QKSS
Qendra Kosovare për Studime të Sigurisë

PROGRAMI KËRCËNIMET E RAJA

MANUALI I SIGURISË KIBERNETIKE PËR ORGANIZATAT E SHOQËRISË CIVILE

Nëntor 2023

Mbështetur nga: USAID

PROGRAMI KËRCËNIMET E RAJA

Autorë: Donika Elshani, Jon Limaj, Vesa Kroci

Rreth Programit Kërcënimet e Reja

Programi Kërcënimet e Reja (The Emerging Threats Programme) është projektuar si një përgjigje ndaj kërcënimeve në rritje të sigurisë vendore, rajonale dhe ndërkombëtare. Qëllimi i tij kryesor është të konsolidojë dhe të ofrojë një kuptim më të mirë të kërcënimeve në zhvillim që vazhdimisht largohen nga konceptualizimi tradicional i sfidave të sigurisë. Duke pasur parasysh shtrirjen e kërcënimeve në zhvillim që lidhen me sigurinë kibernetike dhe dezinformimin, ky program synon të ndërtojë kapacitetet e brendshme organizative për të ofruar ekspertizë të bazuar në dëshmi për të funksionalizuar përgjigjet institucionale ndaj këtyre sfidave. Hulumtimi i bazuar në dëshmi në lidhje me Programin e Kërcënimeve e reja (The Emerging Threats Programme) fokusohet në: infrastrukturën kritike, sigurinë kibernetike, dezinformimin dhe sfidat hibride të sigurisë. Përderisa vlerësimi(et) e nevojave, monitorimi dhe hulumtimi mbeten veprime themelore për t'u zhvilluar në program, QKSS synon të shfrytëzojë ekspertizën e krijuar për të rritur drejtpërdrejt kapacitetet e institucioneve dhe agjencive ekzekutive për t'iu përgjigjur në mënyrë efektive sfidave të sigurisë kibernetike dhe dezinformimit. Programi do të zhvillohet përmes:

- Hulumtimeve më të reja të bazuara në dëshmi në lidhje me kërcënimet në zhvillim si: siguria kibernetike dhe dezinformimi;
- Fushatat për ngritjen e vetëdijes dhe avokim të synuar për të përmirësuar nivelin e të kuptuarit të sfidave që lidhen me sigurinë kibernetike dhe dezinformimin në Kosovë;
- Mbështetje për ngritjen e kapaciteteve për institucionet dhe agjencitë ekzekutive për të zhvilluar mjete dhe strategji për të hartuar përgjigje ndaj kërcënimeve në zhvillim.

Për më shumë informacion, na kontaktoni në: EmergingThreats@qkss.org

Raporti i mëposhtëm është publikuar në kuadër të projektit "Shfletimi i lirë në internet" ("Greater Internet Freedom"), zbatuar nga Internews dhe BIRN Hub, përmes mbështetjes së Agjencisë së Shteteve të Bashkuara për Zhvillim Ndërkombëtar (USAID).

Mbështetur nga:

USAID

Përmbajtja

Hyrje

Zhvillimi i hovshëm i teknologjisë në mbarë botën ka bërë që sfera digjitale të bëhet element gjithnjë e më integral i shoqërive moderne bashkëkohore. Këto avancime teknologjike kanë ndikuar thellësisht në mënyrën se si njerëzit jetojnë, punojnë, komunikojnë dhe kryejnë shërbime nëpërmjet rrjetit global online. Organizatat e shoqërisë civile nuk bëjnë përjashtim në këtë aspekt. Këto të fundit po mbështeten gjithnjë e më shumë në mjete të ndryshme digjitale për t'i kryer operacionet e tyre të përditshme në mënyrë më efikase dhe më të qëndrueshme. Me zhvillimin e platformave dhe aplikacioneve të ndryshme sociale dhe digjitale, organizatat e shoqërisë civile kanë mundësi të komunikojnë në mënyrë të shpejtë dhe efikase me qytetarët, donatorët dhe përkrahësit e tyre në nivel lokal dhe global. Zhvillimi i këtyre teknologjive gjithashtu ka sjellë mundësi të reja për OJQ-të në fushën e aktivizmit dhe ndikimit politik, duke ua mundësuar atyre të organizojnë fushata ndërgjegjësimi dhe t'i promovojnë kauzat e tyre tek një audiencë e gjerë e ndjekësve.

