezervimi dhe rikuperimi i të dhënave
Organizatat duhet të rezervojnë rregullisht të dhënat e tyre dhe të krijojnë një plan rikuperimi për të rivendosur të dhënat e tyre pas një shkeljeje. Një plan rezervë dhe rikuperimi ndihmon për të siguruar një përgjigje më të shpejtë për të minimizuar dëmtimet dhe për të parandaluar ndërprerjen.

Administratorët duhet të rishikojnë rregullisht politikat e menaxhimit të rrezikut, rezervimit dhe rikuperimit për të parandaluar sulmuesit ose ransomëare që të kenë akses në të dhënat rezervë.

**4.**Testimi i penetrimit
Testet e penetrimit janë sulme të simuluara që lejojnë hakerat etikë të identifikojnë dobësitë në sistemet kompjuterike, rrjetet ose aplikacionet. Organizatat mund të përdorin testues të depërtimit të palëve të treta ose të brendshëm për të imituar teknikat e një sulmuesi dhe për të përcaktuar se sa lehtë mund të hakojnë sistemin. Testet e depërtimit janë gjithashtu të dobishme për vlerësimin e pajtueshmërisë me rregulloret e sigurisë. Organizatat përdorin pentestim të rregullt për të identifikuar dobësitë në mënyrë proaktive përpara se një sulmues të mund t'i shfrytëzojë ato.
**5.**Siguria e informacionit është një çështje për të cilën duhet të shqetësohen te gjitha organizatat/kompanitë pavarësisht madhësisë.
84.8% e kompanive u përgjigjën "Po, të gjitha organizatat/kompanitë".
Të dhënat janë një aset i vlefshëm çdo kompani pavarësisht madhësisë së saj. Mbrojtja e saj nga korrupsioni i brendshëm ose i jashtëm dhe aksesi i paligjshëm mbron një kompani nga humbja financiare, dëmtimi i reputacionit dhe humbja e besimit të konsumatorëve. Rregulloret për sigurimin e të dhënave, të vendosura nga qeveria dhe industria dhe standartet e sigurisë e bëjnë të rëndësishme për një kompani që të arrijë dhe të mbajë pajtueshmërinë kudo që ajo bën biznes.
Kompanitë duhet të kenë një plan gjithëpërfshirës të sigurisë së të dhënave. Zbatimi specifik i planit do të varet nga madhësia dhe struktura e sistemeve informatike të organizatës.
**6.**Stafi juaj vazhdimisht ftohet nga Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, të marrë pjesë në aktivitete të ndërgjegjësimit, trajnime në fushën e sigurisë kibernetike.
Kësaj pyetjeje 17% e kompanive u përgjigjën "Po, gjithmonë", ndërsa 15.8% e kompanive u përgjigjën "Po, ndonjëherë". Vihet re se numri i trajnimeve është i vogël pavarësisht nevojave që ka.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) ka përgjegjësinë e mbikëqyrjes së zbatimit të Ligjit Nr.9880/2008 "Për Nënshkrimin Elektronik" , Ligjit Nr.107/2015 "Për Identifikimin Elektronik dhe Shërbimet e Besuara" si dhe Ligji Nr. 2/2017 "Për Sigurinë Kibernetike" dhe të akteve nënligjore të nxjerra në zbatim të tyre.
Disa nga funksionet e AKCESK janë:

- Siguron ndihmë dhe mbështetje metodike për operatorët përgjegjës në fushën e sigurisë kibernetike.
- Kryen aktivitete ndërgjegjësimi dhe edukimi në fushën e sigurisë kibernetike.

Për të realizuar këto funksione AKCESK-u në bashkëpunim me partnerët e saj realizon vazhdimisht fushata ndërgjegjësimi dhe trajnime për rritje kapacitetesh e fokusuar jo vetëm në masat e sigurisë të aplikueshme në infrastrukturat kritike dhe të rëndësishme të informacionit në nivel kombëtar por edhe në trajtimin e kërcënimeve dhe risive në fushën e Sigurisë Kibernetike që afektojnë këto infrastruktura, me qellim rritjen e nivelit të sigurisë në nivel kombëtar.

Prandaj kompanitë duhet të ndërgjegjësohen për rëndësinë e trajnimeve në fushën e sigurisë kibernetike dhe të jenë më pranë kësaj agjensie për të përfituar nga trajnimet, por edhe për të përcjellë problemet që ato kanë në këtë fushë.

