Rokasgrāmata jaunuzņēmumiem

2024

Co-funded by the European Union

GOOD START

Good Digital Hygiene for Startups

Projekta nr: 2022-1-LV01-KA220-VET-000086725 | Project title: Good Digital Hygiene for Startups

Saturs

1.modulis - Izpratne par digitālās higiēnas definīcijām un jēdzieniem

1. daļa — Digitālās higiēnas konceptuālā sistēma

Strauji mainīgajā digitālās uzņēmējdarbības vidē jaunuzņēmumi saskaras ar neskaitāmiem izaicinājumiem, sākot no sīvas konkurences līdz resursu ierobežojumiem. Ņemot vērā šos izaicinājumus, stabilas digitālās higiēnas prakses nodrošināšana ir būtiska jaunuzņēmumu ilgtspējīgai izaugsmei un panākumiem.

Digitālās higiēnas koncepcija balstās uz vairākiem teorētiskiem ietvariem un principiem no dažādām jomām, tostarp kiberdrošības, informācijas pārvaldības un organizatoriskās uzvedības. Ir dažas galvenās teorijas, uz kurām balstās digitālās higiēnas jēdziens:

1. Kiberdrošības teorija

Kiberdrošības teorija ietver dažādus principus un modeļus, kuru mērķis ir izprast un novērst kiberdraudus un ievainojamību. CIP triāde (konfidencialitāte, integritāte, pieejamība) ir kiberdrošības teorijas pamatkoncepcija, uzsverot, cik svarīgi ir aizsargāt datus no nesankcionētas piekļuves (konfidencialitāte), nodrošināt datu precizitāti un uzticamību (integritāti), kā arī uzturēt datu pieejamību autorizētiem lietotājiem (pieejamība). Citas kiberdrošības teorijas, piemēram, padziļinātās aizsardzības modelis un nulles uzticamības modelis, nodrošina sistēmu stabilu kiberdrošības stratēģiju izstrādei un īstenošanai, lai mazinātu riskus un aizsargātu pret kiberuzbrukumiem.

2. Informācijas pārvaldības teorija

Informācijas pārvaldības teorija koncentrējas uz efektīvu informācijas aktīvu pārvaldību organizācijās. Informācijas dzīves cikla pārvaldības modelis ir teorētisks ietvars, kas apraksta posmus, caur kuriem informācija pāriet no radīšanas līdz iznīcināšanai, uzsverot, cik svarīgi ir pārvaldīt informāciju visā tās dzīves ciklā, lai nodrošinātu konfidencialitāti, integritāti un pieejamību. Datu pārvaldības un datu kvalitātes pārvaldības principi ir arī informācijas pārvaldības teorijas pamatā, vadot, kā organizācijas var efektīvi pārvaldīt un aizsargāt savus datu aktīvus.

3. Cilvēka faktoru teorija

Cilvēka faktoru teorija pēta cilvēka uzvedības, izziņas un lēmumu pieņemšanas lomu kiberdrošības kontekstā. Cilvēka kļūdu teorija liecina, ka cilvēka kļūdas ievērojami veicina kiberdrošības incidentus un datu pārkāpumus, uzsverot apmācības, izpratnes un lietojamības nozīmi ar cilvēku saistīto risku

mazināšanā. Plānotās uzvedības teorija un tehnoloģiju pieņemšanas modelis (TAM) ir citi teorētiskie ietvari, kas izskaidro, kā indivīdu attieksme, uzskati un uztvere ietekmē viņu uzvedību pret kiberdrošības prakses un tehnoloģiju pieņemšanu.

4. Organizatoriskās uzvedības teorija

Organizācijas uzvedības teorija pārbauda, kā indivīdi, grupas un struktūras organizācijās mijiedarbojas un ietekmē uzvedību. Tehnoloģiju-organizācijas-vides sistēma ir teorētisks modelis, kas izskaidro faktorus, kas ietekmē informācijas tehnoloģiju ieviešanu un ieviešanu organizācijās, tostarp tehnoloģiskos faktorus, organizatoriskos faktorus un vides faktorus. Evereta Rodžersa izstrādātā inovāciju teorijas izplatīšana pēta, kā jaunas idejas, tehnoloģijas un prakse izplatās sabiedrībās un organizācijās, sniedzot ieskatu digitālās higiēnas prakses pieņemšanā un izplatīšanā jaunuzņēmumos un citos organizatoriskos kontekstos.

5. Atbilstības teorija

Atbilstības teorija pievēršas faktoriem, kas ietekmē indivīdu un organizāciju atbilstību noteikumiem un normām. Plānotās uzvedības teorija un pamatotas rīcības teorija ir teorētiski modeļi, kas izskaidro indivīdu nodomu ievērot noteikumus, pamatojoties uz viņu attieksmi, subjektīvajām normām un uztverto uzvedības kontroli. Šīs teorijas sniedz ieskatu par to, kā jaunuzņēmumi un organizācijas var veicināt atbilstību kiberdrošības noteikumiem un standartiem, izmantojot izglītību, apmācību, stimulus un izpildes mehānismus.

Tādējādi digitālās higiēnas koncepcija integrē daudznozaru perspektīvas un pieejas, lai risinātu sarežģītos kiberdrošības, informācijas pārvaldības, cilvēku uzvedības un organizatoriskās dinamikas izaicinājumus jaunuzņēmumos un citās organizācijās.

Turklāt papildu koncepcijas nodrošina pamatu digitālās higiēnas prakses izpratnei un ieviešanai jaunuzņēmumos, nodrošinot to digitālās infrastruktūras un darbību aizsardzību, integritāti un noturību:

A) Kiberdrošība

Kiberdrošība ir digitālo sistēmu, tīklu un datu aizsardzības prakse pret nesankcionētu piekļuvi, kiberuzbrukumiem un datu aizsardzības pārkāpumiem. Tas ietver dažādas tehnoloģijas, procesus un praksi, kuru mērķis ir aizsargāt digitālos aktīvus un nodrošināt informācijas konfidencialitāti, integritāti un pieejamību.

B) Datu konfidencialitāte

Datu privātums attiecas uz personiskas un sensitīvas informācijas aizsardzību pret nesankcionētu piekļuvi, izmantošanu vai izpaušanu. Tas ietver atbilstību noteikumiem un standartiem, kas reglamentē datu

vākšanu, glabāšanu un apstrādi, piemēram, GDPR, HIPAA vai CCPA, lai aizsargātu personu tiesības uz privātumu.

C) Riska pārvaldība

Riska pārvaldība ietver tādu risku identificēšanu, novērtēšanu un mazināšanu, kas saistīti ar darbību digitālajā vidē. Tas ietver kontroles pasākumu īstenošanu, lai novērstu, atklātu un reaģētu uz iespējamiem draudiem un ievainojamību, kas varētu ietekmēt jaunuzņēmuma darbību, reputāciju vai finanšu stabilitāti.

D) Atbilstība un tiesiskais regulējums

Atbilstība noteikumiem un nozares standartiem ir būtiska jaunuzņēmumiem, lai nodrošinātu juridiskas un ētiskas darbības. Normatīvie regulējumi, piemēram, GDPR, HIPAA, PCI DSS vai SOX, nodrošina vadlīnijas un prasības attiecībā uz datu aizsardzību, drošību un privātumu, kas jaunuzņēmumiem ir jāievēro, lai izvairītos no juridiskām un finansiālām sekām.

E) Informācijas drošības pārvaldības sistēmas (ISMS)

ISMS ietvari, piemēram, ISO / IEC 27001, nodrošina sistemātisku pieeju informācijas aktīvu pārvaldībai un aizsardzībai organizācijās. Tie ietver politikas, procedūras un kontroles pasākumus risku pārvaldībai, atbilstības nodrošināšanai un pastāvīgai informācijas drošības prakses uzlabošanai.

F) Datu pārvaldība

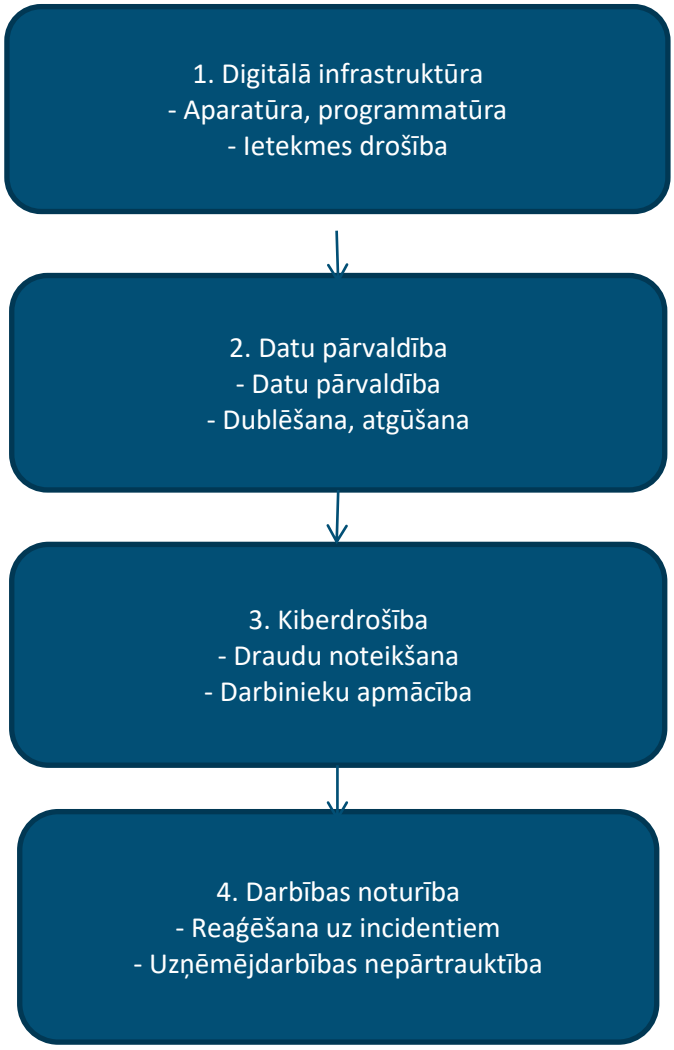
Datu pārvaldība attiecas uz datu aktīvu pārvaldību un pārraudzību organizācijā. Tas ietver politikas, procesu un kontroles izveidi attiecībā uz datu kvalitāti, integritāti un drošību, lai nodrošinātu, ka dati tiek pārvaldīti efektīvi, atbildīgi un ētiski.

G) Reaģēšana uz incidentiem un darbības nepārtrauktības plānošana

Reaģēšana uz incidentiem un darbības nepārtrauktības plānošana ietver sagatavošanos kiberdrošības incidentiem un traucējumiem un reaģēšanu uz tiem. Jaunuzņēmumiem būtu jāizstrādā visaptveroši plāni reaģēšanai uz incidentiem un darbības nepārtrauktības stratēģijas, lai mazinātu kiberuzbrukumu, datu pārkāpumu vai citu traucējumu ietekmi uz to darbību un reputāciju.

Tādējādi digitālā higiēna ietver prakses un protokolu kopumu, kura mērķis ir saglabāt digitālo aktīvu un darbību drošību, efektivitāti un integritāti. Šis konceptuālais ietvars iezīmē galvenās digitālās higiēnas sastāvdaļas, kas pielāgotas jaunuzņēmumu unikālajām vajadzībām un ierobežojumiem.

Jaunuzņēmumu digitālās higiēnas konceptuālā ietvara shēma ir parādīta 1. attēlā.



1.attēls. Digitālās higiēnas konceptuālā ietvara shēma jaunuzņēmumiem

Šajā shēmā ir izklāstīti četri galvenie digitālās higiēnas komponenti jaunuzņēmumiem: digitālā infrastruktūra, datu pārvaldība, kiberdrošība un darbības noturība. Katrs komponents ietver īpašu praksi un protokolus, kuru mērķis ir nodrošināt digitālo aktīvu un darbību drošību, efektivitāti un integritāti starta vidē.

Digitālā infrastruktūra ietver aparatūru, programmatūru un mākoņpakalpojumus, ko jaunuzņēmumi izmanto, lai atbalstītu savu darbību un piegādātu produktus vai pakalpojumus. Tas ietver tādas ierīces kā datori, serveri un tīkla iekārtas, kā arī programmatūras lietojumprogrammas un platformas.

Datu pārvaldība ietver datu aktīvu pārvaldību, glabāšanu un aizsardzību jaunuzņēmumā. Tas ietver datu vākšanu, glabāšanu, izmantošanu un kopīgošanu, kā arī atbilstību normatīvajām prasībām un aizsardzību pret datu aizsardzības pārkāpumiem.

Kiberdrošība ir vērsta uz digitālo aktīvu un operāciju aizsardzību pret kiberdraudiem, piemēram, ļaunprogrammatūru, pikšķerēšanas uzbrukumiem un nesankcionētiem piekļuves mēģinājumiem. Tas ietver proaktīvu pasākumu ieviešanu, lai efektīvi atklātu drošības incidentus, novērstu tos un reaģētu uz tiem.

Darbības noturība ietver darījumdarbības nepārtrauktības un noturības nodrošināšanu revolucionāru notikumu, piemēram, dabas katastrofu, kiberuzbrukumu vai sistēmas kļūmju, gadījumā. Tas ietver plānošanas, sagatavotības un reaģēšanas pasākumus, lai samazinātu dīkstāves laiku un uzturētu kritiskas biznesa funkcijas.

2. attēlā parādīts digitālās higiēnas process un tā faktori jaunuzņēmumu darbībā.

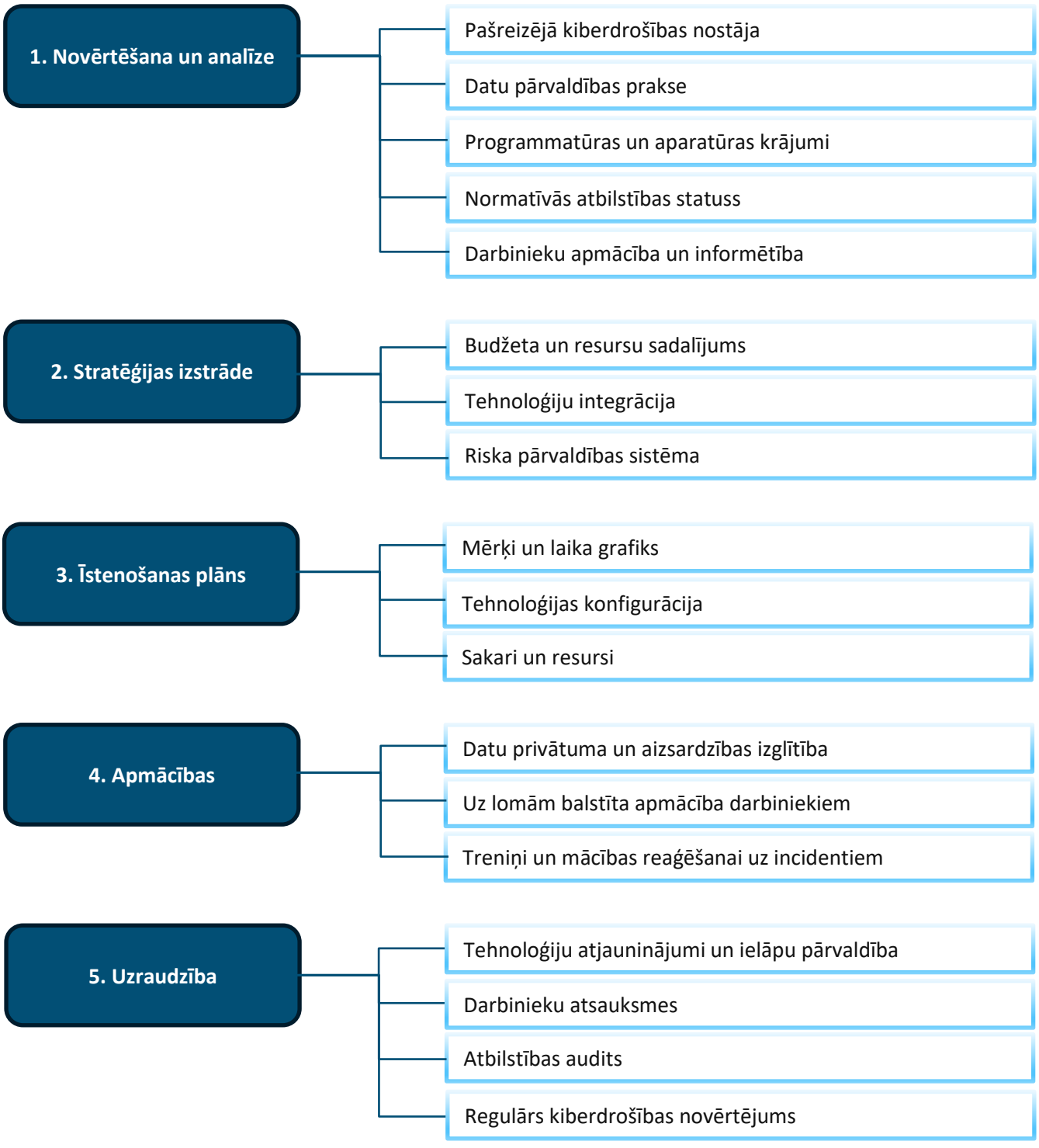
Šis detalizētais attēls ilustrē visaptverošu digitālās higiēnas procesu jaunuzņēmumā, izceļot galvenos faktorus un komponentus katrā posmā, sākot no novērtēšanas un analīzes līdz nepārtrauktai uzraudzībai un uzlabošanai.

Jaunuzņēmums veic rūpīgu savas pašreizējās digitālās prakses un ievainojamības novērtējumu, analizējot iespējamos riskus un draudus savai digitālajai infrastruktūrai un datiem. Pamatojoties uz novērtējuma rezultātiem, jaunuzņēmums izstrādā visaptverošu digitālās higiēnas stratēģiju, kas pielāgota tā vajadzībām un mērķiem, par prioritāti izvirzot uzlabojumu jomas.

Jaunuzņēmums definē skaidrus mērķus un termiņus digitālās higiēnas pasākumu īstenošanai un efektīvai resursu, tostarp budžeta, personāla un tehnoloģiju, sadalei. Jaunuzņēmums nodrošina apmācības un izglītojošus materiālus darbiniekiem par digitālās drošības paraugpraksi, veicinot kiberdrošības izpratnes un atbildības kultūru organizācijā.

Jaunuzņēmums pastāvīgi uzrauga un novērtē savus digitālās higiēnas centienus, veicot regulārus auditus un novērtējumus, lai noteiktu jomas, kurās nepieciešami uzlabojumi un pielāgošanās mainīgajiem draudiem un izaicinājumiem.

Visbeidzot, efektīva digitālās higiēnas prakse ir nepieciešama jaunuzņēmumiem, kas vēlas orientēties sarežģītajā un dinamiskajā digitālās uzņēmējdarbības vidē. Īstenojot šeit izklāstīto konceptuālo satvaru, jaunuzņēmumi var stiprināt savu digitālo infrastruktūru, aizsargāt savus datu aktīvus un uzlabot savu kiberdrošības stāju.



2.attēls. Digitālās higiēnas process un tā faktori startēšanā

2. daļa - Labas digitālās higiēnas vajadzības / pamati jaunuzņēmumiem

Mūsdienu digitālajā laikmetā jaunuzņēmumi lielā mērā paļaujas uz tehnoloģijām, lai veicinātu inovācijas, racionalizētu darbību un sasniegtu klientus. Tomēr līdz ar tehnoloģiju priekšrocībām rodas arī riski, tostarp kiberdraudi, datu aizsardzības pārkāpumi un darbības traucējumi. Lai orientētos šajos izaicinājumos un nodrošinātu ilgtermiņa panākumus, jaunuzņēmumiem par prioritāti ir jānosaka laba digitālās higiēnas prakse.

Laba digitālās higiēnas prakse ietver virkni proaktīvu pasākumu un protokolu, kuru mērķis ir aizsargāt jaunuzņēmuma digitālos aktīvus, infrastruktūru un datus no iespējamiem draudiem, ievainojamības un riskiem.

Labas digitālās higiēnas nepieciešamība jaunuzņēmumiem:

1. Aizsardzība pret kiberdraudiem un uzbrukumiem

Viens no galvenajiem iemesliem labas digitālās higiēnas prakses saglabāšanai ir jaunuzņēmumu aizsardzība pret kiberdraudiem un uzbrukumiem. Laikmetā, kad kibernoziedzība pieaug, jaunuzņēmumi ir galvenie mērķi ļaunprātīgiem dalībniekiem, kas cenšas izmantot savas digitālās infrastruktūras un sistēmu vājās vietas. Kiberuzbrukumiem, piemēram, inficēšanās ar ļaunprogrammatūru, pikšķerēšanas shēmām, izspiedējvīrusu uzbrukumiem un datu aizsardzības pārkāpumiem, var būt postošas sekas jaunuzņēmumiem, tostarp finansiāli zaudējumi, kaitējums reputācijai, juridiskās saistības un darbības traucējumi. Īstenojot stingrus kiberdrošības pasākumus, jaunuzņēmumi var stiprināt savu aizsardzību un mazināt kiberdraudu radītos riskus, aizsargājot savus kritiski svarīgos aktīvus un nodrošinot darbības nepārtrauktību.

2. Sensitīvu datu un intelektuālā īpašuma aizsardzība

Jaunuzņēmumi bieži izmanto sensitīvus datus, tostarp klientu informāciju, patentētas tehnoloģijas, komercnoslēpumus un intelektuālo īpašumu. Labas digitālās higiēnas prakses uzturēšana ir būtiska, lai aizsargātu šo sensitīvo informāciju no nesankcionētas piekļuves, zādzības vai kompromitēšanas. Datu aizsardzības pārkāpumi un neatļauta izpaušana var ne tikai radīt finansiālus zaudējumus un juridiskas saistības, bet arī mazināt klientu uzticību un paļāvību, aptraipot jaunuzņēmuma reputāciju un zīmola tēlu. Ieviešot datu šifrēšanu, piekļuves kontroli un datu zuduma novēršanas pasākumus, jaunuzņēmumi var aizsargāt savus sensitīvos datu aktīvus un saglabāt informācijas konfidencialitāti, integritāti un pieejamību, tādējādi saglabājot klientu, partneru un ieinteresēto personu uzticību.

3. Darbības efektivitātes un produktivitātes uzlabošana

Laba digitālās higiēnas prakse arī palīdz uzlabot darbības efektivitāti un produktivitāti jaunuzņēmumos. Novecojusi programmatūra, neatjaunotas sistēmas un neefektīvas digitālās darbplūsmas var kavēt produktivitāti, kavēt sadarbību un kavēt biznesa izaugsmi. Regulāri uzturot un atjauninot savu digitālo infrastruktūru, jaunuzņēmumi var optimizēt veiktspēju, racionalizēt procesus un novērst vājās vietas, ļaujot darbiniekiem strādāt efektīvāk un lietderīgāk. Turklāt, izmantojot automatizāciju, mākoņtehnoloģijas un digitālos rīkus, jaunuzņēmumi var racionalizēt darbplūsmas, automatizēt ikdienas uzdevumus un uzlabot lēmumu pieņemšanu, veicinot inovāciju un konkurētspēju tirgū.