Me rritjen e gjurmës digjitale të OJQ-ve rritet edhe rreziku që i kanoset privatësisë dhe sigurisë së tyre në sferën digjitale. Sulmet kibernetike kundrejt këtij sektori janë në rritje dhe përfshijnë një seri taktikash, përfshi këtu hakimin e faqeve zyrtare dhe sistemeve të komunikimit të organizatave, vjedhjen e të dhënave të ndjeshme, keqpërdorimin e fondeve dhe shpërndarjen e dezinformatave dhe lajmeve të rreme, ndër të tjera. Pasojat e sulmeve të tilla janë të mëdha dhe përbëjnë rrezik serioz për funksionimin e rregullt të OJQ-ve. Disa prej pasojave me të cilat mund të ballafaqohen këto të fundit janë dëmtimi i reputacionit dhe imazhit të organizatës, e cila ndikon në humbjen e përkrahjes dhe besimit të donatorëve, partnerëve dhe grupeve me të cilat organizata punon, humbje të mëdha financiare, humbje e informacioneve dhe resurseve tjera kyce të organizatës, ndërprerja e shërbimeve dhe operacioneve të rregullta që ofron organizata, dhe në raste ekstreme, mbyllja e përhershme e organizatës.

Kundrejt këtyre rreziqeve, është thelbësore që OJQ-të të ndërmarrin masa konkrete për të përmirësuar sigurinë e tyre kibernetike dhe për të minimizuar rrezikun që u kanoset. Për fat të mirë, OJQ-të nuk duhet të kenë njohuri të avancuara në fushën e teknologjisë informative për tu mbrojtur nga kërcënimet në sferën digjitale. Mjafton që ato të alokojnë një pjesë të kohës, resurseve financiare si dhe atyre njerëzore për të kultivuar një kulturë të sigurisë përmbrenda organizatës.

Ky manual është përpiluar me qëllim që t'u shërbejë OJQ-ve në Kosovë, por jo vetëm, si udhërrëfyes për të zhvilluar dhe implementuar politika dhe strategji organizative të sigurisë. Manuali paraqet praktika të mira dhe udhëzime konkrete se si një organizatë, pavarësisht fushëveprimit të saj, mund të minimizojë rrezikun që i kanoset në sferën digjitale. Disa nga temat që ky manual trajton janë plani i sigurisë dhe zhvillimi i kulturës së sigurisë në një organizatë, mbrojtja e pajisjeve elektronike brenda organizatës dhe sigurimi i qasjes në to, mbrojtja e shënimeve, siguria në internet, siguria fizike dhe si të veprohet në rast të incidenteve.

Plani i sigurisë

Plani i sigurisë është një dokument strategjik që përcakton objektivat, politikat, procedurat dhe masat që një organizatë duhet të ndjekë për të mbrojtur dhe siguruar të dhënat, resurset dhe infrastrukturën e saj nga rreziqet e jashtme. Plani i sigurisë mund të përfshijë aspekte të ndryshme të sigurisë në organizatë, qoftë ajo siguria fizike, siguria kibernetike, siguria operative si dhe ndërgjegjësimi i stafit lidhur me rreziqet dhe praktikat e sigurisë përmes trajnimeve dhe kampanjave sensibilizuese. Qëllimi kryesor i planit të sigurisë është të sigurojë që organizata të ketë një qasje të strukturuar dhe koordinuar për të minimizuar rreziqet dhe për të garantuar që aktivitetet e saj zhvillohen në mënyrë të sigurtë dhe të mbrojtur.

Plani i sigurisë i çdo organizate duhet të bazohet në një proces të detajuar të **vlerësimit të rrezikut**. Si hap i parë për zhvillimin e planit të sigurisë është **identifikimi i kërcënimeve** kryesore me të cilat mund të ballafaqohet organizata dhe të cilat do të ndikonin në rrezikimin e sigurisë të organizatës. Për të pasur një pasqyrë më të qartë të kërcënimeve që i kanosen organizatës, është e rëndësishme **të identifikohen akterët**, qofshin ata individë, grupe apo entitete tjera, të cilët mund të kenë motive dhe interes për ta targetuar ogranizatën përmes sulmeve të ndryshme. Këta individë apo grupe mund të jenë hakerë, kriminelë, konkurrentë të organizatës, autoritete të agjencive shtetërore apo persona të brendshëm me çasje në sistemet kyçe të organizatës. Një hap tjetër i rëndësishëm është **identifikimi i aseteve** që posedon organizata. Këto asete përfshijnë të dhënat e rëndësishme, sistemet e informacionit, pajisjet elektronike, infrastrukturën fizike dhe çdo resurs tjetër që është i rëndësishëm për funksionimin e organizatës.