## KONKLUZIONE DHE REKOMANDIME

Kompanitë që kanë politika të hartuara për sigurinë e informacionit janë më të përgatitura për kërcënime kibernetike dhe mbrojtjen e të dhënave. Në organizatat ku nuk ka politika të sigurisë të hartuara, ka nevojë për një ndërgjegjësim dhe ndryshim të qëndrimit në lidhje me sigurinë kibernetike. Përcaktimi i roleve dhe përgjegjësive për sigurinë e informacionit është i rëndësishëm për të parandaluar incidente të sigurisë dhe sulmet kibernetike. Ndryshimet janë të vazhdueshme në kërcënime kibernetike dhe në teknologjinë e sigurisë, kështu që politikat dhe procedurat duhet të përditësohen rregullisht. Përfshirja në standarde dhe rregullore të industrisë mund të ndihmojë në përmirësimin e sigurisë dhe në fitimin e besimit të klientëve. Është e rëndësishme që i gjithë stafi të jetë në dijeni të politikave dhe praktikave të sigurisë së informacionit. Trajnimi dhe edukimi i stafit lidhur me sigurinë e informacionit janë të nevojshëm për të përmirësuar kulturën e sigurisë në organizatë si dhe ndihmojnë në ruajtjen e të dhënave, minimizimin e rreziqeve, dhe ruajtjen e besimit të klientëve. Organizatat që nuk kanë politika të hartuara për sigurinë e informacionit duhet t'í zhvillojnë dhe t'í zbatojnë këto politika. Ndërgjegjësimi dhe trajnimi i stafit për këto politika janë thelbësore për sigurinë e informacionit dhe mbrojtjen kibernetike.

Rekomandohet që organizatat dhe kompanitë të investojnë në zhvillimin e politikave dhe procedurave të sigurisë së informacionit, të sigurojnë që i gjithë stafi të jetë në dijeni të tyre dhe të kujdesen për trajnimet e duhura për sigurinë kibernetike. Kjo do të ndihmojë në rritjen e ndërgjegjësimit dhe mbrojtjes së të dhënave në një mjedis kibernetik gjithnjë e më të kërcënueshëm.

Kompanitë që kanë politika të hartuara për sigurinë e informacionit janë më të përgatitura për kërcënime kibernetike dhe mbrojtjen e të dhënave. Në organizatat ku nuk ka politika të sigurisë të hartuara, ka nevojë për një ndërgjegjësim dhe ndryshim të qëndrimit në lidhje me sigurinë kibernetike. Përcaktimi i roleve dhe përgjegjësive për sigurinë e informacionit është i rëndësishëm për të parandaluar incidente të sigurisë dhe sulmet kibernetike. Ndryshimet janë të vazhdueshme në kërcënime kibernetike dhe në teknologjinë e sigurisë, kështu që politikat dhe procedurat duhet të përditësohen rregullisht. Përfshirja në standarde dhe rregullore të industrisë mund të ndihmojë në përmirësimin e sigurisë dhe në fitimin e besimit të klientëve. Është e rëndësishme që i gjithë stafi të jetë në dijeni të politikave dhe praktikave të sigurisë së informacionit. Trajnimi dhe edukimi i stafit lidhur me sigurinë e informacionit janë të nevojshëm për të përmirësuar kulturën e sigurisë në organizatë si dhe ndihmojnë në ruajtjen e të dhënave, minimizimin e rreziqeve, dhe ruajtjen e besimit të klientëve. Organizatat që nuk kanë politika të hartuara për sigurinë e informacionit duhet t'í zhvillojnë dhe t'í zbatojnë këto politika. Ndërgjegjësimi dhe trajnimi i stafit për këto politika janë thelbësore për sigurinë e informacionit dhe mbrojtjen kibernetike.

Rekomandohet që organizatat dhe kompanitë të investojnë në zhvillimin e politikave dhe procedurave të sigurisë së informacionit, të sigurojnë që i gjithë stafi të jetë në dijeni të tyre dhe të kujdesen për trajnimet e duhura për sigurinë kibernetike. Kjo do të ndihmojë në rritjen e ndërgjegjësimit dhe mbrojtjes së të dhënave në një mjedis kibernetik gjithnjë e më të kërcënueshëm.