4. Regulatīvās atbilstības un juridisko pienākumu nodrošināšana

Atbilstība regulatīvajām prasībām un juridiskajiem pienākumiem ir vēl viens būtisks aspekts, lai saglabātu labu digitālās higiēnas praksi. Uz jaunuzņēmumiem, kas darbojas dažādās nozarēs, attiecas neskaitāmi likumi, noteikumi un atbilstības standarti, kas reglamentē datu privātumu, drošību un aizsardzību. Šo noteikumu neievērošana var izraisīt bargus pārkāpumus, naudas sodus un juridiskas sekas, apdraudot jaunuzņēmuma dzīvotspēju un reputāciju. Ievērojot normatīvās prasības, piemēram, GDPR, HIPAA, PCI DSS vai SOX, jaunuzņēmumi var apliecināt savu apņemšanos ievērot ētisku uzņēmējdarbības praksi, iegūt klientu un ieinteresēto personu uzticību un mazināt juridiskos un finanšu riskus.

5. Inovācijas veicināšana

Visbeidzot, labas digitālās higiēnas prakses saglabāšana ir būtiska, lai veicinātu inovāciju un pielāgošanās spēju jaunuzņēmumos. Mūsdienu digitālajā ekonomikā, kur tehnoloģiskie sasniegumi un tirgus traucējumi ir ikdienišķa parādība, jaunuzņēmumiem ir jāsaglabā veiklība, noturība un spēja pielāgoties, lai gūtu panākumus konkurences apstākļos. Izmantojot jaunās tehnoloģijas, pieņemot digitālo transformāciju un izkopjot nepārtrauktas pilnveidošanās un mācīšanās kultūru, jaunuzņēmumi var pozicionēt sevi ilgtermiņa panākumiem un ilgtspējai, veicinot inovāciju un radot vērtību saviem klientiem un ieinteresētajām personām.

Rezumējot, labas digitālās higiēnas prakses uzturēšana ir nepieciešama jaunuzņēmumiem, kas meklē ilgtermiņa panākumus, izaugsmi un noturību.

.

3. daļa - Digitālās higiēnas nozīme

Labas digitālās higiēnas uzturēšanas nozīmi nevar pārvērtēt. Sākot ar sensitīvu datu aizsardzību un beidzot ar kiberdraudu mazināšanu, digitālās higiēnas prakse ir būtiska gan indivīdiem, gan organizācijām. Šajā gadījuma pētījumā mēs pētām digitālās higiēnas nozīmi, izmantojot reālās dzīves piemēru, uzsverot tās ietekmi uz drošību, produktivitāti un vispārējo labklājību.

Lai izprastu digitālās higiēnas nozīmi, apskatiet dažas digitālās higiēnas prakses.

1. Iepazīstieties ar TechGenius, dinamisku jaunuzņēmumu, kas atrodas Silīcija ielejā un specializējas progresīvu programmatūras risinājumu izstrādē uzņēmumiem. TechGenius, kas dibināts 2015. gadā, ātri ieguva ievērību tehnoloģiju nozarē, piesaistot labākos talantus un nodrošinot augsta līmeņa klientus. Tomēr, tā kā uzņēmums paplašināja savu darbību un darbaspēku, tas saskārās ar jauniem izaicinājumiem digitālās infrastruktūras pārvaldībā un digitālo aktīvu aizsardzībā.

TechGenius, tāpat kā daudzi jaunuzņēmumi, darbojās straujā vidē, kur inovācijas un efektivitāte bija vissvarīgākās. Tomēr, ņemot vērā ikdienas darbību kņadu, uzņēmums nevērīgi izturējās pret digitālās higiēnas prakses prioritāti. Darbinieki bieži izmantoja vājas paroles, nespēja regulāri atjaunināt programmatūru un neievēroja pamata drošības protokolus, padarot uzņēmumu neaizsargātu pret kiberdraudiem, piemēram, pikšķerēšanas uzbrukumiem un datu pārkāpumiem.

Apzinoties digitālās higiēnas kritisko nozīmi, TechGenius uzsāka ceļojumu, lai uzlabotu savu pieeju kiberdrošībai un datu pārvaldībai. Uzņēmums uzsāka plašu digitālās higiēnas iniciatīvu, kuras mērķis ir izglītot darbiniekus, ieviest labāko praksi un stiprināt savu drošības stāju.

TechGenius digitālās higiēnas iniciatīva ietvēra vairākus galvenos komponentus:

1. Darbinieku apmācība un informētība. Uzņēmums veica visaptverošas apmācības, lai izglītotu darbiniekus par digitālās higiēnas nozīmi. Apskatītās tēmas ietvēra paroļu pārvaldību, e-pasta drošību, drošas pārlūkošanas praksi un datu aizsardzības noteikumus. Interaktīvos semināros un tiešsaistes moduļos darbinieki ieguva dziļāku izpratni par kiberdrošības riskiem un to lomu tā mazināšanā.

2. Politikas izstrāde un īstenošana. TechGenius izstrādāja stingras digitālās higiēnas politikas un procedūras, lai regulētu darbinieku uzvedību un nodrošinātu atbilstību nozares standartiem. Šīs politikas attiecās uz tādām jomām kā paroļu sarežģītība, programmatūras atjauninājumi, piekļuves vadīklas un incidentu reaģēšanas protokoli. Lai stiprinātu atbildību, uzņēmums ieviesa regulāras revīzijas un izpildes mehānismus, lai uzraudzītu šīs politikas ievērošanu.

3. Tehnoloģiskie risinājumi. Papildus izglītības un politikas pasākumiem TechGenius investēja tehnoloģiskos risinājumos, lai uzlabotu savu digitālās higiēnas praksi. Tas ietvēra daudzfaktoru autentifikācijas, šifrēšanas

tehnoloģiju, galapunktu drošības programmatūras un tīkla uzraudzības rīku ieviešanu. Izmantojot šīs tehnoloģijas, uzņēmums stiprināja savu aizsardzību pret kiberdraudiem un aizsargāja savu digitālo infrastruktūru.

TechGenius digitālās higiēnas iniciatīvas īstenošana deva ievērojamus rezultātus:

A. Uzlabota drošības stāja. Piešķirot prioritāti digitālajai higiēnai, TechGenius nostiprināja savu drošības stāju un samazināja kiberdraudu risku. Tādi incidenti kā pikšķerēšanas uzbrukumi un datu aizsardzības pārkāpumi kļuva retāki, samazinot iespējamo ietekmi uz uzņēmuma darbību un reputāciju.

B. Uzlabota produktivitāte. Tā kā bija mazāk drošības incidentu, ar kuriem jācīnās, darbinieki varēja vairāk koncentrēties uz saviem galvenajiem pienākumiem, kā rezultātā palielinājās produktivitāte un efektivitāte visā organizācijā. Racionalizējot digitālās darbplūsmas un samazinot dīkstāves laiku, TechGenius sasniedza labākus rezultātus un nodrošināja izcilus rezultātus saviem klientiem.

C. Aizsargāta reputācija. Kā uzticams programmatūras risinājumu nodrošinātājs, TechGenius reputācija ir atkarīga no tā spējas aizsargāt klientu datus un uzturēt augstus drošības standartus. Demonstrējot apņemšanos ievērot digitālo higiēnu, uzņēmums izpelnījās klientu uzticību un paļāvību, pozicionējot sevi kā uzticamu partneri arvien konkurētspējīgākā tirgū.

D. Izmaksu ietaupījums. Lai gan ieguldījumi digitālajā higiēnā var radīt sākotnējās izmaksas, ilgtermiņa ieguvumi ievērojami pārsniedz izdevumus. TechGenius piedzīvoja izmaksu ietaupījumus, samazinot kiberdrošības incidentu skaitu, samazinot atbilstības sodus un palielinot darbības efektivitāti. Proaktīvi novēršot drošības ievainojamības, uzņēmums izvairījās no potenciāli dārgām sekām, kas saistītas ar datu pārkāpumiem un normatīvo aktu neievērošanu.

TechGenius gadījums uzsver digitālās higiēnas kritisko nozīmi mūsdienu digitālajā vidē. Piešķirot prioritāti kiberdrošības izglītībai, politikas izstrādei un tehnoloģiskajiem risinājumiem, TechGenius spēja mazināt kiberdraudus, uzlabot produktivitāti un aizsargāt savu reputāciju un rezultātus. Šis reālās dzīves piemērs kalpo kā apliecinājums digitālās higiēnas pārveidojošajam spēkam, aizsargājot organizācijas pret mainīgajiem kiberriskiem un veicinot ilgtspējīgu izaugsmi un panākumus.

Vēl viens digitālās higiēnas prakses nozīmes piemērs ir SecureHealth gadījums.

SecureHealth ir veselības aprūpes tehnoloģiju jaunuzņēmums, kas radikāli maina veidu, kā tiek pārvaldīti medicīniskie ieraksti un kā tiem piekļūst. Izmantojot mākonī balstītu platformu, kas izstrādāta, lai racionalizētu pacientu aprūpi un uzlabotu veselības aprūpes rezultātus, SecureHealth ir ātri ieguvusi pievilcību veselības aprūpes nozarē. Tomēr, strauji augot un ieviešot savu platformu, uzņēmums saskārās ar būtiskiem izaicinājumiem pacientu datu drošības un privātuma nodrošināšanā.

Veselības aprūpes organizācijas ir galvenie kiberuzbrukumu mērķi, jo to apstrādātie dati ir sensitīvi. SecureHealth atzīst digitālās higiēnas izšķirošo nozīmi pacientu konfidencialitātes aizsardzībā un normatīvās atbilstības uzturēšanā. Tomēr, ņemot vērā veselības aprūpes IT sistēmu sarežģītību un pastāvīgi mainīgo apdraudējumu vidi, uzņēmumam ir jāsaglabā modrība un proaktīva kiberdrošības risku novēršana.

SecureHealth izmanto proaktīvu pieeju digitālajai higiēnai, īstenojot visaptverošu kiberdrošības programmu, kas pielāgota veselības aprūpes nozares unikālajām vajadzībām. Uzņēmuma prioritāte ir šādām galvenajām sastāvdaļām:

1. Datu šifrēšana un piekļuves kontrole. SecureHealth šifrē pacientu datus gan miera stāvoklī, gan pārsūtīšanas laikā, nodrošinot, ka sensitīva informācija paliek aizsargāta pret nesankcionētu piekļuvi. Piekļuves kontrole ir ieviesta, lai ierobežotu piekļuvi pacientu ierakstiem tikai pilnvarotiem veselības aprūpes speciālistiem, samazinot datu pārkāpumu risku.

2. Regulāri drošības auditi un ielaušanās testēšana. SecureHealth veic regulārus drošības auditus un ielaušanās testus, lai identificētu ievainojamības savās sistēmās un infrastruktūrā. Proaktīvi identificējot un novēršot drošības trūkumus, uzņēmums stiprina savu aizsardzību pret kiberdraudiem un nodrošina atbilstību veselības aprūpes noteikumiem, piemēram, HIPAA.

3. Darbinieku apmācība un informētība. SecureHealth nodrošina visaptverošu kiberdrošības apmācību visiem darbiniekiem, uzsverot digitālās higiēnas nozīmi pacientu datu aizsardzībā. Darbinieki uzzina, kā atpazīt drošības apdraudējumus un reaģēt uz tiem, ieviest drošu praksi savās ikdienas darbplūsmās un ievērot uzņēmuma politikas un procedūras.

SecureHealth digitālās higiēnas iniciatīvu īstenošana ir devusi taustāmus rezultātus:

A. Aizsargāti pacientu dati. Piešķirot prioritāti digitālajai higiēnai, SecureHealth nodrošina pacientu datu konfidencialitāti, integritāti un pieejamību, veicinot uzticību un paļāvību gan veselības aprūpes sniedzēju, gan pacientu vidū.

B. Atbilstība noteikumiem. SecureHealth uztur atbilstību veselības aprūpes noteikumiem, piemēram, HIPAA, demonstrējot savu apņemšanos aizsargāt pacientu privātumu un ievērot nozares standartus attiecībā uz datu drošību un konfidencialitāti.

C. Samazināts datu aizsardzības pārkāpumu risks. Ieviešot stingrus kiberdrošības pasākumus, SecureHealth samazina datu pārkāpumu un citu drošības incidentu risku, aizsargājot savu reputāciju un samazinot iespējamās finansiālās un juridiskās sekas.

SecureHealth pieredze uzsver digitālās higiēnas izšķirošo nozīmi veselības aprūpes nozarē, kur likmes ir augstas un drošības pārkāpumu sekas var būt smagas. Piešķirot prioritāti kiberdrošības pasākumiem,

piemēram, datu šifrēšanai, piekļuves kontrolei, regulārām revīzijām un darbinieku apmācībai, SecureHealth nodrošina pacientu datu drošību un integritāti, galu galā veicinot pacientu aprūpes un rezultātu uzlabošanos.

Lai izprastu digitālās higiēnas nozīmi, apsveriet iespēju izpētīt papildu digitālās higiēnas praksi.

FinTech Innovations ir jaunuzņēmums, kas grauj finanšu pakalpojumu nozari ar inovatīviem digitālo banku risinājumiem. Izmantojot tādas progresīvas tehnoloģijas kā blokķēde un mākslīgais intelekts, FinTech Innovations piedāvā drošus, lietotājdraudzīgus banku pakalpojumus gan patērētājiem, gan uzņēmumiem. Tomēr, uzņēmumam augot un paplašinot savu klientu bāzi, tas saskaras ar pieaugošiem kiberdrošības riskiem, kas apdraud tā platformas drošību un stabilitāti.

Finanšu iestādes ir galvenie kiberuzbrukumu mērķi, jo to rīcībā ir vērtīgi finanšu dati. FinTech Innovations atzīst digitālās higiēnas nozīmi klientu un partneru uzticības un paļāvības saglabāšanā. Tomēr, ņemot vērā finanšu darījumu sarežģītību un kiberdraudu mainīgo raksturu, uzņēmumam ir jāsaglabā modrība un proaktīva rīcība, aizsargājot savus digitālos aktīvus un infrastruktūru.

FinTech Innovations īsteno spēcīgu digitālās higiēnas programmu, lai novērstu kiberdrošības riskus un aizsargātu savu platformu. Uzņēmums koncentrējas uz šādām galvenajām iniciatīvām:

1. Droša autentifikācija un autorizācija. FinTech Innovations ievieš stingrus autentifikācijas mehānismus, piemēram, biometrisko autentifikāciju un daudzfaktoru autentifikāciju, lai pārbaudītu lietotāju identitāti un novērstu nesankcionētu piekļuvi kontiem un darījumiem.

2. Krāpšanas atklāšana reāllaikā. FinTech Innovations izmanto progresīvus analītikas un mašīnmācīšanās algoritmus, lai reāllaikā atklātu un novērstu krāpnieciskas darbības. Analizējot darījumu modeļus un lietotāju uzvedību, uzņēmums var identificēt aizdomīgas darbības un veikt proaktīvus pasākumus, lai mazinātu krāpšanas riskus.

3. Nepārtraukta uzraudzība. FinTech Innovations turpina nepārtraukti uzraudzīt savas sistēmas un tīklus, lai nekavējoties atklātu drošības incidentus un reaģētu uz tiem. Uzņēmumā strādā īpaša kiberdrošības speciālistu komanda, kas uzrauga aizdomīgas darbības, izmeklē drošības brīdinājumus un īsteno savlaicīgas novēršanas darbības, lai novērstu iespējamos draudus.

FinTech Innovations digitālās higiēnas iniciatīvu īstenošana ir devusi ievērojamus rezultātus:

A. Uzlabota klientu uzticība. Piešķirot prioritāti digitālajai higiēnai, FinTech Innovations apliecina savu apņemšanos aizsargāt klientu datus un finanšu aktīvus, veidojot lietotāju un ieinteresēto personu uzticēšanos un paļāvību.

B. Krāpšanas un drošības incidentu skaita samazināšanās. Izmantojot modernus krāpšanas atklāšanas mehānismus un pastāvīgu uzraudzību, FinTech Innovations samazina krāpšanas un drošības incidentu risku, nodrošinot savas platformas un darījumu drošību un integritāti.

C. Darbības nepārtrauktība un noturība. Proaktīvi novēršot kiberdrošības riskus, FinTech Innovations uzlabo savu noturību pret kiberdraudiem un traucējumiem, nodrošinot nepārtrauktu finanšu pakalpojumu sniegšanu saviem klientiem un partneriem.

FinTech Innovations pieredze uzsver digitālās higiēnas izšķirošo nozīmi finanšu pakalpojumu nozarē, kur drošība un uzticēšanās ir vissvarīgākā. Īstenojot stingrus kiberdrošības pasākumus, piemēram, drošu autentifikāciju, krāpšanas atklāšanu un pastāvīgu uzraudzību, FinTech Innovations nodrošina savas platformas drošību un stabilitāti, galu galā veicinot drošāku un aizsargātāku digitālo banku pieredzi saviem klientiem.

Šie piemēri ilustrē digitālās higiēnas būtisko nozīmi sensitīvu datu aizsardzībā, normatīvās atbilstības uzturēšanā un aizsardzībā pret kiberdraudiem dažādās nozarēs, piemēram, veselības aprūpē un finansēs. Digitālās higiēnas prioritāšu noteikšana ir būtiska organizācijām, kas vēlas mazināt riskus, veidot uzticību un veicināt ilgtspējīgu izaugsmi un panākumus mūsdienu digitālajā vidē.

4. daļa – Labas prakses piemērs no jaunuzņēmumiem

Lai ilustrētu efektīvu draudu identificēšanu un preventīvus pasākumus, mēs iedziļināsimies instancē, uzsverot kiberdrošības apmācību darbiniekiem. Šis piemērs palīdzēs uzsvērt darbinieku izglītošanas izšķirošo nozīmi digitālās drošības pasākumu stiprināšanā.

CyberSec Europe

Apraksts

CyberSec Europe ir kiberdrošības jaunuzņēmums, kas atrodas Berlīnē, Vācijā un specializējas drošības risinājumu nodrošināšanā maziem un vidējiem uzņēmumiem (MVU). CyberSec Europe, kas dibināts 2017. gadā, ātri kļuva par uzticamu kiberdrošības pakalpojumu sniedzēju Eiropas tirgū. Tā kā uzņēmums auga un paplašināja savu klientu bāzi, tas atzina kiberdrošības izglītības kritisko nozīmi saviem darbiniekiem.

Neraugoties uz kvalificētu kiberdrošības speciālistu komandu, CyberSec Europe konstatēja, ka ir jāuzlabo darbinieku informētība par kiberdrošības paraugpraksi. Kiberdraudiem kļūstot arvien sarežģītākiem un pieņemot attālinātā darba režīmu, pieauga drošības incidentu, piemēram, pikšķerēšanas uzbrukumu un datu aizsardzības pārkāpumu, risks. CyberSec Europe saprata, ka darbinieku izglītošana par kiberdrošības riskiem un protokoliem ir būtiska, lai saglabātu savu reputāciju kā uzticams kiberdrošības nodrošinātājs.

Risinājums

CyberSec Europe ieviesa visaptverošu drošības apmācības programmu visiem darbiniekiem, koncentrējoties uz galvenajām jomām, piemēram, draudu noteikšanu, reaģēšanu uz incidentiem un atbilstību datu aizsardzības noteikumiem, piemēram, Vispārīgajai datu aizsardzības regulai (GDPR). Apmācības programma tika izstrādāta tā, lai tā būtu interaktīva, saistoša un pielāgota CyberSec Eiropas darbaspēka īpašajām vajadzībām.

Drošības apmācības programma tika ieviesta visā uzņēmumā trīs mēnešu laikā. Tas sastāvēja no vairākiem darbsemināriem, tīmekļsemināriem un praktiskām mācībām, ko vadīja iekšējie kiberdrošības eksperti un ārējie konsultanti. Apmācību programmā iekļautās tēmas:

- ✓ Pikšķerēšanas e-pasta ziņojumu identificēšana un atbildēšana uz tiem
- ✓ Stipru paroļu izveide un pārvaldība
- ✓ Biežāko kiberuzbrukumu pazīmju atpazīšana
- ✓ Sensitīvu datu aizsardzība un GDPR atbilstības nodrošināšana
- ✓ Ziņošana par drošības incidentiem un incidentu reaģēšanas procedūru ievērošana.

Lai veicinātu līdzdalību un iesaistīšanos, CyberSec Europe stimulēja darbiniekus pabeigt apmācības moduļus un piedāvāja atlīdzību par priekšzīmīgu sniegumu drošības izpratnes mācībās. Uzņēmums arī sniedza

darbiniekiem pastāvīgu atbalstu un resursus, piemēram, piekļuvi kiberdrošības rīkiem un tiešsaistes resursiem.

Regulāru drošības apmācību īstenošana deva pozitīvus rezultātus CyberSec Europe:

1. Paaugstināta drošības izpratne. Darbinieki kļuva modrāki un zinošāki par kiberdrošības riskiem, kā rezultātā samazinājās drošības incidentu un datu pārkāpumu skaits.

2. Uzlabota drošības prakse. Darbinieki pieņēma labāko praksi kiberdrošības jomā, piemēram, izmantoja stipras paroles, šifrēja sensitīvus datus un nekavējoties ziņoja par aizdomīgām darbībām.

3. Uzlabota klientu uzticība. CyberSec Europe apņemšanās nodrošināt izglītošanu kiberdrošības jomā apliecināja tās apņēmību aizsargāt klientu datus un privātumu, vairojot klientu uzticēšanos un uzticamību.

4. Gatavība ievērot atbilstību. Izglītojot darbiniekus par GDPR prasībām un citiem normatīvajiem standartiem, CyberSec Europe uzlaboja savu atbilstības stāju un samazināja regulatīvo sodu risku.

CyberSec Europe proaktīvā pieeja kiberdrošības izglītībai uzsver, cik svarīga ir regulāra drošības apmācība jaunuzņēmumiem Eiropā. Ieguldot darbinieku informētībā un spēcināšanā, CyberSec Europe spēja stiprināt savu kiberdrošības aizsardzību, mazināt riskus un veidot uzticēšanos saviem klientiem. Šis reālās dzīves piemērs uzsver drošības apmācības efektivitāti digitālās higiēnas uzlabošanā un jaunuzņēmumu aizsardzībā pret kiberdraudiem Eiropas tirgū.

Labas digitālās higiēnas prakses nodrošināšana ir būtiska, lai jaunuzņēmumi Eiropā varētu uzplaukt mūsdienu digitālajā vidē. Kiberdraudu, datu pārkāpumu un regulatīvo prasību pieaugošā izplatība uzsver, cik svarīgi ir noteikt prioritātes kiberdrošības, datu aizsardzības un atbilstības nodrošināšanas centieniem. Īstenojot stingrus digitālās higiēnas pasākumus, jaunuzņēmumi var aizsargāt savus digitālos aktīvus, aizsargāt sensitīvus datus un veidot uzticēšanos klientiem, partneriem un ieinteresētajām personām. Tomēr, lai sasniegtu un uzturētu labu digitālo higiēnu, ir vajadzīgi saskaņoti centieni, pastāvīga modrība un apņemšanās veikt pastāvīgus uzlabojumus.

Ieteikumi jaunuzņēmumu digitālās higiēnas uzlabošanai Eiropā

- ✓ Jaunuzņēmumiem ieteicams regulāri novērtēt savu digitālās higiēnas praksi, tostarp kiberdrošības stāju, datu pārvaldības protokolus un normatīvās atbilstības statusu. Tas palīdzēs noteikt vājās vietas, trūkumus un jomas, kurās nepieciešami uzlabojumi.
- ✓ Pamatojoties uz novērtējuma rezultātiem, jaunuzņēmumiem ir ieteicams izstrādāt visaptverošas digitālās higiēnas stratēģijas, kas pielāgotas to īpašajām vajadzībām, mērķiem un riska profiliem. Stratēģijās būtu jāpievēršas tādām svarīgām jomām kā kiberdrošība, datu aizsardzība, atbilstība un reaģēšana uz incidentiem.