Secila organizatë ka plan të veçantë të sigurisë që është i përshtatur për nevojat dhe kërkesat e saj specifike. Sidoqoftë, janë disa rregulla dhe praktika universale të cilat mund të merren për bazë gjatë zhvillimit të planit organizativ të sigurisë, të cilat janë përmbledhur më poshtë.

Mbrojtja e pajisjeve elektronike, sigurimi i qasjes në to dhe mbrojtja e shënimeve

Organizatat mbështeten në një gamë të gjerë të pajisjeve elektronike dhe mjeteve digjitale për t'i kryer operacionet e tyre në baza ditore. Prej kompjuterëve, laptopëve dhe smartfonëve e deri tek serverët, ruterët dhe pajisjet e rrjetit, këto pajisje u shërbejnë OJQ-ve për të komunikuar, përpunuar të dhëna, zhvilluar projekte, menaxhuar burimet e tyre, dhe për të kryer shumë aktivitete të tjera që ndërlidhen me veprimtarinë e tyre. Mbrojtja e pajisjeve elektronike është jashtëzakonisht e rëndësishme sepse këto të fundit përmbajnë në vete të gjitha informacionet dhe të dhënat vitale të organizatës. Qasja e paautorizuar në këto pajisje mund të rezultojë në kompromentimin e integritetit dhe konfidencialitetit të këtyre të dhënave.

Më poshtë janë disa hapa të thjeshtë të cilat çdo organizatë mund t'i ndjekë për ta mbrojtur dhe siguruar infrastrukturën e saj elektronike.

Sigurimi i fjalëkalimeve

Organizata dhe stafi përbërës i saj kanë një numër të madh të llogarive online përmes së cilave ata i kryejnë aktivitetet e tyre të lidhura me organizatën. Për shembull, këtu përfshihen llogaritë për qasje në email, llogaritë e rrjeteve sociale, llogaritë për shërbime e-banking, llogaritë për shfrytëzimin e aplikacioneve të ndryshme, etj. Një mënyrë e lehtë dhe efikase për t'i mbrojtur këto llogari është vendosja e një fjalëkalimi të fortë, i cili i posedon këto karakteristika:

Gjatësia

Një fjalëkalimi i fortë përbëhet nga të paktën 8 karaktere. Në princip, sa më i gjatë të jetë fjalëkalimi, aq më vështirë është për ta gjetur apo thyer atë.

Kompleksiteti

Për të qenë fjalëkalimi i fortë, ai duhet të ketë kombinime të ndryshme të shkronjave, numrave dhe simboleve, përfshi përdorimin e shkronjave të mëdha dhe të vogla. Sa më kompleks të jetë fjalëkalimi, aq më vështirë është për ta gjetur apo thyer atë.

Parashikueshmëria

Fjalëkalimet e parashikueshme në parim janë fjalëkalime të dobëta. Përdorimi i emrit, dates së lindjes, numrit të telefonit apo të dhënave tjera të parashikueshme, rrit rrezikut e gjetjes apo thyerjes së fjalëkalimit. Tutje, vendosja e fjalëkalimeve të cilat përbëhen nga një seri e parashikueshme e shifrave numerik, si psh. '12345678' apo '11111111' gjithashtu duhet të evitohet.

Authentifikimi dy- apo multi-faktorial (Two-factor/multi-factor authentication)

Përveç vendosjes së fjalëkalimeve të forta, një metodë shtesë për t'i mbrojtur llogaritë është përdorimi i authentifikimit dy- apo multi-faktorial. Kjo metodë kërkon që përveç fjalëkalimit, përdoruesi të japë edhe një informacion shtesë për të verifikuar identitetin e tij apo saj. Ky informacion shtesë mund të jetë një kod të cilin përdoruesi e pranon përmes token-it, aplikacioneve të authentifikimit apo sms mesazhit. Authentifikimi ua pamundëson sulmuesëve penetrimin në llogari të ndryshme, edhe nëse ata i kanë gjetur apo thyer fjalëkalimet e këtyre llogarive.

Disa metoda të cilat mund të përdoren për authentifikim janë **token-at** apo **çelësat e sigurisë, kodeve të pranuara përmes mesazheve telefonike dhe aplikacionet e authentifikimit**.

Token-at apo çelësat e sigurisë janë pajisje fizike që përdoren për sigurimin e llogarive. Këto pajisje gjenerojnë një kod të njëhershëm ose një seri unike të numrave të cilat pasi të vendosen në platformën e authentifikimit i japin qasje përdoruesit në

llogari. Përdorimi i token-ave është ndër metodat më të sigurta për authentifikim dhe është metoda më e rekomanduar nga ekspertët për mbrojtjen e llogarive.