Një pjesë e konsiderueshme e kompanive nuk ka një anëtar të stafit përgjegjës për sigurinë e informacionit. Një person i tillë është i nevojshëm për të koordinuar dhe implementuar politikat dhe praktikat e sigurisë në të gjitha nivelet e organizatës. Disa kompani nuk konsiderojnë ekspertizën në sigurinë e informacionit si të nevojshme. Në një mjedis ku kërcënimet kibernetike janë të pranishme, ekspertiza për sigurinë e informacionit është jetësore për të adresuar këto sfida. Një pjesë e kompanive nuk ka politika ose procedura të strukturuara për kontratat me palët e treta. Ky është një hap i rëndësishëm për të garantuar që partnerët e tretë trajtohen në mënyrë të sigurt dhe që rreziqet potenciale janë të kufizuara.

Rekomandohet që në të gjitha kompanitë të ketë një anëtar të stafit përgjgjegjës për sigurinë e informacionit. Ky person duhet të ketë ekspertizë dhe të koordinojë të gjitha aspektet e sigurisë së informacionit në organizatë. Kompanitë duhet të investojnë në trajnime dhe konsultim për të rritur ekspertizën e tyre në sigurinë e informacionit. Është e rëndësishme që kompanitë të zhvillojnë dhe të implementojnë politika dhe procedura të strukturuara për kontratat me palët e treta. Kjo do të sigurojë që ndërlidhja me palët e treta të jetë e sigurt dhe e kontrolluar.

Organizatat dhe kompanitë duhet të zhvillojnë një strategji për të identifikuar, gjurmuar dhe lokalizuar të gjitha asetet e tyre, përfshirë softuerin, harduerin, stafin dhe shërbimet. Kjo duhet të përfshijë përdorimin e mjeteve teknologjike të specializuara dhe trajnimin e stafit për të menaxhuar këtë proces. Ato duhet të investojnë në përmirësimin e kontrollit të aksesit ndaj aseteve të informacionit. Kjo përfshin hartimin dhe zbatimin e politikave dhe procedurave të rregulluara për menaxhimin e aksesit, përdorimin e teknologjisë së sigurisë, dhe trajnimin e stafit për të ndjekur praktikat e sigurisë. Organizatat dhe kompanitë duhet të ofrojnë rregullisht trajnime dhe informacion për stafin në lidhje me praktikat e ruajtjes, arkivimit, backup-it dhe shkatërrimit të informacionit. Kjo do të ndihmojë në rritjen e ndërgjegjësimit të tyre për rëndësinë e sigurisë kibernetike. Ato duhet të hartojnë dhe të zbatojnë politika dhe procedura të strukturuara për menaxhimin e aseteve dhe kontrollin e konfigurimit të tyre. Kjo do të ndihmojë në rritjen e sigurisë së aseteve të informacionit dhe në përmbushjen e standardeve të sigurisë dhe ligjore.

Organizatat dhe kompanitë duhet të sigurojnë trajnime të rregullta për stafin në lidhje me praktikat e sigurisë kibernetike. Këto trajnime duhet të përfshijnë masat e sigurisë personale, përdorimin e kompjuterave në mënyrë të sigurt, dhe ndërgjegjësimin për rreziqet e sigurisë kibernetike. Kjo ndihmon në rritjen e ndërgjegjësimit të stafit dhe në parandalimin e incidenteve të sigurisë. Organizatat dhe kompanitë duhet të hartojnë dhe të zbatojnë procese disiplinore të rregullta për punonjësit që shkelin politikat dhe proceset e sigurisë. Këto procese duhet të jenë transparente dhe të ndiqen me kujdes për të forcuar ndërgjegjësimin dhe respektimin e rregullave të sigurisë. Organizatat dhe kompanitë duhet të zbatojnë politika dhe procedura për revokimin e së drejtës së aksesit në rast të ndryshimit të personelit. Ky proces duhet të ndodhë menjëherë pas largimit të personelit për të parandaluar akseset e panevojshme dhe të padëshiruara në informacionin e organizatës.