✓ Jaunuzņēmumiem ieteicams ieguldīt kiberdrošības tehnoloģijās un risinājumos, lai aizsargātu savu digitālo infrastruktūru no kiberdraudiem, ļaunprogrammatūras un datu aizsardzības pārkāpumiem. Tas var ietvert ugunsmūrus, pretvīrusu programmatūru, šifrēšanas tehnoloģijas un ielaušanās atklāšanas sistēmas.

✓ Jaunuzņēmumiem par prioritāti būtu jānosaka datu aizsardzība un privātums, ieviešot stingrus datu pārvaldības protokolus, tostarp šifrēšanu, piekļuves kontroli un datu dublēšanas un atkopšanas mehānismus. Atbilstība tādiem noteikumiem kā GDPR ir būtiska jaunuzņēmumiem, kas apstrādā personas datus.

✓ Jaunuzņēmumiem ieteicams veicināt darbinieku izpratni un izglītošanu kiberdrošības jomā, lai nodrošinātu, ka viņi izprot iespējamos riskus, paraugpraksi un procedūras labas digitālās higiēnas uzturēšanai. Regulāras apmācības sesijas, izpratnes veicināšanas kampaņas un pikšķerēšanas simulācijas var palīdzēt stiprināt izpratni par kiberdrošību.

✓ Jaunuzņēmumiem būtu jāizstrādā un jāīsteno plāni reaģēšanai uz incidentiem, lai efektīvi reaģētu uz kiberdrošības incidentiem, datu aizsardzības pārkāpumiem vai citām ārkārtas situācijām. Plānos būtu jāizklāsta uzdevumi, pienākumi un procedūras incidentu atklāšanai, ierobežošanai un mazināšanai.

✓ Pastāvīga uzraudzība un novērtēšana ir būtiska, lai uzturētu labu digitālo higiēnu. Jaunuzņēmumiem ieteicams regulāri novērtēt savu digitālās higiēnas pasākumu efektivitāti, veikt revīzijas un pārskatus, kā arī veikt nepieciešamos pielāgojumus, lai novērstu jaunus draudus un problēmas.

✓ Jaunuzņēmumiem vajadzētu būt informētiem par jaunākajiem kiberdrošības draudiem, tendencēm un noteikumiem, kas ietekmē viņu nozari. Regulāra kiberdrošības ziņu uzraudzība, dalība nozares forumos un sadarbība ar kiberdrošības profesionāļiem var palīdzēt jaunuzņēmumiem apsteigt mainīgos draudus un riskus.

Apkopojot var teikt, ka digitālās higiēnas prakses uzlabošana ir būtiska jaunuzņēmumiem Eiropā, lai aizsargātu savus digitālos aktīvus, mazinātu riskus un saglabātu ieinteresēto personu uzticēšanos. Īstenojot visaptverošas stratēģijas, investējot kiberdrošības tehnoloģijās, veicinot informētību un pastāvīgi uzraugot mainīgos draudus un pielāgojoties tiem, jaunuzņēmumi var stiprināt savu digitālo noturību un attīstīties konkurences apstākļos.

Galvenās atziņas

- Jaunuzņēmumiem ieteicams par prioritāti noteikt kiberdrošības izglītību saviem darbiniekiem, lai veidotu izpratni un dotu viņiem iespēju efektīvi atpazīt kiberdraudus un reaģēt uz tiem. Apmācības programmām jāaptver tādas tēmas kā pikšķerēšanas izpratne, paroļu pārvaldība un incidentu reaģēšanas protokoli.
- Stingras digitālās higiēnas politikas un procedūru izveide ir būtiska, lai veicinātu kiberdrošības kultūru jaunuzņēmumos. Ieteicams izstrādāt politikas, kas attiecas uz tādām jomām kā paroļu sarežģītība, programmatūras atjauninājumi, piekļuves kontrole un datu aizsardzības noteikumi.
- Regulāras revīzijas un izpildes mehānismi palīdz nodrošināt atbilstību un pārskatatbildību jaunuzņēmumos. Ir ieteicams veikt regulāras revīzijas un īstenot izpildes mehānismus, lai uzraudzītu digitālās higiēnas politikas un procedūru ievērošanu.
- Jaunuzņēmumiem būtu jāiegulda tehnoloģiskos risinājumos, lai uzlabotu savu digitālās higiēnas praksi. Tas ietver kiberdrošības rīku, piemēram, daudzfaktoru autentifikācijas, šifrēšanas tehnoloģiju, galiekārtu drošības programmatūras un tīkla uzraudzības rīku, izmantošanu, lai stiprinātu aizsardzību pret kiberdraudiem.
- Atbilstība normatīvajām prasībām un nozares standartiem ir būtiska, lai jaunuzņēmumi varētu apliecināt savu apņemšanos īstenot ētisku uzņēmējdarbības praksi un aizsargāties pret juridiskām un finansiālām sekām. Jaunuzņēmumiem ir jāievēro tādi noteikumi kā GDPR, HIPAA, PCI DSS vai SOX, lai aizsargātu datu privātumu, drošību un integritāti.
- Digitālās higiēnas koncepcijā ir integrētas atziņas no dažādām disciplīnām, tostarp kiberdrošības, informācijas pārvaldības, cilvēka faktoriem, organizācijas uzvedības un atbilstības teorijas. Izmantojot šīs perspektīvas, jaunuzņēmumi var izstrādāt pieejas, lai efektīvi risinātu sarežģītās kiberdrošības un datu aizsardzības problēmas.

Atsauksmes

1. CyberSec Europe https://www.cyberseceurope.com/
2. FinTech Innovations https://www.fintechinnovation.no/
3. Ncubukezi T., Mwansa L. Best Practices Used by Businesses to Maintain Good Cyber Hygiene During Covid-19 Pandemic. Journal of Internet Technology and Secured Transactions (JITST), Volume 9, Issue 1, 2021.
4. SecureHealth https://www.shpg.com/
5. TechGenius https://techgenius.co.in/
6. Vishwanath A., Seng Neo L., Goh P., Lee S., Khader M., Ong G., Chin. J. Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, Volume 128, 2020, https://doi.org/10.1016/j.dss.2019.113160.
7. Yegen, C., Kirik, A.M., Çetinkaya, A. (2023). Sustainability, Digital Security, and Cyber Hygiene During the Covid-19 Pandemic. In: Mondal, S.R., Yegen, C., Das, S. (eds) New Normal in Digital Enterprises. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-19-8618-5_5

2.modulis - Digitālās higiēnas rīki un integrācija ikdienas rutīnā

1. daļa- Labākie digitālās higiēnas rīki jaunuzņēmumiem

Savstarpēji saistīta pasaule rada plašāku un sarežģītāku digitālo draudu riskus. Tāpēc svarīgāk nekā jebkad agrāk ir tas, lai jaunuzņēmumi piešķirtu būtisku nozīmi kiberdrošībai, lai aizsargātu savus vērtīgos aktīvus un konfidenciālu informāciju. Šajā nodaļā jūs uzzināsiet par dažām galvenajām stratēģijām un praksēm, kuras jaunuzņēmumiem vajadzētu censties īstenot, lai uzlabotu savu drošību tiešsaistē. Tas svārstās no spēcīgu paroļu izveides līdz rūpīgu datu dublēšanas risinājumu ieviešanai. Šī rokasgrāmata sniegs jums zināšanas un rīkus, kas jaunuzņēmumiem jāzina, lai saglabātu drošību tiešsaistē. Šī nodaļa iepazīstinās jūs ar galvenajiem principiem un sniegs virkni ieteikumu, kas palīdzēs jums izveidot spēcīgu pamatu jūsu digitālās higiēnas stratēģijai, kā arī efektīvi aizsargāt savus digitālos aktīvus.

Labas paroļu higiēnas uzturēšana: pamati

Ticketmaster tika iesūdzēts tiesā 2021. gada janvārī par konkurējoša uzņēmuma datorsistēmu uzlaušanu pēc tam, kad konkurējošā uzņēmuma bijušais darbinieks izmantoja savus akreditācijas datus, lai ļautu Ticketmaster slepeni piekļūt konkurenta datoriem. ASV advokāta pienākumu izpildītājs DuCharme paziņoja, ka "Ticketmaster darbinieki vairākkārt ir nelikumīgi piekļuvuši konkurenta datoriem bez atļaujas, lai nozagtu biznesa zināšanas, izmantojot nelikumīgi iegūtas paroles". Šis gadījums noveda pie tā, ka Ticketmaster tika piemērots naudas sods 10 miljonu ASV dolāru apmērā saskaņā ar Datoru krāpšanas un ļaunprātīgas izmantošanas likuma noteikumiem (Jones, 2022). Google Cloud 2023. gada Threat Horizons ziņojumā norādīts, ka 86% drošības pārkāpumu ietver zagtu akreditācijas datu izmantošanu, un akreditācijas datu problēmas ir atbildīgas par vairāk nekā 60% no pārkāpumu pamatcēloņiem - problēmām, kuras varētu palīdzēt atrisināt spēcīgāki organizācijas identitātes pārvaldības flangi.

Saskaņā ar (Keszthely, 2013) kāda cita paroles ņemšanas aktu, tā var tikt pabeigta četros pamata veidos:

1- Noklusējuma vārdi: Datoros un lietojumprogrammās ir iebūvētas noklusējuma paroles. Datoru un kontu paroles var būt anulētas vai daļa no atsevišķas bieži lietotu vārdu kopas, piemēram, "123456", "asdfgh" un "parole".

2- Savienojums starp pieteikšanās vārdu un parolēm: Paroles uzminēšana vai loģika ir tad, kad uzbrucēji veltīs laiku, lai sistemātiski uzminētu lietotājvārdu un paroli. Lietotājs var pat palīdzēt uzbrucējam uzminēt lietotājvārdu un paroli. Daži piemēri ir "parole", "login-login", "qwerty" un "letmein".

3- Vārdnīcas metode: Hakeri apkopos dažas vispārīgas paroles un atlasīs tās no saraksta. Viņi tās lejupielādēs pa vienam, jo rīki darbojas bezsaistē, un, visticamāk, gūs panākumus, ja tie darbosies lēnāk. Turklāt viņiem joprojām būs iespēja pārbaudīt katru sadaļu bez interneta savienojuma.

Lai izvairītos no zaudējumiem, ko izraisa paroļu zādzība, ir jāpiešķir prioritāte spēcīgu, drošu paroļu izvēlei. (Kato & Klyuev, 2013) Tiek ieteikti daži padomi spēcīgu paroļu izveidei:

- **Izmantojiet lielos burtus un pieturzīmes**: Izmantojiet lielos burtus un pieturzīmes, lai izveidotu spēcīgāku paroli.
- **Sajauciet to:** Integrējiet gan burtus, gan ciparus, lai ģenerētu drošākas paroles.
- **Izvairieties no vispārīgas informācijas**: Atturieties no viegli uzminamu vārdu un personiskās informācijas izmantošanas parolēs.
- **Apsveriet garākas paroles:** Tiecieties pēc garākām parolēm, kuras jums ir viegli atcerēties.
- **Izmantojiet paroļu pārvaldniekus**: Izmantojiet programmas, kas ir paredzētas drošai paroļu glabāšanai, piemēram, LastPass.
- **Unikālas paroles**: Formulējiet dažādas paroles dažādiem kontiem.

Papildus drošu paroļu paradumu praktizēšanai kā indivīdam, tā uzņēmumiem ir jāievieš politika, kas vērsta uz paroļu drošības uzlabošanu. (Inglesant & Sasse, 2010) Ierosina, ka organizācijas līmenī paroles vadlīnijām vajadzētu koncentrēties uz lietotāju. Vadlīnijām jāatspoguļo lietotāju unikālās prasības un prasmes ikdienas darbā. Organizācijas var maksimāli palielināt drošību, vienlaikus stiprinot lietotāju efektivitāti un lietderību paroļu pārvaldībā, ievērojot cilvēka un datora mijiedarbības principus un uzskaitot konkrētu lietojumu. Turklāt uzņēmumiem jācenšas analizēt un piemērot stingrus paroļu izveides standartus, izmantojot jaunas paroļu metodes un ierīces, piemēram, Telepathwords. Turklāt uzņēmumiem noteikti jāpalīdz darbiniekiem preventīvi izmantot vājas vai ietekmētas paroles. Izmantojot šīs metodes, tās ievērojami uzlabos drošību (Blocki & Liu, 2023).

Vital İnfrastructure aizsardzība ar divfaktoru autentifikāciju

Divfaktoru autentifikācija (2FA) ir drošības pasākums, kas pieprasa lietotājiem nodrošināt sekundāro komponentu lietotāja apstiprināšanai. Šī metode paroles autentifikācijas sistēmai pievieno autentifikācijas faktoru. Ir dažas priekšrocības, kas novērtēšanas platformai būtu, ieviešot 2FA (Tellini & Vargas, 2017):

- **Nesankcionētas piekļuves iespējas novēršana**: 2FA pārsniedz tikai lietotājvārda un paroles izmantošanu. Tā autentifikācijai izmanto pilnīgi atsevišķu sistēmu.
- **Aizsardzība pret paroles zādzību:** Lietotājvārdi un paroles tiek nozagtas katru dienu. Izmantojot 2FA, uzbrucējam būtu nepieciešams vairāk nekā tikai lietotāja vārds un paroles akreditācijas dati, lai iegūtu nelikumīgu piekļuvi.
- **Samazināts nesankcionētas piekļuves risks**: Izmantojot 2FA, neautorizēta vai nepierādīta piekļuve ir mazāk iespējama papildu autentifikācijas slāņa dēļ, kas hakerim būtu nepieciešams, lai pabeigtu piekļuvi kontam, un viņam būtu nepieciešams lietotāja tālrunis vai tālrunī ģenerēts kods.
- **Paaugstināta lietotāju uzticība:** Uzticēšanās un ticība platformai var palielināties, ja lietotāji zina, ka viņu konts ir aizsargāts ne tikai ar paroli.

- **Atbilstība drošības standartiem:** Izmantojot 2FA, jūsu pieteikšanās var atbilst tiešsaistes drošības paraugpraksei, un to var pieprasīt īpaši noteikumi vai standarti jūsu nozarē.
- **Biežāk sastopamo paroļu problēmu mazināšana:** 2FA palīdz mazināt bieži sastopamas paroļu problēmas, piemēram, sliktu paroļu izvēli un atkārtotu izmantošanu. Samazinot paļaušanos uz vienu paroli, 2FA var palīdzēt mums izmantot sarežģītākas paroles.

2FA ir divpakāpju verifikācijas process, kurā lietotājiem pirms piekļuves piešķiršanas galalietotājam ir jānodrošina divu dažādu veidu autentifikācijas faktori. Trīs veidu faktori ir kaut kas, ko lietotājs zina (zināšanu faktors), kaut kas, kas lietotājam ir (valdījuma faktors), un kaut kas, kas ir lietotājs (neatņemamas īpašības faktors). (De Cristofaro, Du, Freidigers, & Norcie, 2013). Divfaktoru autentifikācijas metode padara uz paroli centrētas autentifikācijas metodes drošākas. Pakalpojumi var izmantot dinamiskas faktoru kombinācijas, lai ievērojami palielinātu lietotāju akreditācijas datu pārliecību, kvantificējot riskus un ieguvumus (Han, Sun, Shen, Chang, & Shen, 2013).

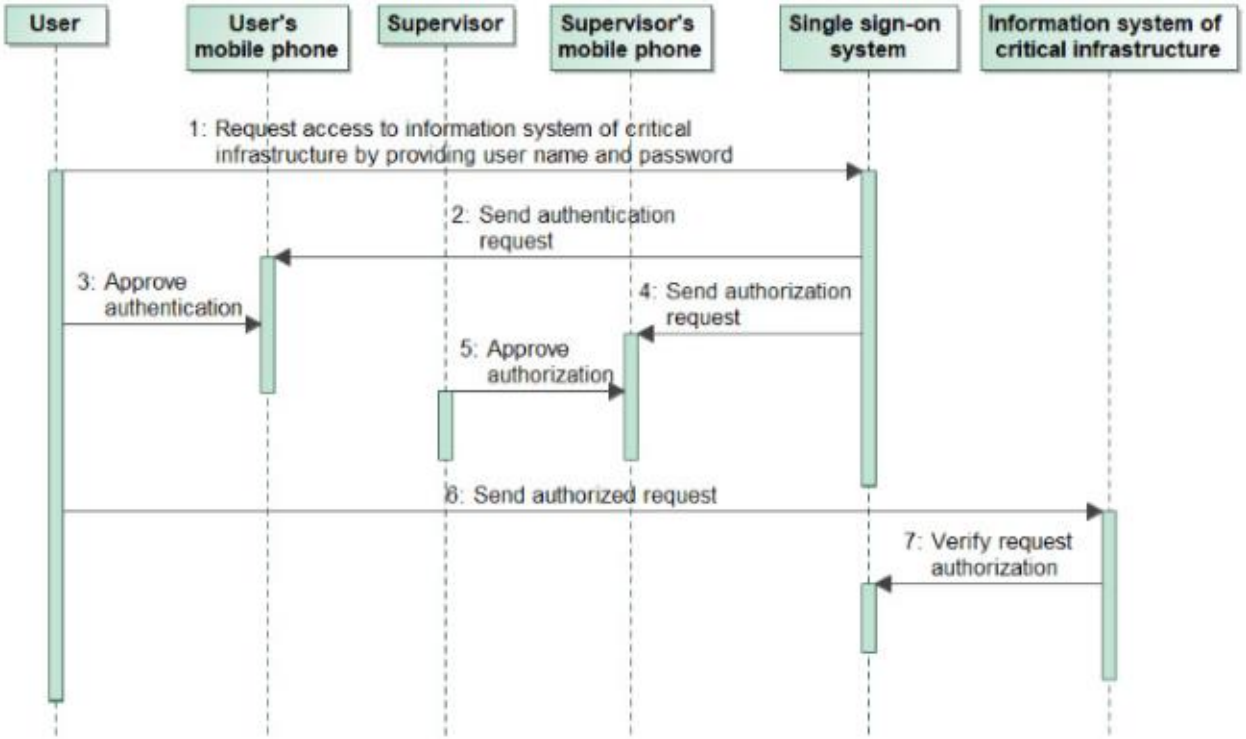
Class type	Class description	Examples
Knowledge	Something known	Password Key phrase Secret question Personal question
Possession	Something held	One time password generator Grid token Smart card
Inherence (biometrics)	Something about the person	Fingerprint scan Iris scan Voice recognition

1.tabula: Dažas autentifikācijas faktoru klases

Avots : (Pearce, Zeadally, & Hunt, 2010).

(Bruzgiene & Jurgilas, 2019) nodrošina autentifikācijas metodi, kas darbojas trīs soļu procesā, lai nodrošinātu attālinātu piekļuvi kritiskās infrastruktūras informācijas sistēmām. Pirmkārt, lietotājs ievada savu konta ID un paroli. Kad ir ievadīta pareizā informācija, uz lietotāja mobilo ierīci tiks nosūtīts vietējās drošības iestādes (LSA) autentifikācijas pieprasījums. Tad lietotājam ir jāapstiprina pieprasījums ar vienu pieskārienu tālruņa ekrānam; tas ļaus mobilajai ierīcei nosūtīt autorizācijas pieprasījumu lietotāja vadītājam(-iem), lai noteiktu piekļuves tiesību līmeni attālajai sistēmai. Kad projekta vadītājs(-i) ir veiksmīgi apstiprinājis lietotāja pieprasījumu, pieprasītājam lietotājam tiek piešķirtas piekļuves tiesības attālajai sistēmai.

1.attēls: Piedāvātā autentifikācijas metode: (Bruzgiene & Jurgilas, 2019)



Avots : (Bruzgiene & Jurgilas, 2019)

Savlaicīgi programmatūras atjauninājumi: sistēmas drošības stiprināšana

Programmatūras atjauninājumi ir ļoti svarīgi, jo tie novērš kļūdas vai uzlabo programmatūras, piemēram, draiveru un operētājsistēmu, veiktspēju (Mathur, Malkin, Harbach, Péer, & Egelman, 2018). Atjauninot programmatūru, jūs nodrošināt, ka tā ir saderīga ar citām programmatūras un aparatūras sistēmām, un gādājat par savu sistēmu drošību un aizsardzību, palaižot jaunāko programmatūras versiju. Atjauninājumi ietver drošības atjauninājumus, kas nepieciešami, lai aizsargātu datoru no ļaunprātīgas programmatūras un ievainojamības, līdzekļu atjauninājumus, kuru nopietnība ir dažāda, jo tie var ietvert jebko, sākot no nelieliem kļūdu labojumiem līdz būtiskām darbplūsmas izmaiņām, un kumulatīvo atjauninājumu, kas prasa instalēt visus iepriekšējos atjauninājumus pirms jaunākā atjauninājuma sasniegšanas (Vaniea, Raders, & Wash, 2014). Šie uzlabojumi palīdz uzturēt programmatūras sistēmu drošību un funkcionalitāti. Šī iemesla dēļ ir svarīgi pārliecināties, ka esat informēts par visiem nepieciešamajiem atjauninājumiem.

Tomēr daudzi lietotāji mēdz izvairīties no savas programmatūras atjaunināšanas vairāku faktoru dēļ. Šie faktori ietver atjaunināšanas izmaksas, piemēram, laiku, kas nepieciešams instalēšanai, nepieciešamību pēc pārstartēšanas un izmantotās diska vietas; atjauninājuma nepieciešamību, ieskaitot lietotāja apmierinātību

ar pašreizējo sistēmu, atjauninājuma iemeslu skaidrību un atjauninājuma nozīmīgumu, kā to uztver lietotājs; un atjaunināšanas risku, kas ietver bažas par datu zudumu atjaunināšanas laikā un iespēju, ka jebkurš atjauninājums varētu saturēt kādu vīrusu vai ļaunprātīgu programmatūru, kas varētu padarīt sistēmu ievainojamu (Mathur, Malkin, Harbach, Péer, & Egelman, 2018). Programmatūras neatjaunināšana var padarīt datoru sistēmas uzņēmīgas pret hakeru darbībām, kuri varētu mēģināt inficēt datorus ar jauniem vīrusiem. Tas var arī radīt nopietnas sekas jūsu datoriem. Ne tikai neaizsargātas drošības nepilnības padarīs sistēmu mazāk drošu, bet tās arī ir iemesls, kāpēc lielākā daļa vīrusu ir tik veiksmīgi.

Programmatūras atjauninājumu piegādes politika ir organizāciju izstrādāta politika, kas nosaka termiņus un metodes drošības saistītu programmatūras atjauninājumu izvērtēšanai un piegādei. Šī politika koncentrējas uz tūlītēju drošības atjauninājumu piegādi noteiktā laika intervālā (ierobežojumā), lai samazinātu ievainojamības logu, ja ierobežojums to ļauj. Organizācijas var pieņemt stratēģiskāku pieeju, atkarībā no resursu ierobežojumiem. Inovatīvi risinājumi varētu ietvert, piemēram, vienādranga Blockchain sistēmas un liela mēroga pārklājuma tīklus, lai nodrošinātu ļoti efektīvu un ātru drošības atjauninājumu izplatīšanu plašiem galalietotāju tīkliem (Mugarza, Flores, & Montero, 2020). Politika ir sadalīt dažādas plāksteru kategorijas un to saistītos termiņus izvērtēšanai un piegādei, lai nodrošinātu, ka atjauninājumi dažādos līmeņos tiek izvērtēti atbilstoši to nepieciešamībai, izmaksām un saistītajiem riskiem pirms ieviešanas.