Aplikacionet për authentifikim janë softuerë që instalohen në pajisjet elektronike të përdoruesit dhe shërbejnë si mënyrë e sigurtë për të gjeneruar dhe verifikuar kodin authentifikues për hyrje në llogari të ndyrshme online. Ngjajshëm me token-at, ky aplikacion gjeneron një kod unik i cili i jep qasje përdoruesit në llogari. Kjo metodë është më e përshtatshme sepse është e integruar në pajisje elektronike, sic janë telefonat e mençur apo tabletat.

Një mënyrë tjetër për t'i siguruar llogaritë është përmes authentifikimit përmes sms kodit. Sa herë që përdoruesi dëshiron të kyçet në një llogari, ai apo ajo pranon një kod unik përmes mesazhit telefonik, i cili pasi të vendoset në faqen e authentifikimit, i jep qasje përdoruesit në llogari. Kjo është ndër metodat për të përhapura të authentifikimit, mirëpo njëkohësisht është edhe më pak e sigurta. Kjo sepse pajisjet elektronike, sikurse telefonat, mund të përgjohen apo të bien pre e hakimeve.

Sigurimi i pajisjeve të organizatës

Krahas sigurimit të llogarive, është me rëndësi edhe siguria e të gjitha pajisjeve me të cilat disponojnë punëtorët siç janë kompjuterët, llaptopët, telefonat personal, USB -të, etj. Këto të fundit luajnë rol tejet të rëndësishëm në sigurinë fizike dhe kibernetike të organizatës, duke qenë se ato janë portali kryesor përmes së cilit të dhënat dhe sistemet e organizatës mund të ekspozohen. Andaj, pajisjet duhet të sigurohen edhe fizikisht, qofte nga vjedhja apo humbja e tyre. Më poshtë janë listuar disa praktika të mira të përgjithshme për mbrojtjen e pajisjeve të lartë-përmendura:

Blerja e pasijeve të sigurta

Si hap i parë, është e rëndësishme që pajisjet e blera nga organizata të jenë të prodhuara nga kompani të besueshme, të cilat punojnë konform me standardet botërore të prodhimit të pajisjes në fjalë.

Enkriptimi i të dhënave

Ekriptimi është ndër metodat më efikase të mbrojtjes së pajisjeve të një organizate. Enkriptimi nënkupton transformimin e të dhënave të ndryshme në një formë të padeshifrueshme, ku vetëm ata që e kanë 'çelësin' e duhur janë në gjendje t'i kthejnë të dhënat në formën origjinale.

Vendosja e fjalëkalimeve të forta

Sigurimi i pajisjeve të organizatës përmes fjalëkalimeve të forta është po aq i rëndësishëm sa sigurimi i llogarive online përmes së cilave organizata i kryen aktivitetet e saj ditore. Rekomandimet e listuara më lartë lidhur me sigurimin e fjalëkalimeve vlejnë edhe në sigurimin e qasjes në pajisje të organizatës, siç janë laptopët, kompjuterët, telefonat, printerët, etj.

Sigurimi fizik i pajisjeve

Pajisjet duhet të mbrohen edhe fizikisht, duke i vendosur ato në hapësira të sigurta brenda zyreve dhe duke i monitoruar ato vazhdimisht. Kjo e fundit mund të implementohet përmes vendosjes së kamerave të sigurisë në ambientet ku janë të vendosura pajisjet në fjalë. Një tjetër praktikë që rekomandohet është mbajtja e një regjistri të pajisjeve që posedon organizata si dhe çdo hyrje/dalje nga pajisja në fjalë.

Mbrojta e pajisjeve nga ndërhyrjet nga distanca

Një nga rreziqet kryesore për pajisjet e organizatës - përveç humbjes, dëmtimit apo vjedhjes së tyre - është ndërhyrja nga largësia, e njohur ndryshe si 'hakimi' i tyre. Kjo u mundëson personave apo entiteve të paautorizuara jashtë organizatës të fitojnë qasje në pajisjet, të dhënat dhe sistemet e organizatës, pa pasur asnjë kontakt fizik me to.

Termi ombrellë që i përmbledhë llojet e ndryshme të sulmeve nga largësia është 'malware', që në shqip do të mund të përkthehej në 'softuer keqdashës'. Këto të fundit mund t'i 'infektojnë' pajisjet dhe llogaritë e organizatës përmes kanaleve të ndryshme, përfshi përmes postës elektronike, ueb-faqeve të ndryshme, USB-ve, etj. Sulmet e tilla përbëjnë një ndër rreziqet më të mëdha që mund t'i kanosen një organizate, sepse ato mund të qojnë deri te vjedhja e të dhënave të rëndësishme, dëme financiare, deri te cenueshmëria e sigurisë së stafit të organizatës.