Siguria fizike dhe mjedisore është një aspekt kritik për sigurinë e informacionit dhe mbrojtjen kibernetike. Politikat dhe procedurat e saj janë thelbësore për të parandaluar rreziqet ndaj mjedisit fizik dhe të sigurojnë integritetin e të dhënave. Organizatat dhe kompanitë duhet të hartojnë dhe të zbatojnë procedura të qarta për sigurinë fizike dhe mjedisore, duke përfshirë politika për aksesin fizik dhe ruajtjen e aktivitetit të vizitorëve. Siguria fizike dhe mjedisore duhet të monitorohet dhe verifikohet rregullisht për të identifikuar dhe adresuar rreziqe potenciale. Serverat duhet të mbahen në ambiente të sigurta me sisteme të kondicionimit të ajrit dhe burime rezervë për energjinë për të siguruar që operacionet të vazhdojnë pa ndërprerje. Organizatat dhe kompanitë duhet të zbatojnë politika të rrepta për aksesin me fjalekalim dhe të hartojnë procese të rregullta për backup dhe ruajtje të kopjeve të të dhënave personale në ambiente të sigurta. Kontrolli i aksesit në sistemet e teknologjisë së informacionit dhe gjurmimi i personave duhet të jetë procedurë e zakonshme dhe duhet të ndiqet rregullorja për mbrojtjen e të dhënave personale. Shkatërrimi i pajisjeve dhe mediave fizike që mbajnë të dhëna personale duhet të bëhet në mënyrë të dokumentuar dhe të sigurt për të parandaluar rreziqe të sigurisë dhe shkeljen e privatësisë. Përmes këtyre masave, organizatat dhe kompanitë mund të përmirësojnë mbrojtjen e informacionit, sigurinë kibernetike dhe integritetin e të dhënave personale. Këto masa gjithashtu ndihmojnë në zbatimin e rregulloreve dhe në zvogëlimin e rreziqeve për pasoja negative që rezultojnë prej shkeljeve të sigurisë.

Shumica e kompanive nuk po ndjekin një plan të strukturuar për përditësimin dhe përmirësimin e sistemeve të tyre, duke rrezikuar sigurinë kibernetike dhe qëndrueshmërinë e operacioneve. Vetëm një përqindje e vogël e kompanive është e sigurt se ata mund të rifillojnë menjëherë aktivitetin pas incidenteve të mundshme. Kjo sjell pasoja si dëme financiare, rënie të produktivitetit, dhe humbje të imazhit të kompanisë. Shumica e kompanive nuk përditësojnë sistemet antivirus në mënyrë të rregullt, duke u ekspozuar ndaj rreziqeve të sigurisë kibernetike dhe infektimit me malware. Organizatat dhe kompanitë duhet të: Hartojnë plane të detajuara të sigurisë për mbrojtjen e të dhënave dhe sigurinë kibernetike. Këto plane duhet të përfshijnë procedura të qarta për kopjet rezervë të të dhënave, monitorimin e përditësimeve të sistemeve, dhe menaxhimin e incidenteve të sigurisë; Sigurohen që të përditësojnë në mënyrë të rregullt sistemet dhe aplikacionet;

Ofrojnë trajnime të rregullta për stafin në lidhje me sigurinë kibernetike dhe rreziqet e mundshme; Identifikonjnë dhe zëvendësojnë pajisjet dhe sistemet e vjetra që janë më të prekshme nga rreziqet kibernetike me teknologji më të përparuara dhe të sigurta; Përcaktojnë procedurat e ndërhyrjes në raste emergjencash dhe identifikojnë personat përgjegjës për veprimet në rast krizash; Përditësojnë sistemet antivirus; Përmirësojnë ndërgjegjësimin e personelit; Sigurohen që të përdorin teknologjitë dhe mjetet e duhura për të bërë backup të të dhënave dhe për të siguruar që informacioni të jetë i arritshëm edhe pas incidenteve;Enkriptimin e të dhënave që ruajnë dhe transmetojnë; Njohjen e kuadrit ligjor mbi të dhënat personale.

Përmirësimi i sigurisë kibernetike dhe mbrojtja e të dhënave janë procese të vazhdueshme, dhe këto rekomandime do të ndihmojnë organizatat dhe kompanitë të përmirësojnë qëndrueshmërinë e tyre ndaj rreziqeve të sigurisë kibernetike.

ASDO
ALBANIA SUSTAINABLE
DEVELOPMENT ORGANIZATION


**Disclaimer**

The opinions expressed in this publication are those of the authors. They do not reflect the opinions or views of the Swiss Agency for Development and Cooperation (SDC)

Supported by:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Ambasada e Zvicrës në Shqipëri**