Šeit ir programmatūras atjaunināšanas ieteikumi biznesam [1]:

- **Savlaicīga uzstādīšana:** Savlaicīga drošības atjauninājumu instalēšana var palīdzēt aizsargāt sistēmas no ievainojamības un apdraudējumiem.
- **Skaidra komunikācija:** Lietotāji bieži ir atturīgi pret atjauninājumiem, jo viņi nesaprot, kāpēc tie ir nepieciešami. Ir svarīgi paziņot, kāpēc atjauninājums ir svarīgs un ka tas nav tikai nejaušs ielāps, ko nodrošina pārdevējs. Ir arī lietderīgi pieminēt, ka daži atjauninājumi ir ielāpi drošības caurumiem, kas, iespējams, jau ir izmantoti.
- **Samaziniet traucējumus:** Iespējojiet sistēmā klusas instalācijas vai konfigurācijas, kas atvieglotu atjauninājumu lietošanu. Vēl viens veids, kā samazināt traucējumus, ir izplatīt un izvietot atjauninājumus stundās, kas nav pīķa stundas.
- **Lietotāju izglītošana:** Izglītot galalietotājus par programmatūras atjauninājumu nozīmi sistēmas drošības un funkcionalitātes uzturēšanā, lai veicinātu proaktīvu atjaunināšanas darbību.
- **Testēšanas procedūras:** Uzlabot testēšanas procedūras, lai nodrošinātu, ka atjauninājumi pirms ieviešanas tiek rūpīgi pārbaudīti attiecībā uz saderību un iespējamiem riskiem.
- **Diferencējiet atjauninājumus:** Atšķiriet drošības atjauninājumus no līdzekļu atjauninājumiem, lai lietotāji saprastu katra veida atjauninājumu vērtību un attiecīgi noteiktu to prioritāti.
- **Kumulatīvie atjauninājumi:** Apsveriet kumulatīvo atjauninājumu ietekmi un mudiniet lietotāju instalēt kritiskos drošības ielāpus.

[1] (sastādīts no (Mathur, Malkin, Harbach, Péer, & Egelman, 2018), (Di Tizio, Armellini, & Massacci, 2022), (Vaniea, Rader, & Wash, 2014))

Pretvīrusu aizsardzība: sistēmas integritātes aizsardzība

Saskaņā ar (Rohith & Kaur, 2021), pretvīrusu programmatūra ir specializēta programma, kas aizsargā operētājsistēmu no vīrusiem, spiegprogrammatūras, hakeru uzbrukumiem un citas nesankcionētas piekļuves datoram, lai novērstu vērtīgu personīgo datu zādzību vai nesankcionētu datora kontroli, ko veic cita datora lietojumprogramma (bezmaksas programmatūra, daļēji bezmaksas programmatūra un komerciāla programmatūra). Pretvīrusu programmatūra tiek izmantota, lai atklātu datorvīrusus, kas var ietekmēt datorfailus, lietojumprogrammas un operētājsistēmas. Tāpēc to var iestatīt regulārai failu un datora atmiņas pārskatīšanai, lai atklātu jebkādu zināmu vīrusu parakstu, tādējādi novēršot iespējamu datora sistēmas un tās failu inficēšanos. Ir svarīgi regulāri atjaunināt pretvīrusu programmatūru ar jaunākajām definīcijām un vīrusu parakstiem, jo jauni vīrusi un to variācijas parādās regulāri. Atklājot jaunākos vīrusu draudus, pretvīrusu programmatūras atjaunināšana nodrošina spēcīgu aizsardzību pret datoru draudu pastāvīgu attīstību (Naie & Teymournejad, 2012).

Vairākas pazīmes ir saistītas ar datorvīrusu klātbūtni datorā, no kurām dažas ir sīkāk aprakstītas tālāk. Katrs no šiem simptomiem var liecināt par vīrusa problēmu. Tāpēc ir ļoti svarīgi pēc iespējas ātrāk skenēt sistēmu ar pretvīrusu programmatūru (Kumar, 2008):

- Lēnāks dators
- Pamatuzdevumi prasa ilgāku laiku
- Bloķēšana un avārijas
- Pastāvīga diska darbība
- Pārmērīga CPU izmantošana
- Interneta pārlūkošana ir daudz lēnāka nekā iepriekš.
- Pieteikumi netiks startēti.
- Uznirstošie logi un nelūgti ziņojumi ar pieaugušajiem paredzētu saturu.
- Cieto disku zīmuļu numuri.
- CD-ROM diskdziņa atvēršana un aizvēršana.

Ja negaidīti saskaraties ar vienu vai vairākām no šīm situācijām, sazinieties ar savu IT administratoru vai veiciet nepieciešamās vīrusu pārbaudes. Ir svarīgi atzīmēt, ka pretvīrusu programmas uzstādīšana visās sistēmās ir būtiska, pat ja tā nav labākā. Tas palīdz radīt augstāku grūtības līmeni uzbrucējiem, kuri mēģina apdraudēt sistēmas drošību (Min & Varadharajan, 2015). Virzoties uz priekšu, (Ncube & Maiden, 2004) sniedz vērtīgas atziņas par izaicinājumiem un apsvērumiem, kas jāizpēta, izvēloties pretvīrusu programmatūru organizācijai:

1. Anketas izmantošana kopā ar citām izcelšanas metodēm.

2. Pārliecinieties, ka jautājumi ir īsi un līdz brīdim, kad saņemat labas atbildes no piegādātājiem.

3. Pieprasiet dokumentāciju ar atbildēm uz anketas jautājumiem, lai varētu labāk saskaņot produkta aprakstu ar faktisko produktu.

4. Skaidri definējiet, ko jūs sakāt produktā un cik tālu jūs pārbaudīsit, tas palīdzēs jums labāk definēt testa gadījumu.

5. Saprotiet, ka mēs būsim ierobežoti ar laiku, kamēr mēs izvēlamies COT programmatūru un izpētīsim procesa apraksta veidnes, lai tās būtu ātrākas dažādos gadījumos.

6. Ziniet, ka jūs nevarat pārbaudīt visu. Dažām prasībām var būt ierobežojumi.

Datu dublējumi: vairogs pret zaudējumiem

Lai arī neparedzēti un negaidīti notikumi un kiberincidenti var radīt ievērojamu kaitējumu organizācijas datiem, šeit nāk talkā datu rezerves kopijas. Datu rezerves kopijas ir kritiska kiberdrošības sastāvdaļa un droša digitālās vides uzturēšana. Datu rezerves kopijas var būt lielisks rīks organizācijām drošības pārkāpumu gadījumā. Papildus datu aizsardzībai no zuduma, rezerves kopiju sistēmas nodrošina iespēju atjaunot failu iepriekšējās versijas, tādējādi aizsargājot failu vēsturi. Lielākā daļa rezerves rīku var saglabāt vairākus viena un tā paša faila gadījumus dažādos formātos, katram no tiem piešķirot laika zīmogu. Arī saspiešana un šifrēšana ir gandrīz visu rezerves sistēmu izplatītas iezīmes. Saspiešana palīdz lietotājiem pārraidīt failus tīklā vai internetā, kad tie tiek kopīgoti (Sampaio & Bernardino, 2015).

Datu rezerves kopēšanas sistēmu tehnikas ietver pilnu rezerves kopiju, kas izveido pilnu visu datu kopiju, diferenciālo rezerves kopiju, kas saglabā datu izmaiņas kopš pēdējās pilnās rezerves kopijas, un inkrementālo rezerves kopiju, kas saglabā tikai tās datu daļas, kas ir mainījušās kopš iepriekšējās rezerves kopijas veikšanas (Nadee & Somwang, 2021). Katra metode sniedz dažādas sekas un piemērotību rezerves operācijām. Uzticamas rezerves kopijas ir ievērojamas, jo daži dati ir nenovērtējami, un to atkārtota izveide prasa daudz laika un naudas (Traeger, Joukov, Sipek, & Zadok, 2006). Rezerves kopijas dati ne tikai novērš datu zudumu, bet arī ļauj atjaunot vecāku versiju (Sampaio & Bernardino, 2015). Šī divējādā funkcionalitāte ir svarīga gan datu atjaunošanai, gan atbilstībai noteiktiem juridiskiem standartiem. Šeit ir daži labākās prakses piemēri mazo uzņēmumu rezerves kopijām (Rock, 2023):

Datu aizsardzības stratēģija: mazajiem uzņēmumiem ir jāizstrādā detalizēts datu aizsardzības plāns, kas būs daļa no to BCP (uzņēmējdarbības nepārtrauktības plāns) vai DRP (katastrofu seku novēršanas plāns).

Dublēšanas risinājumi: uzņēmumiem nevajadzētu izmantot vienkāršus dublēšanas risinājumus, bet drīzāk tiem vajadzētu izvēlēties dažus spēcīgus BC / DR (uzņēmējdarbības nepārtrauktības / katastrofu atkopšanas) risinājumus, kas garantē minimālus darbības pārtraukumus.

Dublēšanas biežums un krātuve: Regulāras dublēšanas ir būtiskas, un mūsdienu dublēšanas risinājumi bieži veic dublēšanu. Ieteicams izmantot hibrīda rezerves aizsardzību, kas datus glabā gan uz vietas, gan mākonī.

Drošība un atbilstība: ir svarīgi aizsargāt dublējumus no kiberuzbrukumiem, kā arī ievērot datu saglabāšanas politikas. Dublējumu šifrēšana pārsūtīšanas laikā un miera stāvoklī būtu papildu drošība.

Datu dublēšana drošās ierīcēs: konfigurējiet dublēšanas ierīces izejošajai saziņai tikai drošā lokālajā tīklā. Šī pieeja palīdzēs novērst to, ka kibernoziedznieks pārņem kontroli pār jūsu dublējumiem.

Datu dublēšana atsevišķās ierīcēs: dublēšanas ierīces noteikti turiet atsevišķi no vietējā tīkla, lai izvairītos no dublējumu ietekmes, kad lokālajā tīklā parādās izspiedējprogrammatūra. Viena no datu dublēšanas mākonī priekšrocībām ir tā, ka to var izdarīt no jebkuras savienotas vietas, prom no galvenajiem organizācijas birojiem.

Izmantojiet šifrētus dublējumus: izmantojiet šifrētu glabāšanu un pārsūtīšanu, lai aizsargātu kritiskos datus no nesankcionētas piekļuves, manipulācijām un bojājumiem.

Dublējiet visus galapunktu datus, izmantojot atkopšanas programmatūru: ļoti svarīgs datu zuduma avots ir pazaudēti, nozagti vai bojāti klēpjdatori/galddatori. Tā rezultātā jūsu nespēja dublēt vai atjaunot zaudētos datus. Zinot, ka dublēšanas ierīces ir galddatoru un serveru formā, vienmēr atlasiet atkopšanas risinājumus, lai aizsargātu visus datus jebkurā datorā, un attiecīgi atlasiet galapunktu dublējumu.

Sargi pret ļaunprātīgu kodu: izpratne par ļaunprogrammatūras novēršanas risinājumiem

Ļaunprātīgie izpildāmie faili ir nesankcionētas programmas, kas izveidotas, lai inficētu vai bojātu datoru sistēmu, un tās rada lielu apdraudējumu datora drošībai (Ye, Wang, Li, & Ye, 2007). Lietotāji parasti ir ļaunprātīgas programmatūras upuri, to pat neapzinoties. Tā ir programma, kas darbojas lietotāja datorā fonā bez viņu zināšanas un veic tādas darbības kā informācijas zādzība, vīrusi, kas pilnībā iztīra jūsu ierīces, vai Trojas zirgi, kas var vai nevar izdzēst jūsu failus. Spiegprogrammatūra, vīrusi, tārpi, Trojas zirgi, izspiedējprogrammatūra un reklāmprogrammatūra ir bieži sastopamās ļaunprātīgās programmatūras versijas. Katram uzņēmumam vajadzētu veikt savu sistēmu rezerves kopēšanu vairāk nekā vienu reizi dienā un izmantot robustu pretļaunprātīgo programmatūru. Izvēloties pretļaunprātīgo programmatūru uzņēmumam, ir jāņem vērā vairāki faktori, lai nodrošinātu, ka risinājums atbilst organizācijas vajadzībām vai mērķiem (Alharbi, Alzahrani, Asseri, & Taramisi, 2020):

Drošības elementi: Reāllaika piekļuve, ugunsmūra aizsardzība un ielaušanās noteikšana ir galvenie drošības līdzekļi, kas jāiekļauj ļaunprogrammatūras novēršanas programmā. Šīs funkcijas ir būtiskas efektīvai draudu pārvaldībai un tam, lai pārliecinātos, ka nav tādu draudu, kas tiek palaisti garām.

Darbības iezīmes: Ļaunprogrammatūras novēršanas programmatūras darbības funkcijas, kas jums jāmeklē, ietver to, cik viegli ir izvietot un lietot programmatūru, kādas pārvaldības iespējas programmatūrai ir un kā tā tiks integrēta ar jūsu esošajām sistēmām.

Efektivitāte: Novērtējiet ļaunprogrammatūras novēršanas programmatūras efektivitāti, atklājot un noņemot kaitīgu programmatūru. Meklējiet risinājumus, kuriem ir augsts noteikšanas procents līdz 100% un minimāls aplami pozitīvs procents.

Mērogojamība: Izvēlieties risinājumu, kas var mērogot atbilstoši uzņēmuma vajadzībām, kad tas aug. Pārliecinieties, vai ļaunprogrammatūras novēršanas programmatūras risinājums var apmierināt jūsu organizācijas pašreizējās vajadzības un apmierināt nākotnes vajadzības.

Pārbaudiet piegādātāja reputāciju: Laba reputācija ir reta prece programmatūras nozarē, taču tā ir viena no vērtīgākajām jebkura programmatūras pārdevēja iezīmēm. Meklējiet ļaunprogrammatūras novēršanas programmatūras piegādātājus ar ilgu augstas kvalitātes drošības risinājumu vēsturi. Vai tos ir atzinušas neatkarīgas testēšanas organizācijas?

Izmaksas: Pirmā lieta, kas jāapsver, ir anti-ļaunprātīgas programmatūras cena. Dažādi piegādātāji nodrošina savu programmatūru dažādos cenu punktos un licencēšanas opcijās, tāpēc pārliecinieties, vai tā ietilpst jūsu budžetā. Dažas organizācijas to var klasificēt kā svarīgu faktoru, bet citas to var klasificēt kā ne pārāk svarīgu.

Atbalsts un atjauninājumi: Novērtējiet piegādātāja atbalsta un atjauninājumu ierakstus. Atrodiet piegādātāju, kas nodrošina regulārus atjauninājumus un tehnisko atbalstu, ja rodas problēmas.

Saderība ir viena no lietām, kas organizācijai ir jāpārbauda no saraksta, jo neviena programmatūra nevar būt efektīva, ja rodas saderības problēmas. Saderības problēmas ir viens no lielākajiem iemesliem, kāpēc organizācijas programmatūra kļūst neefektīva.

2. daļa - Kā padarīt digitālo higiēnu par ieradumu jaunuzņēmumu operācijās

Kiberdrošības un kiberveselības prakses kultūras izveide jaunuzņēmuma ikdienas darbībā ir ļoti svarīga. Kiberveselības prakses ir tādas pašas kā personīgā higiēna, tās nodrošina nepieciešamos protokolus, kurus jāievēro, lai saglabātu personīgos un uzņēmuma datus/informāciju drošībā un aizsargātībā (Alkhaledi & Hawamdeh, 2023). Jaunuzņēmumi, kuriem trūkst līdzekļu, nevar atļauties kiberdrošības incidentu izraisītās sekas. Biznesa sekas neaprobežojas tikai ar finansiālu ietekmi, bet ietver arī klientu uzticības zaudēšanu, reputācijas kaitējumu un iespējamas juridiskas sekas, kas jaunuzņēmumiem var nozīmēt atšķirību starp veiksmīgu mērogošanu vai priekšlaicīgu neveiksmi. Daudzās organizācijās joprojām pietrūkst labas kiberveselības uzvedības, pat ja daudz ir darīts, lai risinātu kiberveselības jautājumu (Kalhoro, Rehman, Ponnusamy, & Shaikh, 2021).

Laba kiberhigiēnas uzvedība ir būtiska, lai samazinātu kiberdraudus un ikdienas izaicinājumus kiberhigiēnas jautājumu risināšanā. Šī nodaļa kalpo, lai ieskicētu un paplašinātu stratēģijas, kas katru dienu tiek ieviestas jaunuzņēmumiem, lai izveidotu ikdienas digitālās higiēnas rutīnu.

2.1. Jaunuzņēmuma digitālās veselības novērtēšana

Kiberdrošības riska novērtējums ir būtiska uzņēmējdarbības plānošanas sastāvdaļa; tas ietver riska identificēšanu un novērtēšanu organizācijas digitālajiem aktīviem un darbībām. Pielietotā kiberdrošības riska novērtēšanas metode ļauj organizācijai novērtēt savu drošības stāvokli, piešķirt vērtību tās informācijai un sistēmām, novērtēt esošās drošības infrastruktūras un aktivitāšu efektivitāti, kā arī noteikt kaitējuma apmēru, ja konkrētie riski tiek realizēti. Prioritizējot identificētos riskus, organizācijas var efektīvi sadalīt resursus, lai stiprinātu savu aizsardzību un nodrošinātu uzņēmējdarbības nepārtrauktību.

Daudzi pētījumi piedāvā vērtīgus secinājumus par dažādiem kiberdrošības riska novērtējuma aspektiem, kas var būt noderīgi uzņēmējdarbībā. (Chavez, ve diğerleri, 2020) norāda, ka informācijas vajadzību novērtēšana ir arī viens no galvenajiem soļiem efektīvā noviržu apstrādē MVU ar digitālo rīku izmantošanu. Informācijas veidu noteikšana, kas ir nepieciešama procedūru veikšanai, un datu kritiskuma līmeņa noteikšana palīdzēs samazināt digitālo sistēmu integrēšanas risku. (Elmarady & Rahouma, 2021) apkopojusi riska novērtēšanas procesu aviācijas kiberdrošībā, bet šīs prakses var izmantot kā vispārīgu ietvaru riska novērtēšanai MVU:

1. Nosakiet sistēmas, kurām nepieciešama aizsardzība. Ar izpratni par to, ko sistēmas tika definētas, potenciālo draudu identificēšana šīm sistēmām izklausās vienkārša.

   • Atpazīstiet iespējamos draudus, izprotot sistēmas.

   • Definējiet novērtējamo sistēmu robežas un aprakstiet tās.

2. Uzskaitiet visas lietas, kas varētu notikt, lai radītu zaudējumus vai kaitējumu sistēmai. Saprast, kas tieši vai netieši varētu izraisīt drošības mērķa neizpildi un kāda ir atšķirība starp draudiem un ievainojamību.

   • Nosakiet scenārijus, kas varētu tieši vai netieši kaitēt sistēmai.

   • Novērtējiet draudus, kas var ietekmēt sistēmas integritāti, konfidencialitāti un pieejamību.

3. Novērtēt draudu iespējamību un ietekmi. Novērtējot pamatu, kurā var veikt draudus, ir jāņem vērā daudzi faktori.

   • Novērtējiet draudu iespējamību.

   • Novērtēt draudu iespējamo ietekmi uz drošību, efektivitāti, ekonomiku, politiku un sabiedrības uzticēšanos.

4. Nosakiet riska līmeņus. Novērtējiet riska līmeņus.

- Analizējiet riska profilu, izmantojot varbūtību, ievainojamības novērtējumus un draudu ietekmi.
- Pārvērst riska līmeņus kvalitatīvos terminos un noteikt riska panesamību.
- Kategorizējiet riska līmeņus, izmantojot standartizētu metodoloģiju.

Īstenot riska mazināšanas pasākumus, kas vajadzīgi, lai samazinātu riskus līdz pieņemamam līmenim. Veicot šīs darbības, organizācijas var efektīvi novērtēt kiberdrošības riskus, identificēt draudus un ieviest politikas, lai aizsargātu kritiskās sistēmas.

2.2. Digitālās higiēnas kultūras izveide

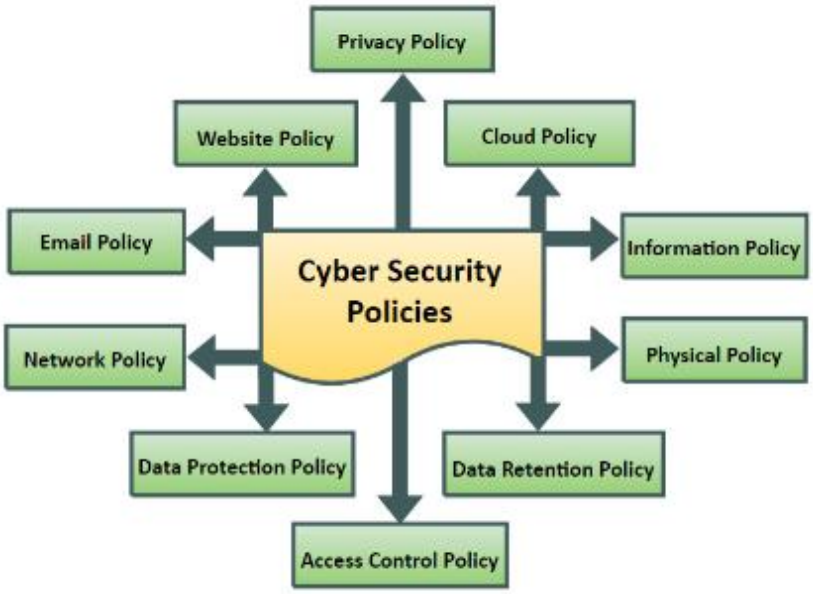
Digitālās higiēnas kultūra un plaukstoša digitālā ekosistēma vispirms jāiedzīvina organizācijā kā pirmais nosacījums. Tas ir jādara no augšas uz leju, vadībai vadot šo procesu. Nepietiek tikai runāt par digitālo labklājību, tas ir jāpārņem augstākajai vadībai. Tas sākas ar politiku izstrādi. Līderiem jāveido un jāīsteno visaptveroša politika, kas regulē datu pārvaldību un paaugstina drošību. Regulāras apmācību sesijas ir ļoti nepieciešamas. Tām jābūt regulārām programmām, lai radītu izpratni darbinieku vidū par to, kā palikt drošiem un iepazīstināt ar jaunākajām digitālās drošības labajām praksēm. Atvērta komunikācija ir ļoti svarīga. Ir ļoti svarīgi, lai organizācijā būtu caurredzama kultūra, kur darbinieki jūtas ērti sazinoties, var izteikt savas bažas un arī ziņot, ja viņi pamana kaut ko aizdomīgu, kas varētu radīt drošības problēmas. Tas ir vienīgais veids, kā mēs varam nodrošināt kultūru, kas uztur digitālo higiēnu un drošību.