Më poshtë janë listuar disa praktika të mira të përgjithshme për t'u mbrojtur nga sulmet 'malware':

Përditësimi i rregullt i të gjitha sistemeve operacionale

Përditësimi i rregullt i të gjitha sistemeve operacionale që i shfrytëzon organizata, sikurse Windows, Mac, Linux dhe Android, është njëra ndër metodat më të lehta dhe efikase për t'iu shmangur sulmeve të lart-përmendura. Është e rëndësishme që përditësimi të bëhet rregullisht, sepse sulmet 'malware' janë vazhdimisht në ndryshim e sipër, secilën herë duke sjellë me vete rreziqe të reja dhe të panjohura. Kjo vlenë jo vetëm për llaptopët dhe kompjuterët që shfrytëzohen nga stafi i organizatës, por edhe për telefonat mobil, të cilët duhet të jenë poashtu të përditësuar.

Instalimi i programeve anti-malware

Instalimi i programeve anti-malware është një tjetër mënyrë për t'u mbrojtur nga sulmet nga distanca. Ekzistojnë programe të tilla të cilat janë falas dhe të besueshme të cilat lehtësisht mund të shfrytëzohen nga organizata.

Vetëdijësimi i stafit rreth sigurisë gjatë shfletimit në internet

Vetëdijësimi i stafit rreth sigurisë gjatë shfletimit në internet është një tjetër praktikë përmes së cilës mund të parandalohen sulmet nga distanca. Stafi i organizatës duhet të jenë të kujdesshëm se çfarë faqe shfletojnë në internet, duke mos klikuar në vegëza të dyshimta dhe duke mos shkarkuar ose hapur dokumente nga burime jo të besueshme.

Sigurimi fizik i pajisjeve

Pajisjet duhet të mbrohen edhe fizikisht, duke i vendosur ato në hapësira të sigurta brenda zyreve dhe duke i monitoruar ato vazhdimisht. Kjo e fundit mund të implementohet përmes vendosjes së kamerave të sigurisë në ambientet ku janë të vendosura pajisjet në fjalë. Një tjetër praktikë që rekomandohet është mbajtja e një regjistri të pajisjeve që posedon organizata si dhe çdo hyrje/dalje nga pajisja në fjalë.

Një tjetër rrezik shumë i përhapur kur bëhet fjalë për sulmet nga distanca janë të ashtu-quajtura sulmet e '**phishing**-ut'. Përmes këtyre të fundit, persona, grupe apo entitete tjera keqdashëse mund të marrin kontroll mbi llogaritë dhe pajisjet e OJQ-ve, të vjedhin informacione të ndjeshme dhe të shkaktojnë dëme të konsiderueshme. Kjo teknikë e sulmit zakonisht përfshin **dërgimin e mesazheve të rreme** elektronike ose krijimin e faqeve të internetit të rreme që duken si faqet zyrtare të organizatës. Duke pranuar mesazhe apo faqe të internetit të cilat në shikim të parë duken të besueshme, punonjësit rrezikojnë të ndajnë me keqdashësit informacione konfidenciale, sikurse fjalëkalimet, të dhënat bankare apo personale, etj.

Për t'iu shmangur sulmeve 'phishing', organizata dhe punonjësit e saj mund t'i ndjekin disa hapa të thjeshtë dhe efektiv, sikur më poshtë:

Verifikimi i burimit të mesazheve/ faqeve në internet

Çdo mesazh që pranohet në llogaritë dhe pajisjet e organizatës duhet të lexohet me kujdes dhe me vëmendje të shtuar. Faqet me prapavi të dyshimta apo të pa-identifikueshme duhet të evitohen çdo here. Njëherit, mesazhet nga persona të panjohur të cilët kërkojnë informacione lidhur me organizatën gjithashtu duhet të raportohen. Rekomandohet që punonjësit të verifikojnë email adresat përmes së cilave i pranojnë mesazhet, si dhe rekomandohet shmangja e shkarkimit të dokumenteve të dyshimta të dërguara përmes email-it.

Ndërgjegjësimi i stafit për sulmet 'phishing'

Mënyra më e mirë për t'iu shmangur sulmeve 'phishing' është duke ditur se si të identifikohen këto sulme dhe si të reagohen në rast të sulmit. Trajnimi i punonjësve të organizatës rreth teknikave dhe shenjave të para të sulmeve 'phishing' është thelbësor për të mbrojtur organizatën nga sulme tentative në të ardhmen.