2.2.1. Politikas izstrāde

Spēcīgas kiberdrošības politikas izveide ir ļoti svarīga mazajiem un vidējiem uzņēmumiem (MVU), lai nodrošinātu to digitālos aktīvus un garantētu darbības nepārtrauktību. Pētījumi ir parādījuši, ka MVU saskaras ar vairākiem izaicinājumiem, tostarp budžeta trūkumu, speciālistu nepieejamību un kiberdraudu pieaugumu (Neri, Niccolini, & Martino, 2023). Tādēļ MVU nepieciešams uzlabot savu kiberdrošības apziņu un gatavību. Kiberdrošības pasākumu ieviešana var ievērojami samazināt datu pārkāpumus un uzlabot iekšējo procesu drošību, kā arī izveidot uzticamu sistēmu ar pietiekamu informācijas apstrādes jaudu (Hasani, O'Reilly, Dehghantanha, Rezania, & Levallet, 2023). Turklāt MVU noturību pret kiberuzbrukumiem var uzlabot, īstenojot kiberdrošības politikas. Visaptverošas pieejas īstenošana kiberdrošībai var uzlabot MVU spēju prognozēt, atklāt, izturēt, atgūties un attīstīties pēc kiberuzbrukuma (Carias, Borges, Labaka, Arrizabalaga, & Hernantes, 2020).

Uzņēmumiem, izstrādājot kiberdrošības politiku, būtu jāņem vērā dažādas jomas un atbilstoši savām vajadzībām jāizstrādā kiberdrošības politika attiecīgajā jomā. Lai veicinātu savu kiberdrošības politiku un praksi, asociācijas var izmantot šīs daļas, lai izstrādātu kiberdrošības politikas taksonomiju. Kiberdrošības politikas taksonomijas komponenti, kas minēti (Mishra, Alzoubi, Gill, & Anwar, 2022), ir parādīti 2. attēlā:

2.attēls: Kiberdrošības politikas taksonomija



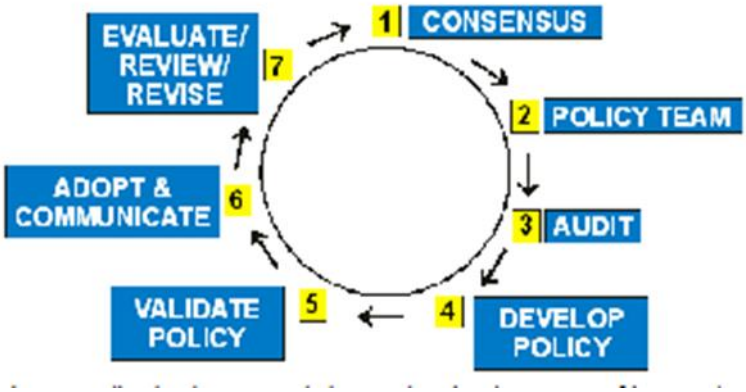
Avots: (Mishra, Alzoubi, Gill, & Anwar, 2022)

1. Privātuma politika: Koncentrējas uz sensitīvu personu datu aizsardzību un atbilstības nodrošināšanu datu aizsardzības noteikumiem.
2. Tīmekļa vietnes drošība: Ietver tīmekļa vietņu aizsardzību no kiberdraudiem un ievainojamībām, lai aizsargātu lietotāju datus.
3. Mākoņdatošanas drošība: Risina drošības pasākumus mākoņpakalpojumiem, lai aizsargātu mākonī glabātos datus.
4. E-pasta drošība: Koncentrējas uz e-pasta saziņas drošību un e-pasta bāzētu kiberdraudu novēršanu.
5. Fiziskā drošība: Ietver fiziskās piekļuves aizsardzību IT infrastruktūrai un kritiskajiem resursiem, lai novērstu nesankcionētu piekļuvi.
6. Tīkla drošība: Koncentrējas uz datoru tīklu aizsardzību no kiberdraudiem un nesankcionētas piekļuves.
7. Informācijas drošība: Ietver pasākumus, lai aizsargātu sensitīvu informāciju.
8. Piekļuves kontrole: Ietver lietotāju piekļuves pārvaldību sistēmām un datiem, lai novērstu nesankcionētu piekļuvi.
9. Datu glabāšana: Risina politikas datu glabāšanu un pārvaldīšanu visā to dzīves ciklā.
10. Datu aizsardzība: Koncentrējas uz datu aizsardzību no zuduma, zādzības vai nesankcionētas piekļuves, izmantojot šifrēšanu un drošības kontroles.

Kad zināt nepilnības un mērķus, varat izstrādāt kiberdrošības politikas, lai aptvertu šīs jomas. Noderīgs ietvars politikas izstrādei ir izklāstīts (Lubua & Pretorius, 2019) 3.attēlā. Politikas izstrādes cikls ietver jautājumu atzīšanu, kuriem būs nepieciešama kāda veida politika, politikas komandas izveidi, sanāksmes un dalībnieku iesaisti, politikas validēšanu, politikas pieņemšanu ar katru nozīmīgo lēmumu, politikas pārvaldību ne ilgāk kā trīs gadus, politikas samazināšanu, kā arī atsauksmju un izmaiņu integrēšanu. Visā procesā ir svarīgi iesaistīt ieinteresētās puses, gūstot ieguldījumu no dažādām cilvēku grupām. Politikai ir arī

jābūt formalizētai, pārliecinoties, ka tā ir saskaņota ar mūsu organizācijas mērķiem un jebkādām juridiskām prasībām. Politikas ir regulāri jāpārskata, atjauninot tās, kad tās ir novecojušas. Regulāras pārbaudes ir jāveic un nepieciešamās izmaiņas jāievieš. Politikas attiecīgi izaicinās un arī veicinās vides pārmaiņas organizācijā vai konkrētā kontekstā.

3.attēls: Politikas izstrādes cikls



Avots : (Lubua & Pretorius, 2019)

2.2.2. Regulāra apmācība

Svarīgs apsvērums, izglītojot darbiniekus par labākajām kiberdrošības higiēnas praksēm, ir izpētīt daudzos faktorus, kas ietekmē viņu uzvedību un zināšanas. Nesenā pētījumā (Cain, Edwards, & Still, 2018) norādīts, ka lietotāji bieži nav informēti par galvenajiem soļiem, kas jāveic, un to ietekmi, tādējādi ietekmējot viņu uzvedību. Lielākajai daļai lietotāju trūkst izpratnes par to, ko tieši nozīmē ievērot labākās drošības prakses, pat ja viņi ir informēti par iesaistītajiem riskiem. Daudzi lietotāji var arī apzināties riskus, bet joprojām nespēj veikt atbilstošus piesardzības pasākumus, lai labāk izprastu drošības koncepciju. Citā pētījumā (Neigel, Claypoole, Waldfogle, Acharya, & Hancock, 2020) tiek sniegti faktori, piemēram, cilvēkfaktori, kas veicina kiberdrošības pārkāpumus un riskus. Sliktas kiberdrošības higiēnas prakses, informētības trūkums, uzvedības aizspriedumi, izglītības trūkumi un nepietiekama apmācība būtiski veicina cilvēkfaktorus, kurus var risināt ar izglītību un informētību, tādējādi ievērojami samazinot ievainojamību un uzlabojot kiberdrošības noturību..

Kiberdrošības apmācība darbiniekiem ir būtiska, lai organizācijas varētu proaktīvi pievērsties savu informācijas aizsardzībai. Darbinieku apmācība ne tikai izglīto darbiniekus, bet arī veicina visu darbinieku informētību par esošajiem kiberdraudiem, kādas var būt sekas veiksmīgam kibernoziedznieka uzbrukumam un kā rīkoties, ja tas destabilizē organizāciju. Organizācijai ir jāapmāca visi savi darbinieki, lai padarītu viņus

labi informētus par kiberdrošību un izskaidrotu jebkādus draudus uzņēmuma vērtīgajiem aktīviem (Singh, Mohanty, Swagatika, & Kumar, 2020).

Šeit ir dažas labākās prakses kiberkiberdrošības apmācībai (Mughal, 2019) :

- Regulāra apmācība: turpiniet nodrošināt drošības apmācību uzņēmuma galalietotājiem, lai viņi būtu informēti par jaunajiem draudiem, kas vienmēr parādās viņu pienākumos.
- Pielāgots saturs: vienmēr izmantojiet pielāgotu apmācības saturu, kura pamatā ir IoT ierīces risks un bažas par galalietotāja lomu.
- Interaktīva mācīšanās: Ir svarīgi zināt, kas iesaista gala lietotājus un viņu mācību procesu par, kas palīdz mijiedarboties un simulēt darbnīcas, lai turpinātu iesaistīt lietotāju šādi.
- Skaidra komunikācija: vienmēr vislabāk informējiet par IoT drošības un ierobežojumu politiku, pamatojoties uz tās praksi, un lietotājs to apzinās.
- Pastiprināšana un atgādinājumi: Turpiniet atgādināt gala lietotājam par drošību un vienmēr turpiniet nodrošināt galalietotāju informētību.
- Stimuli un atlīdzības: nodrošināt un veicināt labu kiberdrošības praksi, izmantojot atlīdzības un stimulus, kas mudina galalietotājus pabeigt apmācību vai ziņot par incidentiem.
- Novērtēšana un atgriezeniskā saite: pārraugiet lietotāja uzvedību un to, kā darbojas programmas darbinieks, ja ir parādīta jebkāda iesaistīšanās.

2.2.3. Organizatoriskā kultūra

Kā kultūras gatavības koncepciju var piemērot jūsu organizācijas kiberdrošības sagatavotībai? Pētījumi ir parādījuši, ka organizācijas ar spēcīgu kiberdrošības kultūru ir labāk sagatavotas, lai tiktu galā ar kiberdraudiem (Berlilana, Noparumpa, Ruangkanjanases, Hariguna, & Sarmini, 2021). Kiberdrošības kultūra ir neatņemama daļa no kopējās organizācijas kultūras, kas veido risku pārvaldības sistēmas, pārvaldību, politikas un darbinieku uzvedību, kas saistīta ar kiberdrošību (AL-Nuaimi, 2024). Turklāt organizācijas var veicināt darbinieku atbilstību informācijas drošības politikām, izmantojot augstākās vadības atbalstu un organizācijas kultūru, vadot drošības iniciatīvas, efektīvi komunicējot un aktīvi iesaistot darbiniekus (Hu, Dinev, Hart, & Cooke, 2012). Vienota drošības kultūra palīdz visiem darbiniekiem, neatkarīgi no nodaļas vai darba lomas, saprast kiberdraudu riskus. Tas palīdz labāk saskaņot viņu stratēģijas šo informācijas drošības risku mazināšanai (Fritzvold, 2017).

Tehnoloģiju-Organizācijas-Vides (TOE) ietvars, ko izstrādāja Tornatzky un Fleischer (1990), ir visaptverošs ietvars, kas nodrošina pamatu dažādu Informācijas Sistēmu (IS) un Informācijas Tehnoloģiju (IT) produktu un pakalpojumu pieņemšanas izpētei organizācijās (Gangwar, Date, & Ramaswamy, 2015). Šis ietvars pārstāv ne tikai tehnisko inovācijas aspektu, bet arī organizatorisko un vides skatījumu, lai izskaidrotu un izpētītu tehnoloģijas pieņemšanu (Rahayu & Day, 2015). Līdz ar to TOE ietvars aptver šīs trīs dimensijas, lai ilustrētu skaidru kopējo ainu par faktoriem, kas ietekmē inovāciju pieņemšanu organizācijās. Pēc (Hasan, Ali, Kurnia, & Thurasamy, 2021) domām, galvenie faktori, kas ietekmē kiberdrošības gatavību organizācijās, balstoties uz TOE ietvaru, ietver:

Tehnoloģiskie faktori

Organizācijas IT infrastruktūras briedumam ir nozīmīga loma, lai uzlabotu organizācijas gatavību cīnīties pret kiberuzbrukumiem. Nobriedis IT infrastruktūrā, ja nepieciešamie resursi ir piesardzīgi pret tās ekspertiem, IT ierīcēm un lietotāju programmatūras lietojumprogrammām, var uzlabot gatavību.

Organizatoriskie faktori

Augstākās vadības atbalsts kiberdrošībai, organizatoriskā struktūra un organizācijas kultūra ir svarīgi faktori kiberuzbrukumu gatavībai. Augstākās vadības atbalstam ir pozitīvi nozīmīga ietekme uz gatavību kiberdrošībai.

Vides faktori

Pārdevēju / partneru attiecības, valdības noteikumi un rūpniecības politika ir ārējie vides apstākļi, kas pozitīvi palīdz palielināt organizācijas gatavību cīnīties pret kiberuzbrukumiem.

Kiberdrošības kultūras attīstīšana ir sarežģīts process, kas ņem vērā organizācijas kultūru, apakškultūras un ietvarus. Organizācijas kultūra ir identificēta kā būtisks faktors drošības kultūru veidošanā, un drošības kultūru ir definējusi kā apakškultūru organizācijā. Lai izveidotu drošības kultūru, kas ir daļa no organizācijas, organizācija var izpētīt kultūru caur dimensijām, piemēram, artefaktiem un ierosināt vērtības, kopīgas pieņēmumus, organizācijas zināšanas un nepieciešamās operatīvās prakses (Uchendu, Nurse, Bada, & Furnell, 2021).

Liksim 1. un 2. daļu kopā: ikdienas paradumi labākai digitālajai higiēnai

Spēcīga digitālā higiēnas kultūra ir nepieciešama pastāvīgi mainīgajā jaunuzņēmumu ekosistēmā. Šo kultūru vadot no augšas uz leju, vadība uzsvēra kiberdrošības un datu aizsardzības nozīmi. Lai veicinātu šo kultūru, jaunuzņēmumiem jāievieš regulāras rezerves kopijas ar hibrīda aizsardzību, kur datu glabā gan uz vietas, gan mākoņu sistēmās. Tas palīdzēs aizsargāties pret kiberuzbrukumiem un sistēmas traucējumiem, nodrošinot, ka dati vienmēr ir drošībā. Šifrētām rezervēm ir arī īpaša nozīme, īpaši nozaru, piemēram, veselības aprūpes jomā, kur datu aizsardzības atbilstībai nav alternatīvas.

Ir būtiski izvietot pretvīrusu programmatūru, kas nodrošina plašu funkciju komplektu, ieskaitot reāllaika skenēšanu, uzvedības uzraudzību, e-pasta aizsardzību un tīmekļa filtrēšanu, lai aizsargātu sistēmas no kaitīgas programmatūras inficēšanās. No otras puses, jaunuzņēmumiem regulāri jāveic proaktīvi kiberdrošības riska novērtējumi, lai noteiktu iespējamos draudus, novērtētu to varbūtību un ietekmi, kā arī riska līmeņus. Šie novērtējumi palīdzēs veikt efektīvas mazināšanas pasākumus, lai aizsargātu kritiskās sistēmas.

Izstrādāt visaptverošas datu pārvaldības politikas un protokolus, lai nodrošinātu drošu datu apstrādi, ir prioritāte. Politikām jāapraksta labās prakses politikas un procedūras datu aizsardzībā, drošajā komunikācijā un labā digitālajā higiēnā. Regulāra apmācība darbiniekiem. Darbiniekiem jābūt labāk informētiem par digitālajiem draudiem un to, ko viņi var darīt, lai palīdzētu tos novērst. Tas palīdzēs saglabāt darbiniekus informētus par jaunākajiem draudiem un drošības pasākumiem.

Lai nodrošinātu vidi, ļoti svarīga ir atvērta komunikācija, kas organizatoriski ļauj darbiniekiem ērti paaugstināt drošības problēmas, ziņot par aizdomīgām darbībām un apspriest iespējamos draudus. Labai ikdienas praksei kiberhigiēnā, piemēram, spēcīgu paroļu izveidei, programmatūras ielāpu uzturēšanai, datu šifrēšanai un drošu saziņas kanālu izmantošanai, ir jākļūst par darbinieku ieradumu.

Vēl viens ekonomiski izdevīgs elements, kas jāņem vērā, ir apskatīt dažādas pretvīrusu risinājumu iespējas, to izmaksas, atbalstu, atjauninājumus un saderību ar jūsu budžetu un darbības veidu. Tāpat kā jaunuzņēmumiem nevajadzētu uzskatīt iepriekš minētos elementus par papildu risinājumiem, tāpat jaunuzņēmumiem nevajadzētu uzskatīt šos elementus par papildu. Jaunuzņēmumiem ir nepieciešams būt drošiem tiešsaistē, aizsargāt savus aktīvus un izveidot uzticību ar saviem klientiem un partneriem, tāpēc, lai to izdarītu, jaunuzņēmumiem ir nepieciešams iekļaut digitālo higiēnu un kiberdrošību savā DNS. Jaunuzņēmumiem ir nepieciešams iekļaut digitālo uzturēšanu un kiberhigiēnu savā ikdienas darbībā, tas ir vienīgais patiesais veids, kā paaugstināt to tiešsaistes drošību, tādējādi padarot tos kiberdrošus. Kiberhigiēna ir zobu tīrīšana un drošie digitālie darbības veidi, bet kiberdrošība ir kā aizsargplēve zobu tīrīšanas laikā. Ja viens no tiem jums ir, otrais ir nepieciešams.

3. daļa — Digitālās higiēnas integrācija: gadījuma izpēte un Labas prakses piemērs no jaunuzņēmumiem

Labākā prakse: populārākie digitālās higiēnas rīki jaunuzņēmumiem

Konteksts: Šajā digitālajā laikmetā jaunuzņēmumiem un jebkuram uzņēmumam, ja tā operatīvā darbība ir ļoti atkarīga no tehnoloģijām, ir ļoti svarīgi ievērot digitālo higiēnu, lai pasargātu no visiem digitālajiem draudiem un datu pārkāpumiem. Katram jaunuzņēmumam vajadzētu būt noteiktiem digitālās higiēnas rīkiem, kas palīdzēs tiem aizsargāt savus digitālos aktīvus, lai tie varētu bez pārtraukuma turpināt savu operatīvo darbību.

Labāko digitālās higiēnas rīku noteikšana: Jaunuzņēmumiem ir jānodrošina sevi ar digitālās higiēnas rīku komplektu, lai risinātu dažādus kiberdrošības aspektus. Šeit ir saraksts ar dažiem rīkiem no uzņēmumiem un organizācijām, kurām uzticas liels skaits cilvēku.

1. **Pretvīrusu programmatūra**: Pretvīrusu programmatūra ir kontroles sistēma, kas bloķē, atklāj un novērš vīrusus un citu ļaunprātīgu programmatūru konkrētā programmatūrā, kā arī aizsargā datus no tiešsaistes draudiem.
2. **Ugunsmūri**: Vēl viena tīkla drošības sistēma ir ugunsmūri, kas paredzēti interneta drošības ierīcēm, lai novērstu nesankcionētu piekļuvi tīklam.
3. **Paroļu pārvaldnieki**: Tie palīdzēs izveidot un uzturēt spēcīgas, unikālas paroles visām vietnēm.
4. **Šifrēšanas rīki**: Šifrējiet datus gan miera stāvoklī, gan pārsūtīšanas laikā, nodrošinot, ka sensitīvie dati nav lasāmi neautorizētiem lietotājiem.
5. **2-faktoru autorizācija (2FA)**: Pievieno papildu drošību pieteikšanās laikā.
6. **Virtuālie privātie tīkli (VPN)**: Nodrošina drošus un šifrētus savienojumus, lai uzturētu privātumu un datu drošību publiskajos tīklos.
7. **Droša mākoņkrātuve**: piedāvā vietu, kur drošā vietā varat dublēt failus. Ļaujot tajā nokļūt tikai noteiktiem cilvēkiem.

Digitālo higiēnas rīku efektivitātes pārbaude

Pirmkārt, mums jāpārliecinās, ka mūsu izvēlētie rīki bija noderīgi:

1. **Saderības pārbaude**: Pārliecinieties, vai izvēlētie rīki ir saderīgi ar startēšanas pašreizējām sistēmām un turklāt nedrīkst traucēt darbplūsmām.
2. **Lietojamības novērtējums**: Mums ir jāveic uzdevumi, izmantojot rīkus. Lai veiksmīgi veiktu ikdienas uzdevumus, izmantojot rīku, tas nepatērē pārāk daudz laika un datu ievades.
3. **Drošības audits**: Lai pārbaudītu efektivitāti, rīki tiks regulāri izmantoti, lai pamanītu, vai tie ir patiesi droši pret jaunākajiem kiberdraudu veidiem.
4. **Apmācība un informētība**: Komandas izglītošana par digitālās higiēnas nozīmi un rīku ētisku un pareizu izmantošanu.

Digitālās higiēnas kultūras izveide

Konteksts: Kiberhigiēnas kultūras veidošana katrā jaunuzņēmumā ir tikpat svarīga kā pati tehnoloģija. Izpratne par kiberdrošību un gatavība ir ideja veicināt vidi, kurā katrs darbinieks katrā jaunuzņēmumā apzinās kiberdrošības nozīmi un savu lomu aizsardzībā pret draudiem.

Digitālās higiēnas kultūras izveide jūsu uzņēmumā:

1. **Vadības piemērs**: Tiešajiem vadītājiem ir jārāda piemērs un jāievēro laba digitālā higiēna.
2. **Regulāra apmācība**: Izglītojiet darbiniekus, kad rodas jauni draudi.
3. **Skaidra politika**: Jābūt skaidrai un precīzi definētai iekšējai politikai attiecībā uz labu digitālo higiēnu.
4. **Atvērtas komunikācijas veicināšana**: Izveidojiet kultūru, kurā darbinieki tiek atalgoti par digitālās higiēnas jautājumu pārzināšanu vai redzēšanu.

5. **Atbilstības atalgošana**: Apbalvojiet darbiniekus, kuri parāda, ka viņi pārsniedz digitālās higiēnas bāzes līniju.

Rezultāti un ietekme - Gaidāmie digitālās higiēnas kultūras rezultāti jaunuzņēmumam:

- **Samazināts kiberuzbrukumu risks**: Labi informēta komanda ir pirmā aizsardzības līnija.
- **Uzlabota datu aizsardzība**: Aizsargājiet savu un klientu uzņēmumus, ievērojot atbilstošu digitālo higiēnu.
- **Normatīvā atbilstība:** Ievērojiet kiberdrošības noteikumus un izvairieties no finansiālām un citām sankcijām.

Galvenās atziņas: Jaunuzņēmumiem ir jāiegūst pareizie pamati, ja viņi vēlas gūt panākumus ilgtermiņā. Lai samazinātu pārkāpuma ilgtermiņa izmaksas un paātrinātu atveseļošanās periodu, ja notiek vissliktākais, ir svarīgi izmantot populārākos digitālās higiēnas rīkus un iestrādāt kibernoturības kultūru uzņēmumā.

Gadījuma izpēte: SecureTech Startup - digitālās higiēnas izmantošana kiberdrošībai

Kopsavilkums: SecureTech ir finanšu tehnoloģiju jaunuzņēmums, kas saprata digitālās higiēnas nozīmi sava uzņēmuma nodrošināšanā. Šī gadījuma izpēte sniegs pārskatu par dažādiem rīkiem un kultūras izmaiņām, ko viņi veica savā organizācijā, lai radītu vēl lielāku pārliecību, ka uzbrucēji nevarētu izlauzties savā digitālajā telpā.

Ievads: Kiberdraudu straujas attīstības laikmetā SecureTech ir jāveic ļoti grūts uzdevums, tādējādi aizsargājot savus digitālos aktīvus un klientu datus. Jaunuzņēmuma sākumposmā uzņēmuma vadība saprot, ka stabila digitālā higiēna ir ne tikai nepieciešamība, bet arī ļoti būtiska konkurences priekšrocība.

Situācijas analīze: Pēc sākotnējā kiberdrošības novērtējuma uzņēmums atklāja, ka viņiem ir daudz jomu, kas jāuzlabo. SecureTech uzlaboja izmantojamos rīkus attiecībā uz digitālo higiēnu un darbinieku vispārējo izpratni par kiberdrošību.

Digitālo higiēnas rīku identificēšana: Izvērtējot daudzus rīkus, kas saistīti ar digitālo higiēnu, SecureTech ir identificējis komplektu, kas risinās viņu īpašo situāciju.

1. **BitDefender**: Aizsargā visas jūsu ierīces no dažādiem apdraudējumiem.
2. **Cisco Firewalls**: Uzrauga un kontrolē tīkla trafiku.
3. **LastPass**: Paroļu pārvaldnieks pēc izvēles.
4. **VeraCrypt**: Šifrē visus jūsu datus.
5. **Duo Security**: Izmanto divfaktoru autentifikācijai.
6. **NordVPN**: Aizsargā jūsu attālo savienojumu un darbu no ziņkārīgo acīm.
7. **Dropbox Business**: Droši glabā dublējumus un failus mākonī.

Digitālās higiēnas kultūras izveide: SecureTech vadība izstrādāja un ieviesa uzņēmumā digitālās higiēnas programmu.

Izpilddirektora apņemšanās: Atbalstu programmas izmantošanai visā uzņēmumā palīdzēja izpilddirektors, piešķirot tai savu apstiprinājuma zīmogu.

1. **Ikmēneša kiberdrošības apmācība**: Tika rīkoti semināri, lai informētu komandu par jaunākajiem draudiem un tendencēm.
2. **Digitālā higiēnas rokasgrāmata:** Visaptverošs politiku un procesu kopums tika nodrošināts visiem saistītajiem uzņēmumiem.
3. **Drošības čempioni:** Atlasītie partneri tika apmācīti par kiberdrošības aizstāvjiem attiecīgajās nodaļās.
4. **Atlīdzība un atzinība par drošiem ieradumiem:** Personas ar izcilu digitālo higiēnu tika atzītas un apbalvotas.

Izaicinājumi un risinājumi: iebildumi pret mūsu pārmaiņām: jaunu rīku pieņemšana, kultūras maiņa mūsu digitālās higiēnas praksē.

1. Ceļu bloķēšanas samazināšana: Pārliecinājāmies, ka jaunās digitālās rīkkopas palielināja katras mūsu komandas efektivitāti, nevis palēnināja tās.

2. Drošības apmācības izspēle: Īstenota uz spēlēm balstīta drošības apmācības programma, kas sarindotu komandas pēc to kiberprasmēm.

3. **Komandas informēšana:** Nepārtraukti informēja par TeamSecureTech progresu un to, kā viņu digitālās higiēnas centieni ietekmēja viņu uzņēmuma drošību.

Rezultāti: Gada laikā SecureTech ziņoja:

- **100% digitālās higiēnas rīka pieņemšana –** Darbinieki pilnībā pieņēma izvēlētos rīkus
- **Pikšķerēšanas mēģinājumu samazinājums par 80% –** Lielāka darbinieku informētība ļāva ātrāk atpazīt aizdomīgus e-pastus un ziņot par tiem
- **Uzlabota atbilstības stāja –** Visi normatīvie standarti tika izpildīti, un naudas sodi netika piemēroti

Secinājums: SecureTech ļoti proaktīvā nostāja digitālās higiēnas jomā ir ievērojami uzlabojusi kiberdrošību un attīstījusi modrības un atbildības kultūru. Šī gadījuma izpēte parāda, kā sarežģītu draudu vidi var uzvarēt, izmantojot efektīvu kontroles sistēmu, kas darbojas vienoti ar uzņēmuma transformāciju kultūrā.

Līdzņemšana:

Pareizā rīka izvēle ir būtiska: Jaunuzņēmumiem ir jāmeklē digitālās higiēnas rīki, kas atbilst viņu īpašajām vajadzībām un darbplūsmām

Kultūra veicina atbilstību: spēcīgas digitālās higiēnas kultūras veidošana var samazināt kiberdrošības riskus

Tas ir uzlabošanas process: Kiberdrošība nav stāvoklis, bet gan nepārtraukts process, tā nav vienreizēja darbība, un tai ir nepieciešami regulāri atjauninājumi un apmācības

Atsauksmes

Alharbi, B., Alzahrani, H., Asseri, A., & Taramisi, K. (2020). Anti-malware efficiency evaluation framework. *2020 2nd International Conference on Computer and Information Sciences (ICCIS)* (s. 1-4). IEEE.

Alkhaledi, R., & Hawamdeh, S. (2023). Electronic health records and cyber hygiene: a qualitative study of the awareness, knowledge, and experience of physicians in Kuwait. *Proceedings of the Association for Information Science and Technology, 60(1)*, s. 21-30.

AL-Nuaimi, M. N. (2024). Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review. *Global Knowledge, Memory and Communication, 73* ((1/2)), 1-23.

Berlilana,Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. *Sustainability, 13*(24), 13761.

Blocki, J., & Liu, P. (2023). Towards a rigorous statistical analysis of empirical password datasets. *2023 IEEE Symposium on Security and Privacy (SP)*, 606-625.

Bruzgiene, R., & Jurgilas, K. (2019). Securing remote access to information systems of critical infrastructure using two-factor authentication. *Electronics, 10*(15), 1819.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications, 42*, 36-45.

Carias, J. F., Borges, M. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). a systematic approach to cyber resilience operationalization in SMEs. *IEEE Access*, *8*, s. 174200-174221.

Chavez, Z., Hauge, J. B., Bellgran, M., Gullander, P., Johansson, M., Medbo, L., & Ström, M. (2020). Digital tools and information need assessment for efficient deviation handling in SMEs. *Advances in Transdisciplinary Engineering., 13*(SPS2020), 24 - 35.

De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2013). A comparative usability study of two-factor authentication. *arXiv preprint, 1309*, 5344.

Di Tizio, G., Armellini, M., & Massacci, F. (2022). Software updates strategies: A quantitative evaluation against advanced persistent threats. *IEEE Transactions on Software Engineering, 49*(3), 1359-1373.

Elmarady, A. A., & Rahouma, K. (2021). Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. *IEEE Access, 9*, 143997-144016.

Fritzvold, E. (2017). Cyber Security in Organizations. *(Master's thesis, University of Stavanger, Norway)*.

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management, 28*(1), 107-130.

Han, W., Sun, C., Shen, C., Chang, L., & Shen, S. (2013). Dynamic combination of authentication factors based on quantified risk and benefit. *Security and Communication Networks, 7*(2), 385-396.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications, 58*, 102726.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business &Amp; Economics, 3*(5).

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-660.

Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. *Proceedings of the Sigchi conference on human factors in computing system*, (s. 383-392).

Jones, C. (2022, 11 24). *Expert Insights*. https://expertinsights.com/insights/the-most-significant-password-breaches/ Dresden alındı

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting key factors of cyber hygiene behavior among software engineers: a systematic literature review. *IEEE Access*, *9*, s. 99339-99363.

Kato, K., & Klyuev, V. (2013). Strong passwords: Practical issues. *2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems(IDAACS). 2*, s. 608-613. IEEE.

Keszthely, A. (2013). About passwords. *Acta Polytechnica Hungarica*, 99-118.

Kumar, P. (2008). Computer virus prevention & anti-virus strategy. *Sahara Arts & Management Academy Series.*

Lubua, E. W., & Pretorius, P. D. (2019). Cyber-security policy framework and procedural compliance in public organizations. *Proceedings of the International Conference on Industrial Engineering and Operations Management*, (s. 1-13).

Mathur, A., Malkin, N., Harbach, M., Péer, E., & Egelman, S. (2018). Quantifying users' beliefs about software updates., (s. Proceedings 2018 Workshop on Usable Security.).

Min, B., & Varadharajan, V. (2015). Design, implementation, and evaluation of a novel anti-virus parasitic malware. *Proceedings of the 30th Annual ACM Symposium on Applied Computing*, (s. 2127-2133).

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors, 22*(2), 538.

Mugarza, I., Flores, J. L., & Montero, J. L. (2020). Security issues and software update management in the industrial Internet of Things (IoT) era. *Sensors, 20*(24), Sensor.

Mughal, A. A. (2019). Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges. *Applied Research in Artificial Intelligence and Cloud Computing, 2*(1), 1-31.

Nadee, P., & Somwang, P. (2021). Efficient incremental data backup of unison synchronize approach. *Bulletin of Electrical Engineering and Informatics, 10*(5), 2707-2715.

Naie, H., & Teymournejad, K. (2012). Choosing the best anti-virus in the world by application of the TOPSIS method. *Life Science Journal, 9*(4).

Ncube, C., & Maiden, N. (2004). Selecting cots anti-virus software for an international bank: Some lessons learned. *Proceedings 1st MPEC Workshop.*

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*(92), 101731.

Neri, M., Niccolini, F., & Martino, L. (2023). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information &Amp; Computer Security, 32*(1), 38-52.

Pearce, M., Zeadally, S., & Hunt, R. (2010). Assessing and improving authentication confidence management. *Information Management & Computer Security, 18*(2), 124-139.

Rahayu, R., & Day, J. (2015). Rahayu, R., & Day, J. (2015). Determinant factors of e-commerce adoption by SMEs in developing country: evidence from Indonesia. *Procedia-social and behavioral sciences, 195*, 142-150.

Rock, T. (2023, 10). *Invenioit*. https://invenioit.com/continuity/10-best-practices-for-small-business-backup/ adresinden alındı

Rohith, C., & Kaur, G. (2021). A comprehensive study on malware detection and prevention techniques used by anti-virus. *2021 2nd International Conference on Intelligent Engineering and Management (iciem)* (s. 429-434). IEEE.

Sampaio, D., & Bernardino, J. (2015). Open source backup systems for SMEs. *New Contributions in Information Systems and Technologies*, 823-832.

Sampaio, D., & Bernardino, J. (2015). Open-source backup systems for SMEs. *New Contributions in Information Systems and Technologies: Volume 1*, 823-832.

Singh, D., Mohanty, N. P., Swagatika, S., & Kumar, S. (2020). Cyber-hygiene: The key concept for cyber security in cyberspace. *Test Engineering and Management*, 8145-8152.

Tellini, N., & Vargas, F. (2017). *Two-Factor Authentication: Selecting and implementing a two-factor authentication method for a digital assessment platform.*

Traeger, A., Joukov, N., Sipek, J., & Zadok, E. (2006). Using free web storage for data backup. *Proceedings of the Second ACM Workshop on Storage Security and Survivability.*

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, 102387.

Vaniea, K. E., Rader, E., & Wash, R. (2014). Betrayed by updates: how negative experiences affect future security. *Proceedings of the SIGCHI conference on human factors in computing systems*, (s. 2671-2674).

Ye, Y., Wang, D., Lİ, T., & Ye, D. (2007). IMDS: Intelligent malware detection system. *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*, (s. 1043-1047).

3.modulis – Digitālā higiēna jaunuzņēmumos

1. daļa - Digitālās higiēnas loma jaunuzņēmumu izaugsmē un drošībā

Tāpat kā labas fiziskās veselības saglabāšana, stingras digitālās higiēnas uzturēšana ir būtiska, lai tiešsaistē būtu drošāk. Digitālajai higiēnai vajadzētu kļūt par rutīnu mums visiem gan personīgajā tiešsaistes dzīvē, gan profesionālajā darbībā.

Kā jaunuzņēmumiem, definējot iekšējos noteikumus un politiku, jums ir jāiekļauj arī digitālās higiēnas noteikumi un labākā prakse, kas jāievēro visiem darbiniekiem.

Lielākā daļa mūsu darba aktivitāšu tiek veiktas, izmantojot tiešsaistes digitālās vides. Tātad, jums ir jāapzinās iespējamie riski un jāievieš īpašas politikas, lai tos mazinātu un uzturētu labu digitālo higiēnu savā jaunuzņēmumā.

Pirms apsverat digitālās higiēnas politikas ieviešanu, kas ir tikai formāls uzdevums, kas jums jāpārbauda, padomājiet par visiem ieguvumiem, ko tā var sniegt.

Tātad digitālās higiēnas politikas ieviešana jūsu jaunizveidotajam uzņēmumam nav jauka, bet gan obligāta prasība, lai aizsargātu savu darbinieku profesionālo un personīgo dzīvi. Ja jums ir nepieciešami daži iemesli, lai uzsvērtu digitālās higiēnas prakses nepieciešamību jaunuzņēmumos, pārskatīsim dažus iemeslus, kāpēc digitālā higiēna viņiem ir ļoti svarīga.

Jaunuzņēmumi ir mazas organizācijas, ar ierobežotiem resursiem un bez lielāku organizāciju spēcīgās drošības infrastruktūras. Tas padara tos par pievilcīgiem mērķiem kibernoziedzniekiem un uzņēmīgākiem pret kiberdraudiem. Digitālās higiēnas politika palīdz īstenot efektīvus drošības pasākumus un mazināt iespējamos riskus.

Visbeidzot, jaunuzņēmumiem digitālās higiēnas politika kalpo kā pamatelements drošībai, uzticības veidošanai, mērogojamībai, rentabilitātei un darbības efektivitātei. Tas palīdz noteikt toni atbildīgai un drošai digitālajai praksei, kas ir būtiska jaunuzņēmuma noturīgiem panākumiem un izaugsmei mūsdienu digitālajā uzņēmējdarbības vidē.

2. daļa - Digitālās higiēnas prakses ieviešanas priekšrocības jaunuzņēmumos

Kādi ir ieguvumi no labas digitālās higiēnas prakses ieviešanas?

Vienkāršiem vārdiem sakot, labas digitālās higiēnas praktizēšana padara jūsu klātbūtni tiešsaistē drošu un veselīgu mūsdienu tehnoloģiju virzītajā biznesa vidē. Tātad ieguvumi ir divos līmeņos:

1. **Drošība un uzturēšana**
2. **Veselība**

Noskaidrosim galvenos ieguvumus!

1. **Drošība un uzturēšana**

Labas digitālās higiēnas politikas un paraugprakses īstenošana nodrošinās jūsu darbavietas (un personīgās) digitālās vides drošību. Neaizmirstiet definēt uzturēšanas noteikumus, lai pārliecinātos, ka visi darbinieki ir informēti par iekšējo politiku un ka noteikumi ir atjaunināti ar jauniem iespējamiem draudiem.

Ieteicams periodiski veikt kiberdrošības izpratnes apmācību, lai pārliecinātos, ka jūsu komandai ir nepieciešamās zināšanas, lai pareizi reaģētu uz iespējamiem jauniem kiberdraudiem.

Kā mēs varam apkopot galvenos ieguvumus jaunuzņēmumiem, kad tie ievieš un uztur labu digitālās higiēnas praksi, lai aizsargātu savu drošību digitālajā vidē?

- **Drošības un datu privātuma ievērošana**

Sensitīvas informācijas aizsardzība ir būtiska. Regulāra programmatūras atjaunināšana, spēcīgu paroļu izmantošana un šifrēšanas metožu ieviešana var palīdzēt aizsargāt sensitīvus datus no kiberdraudiem. Laba digitālā higiēna palīdz aizsargāt sensitīvu informāciju un novērš nesankcionētu piekļuvi, samazinot datu pārkāpumu risku. Datu aizsardzības noteikumu ievērošana nodrošina, ka jaunuzņēmums izvairās no juridiskām problēmām un veido uzticību klientiem.

Arī finanšu un klientu datu aizsardzība ir ārkārtīgi svarīga jaunizveidotiem uzņēmumiem. Digitālā higiēna nodrošina drošus tiešsaistes darījumus un finanšu datu integritāti.

- **Reputācijas vadība un uzticības veidošana**

Klienti un partneri uzticas uzņēmumiem, kas par prioritāti izvirza digitālo drošību. Demonstrējot apņemšanos ievērot digitālo drošību un privātumu, var uzlabot jaunuzņēmuma reputāciju un veidot uzticību klientiem, investoriem un partneriem. Tāpat var izvairīties no drošības incidentu negatīvās ietekmes. Labi uzturēti digitālie aktīvi, tostarp lietotājdraudzīga tīmekļa vietne un droši tiešsaistes darījumi, veicina profesionālu tēlu.

- **Atbilstība un tiesiskā aizsardzība: normatīvo aktu prasību izpilde**

Daudzās nozarēs ir stingri noteikumi attiecībā uz datu aizsardzību un privātumu. Nozarei specifisku noteikumu un atbilstības standartu ievērošana palīdz jaunuzņēmumiem izvairīties no juridiskiem sarežģījumiem, naudas sodiem un reputācijas kaitējuma. Šo noteikumu pieņemšana ne tikai aizsargā jaunuzņēmumu no juridiskām sekām, bet arī palīdz veidot uzticamu zīmola tēlu.

Vēl viens svarīgs aspekts ir revīzijas un pārskati. Regulāra digitālās prakses revīzija nodrošina, ka jaunuzņēmums joprojām atbilst mainīgajiem noteikumiem un nozares standartiem.

- **Darbības nepārtrauktība: dīkstāves mazināšana**

Kiberdrošības incidenti, piemēram, ļaunprogrammatūras uzbrukumi vai datu zudums, var izraisīt ievērojamu dīkstāvi. Digitālās higiēnas pasākumi palīdz novērst un mazināt šādus incidentus, nodrošinot nepārtrauktu uzņēmējdarbību.

- **Izmaksu ietaupījumi: izvairīšanās no finansiāliem zaudējumiem**

Atgūšanās no kiberdrošības incidenta var būt dārga. Regulāras dublēšanas un drošas uzglabāšanas metodes var novērst datu zudumu, ietaupot startēšanu no potenciāli augstajām izmaksām, kas saistītas ar zaudētās informācijas atgūšanu. Ieguldījumi digitālās drošības pasākumos agrīnā posmā ir proaktīva pieeja, kas palīdz novērst iespējamus finansiālus zaudējumus kiberuzbrukumu, piemēram, izspiedējvīrusu vai datu aizsardzības pārkāpumu, dēļ.

- **Inovācija un izaugsme: inovācijas veicināšana**

Droša digitālā vide ļauj jaunuzņēmumiem koncentrēties uz inovācijām, pastāvīgi nenovēršot uzmanību no kiberdrošības problēmām. Tas veicina radošumu un paātrina biznesa izaugsmi. Automatizējot ikdienas uzdevumus un optimizējot digitālās darbplūsmas, jaunuzņēmumi var atbrīvot laiku un resursus, lai koncentrētos uz inovācijām un stratēģiskām iniciatīvām. Laba digitālā higiēna nodrošina, ka jaunuzņēmums ir tehnoloģiski gatavs ieviest jaunus rīkus un tehnoloģijas, saglabājot konkurētspēju tirgū.

- **Klientu uzticība un lojalitāte: klientu informācijas aizsardzība**

Klienti, visticamāk, sazināsies ar uzņēmumiem, kas par prioritāti izvirza viņu personiskās informācijas drošību. Digitālā higiēna veido klientu uzticību un lojalitāti, veicinot ilgtermiņa attiecības..

- **Piegādes ķēdes drošība: piegādātāju un partneru drošības nodrošināšana**

Laba digitālās higiēnas prakse sniedzas tālāk par jaunuzņēmuma iekšējām sistēmām, iekļaujot drošu saziņu un datu apmaiņu ar pārdevējiem un partneriem, nodrošinot drošu piegādes ķēdi no gala līdz galam.

- **Spēja pielāgoties jauniem draudiem: apsteigt draudus**

Digitālā higiēna ietver informācijas sniegšanu par jaunākajiem kiberdrošības apdraudējumiem un to novēršanas pasākumu īstenošanu. Šai pielāgošanās spējai ir izšķiroša nozīme pastāvīgi mainīgajā kiberdraudu vidē.

2. **Veselība**

Mēs esam satriekti par daudzajām digitālajām tehnoloģijām un tiešsaistes platformām, kuras mēs izmantojam dienas laikā. Mēs nedrīkstam atstāt novārtā ietekmi, kāda tiem var būt uz mūsu garīgo veselību. Ja darba laikā mēs ievērojam spēkā esošos noteikumus no mūsu organizācijām, mūsu personīgajā dzīvē mums vajadzētu ieviest arī labu digitālo higiēnu. Esiet piesardzīgi ar ekrāna laiku, izvairieties no pārmērīgas ekspozīcijas un virsstundām sociālajos medijos, kā arī izmantojiet paroļu pārvaldnieku un divfaktoru autentifikāciju saviem kontiem, jūs nodrošināsiet tikai drošību.

Labas digitālās higiēnas prakses ieviešana tikai labvēlīgi ietekmē darbinieku produktivitāti un morāli. Uzmanības novēršana tiek samazināta, un darbinieki var būt produktīvāki, ja viņi pastāvīgi nerisina drošības jautājumus. Droša digitālā vide veicina pozitīvu atmosfēru darbavietā un uzlabo morāli.

Kā papildu ieguvumus varam minēt arī digitālās higiēnas prakses ieviešanu un uzturēšanu:

- **Efektīva darbplūsma.** Pareiza digitālo līdzekļu un failu organizācija var racionalizēt darba procesus, ļaujot darbiniekiem ātri atrast informāciju un efektīvāk veikt uzdevumus.
- **Sadarbības.** Digitālās higiēnas prakse, piemēram, sadarbības rīku un mākoņkrātuves izmantošana, uzlabo komandas darbu, nodrošinot centralizētu platformu saziņai un failu koplietošanai.
- **Viegla pielāgošanās izaugsmei un mērogojamība**. Mērogojamu digitālo risinājumu ieviešana jau no paša sākuma ļauj jaunuzņēmumiem augt bez būtiskiem traucējumiem vai nepieciešamības pēc digitālās infrastruktūras kapitālremonta.
- **Elastība.** Tīras un organizētas digitālās vides uzturēšana nodrošina elastību, lai pielāgotos mainīgajām biznesa vajadzībām un tirgus tendencēm**.**
- **Veiklība.** Jaunuzņēmumi, kas pazīstami ar savu veiklību, gūst labumu no efektīvām darbplūsmām un sadarbības, ko nodrošina labi īstenota politika.

Rezumējot, jaunuzņēmumiem digitālās higiēnas politika kalpo kā pamatelements drošībai, uzticības veidošanai, mērogojamībai, rentabilitātei un darbības efektivitātei. Tas palīdz noteikt toni atbildīgai un drošai digitālajai praksei, kas ir būtiska jaunuzņēmuma noturīgiem panākumiem un izaugsmei mūsdienu digitālajā uzņēmējdarbības vidē.

3. daļa — Digitālās higiēnas neievērošanas iespējamie draudi un sekas

Eiropas Savienības Kiberdrošības aģentūra (ENISA) 2023. gada martā publicēja plašu ziņojumu par kiberdrošības apdraudējumiem un problēmām 2030. gadā, lai palielinātu dalībvalstu un ieinteresēto personu informētību par nākotnes draudiem un pretpasākumiem (Mattioli et al., 2023). Daudzi no konstatētajiem draudiem ir aktuāli jau šodien, un nākamajos gados tie joprojām būs aktuāli. 2023. gada oktobrī tā pati aģentūra publicēja ziņojumu par draudiem, par kuriem tika ziņots 2022. gada jūlijā un 2023. gada jūnijā: ENISA Threat Landscape 2023 (Lella, 2023).