Sigurimi i të dhënave: Ruajtja, shkëmbimi dhe komunikimi i tyre

Mirëmbajtja e sigurisë kibernetike në një OJQ varet shumë edhe nga komponentat vitale si komunikimi dhe ruajtja apo shkëmbimi i të dhënave. OJQ-të trajtojnë rregullisht informacione konfidenciale në lidhje me përfituesit, donatorët dhe misionet e tyre, si dhe të tjera dhëna konfidenciale sikurse fjalëkalimet, llogaritë bankare dhe të dhënat personale të stafit, të cilat mund të bien pre e sulmeve nga jashtë. **Enkriptimi** është metoda më e përhapur e cila rekomandohet për të siguruar komunikim të sigurt brenda organizatës. Enkriptimi është procesi i kodimit të të dhënave në një mënyrë që bëhet e vështirë për të tjerët t'i kuptojnë ose t'i lexojnë ato pa autorizim. Enkriptimi përdor një algoritëm matematik ose një çelës të veçantë për të koduar të dhëna, të cilat mund të lexohen vetëm nga personat që e kanë çelësin në fjalë.

Njëra ndër llojet për të përhapura të enkriptimit është i ashtu-quajturi **'enkriptimi nga fundi në fund'**. Ky lloj enkriptimi garanton se vetëm personi që dërgon mesazhin dhe personi i synuar për të marrë mesazhin mund të lexojnë përmbajtjen e tij. Asnjë person tjetër, duke përfshirë ofruesin e shërbimit ose ndonjë person të tretë, nuk ka mundësi të hyjë ose të lexojë mesazhin. Organizatat duhet të shtyjnë përpara **praktika të komunikimit përmes mjeteve të cilat e kanë enkriptimin e integruar**, sikurse Signal apo Whatsapp. Organizata gjithashtu duhet të ketë rregullore se sa gjatë mund të mbahen mesazhet e dërguara në llogaritë e organizatës. Kur është fjala te komunikimi përmes postës elektronike, preferohet të përdoret një sistem i gjerë në organizatë, me ç'rast eliminohet rreziku i përdorimit të email adresave private nga punonjësit.

Një tjetër aspekt i rëndësishëm kur bëhet fjalë për sigurimin e të dhënave të organizatës është ruajtja e tyre. Ruajtja e të dhënave një **"cloud"** ose **"re e kompjuterizuar"** është opsioni më i rekomanduar nga ekspertët e sigurisë digjitale në ditët e sotme. Kjo metodë lejon organizatat të ruajnë të dhënat e tyre nëpër serverë të largët që menaxhohen nga kompani të specializuara në shërbimet e ruajtjes së të dhënave, siç janë, për shembull, Google dhe Microsoft.

Disa nga avantazhet e ruajtjes së të dhënave në 'cloud' përfshijnë:

Qasje në të dhënat nga kudo: Ruajtja e të dhënave në 'cloud' u jep punonjësve të organizatës qasje në to pavarësisht se ku ndodhen, mjafton që ata të jenë të lidhur me internet. Kjo e bën këtë metodë ideale, sidomos për organizatat që kanë punonjës të shpërndarë gjeografikisht ose që kanë nevojë për qasje të lehtë në të dhënat në lëvizje.

Siguri e shtuar në rast të incidenteve: Shumica e shërbimeve në "cloud" ofrojnë shërbimet e rezervës automatike, duke siguruar që të dhënat janë të sigurta edhe në rast të humbjes së pajisjeve fizike ose ngjarjeve të tjera të pakëndshme.

Megjithatë, është thelbësore që organizatat të marrin parasysh disa konsiderata të sigurisë kur përdorin shërbime të ruajtjes në "cloud". Kjo përfshin sigurimin e enkriptimit të të dhënave, çoftë përmes fjalëkalimit apo authentifikimit dy-faktorial, zgjedhjen e një kompanie të besueshme që ofron shërbime të "cloud", si dhe hartimin e një politike të qartë përkatëse të sigurisë që përcakton se si të dhënat duhet të trajtohen dhe ruhen në këtë mjedis.