Lai gan šo ziņojumu auditorija un ieinteresētās personas ir plašas gan no publiskā, gan privātā sektora, tie ir īpaši svarīgi jaunuzņēmumu kontekstā. Pēdējās ir īpaši neaizsargātas pret kiberdraudiem vairāku faktoru kombinācijas dēļ, kas bieži vien ir saistīti ar to struktūru, resursu ierobežojumiem un strauji mainīgo uzņēmējdarbības vides raksturu. Tā kā jaunietekmes uzņēmumi savā darbībā arvien vairāk paļaujas uz tehnoloģijām un tiešsaistes platformām, tie kļūst jutīgāki pret kiberuzbrukumiem. Kā norādīts iepriekš, iespējamās sekas, kļūstot par kiberdraudu upuriem, ietver datu pārkāpumus, finansiālus zaudējumus, kaitējumu reputācijai un pat uzņēmējdarbības pārtraukšanu. Jaunuzņēmumi bieži apstrādā sensitīvu informāciju, vienlaikus trūkstot infrastruktūrai un resursiem, kas ir lielākām organizācijām, padarot tos par pievilcīgiem mērķiem kibernoziedzniekiem, kuri cenšas izmantot ievainojamības.

Jaunuzņēmumu ievainojamība kiberdraudiem var ievērojami ietekmēt gan ekonomiku kopumā, gan dažādas citas sabiedriskās struktūras. Piemēram, jaunuzņēmumu ievainojamība var ietekmēt plašākas ekonomiskās un sabiedriskās jomas, izraisot ekonomiskos zaudējumus, darbavietu zudumu un bezdarbu, inovāciju palēninašanos, intelektuālā īpašuma zaudējumus, klientu uzticības mazināšanos, piegādes ķēžu traucējumus, regulatīvas un juridiskas sekas, valdības iejaukšanās pieaugumu un pat nacionālās drošības problēmas. Tādēļ jaunuzņēmumiem ir jāapzinās un jāpalielina izpratne par visiem esošajiem un potenciālajiem nākotnes draudiem, lai pasargātu sevi un sabiedrību kopumā.

Visaptveroša izpratne par kiberdraudiem un spēcīgu drošības pasākumu ieviešana ir būtiska jaunuzņēmumiem, lai mazinātu riskus un izveidotu noturīgu pamatu ilgtermiņa panākumiem digitālajā vidē. Lai palīdzētu palielināt izpratni par dažādiem kiberdraudiem, zemāk prezentēsim tos, kas ir iekļauti „ENISA Threat Landscape 2023” ziņojumā (Lella, 2023).

Galvenie ziņojumā iekļautie draudi ir izspiedējprogrammatūra, ļaunprogrammatūra, sociālā inženierija, datu apdraudējumi, pakalpojumatteice, interneta draudi, manipulācija ar informāciju un piegādes ķēdes uzbrukumi. Mēs tos definējām un pēc tam iekļāvām definīcijas no ziņojuma "ENISA Threat Landscape 2023".

1. **Izspiedējvīrusi.** Izspiedējvīruss ir ļaunprātīgas programmatūras veids, kas paredzēts, lai bloķētu piekļuvi datorsistēmai vai failiem, līdz uzbrucējam tiek samaksāta naudas summa vai izpirkuma maksa. Tas var šifrēt failus, padarot tos nepieejamus upurim.
2. **Ļaunprātīga programmatūra.** Ļaunprātīga programmatūra, saīsinājums no ļaunprātīgas programmatūras, ir termins, ko izmanto, lai aprakstītu jebkuru programmatūru vai kodu, kas izveidots ar nolūku kaitēt datorsistēmai, nozagt datus vai traucēt normālu darbību. Tas ietver dažādus veidus, piemēram, vīrusus, tārpus un Trojas zirgus.
3. **Sociālā inženierija.** Sociālā inženierija ir metode, kā manipulēt ar indivīdiem, lai atklātu sensitīvu informāciju vai veiktu darbības, kas var apdraudēt drošību. Metodes ietver pikšķerēšanu, uzdošanos par citu personu un psiholoģiskas manipulācijas, lai izmantotu cilvēku uzvedību.
4. **Datu apdraudējums.** Datu apdraudējums ietver tīšas vai neapzinātas darbības, kas apdraud datu konfidencialitāti, integritāti vai pieejamību. Tas ietver datu aizsardzības pārkāpumus, noplūdes vai jebkādu neatļautu piekļuvi sensitīvai informācijai vai tās izpaušanu.
5. **Pakalpojuma atteikums (DoS).** Pakalpojuma atteikums ir uzbrukums, kura mērķis ir traucēt vai atspējot datorsistēmas, tīkla vai pakalpojuma normālu darbību, padarot to īslaicīgi vai uz nenoteiktu laiku nepieejamu lietotājiem. Izkliedētais pakalpojuma atteikums (DDoS) ietver vairākas sistēmas, kas koordinē uzbrukumu.
6. **Interneta draudi.** Interneta apdraudējumi ir tīši vai netīši interneta vai elektronisko sakaru traucējumi, kas izraisa pārtraukumus, elektrības padeves pārtraukumus, atslēgšanos vai cenzūru. Šos draudus var radīt dažādi faktori, tostarp kiberuzbrukumi, tehniskas problēmas vai valdības virzītas darbības.
7. **Informācijas manipulācijas.** Manipulācija ar informāciju ietver tīšus, koordinētus centienus negatīvi ietekmēt vērtības, procedūras un politiskos procesus. Tas var ietvert maldinošas informācijas izplatīšanu, viltus ziņas vai tādu darbību veikšanu, kas manipulē ar sabiedrisko domu vai traucē normālu informācijas plūsmu.
8. **Piegādes ķēdes uzbrukumi.** Piegādes ķēdes uzbrukumi ir vērsti uz attiecībām starp organizācijām un to piegādātājiem. Šie uzbrukumi ir saistīti ar piegādes ķēdes drošības apdraudēšanu, lai iegūtu nesankcionētu piekļuvi vai ietekmi uz mērķa organizāciju. Kā piemērus var minēt programmatūras atjauninājumu vai aparatūras komponentu kompromitēšanu.

Galvenie apdraudējumi, kas definēti ziņojumā "ENISA Threat Landscape 2023"

„ Izspiedējvīrusi”

Saskaņā ar ENISA (Eiropas Savienības Kiberdrošības aģentūras) ziņojumu par izspiedējvīrusu uzbrukumu draudu ainavu, izspiedējvīruss tiek definēts kā uzbrukuma veids, kurā draudu dalībnieki pārņem kontroli pār mērķa aktīviem un pieprasa izpirkuma maksu apmaiņā pret aktīvu pieejamības atjaunošanu. Šī darbību neitrāla definīcija ir nepieciešama, lai aptvertu mainīgo izspiedējvīrusu draudu ainavu, vairāku izspiešanas tehniku izplatību un dažādos mērķus, kas nav tikai finansiāli ieguvumi, ko izvirza uzbrucēji. Izspiedējvīrusi atkal ir bijuši vieni no galvenajiem draudiem ziņojuma periodā, ar vairākiem augsta profila un plaši publicētiem incidentiem.

Ļaunprātīga programmatūra

Ļaunprogrammatūra, ko dēvē arī par ļaunprātīgu kodu un ļaunprātīgu loģiku, ir visaptverošs termins, ko izmanto, lai aprakstītu jebkuru programmatūru vai aparātprogrammatūru, kas paredzēta neatļauta procesa veikšanai, kas negatīvi ietekmē sistēmas konfidencialitāti, integritāti vai pieejamību.

Sociālā inženierija

Sociālā inženierija aptver plašu darbību spektru, kas mēģina izmantot cilvēku kļūdas vai cilvēku uzvedību ar mērķi iegūt piekļuvi informācijai vai pakalpojumiem. Tā izmanto dažādas manipulācijas formas, lai maldinātu upurus pieļaut kļūdas vai nodot sensitīvu vai slepenu informāciju. Lietotāji var tikt ievilināti atvērt dokumentus, failus vai e-pastus, apmeklēt tīmekļa vietnes vai piešķirt piekļuvi sistēmām vai pakalpojumiem. Lai gan izmantojamie kārdinājumi un triki var ļaunprātīgi izmantot tehnoloģijas, tiem ir jāpaļaujas uz cilvēka elementu, lai gūtu panākumus. Šo draudu ainavu galvenokārt veido šādi uzbrukuma veidi: pikšķerēšana, mērķēta pikšķerēšana, vaļu pikšķerēšana, SMS pikšķerēšana, balss pikšķerēšana, ūdens caurumu uzbrukums, vilināšana, ieganstа radīšana, pakalpojuma apmaiņa, medus lamatas un biedējoša programmatūra. Lai gan sociālās inženierijas paņēmieni bieži tiek izmantoti, lai iegūtu sākotnēju piekļuvi, tie var tikt izmantoti arī vēlākos incidenta vai pārkāpuma posmos. Nozīmīgi piemēri ir biznesa e-pasta kompromitēšana (BEC), krāpšana, izlikšanās, viltošana un izspiešana.

Draudi datiem

Datu pārkāpums GDPR ir definēts kā jebkurš drošības pārkāpums, kas izraisa nejaušu vai nelikumīgu personas datu iznīcināšanu, nozaudēšanu, izmainīšanu vai nesankcionētu izpaušanu vai piekļuvi personas datiem, kas tiek pārraidīti, glabāti vai citādi apstrādāti (GDPR 4.12. pants). Tehniski runājot, draudus datiem var galvenokārt klasificēt kā datu pārkāpumus vai datu

noplūdes. Lai gan bieži šie jēdzieni tiek izmantoti savstarpēji aizvietojami, tie būtībā nozīmē atšķirīgas lietas, kas lielākoties atšķiras pēc to notikšanas veida. Datu pārkāpums ir tīšs kiberuzbrukums, ko veic kibernoziedznieks ar mērķi iegūt nesankcionētu piekļuvi un izplatīt sensitīvus, konfidenciālus vai aizsargātus datus. Citiem vārdiem sakot, datu pārkāpums ir apzināts un spēcīgs uzbrukums sistēmai vai organizācijai ar nodomu nozagt datus. Datu noplūde ir notikums (piemēram, konfigurācijas kļūdas, ievainojamības vai cilvēka kļūdas), kas var izraisīt nejaušu sensitīvu, konfidenciālu vai aizsargātu datu zudumu vai izpaušanu (tīšos uzbrukumus dažkārt dēvē par datu izpaušanu).

Draudi pieejamībai: pakalpojuma atteikums

Pieejamība ir draudu un uzbrukumu pārpilnības mērķis, starp kuriem izceļas DDoS. DDoS ir vērsts uz sistēmas un datu pieejamību, un, lai gan tas nav jauns drauds, tam ir nozīmīga loma kiberdrošības apdraudējumu vidē. Uzbrukumi notiek, ja sistēmas vai pakalpojuma lietotāji nevar piekļūt attiecīgajiem datiem, pakalpojumiem vai citiem resursiem. To var panākt, izsmeļot pakalpojumu un tā resursus vai pārslogojot tīkla infrastruktūras komponentus.

Draudi pieejamībai: interneta draudi

Draudi interneta pieejamībai attiecas uz tīšiem vai netīšiem interneta vai elektronisko sakaru pārtraukumiem, kas izraisa interneta darbības traucējumus, atslēgumus, pārtraukumus vai cenzūru. Interneta darbības traucējumi var rasties valdības noteikto interneta atslēgumu, ciklonu, masveida zemestrīču, elektroenerģijas pārrāvumu, kabeļu bojājumu, kiberuzbrukumu, tehnisku problēmu un militāro darbību dēļ. Šie draudi kļūst daudzveidīgāki un pieaug, sasniedzot jaunu rekordu šajā ziņošanas periodā un izraisot milzīgus naudas zaudējumus nacionālajām ekonomikām.

Informācijas manipulācijas

Ārvalstu informācijas manipulācija un iejaukšanās (FIMI) apraksta galvenokārt nelikumīgu uzvedības modeli, kas apdraud vai var negatīvi ietekmēt vērtības, procedūras un politiskos procesus. Šādai darbībai ir manipulatīvs raksturs, un tā tiek veikta apzināti un koordinēti. FIMI var veikt valsts vai nevalstiski dalībnieki, tostarp to pilnvarotie savā teritorijā un ārpus tās, savukārt šajā ziņojumā mēs pētām draudus neatkarīgi no to izcelsmes.

Piegādes ķēdes uzbrukumi

Piegādes ķēdes uzbrukums ir vērsts uz attiecībām starp organizācijām un to piegādātājiem. Šajā ETL ziņojumā mēs izmantojam definīciju, kas norādīta ENISA draudu ainavā piegādes ķēdes

uzbrukumiem, kurā uzbrukums tiek uzskatīts par piegādes ķēdes sastāvdaļu, ja tas sastāv no vismaz divu uzbrukumu kombinācijas. Lai uzbrukumu klasificētu kā piegādes ķēdes uzbrukumu, gan piegādātājam, gan klientam jābūt mērķiem. SolarWinds bija viens no pirmajiem šāda veida uzbrukuma atklājumiem un parādīja piegādes ķēdes uzbrukumu iespējamo ietekmi. Tika novērots, ka draudu dalībnieki turpina izmantot šo avotu, lai veiktu savas operācijas un iegūtu nostiprinājumu organizācijās, gūstot labumu no plašās ietekmes un lielā upuru skaita šādos uzbrukumos.

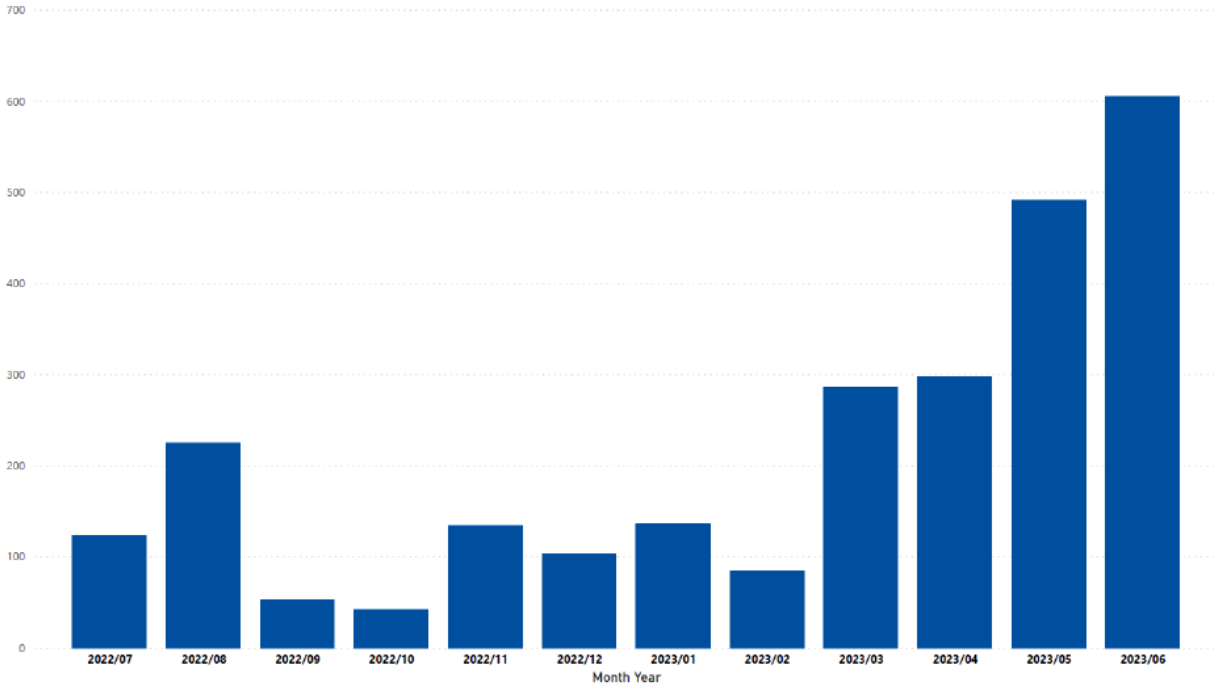
Lella, I.; Tsekmezoglou, E.; Theocharidou, M.; Magonara, E.; Malatras, A.; Naydenov, R.S.; Ciobanu, C. (2023). ENISA Threat Landscape 2023. ENISA, pp. 6-8

Papildus iepriekš definētajiem kiberdraudiem (izspiedējprogrammatūra, ļaunprogrammatūra, sociālā inženierija, datu apdraudējumi, pakalpojuma atteikums, interneta draudi, manipulācija ar informāciju un piegādes ķēdes uzbrukumi) jaunuzņēmumi var saskarties ar dažādiem citiem kiberdrošības apdraudējumiem. Daži papildu draudi, kas jāapzinās, ir šādi:

1. **Pikšķerēšanas uzbrukumi.** Pikšķerēšana ietver maldinošu e-pastu, ziņojumu vai vietņu izmantošanu, lai ar viltu izvilinātu personas, atklājot sensitīvu informāciju, piemēram, lietotājvārdus, paroles vai finanšu informāciju. Pikšķerēšanas uzbrukumi var būt ļoti mērķtiecīgi (šķēpu pikšķerēšana) vai izplatītāki.
2. **Man-in-the-Middle (MitM) uzbrukumi.** MitM uzbrukumos neatļauta vienība pārtver un, iespējams, maina saziņu starp divām pusēm. Tas var novest pie datu zādzības, noklausīšanās vai ļaunprātīga satura ievadīšanas saziņas plūsmā.
3. **Nulles dienas ekspluatācija.** Nulles dienas ievainojamība ir programmatūras ievainojamība, kas piegādātājam nav zināma un nav labota. Draudu dalībnieki var izmantot šīs ievainojamības, pirms tiek izstrādāts labojums, radot risku jebkurai organizācijai, kas izmanto skarto programmatūru.
4. **Uzlabotie pastāvīgie draudi (APT).** APT ir sarežģīti un mērķtiecīgi kiberuzbrukumi, ko parasti organizē labi finansēti un organizēti draudu dalībnieki. Šie uzbrukumi bieži ir saistīti ar ilgstošu un slepenu iefiltrēšanos tīklā, kura mērķis ir nozagt sensitīvu informāciju.
5. **5. IoT (lietu interneta) ievainojamības.** Tā kā jaunuzņēmumi arvien vairāk integrē IoT ierīces savās darbībās, šīs ierīces var kļūt par potenciāliem kiberuzbrukumu mērķiem. Nedrošas IoT ierīces var tikt izmantotas, lai iegūtu nesankcionētu piekļuvi tīkliem vai uzsāktu uzbrukumus.
6. **Kriptonauda.** Kriptonauda ietver nesankcionētu datora vai tīkla resursu izmantošanu, lai iegūtu kriptovalūtu. Kibernoziedznieki var inficēt sistēmas ar ļaunprātīgu programmatūru, kas klusībā mīnē kriptovalūtu, ietekmējot sistēmas veiktspēju.

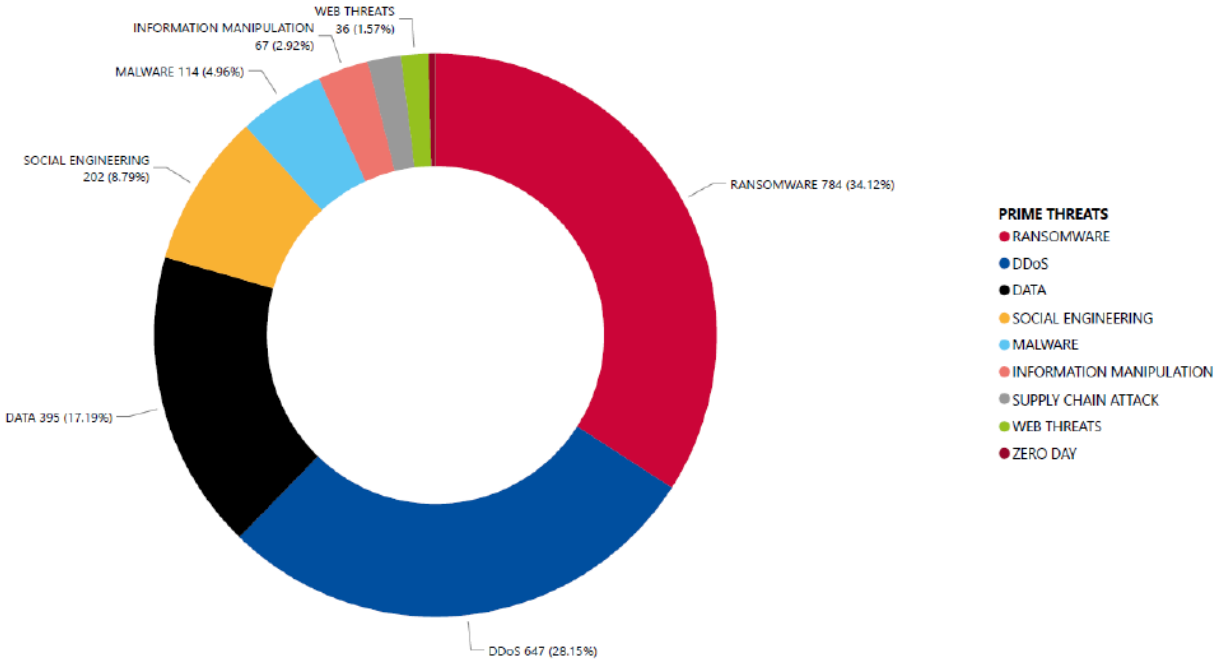
7. **Starpvietņu skriptēšana (XSS).** XSS uzbrukumi ietver ļaunprātīgu skriptu injicēšanu tīmekļa lapās, kuras skatās citi lietotāji. Tas var izraisīt lietotāju datu zādzību, sesijas nolaupīšanu vai ļaunprātīgas programmatūras izplatīšanu citiem lietotājiem.
8. **SQL Injekcijas.** SQL injekcijas uzbrukumi notiek, kad ļaunprātīgs SQL kods tiek ievadīts ievades laukos, ļaujot uzbrucējiem manipulēt ar datu bāzi. Tas var izraisīt nesankcionētu piekļuvi, datu manipulācijas vai datu ieguvi.
9. **Bezfailu ļaunprātīga programmatūra.** Bezfailu ļaunprātīga programmatūra darbojas atmiņā, nevis paļaujas uz izpildāmiem failiem. Tas apgrūtina tradicionālo pretvīrusu risinājumu noteikšanu, jo var nebūt fiziska faila, ko analizēt.
10. **Akreditācijas datu pildījums.** Akreditācijas datu pildīšanas uzbrukumos kibernoziedznieki izmanto nozagtu lietotājvārdu un paroļu kombinācijas no viena pakalpojuma, lai iegūtu nesankcionētu piekļuvi citam pakalpojumam, kurā lietotāji ir atkārtoti izmantojuši akreditācijas datus.
11. **DNS izlikšanās un ķešatmiņas saindēšanās.** DNS izlikšanās ietver domēnu nosaukumu sistēmas (DNS) vaicājumu novirzīšanu uz ļaunprātīgām vietnēm. Ķešatmiņas saindēšanās manipulē ar DNS kešatmiņas datiem, novirzot lietotājus uz neparedzētiem un potenciāli kaitīgiem galamērķiem.