Shfletimi i sigurtë në internet

Është e rëndësishme që gjatë shfletimit në internet, punonjësit e OJQ-ve të sigurohen që informatat e tyre të ndjeshme të mos ekspozohen ndaj rreziqeve të sigurisë. Kjo mund të arrihet duke i përcjellur disa praktika të thjeshta dhe efektive si më poshtë:

Përdorimi i faqeve dhe lidhjeve të sigurta (HTTPS/VPN)

Rekomandohet që sa herë punonjësit e organizatës të vizitojnë një faqe të internetit, të përdorin protokollin **'https'**, i cili siguron një lidhje të sigurtë që parandalon ndërhyrjet e treta dhe zbulimin e të dhënave të shfletuesit. Po ashtu, përdorimi i një **'VPN (Virtual Private Network)'** gjithashtu rekomandohet për të shtuar nivelin e sigurisë dhe për të fshehur identitetin dhe vendndodhjen e përdoruesve.

Parandalimi i sulmeve 'phishing'

Punonjësit e organizatës duhet të evitojnë çdo faqe të dyshimtë në internet përmes së cilës mund të kompromentohen të dhënat e organizatës. Po ashtu, ata duhet të mbajnë vigjilencë të veçantë kur shfletojnë në internet për të parandaluar kompromentimin e informacioneve konfidenciale si të dhënat bankare, fjalëkalimet, apo të dhënat personale të stafit. OJQ-të duhet të vendosin masa të forta të sigurisë së emailit për të ruajtur integritetin e punës së tyre. Kjo përfshin zbatimin e filtrave të sofistikuar të spamit dhe programeve anti-malware, trajnimin e rregullt të personelit se si të identifikojë dhe trajtojë rreziqet e postës elektronike, dhe sigurimin e transmetimit të sigurt të të dhënave të rëndësishme përmes enkriptimit.

Përditësimi i rregullt i shfletuesve në internet

Përditësimet e shfletuesve të internetit si Google Chrome, Safari dhe Mozilla Firefox, përbëjnë një mënyrë të mirë dhe të lehtë për të siguruar që shfletimi në internet të jetë i sigurt dhe pa pasoja për organizatën. Përditësimet e rregullta sigurojnë përmirësime të sigurisë dhe i bëjnë pajisjet e organizatës më të sigurta nga sulmet potenciale.

Siguria fizike në OJQ

Përkundër që siguria kibernetike është e rëndësisë së veçantë për funksionimin e rregullt të një OJQ-je, nuk duhet lënë anash edhe masat e sigurisë fizike, përfshi sigurinë e pajisjeve, inventarit dhe punonjësve të organizatës. Sulmet fizike sikurse vjedhja apo humbja e pajisjeve/inventarit, shpesh kanë pasoja të rëndësishme si për sigurinë fizike, ashtu edhe për sigurinë e informacionit. Duke ndjekur hapat e mëposhtëm, OJQ-të mund të parandalojnë sulmet fizike që u kanosen:

Kontrolli i hyrjeve dhe daljeve në ambientet e zyrës

Organizata duhet të mbajë një regjistër të rregullt të çdo personi që viziton ambientet e zyrës. Ky regjistër duhet të përmbajë të dhëna identifikuese të personave në fjalë, përfshi emrin dhe mbiemrin, datën dhe orën e vizitës si dhe arsyen e vizitës. Në këtë mënyrë, organizata parandalon hyrjet e pa-autorizuara të cilat mund të çojnë deri te cenueshmëria e sigurisë fizike dhe asaj të informacionit.

Mbajtja e pajisjeve në hapësira të sigurta dhe të monitoruara vazhdimisht

Pajisjet elektronike dhe çdo pajisje tjetër me rëndësi për organizatën duhet të mbahen në ambiente të sigurta dhe të mbyllura. Qasja në këto pajisje duhet të jetë e limituar vetëm për stafin e organizatës. Gjithashtu rekomandohet vendosja e kamerave të sigurisë dhe sistemeve të alarmit në mënyrë që pajisjet të jenë nën vëzhgim të vazhdueshëm.

Ruajtja e dokumenteve dhe materialeve tjera fizike

Ndonëse një pjesë e madhe e aktiviteteve të përditshme të OJQ-ve veçse janë bartur në sferën virtuale, organizatat vazhdojnë të prodhojnë kopje fizike të dokumenteve dhe materialeve tjera. Është me rëndësi që kopjet e dokumenteve që përmbajnë çfarëdo lloj informacioni konfidencial të organizatës të mbahen në ambiente të mbyllura dhe të sigurta. Rekomandohet që këto të mbahen në kabinete të mbyllura të cilat janë të qasshme vetëm për personat e autorizuar në organizatë. Tutje, organizatat rekomandohen të kenë një makinë për shkatërrimin e letrës, duke u siguruar kështu që të dhënat në dokumentet të cilat nuk i nevojiten më organizatës të mos bien në duar të gabuara.