Kā jau minēts, ziņojums "ENISA Threat Landscape 2023" (Lella, 2023) liecina, ka galvenie draudi visā pasaulē un ES ir šādi: izspiedējprogrammatūra, ļaunprogrammatūra, sociālā inženierija, datu apdraudējumi, pakalpojumatteice, interneta draudi, manipulācijas ar informāciju un piegādes ķēdes uzbrukumi.



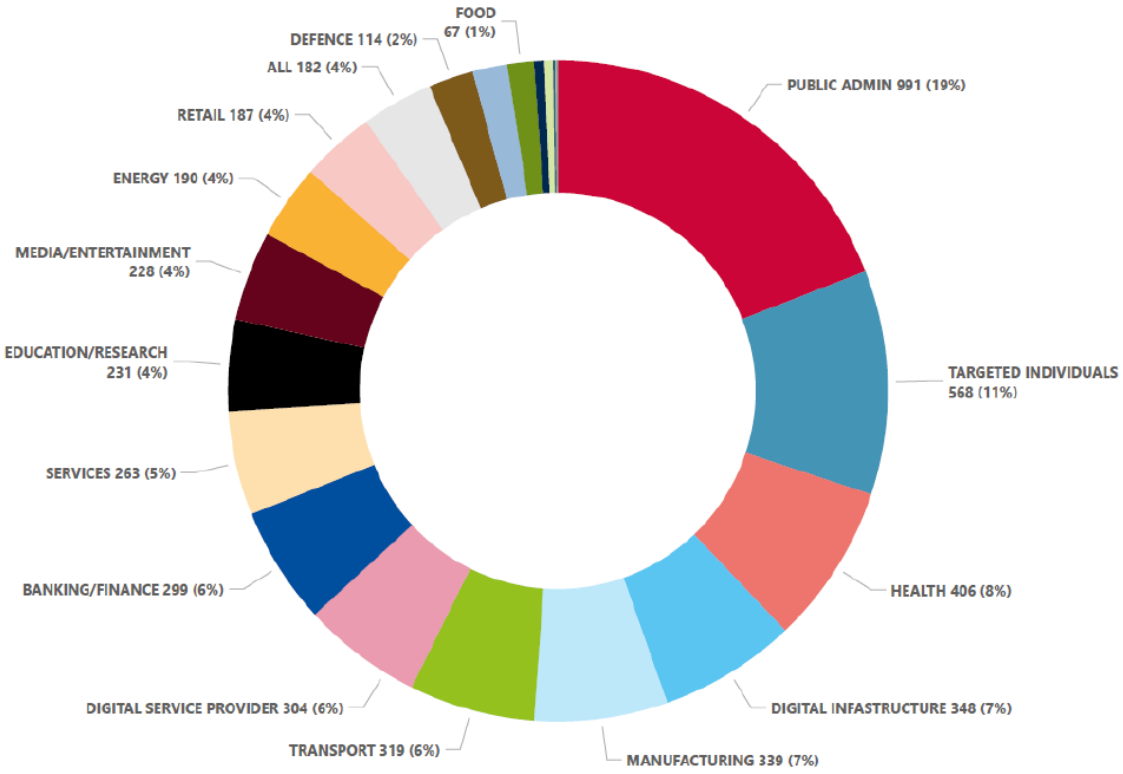
1.attēls. ES notikumu hronoloģisks pārskats (novēroto incidentu skaits mēnesī) (Lella, 2023)

Ziņojumā ir atspoguļots (1. attēls) kiberuzbrukumu skaita pieaugums 2023. gada pirmajā pusē. Šis pieaugums atspoguļojas gan pasaules, gan ES līmenī. Pieaugums varētu atspoguļot ne tikai skaita pieaugumu, bet arī informētību par šādiem notikumiem. Tomēr šī tendence ir satraucoša.



2.attēls. Apdraudējumu skaita sadalījums pa draudu grupām ES (Lella, 2023)

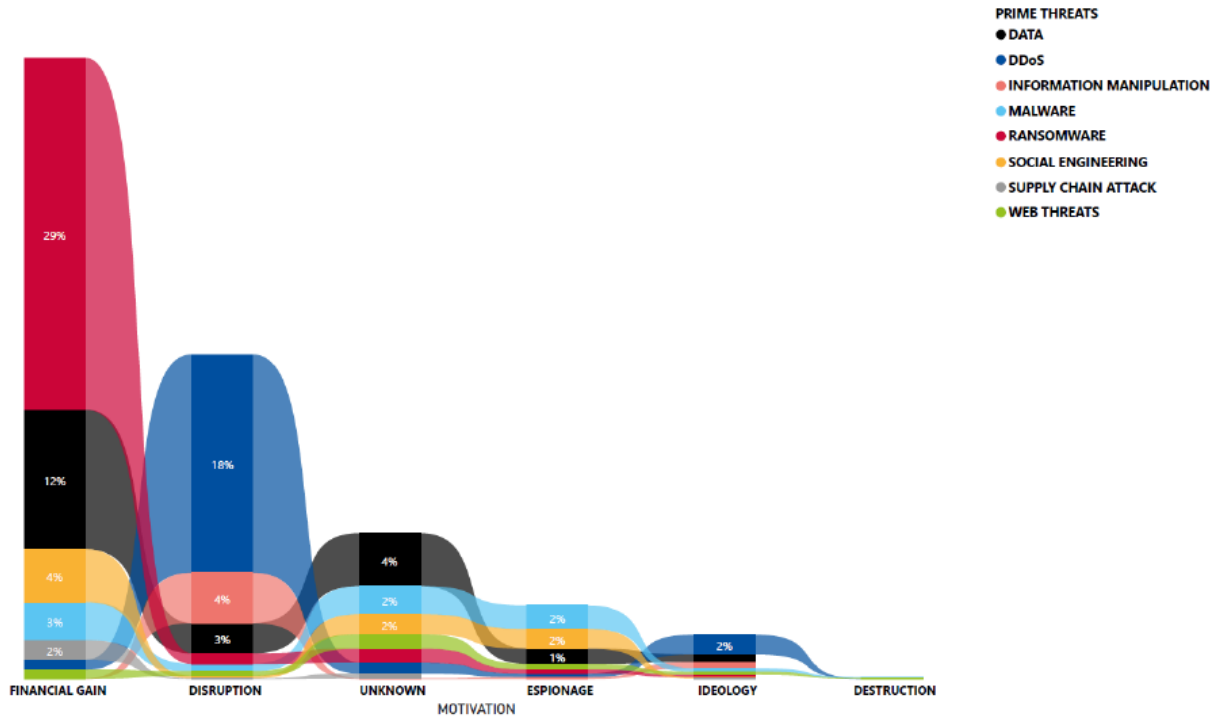
2. attēlā mēs redzam, ka visbiežāk draudi bija: izspiedējprogrammatūra, pakalpojuma atteikums, draudi datiem, sociālā inženierija un ļaunprātīga programmatūra. Tiem sekoja informācijas manipulācijas, piegādes ķēdes uzbrukumi, interneta draudi un nulles diena.



3.attēls. Mērķnozaru skaits uz incidentu skaitu (2022. gada jūlijs – 2023. gada jūnijs) (Lella, 2023)

Nozaru analīze atklāj, ka draudi pārsniedz konkrētu nozaru vai sektoru robežas, ietekmējot plašu jomu spektru (Lella, 2023). Tas varētu būt saistīts ar mūsdienu digitālās pasaules augsto savstarpējo savienojamību.

Kopējā globālajā vidē liels skaits pasākumu bija vērsti uz organizācijām valsts pārvaldes (19%) un veselības (8%) nozarēs. Mēs redzam, ka viens no galvenajiem apdraudētajiem dalībniekiem ir privātpersonas (11%). Lai gan tas var šķist nesaistīts ar jaunuzņēmumiem un privāto sektoru, šīs personas var būt darbinieki dažos jaunizveidotos uzņēmumos, un viņi var netīši apdraudēt uzņēmumus.



4.attēls. Draudu dalībnieku motivācija katrai draudu kategorijai (Lella, 2023)

Ziņojumā ir arī izklāstīta kiberuzbrukumu motivācija noteiktajā periodā (Lella, 2023). Kā redzams 4. attēlā, lielākajai daļai uzbrukumu bija finansiāls ieguvums, kam sekoja traucējumi, nezināmais, spiegošana un ideoloģija. Izspiedējvīrusi veido gandrīz 30% no uzbrukumiem, kas veikti, lai gūtu finansiālu labumu, kam seko draudi datiem, sociālajai inženierijai un ļaunprātīgai programmatūrai.

Izpratne par kiberdraudu iemesliem un draudu veidiem var informēt un vadīt stratēģiju, ko izmanto jaunizveidotie uzņēmumi, lai izstrādātu un ieviestu digitālās higiēnas praksi. Piemēram, jaunizveidotie uzņēmumi un privātais sektors galvenokārt tiek mērķēti finansiālu ieguvumu dēļ. Zinot, ka izspiedējvīrusi, draudi datiem, sociālā inženierija un ļaunprātīga programmatūra galvenokārt tiek izmantoti šādiem mērķiem, jaunizveidotie uzņēmumi varētu koncentrēt savu digitālās higiēnas stratēģiju uz piekļuves datiem aizsardzību un klientu un darbinieku izglītošanu, lai aizsargātu sevi no sociālās inženierijas draudiem.

Lai palīdzētu saprast, kā jaunuzņēmumam būtu jāvēršas pret kiberdraudiem un kas tam jādara, lai sevi aizsargātu, mēs sagatavojām labas prakses piemēru. Tas parādīs, kā uzņēmumam būtu jātiek galā ar iespējamiem draudiem un kā jāsagatavojas, lai novērstu kibernotikumus.

4. daļa – 1 laba prakse no jaunuzņēmumiem

Lai labāk saprastu, kā identificēt draudus un kā iepriekš rīkoties situācijā, aplūkosim šādu piemēru. Mēs koncentrējām piemēru uz ievainojamību, kas var rasties no tiešsaistes maksājumiem, kas ir plaši izplatīta situācija, tā var ietekmēt gan uzņēmumu, gan klientus kiberuzbrukuma situācijā.

Digitālā higiēna tiešsaistes maksājumu drošībā

Konteksts

Strauji mainīgajā mobilo lietotņu izstrādes vidē, kur inovācijas krustojas ar finanšu darījumiem, ir ārkārtīgi svarīgi nodrošināt drošību lietotnei, kas apstrādā tiešsaistes maksājumus. Kā piemēru var minēt uzņēmumu, kas piedāvā mobilās lietotnes abonementu, kas var radīt ievainojamību, kas saistīta ar viņu maksājumu apstrādi. Viņu tiešsaistes maksājumu apstrādes sistēmas iespējamā ievainojamība varētu pakļaut gan uzņēmumu, gan tā klientus finanšu krāpšanas riskiem.

Jaunuzņēmumam ir jāanalizē situācija, jāidentificē riski un jāievieš risinājumi, lai novērstu jebkādas ievainojamības un finanšu krāpšanas situācijas.

1. darbība. Situācijas analīze

Kā pirmais solis digitālās higiēnas procesā mums ir situācijas analīze. Šajā posmā ir svarīgi identificēt ievainojamības un novērtēt šo ievainojamību risku un ietekmi drošības pārkāpuma gadījumā.

Maksājumu drošības ievainojamības identificēšana:

Uzņēmums veica rūpīgu lietotnes maksājumu apstrādes funkcionalitātes analīzi, lai identificētu iespējamos vājos punktus, tostarp nedrošas maksājumu vārtejas, darījumu šifrēšanas ievainojamības un iespējamos nesankcionētas piekļuves punktus.

Visaptverošas maksājumu lietotnes analīzes veikšana, lai identificētu iespējamās vājās vietas, ietver sistemātisku un rūpīgu dažādu lietojumprogrammas komponentu pārbaudi. Vispārīgas pamatnostādnes šādas analīzes veikšanai varētu ietvert::

1. **Riska novērtējums:** Identificējiet un izprotiet maksājumu lietotnes kritiskos komponentus, tostarp lietotāju autentifikāciju, datu glabāšanu, maksājumu apstrādi un saziņu ar ārējiem serveriem.
2. **Normatīvā atbilstības pārbaude:** Pārliecinieties, ka maksājumu lietotne atbilst attiecīgajiem nozares normatīvajiem standartiem un atbilstības prasībām, piemēram, maksājumu karšu nozares datu drošības standartam (PCI DSS).

3. **Datu plūsmas kartēšana:** Kartējiet sensitīvu datu (piemēram, kredītkaršu informācijas) plūsmu lietotnē no ievades līdz glabāšanai un pārsūtīšanai. Nosakiet iespējamos ievainojamības punktus šajā datu plūsmā.
4. **Tīkla drošība:** Novērtējiet tīkla sakaru drošību, tostarp drošu protokolu (HTTPS), šifrēšanas un drošligzdu slāņa (SSL) sertifikātu izmantošanu.
5. **Autentifikācijas mehānismi:** Novērtējiet lietotāju autentifikācijas mehānismu stiprumu. Daudzfaktoru autentifikācijas ieviešana, lai pievienotu papildu drošības slāni.
6. **Maksājumu vārtejas drošība:** Pārbaudiet integrāciju ar maksājumu vārtejām, nodrošinot, ka tiek izmantoti droši un cienījami pakalpojumi. Regulāri atjauniniet un ielāgojiet maksājumu vārtejas programmatūru.
7. **Datu šifrēšana:** Ieviesiet pilnīgu šifrēšanu, lai aizsargātu sensitīvus lietotāja datus visā transakcijas procesā.
8. **Ievainojamības skenēšana un ielaušanās testēšana:** Veiciet regulāru ievainojamības skenēšanu un ielaušanās testus, lai identificētu iespējamās vājās vietas un simulētu reālās pasaules uzbrukumu scenārijus. Tas var ietvert automatizētu rīku izmantošanu vai tādu trešo pušu drošības uzņēmumu nolīgšanu, kuriem ir pieredze ielaušanās testēšanā.
9. **Koda pārskatīšana:** Veiciet rūpīgu koda pārskatīšanu, lai noteiktu lietotnes pirmkoda ievainojamības vai nepilnības. Kodēšanas prakse atbilst drošības paraugpraksei.
10. **Plāns reaģēšanai uz incidentiem:** Izstrādāt un īstenot plānu reaģēšanai uz incidentiem, lai nekavējoties novērstu un mazinātu iespējamos drošības pārkāpumus. Tas ietver procedūru ieviešanu lietotāju informēšanai par drošības incidentu.
11. **Trešo pušu drošības auditi:** Apsveriet iespēju iesaistīt trešo pušu drošības firmas, kas specializējas lietojumprogrammu drošības auditos. Šie uzņēmumi var sniegt neatkarīgu perspektīvu un specializētas zināšanas, lai identificētu vājās vietas.

Šos punktus varat izmantot kā kontrolsarakstu, lai veiktu analīzi.

Drošība ir nepārtraukts process, un regulāras pārbaudes un atjauninājumi ir būtiski, lai būtu soli priekšā jaunajiem draudiem. Iepriekš minētie kontrolsaraksta punkti laika gaitā var mainīties atkarībā no iespējamajiem draudiem un kiberdrošības ainavas. Sadarbība ar trešo pušu drošības firmām vai konsultantiem var nodrošināt papildu zināšanas un ieskatus, īpaši, ja runa ir par rūpīgām drošības auditēm un penetrācijas testēšanu. Ir būtiski prioritizēt maksājumu lietotņu drošību, lai aizsargātu gan uzņēmumu, gan tā lietotājus no potenciāliem riskiem un pārkāpumiem.

Pieņemsim, ka kārtējā drošības audita laikā starta drošības komanda identificē iespējamu trūkumu šifrēšanas protokolā, ko izmanto maksājumu datu pārsūtīšanai savā mobilajā lietotnē. Pēc tam komandai ir jānovērtē ievainojamība un tās ietekme uz uzņēmumu un lietotājiem.

Risku un seku novērtēšana:

Pēc maksājumu drošības ievainojamību identificēšanas ir svarīgi apsvērt riskus un ietekmi gan uz uzņēmumu, gan lietotājiem. Šī procesa daļa ietver uzņēmuma un lietotāju risku novērtēšanu un identificēto ievainojamību prioritāšu noteikšanu atbilstoši potenciālajai ietekmei.

1. **Ietekmes novērtējums:** Novērtējiet drošības pārkāpuma iespējamo ietekmi gan uz uzņēmumu, gan tā lietotājiem, ņemot vērā finansiālos zaudējumus, kaitējumu reputācijai un iespējamās juridiskās sekas.
2. **Prioritāšu noteikšana:** Piešķiriet prioritāti ievainojamībai, pamatojoties uz potenciālās ietekmes smagumu un izmantošanas iespējamību.

Novērtējot riskus, kas saistīti ar šifrēšanas protokola vājumu, drošības komanda novērtē ievainojamības apmēru, ņemot vērā tādus faktorus kā izmantotā šifrēšanas algoritma veids, potenciālās izmantošanas apjoms un ietekme uz lietotāju datu drošību.

Riska analīzes mērķis ir izprast šifrēšanas ievainojamības iespējamās sekas, tostarp nesankcionētas piekļuves risku sensitīvai maksājumu informācijai un iespējamo ietekmi uz uzņēmuma reputāciju.

2. darbība. Risinājuma meklēšana

Risinājumi iespējamām maksājumu drošības ievainojamībām ietvertu:

1. **Droša maksājumu vārtejas integrācija:** Uzlabot maksājumu apstrādes sistēmu, lai to integrētu drošā maksājumu vārtejā, nodrošinot, ka visi darījumi tiek šifrēti un aizsargāti pret pārtveršanu pārsūtīšanas laikā.
2. **Pilnīga šifrēšana:** Ieviesiet pilnīgu šifrēšanu visiem maksājumu darījumiem, aizsargājot sensitīvus lietotāja datus no nesankcionētas piekļuves katrā darījuma procesa posmā.
3. **Lietotāju autentifikācijas uzlabojumi:** Stiprināt lietotāju autentifikācijas pasākumus, iekļaujot daudzfaktoru autentifikāciju, lai nodrošinātu, ka tikai autorizēti lietotāji var piekļūt programmai un veikt darījumus tajā.
4. **Regulāri drošības auditi un atbilstības pārbaudes:** Ieviest regulārus drošības auditus, kas īpaši vērsti uz maksājumu apstrādes funkcionalitāti, veicot atbilstības pārbaudes nozares standartiem un noteikumiem.

Konkrētāk rūpējoties par šifrēšanas protokola vājumu, ko mēs izmantojām kā piemēru, reakcija un mazināšana ietvertu:

1. **Tūlītēja ierobežošana:** Uzņēmums nekavējoties rīkojas, lai ierobežotu ievainojamību, īslaicīgi atspējojot ietekmēto šifrēšanas protokolu, lai novērstu turpmāku iespējamu izmantošanu.
2. **Saziņa ar ieinteresētajām personām:** Uzņēmums uzsāk pārredzamu saziņu ar saviem lietotājiem, informējot viņus par identificēto šifrēšanas ievainojamību, skartās funkcijas pagaidu apturēšanu un pašreizējiem centieniem risināt šo problēmu.
3. **Drošības ekspertu iesaistīšana:** Uzņēmums piesaista ārējo kiberdrošības ekspertu pakalpojumus, lai veiktu padziļinātu šifrēšanas ievainojamības analīzi un sniegtu ieteikumus stabilākam un drošākam šifrēšanas risinājumam.
4. **Ielāpa izstrāde:** Pamatojoties uz drošības ekspertu ieteikumiem, izstrādes komanda izveido ielāpu, kas novērš šifrēšanas ievainojamību. Tas ietver drošāka šifrēšanas algoritma ieviešanu un saderības nodrošināšanu ar esošajām sistēmām.
5. **Iekšējā testēšana:** Pirms ielāpa izvietošanas uzņēmums veic rūpīgu iekšējo testēšanu, lai pārliecinātos, ka atjauninātie šifrēšanas pasākumi nerada jaunas ievainojamības vai netraucē maksājumu lietotnes funkcionalitāti.
6. **Ielāpa izvietošana:** Kad ielāps tiek uzskatīts par efektīvu un drošu, uzņēmums izvieto atjauninājumu visās lietotāju ierīcēs, atjaunojot maksājumu funkcionalitāti ar uzlabotiem šifrēšanas pasākumiem.
7. **Pēcīstenošanas uzraudzība:** Uzņēmums cieši uzrauga lietotnes veiktspēju pēc ieviešanas, lai nodrošinātu, ka šifrēšanas ielāps veiksmīgi mazina ievainojamību un nerada neparedzētas problēmas.
8. **Lietotāju izglītošana:** Lai atjaunotu lietotāju uzticību, uzņēmums lietotnē varētu uzsākt izglītojošu kampaņu, informējot lietotājus par šifrēšanas ievainojamību un darbībām, kas veiktas, lai to novērstu, un sniedzot padomus par drošas lietošanas prakses uzturēšanu.

Šīs reakcijas soļi ir specifiski identificētajai problēmai. Ja drošības auditā tiek konstatēta cita problēma, šai problēmai tiks izmantoti konkrēti risinājumi.

3. darbība. Rezultāti un ietekme

Uzņēmuma mērķtiecīgā pieeja digitālajai higiēnai lietotņu drošībā tiešsaistes maksājumiem deva pozitīvus rezultātus:

- Nav neautorizētu darījumu vai drošības pārkāpumu gadījumu viena gada laikā.

- Palielināta lietotāju pārliecība un uzticēšanās lietotnei, kā rezultātā pieaug darījumu skaits un pozitīvas lietotāju atsauksmes.
- Atbilstība nozares noteikumiem, pozicionējot uzņēmumu kā drošu un uzticamu platformu tiešsaistes maksājumiem.

Galvenās atziņas

Jaunuzņēmumi, kas piedāvā maksājumu apstrādes lietotnes, no šī piemēra var gūt vērtīgu ieskatu:

- Piešķiriet prioritāti drošu maksājumu vārteju integrācijai, lai aizsargātu darījumu datus.
- Ieviesiet pilnīgu šifrēšanu, lai aizsargātu lietotāja datus visā maksājuma procesā.
- Uzlabojiet lietotāju autentifikācijas pasākumus, iekļaujot daudzfaktoru autentifikāciju papildu drošībai.
- Veiciet regulārus drošības auditus un atbilstības pārbaudes, lai apsteigtu iespējamās ievainojamības un nodrošinātu atbilstību nozares standartiem.

Ieviešot šo digitālās higiēnas praksi, maksājumu apstrādes lietotņu izstrādātāji var palīdzēt izveidot drošu un uzticamu platformu, veicinot to lietotāju uzticēšanos, kuri iesaistās tiešsaistes finanšu darījumos.

Atsauksmes

Mattioli, R.; Malatras, A.; Hunter, E.N.; Biasibetti Penso, M.G.; Bertram, D.; Neubert, I. (2023). Identifying Emerging Cyber Security Threats and Challenges for 2030. ENISA

Lella, I.; Tsekmezoglou, E.; Theocharidou, M.; Magonara, E.; Malatras, A.; Naydenov, R.S.; Ciobanu, C. (2023). ENISA Threat Landscape 2023. ENISA

Digital hygiene: the most important unfinished business: https://www.telefonica.com/en/communication-room/blog/digital-hygiene-the-most-important-unfinished-business/

What is Cyber Hygiene? Definition, Benefits, & Best Practices: https://securityscorecard.com/blog/what-is-cyber-hygiene-definition-benefits-best-practices/

What is cyber hygiene and why is it important?:

https://www.techtarget.com/searchsecurity/definition/cyber-hygiene