Reagimi ndaj incidenteve të sigurisë

Ndonëse praktikat e lartpërmendura ndihmojnë në parandalimin e incidenteve të sigurisë përbrenda organizatës, ato nuk e eliminojnë plotësisht mundësinë që incidentet të ndodhin. Është e rëndësishme që në raste kur incidentet ndodhin, punonjësit e organizatës të dijnë se si të reagojnë në mënyrë të shpejtë dhe efektive.

Çdo organizatë duhet ta ketë të përpiluar një **plan të reagimit ndaj incidenteve**, si pjesë e integruar e planit të përgjithshëm të sigurisë të organizatës. Ndër të tjera, plani i reagimit ndaj incidenteve duhet t'i ketë të specifikuara elementet e mëposhtme:

Hapat specifikë që do të ndiqen në rast të një incidenti, duke përfshirë identifikimin dhe konfirmimin e incidentit, ndërhyrjen për parandalimin e përhapjes së tij, hetimin dhe vlerësimin e dëmeve, si dhe komunikimin e rregullt me personelin dhe autoritetet e nevojshme.

Vlerësimi i dëmeve të shkaktuara, përfshi dëmet financiare, ndaj reputacionit dhe dëmet tjera që lidhen me aktivitetet e përditshme të organizatës. Pasi të jetë bërë vlerësimi i dëmit, organizata duhet të ketë një procedurë të rregullt për raportimin e incidentit te personeli i lartë drejtues, si dhe për komunikimin me autoritetet e sigurisë dhe personelin e brendshëm. Komunikimi është aspekt tejet i rëndësishëm i procesit të rehabilitimit nga incidenti i shkaktuar. Çfarë informata ndahen me publikun lidhur me incidentin, si ndahen këto informata dhe nga kush, përcaktojnë mënyrën se si kjo ngjarje do të përceptohet nga akterë jashtë organizatës, andaj personat përgjegjës për menaxhimin e incidentit duhet t'i marrin parasysh këta faktorë.

Çdo informatë, fotografi apo lëvizje që lidhet me incidentin duhet ruajtur si **dëshmi**. Në këtë rast është shumë me rëndësi që të parandalohet dëmtimi i mëtejmë dhe duhet ndërmarrë hapa të menjëhershëm për të adresuar problemet, dobësitë dhe cenueshmëritë që kanë shkaktuar incidentit.

Trajnimin dhe sensibilizimin e rregullt të stafit në lidhje me procedurat e reagimit ndaj incidenteve.

Një aspekt tjetër i rehabilitimit pas një incidenti të sigurisë që shpesh nuk i jepet rëndësia e duhur është **mbështetja emocionale për stafin** të cilët janë prekur nga incidenti. Incidentet e sigurisë, sidomos ato të mëdha ose të rënda, mund të shkaktojnë ankth, frikë, stres, dhe ndjenja të tjera negative te stafi. Krijimi i një mjedisi të hapur ku punonjësit ndihen të lirë të flasin për ndjenjat e tyre dhe frikën e tyre ndihmon në zbutjen e stresit dhe përmirësimin e mirëqenies emocionale të tyre. Në raste të caktuara organizata rekomandohet të ofrojë shërbime të këshillimit të psikologut apo specialistëve të tjerë të shëndetit mendor.

Katalogimi në botim – **(CIP)**

Biblioteka Kombëtare e Kosovës "Pjetër Bogdani"

519.718(047)

Elshani, Donika

Manuali i sigurisë kibernetike për organizatat e shoqërisë civile / Donika Elshani, Jon Limaj, Vesa Kroci. - Prishtinë : QKSS, 2023. - 8 f. ; 28 cm. 1. Limaj, Jon 2. Kroci, Vesa

ISBN 978-9951-842-08-2

Rreth QKSS

E themeluar në prill të vitit 2008, Qendra Kosovare për Studime të Sigurisë (QKSS) është një organizatë e specializuar dhe e pavarur joqeveritare. Qëllimi primar i QKSS është të promovojë demokratizimin e sektorit të sigurisë në Kosovë dhe të përmirësojë punën kërkimore dhe avokuese në lidhje me sigurinë, sundimin e ligjit dhe bashkëpunimin rajonal dhe ndërkombëtar në fushën e sigurisë.

QKSS synon të rrisë efektivitetin e Reformës së Sektorit të Sigurisë duke mbështetur programet e këtij sektori përmes hulumtimeve, eventeve, trajnimeve, avokimit dhe këshillave të drejtpërdrejta për politikë-bërësit.

Avancimi i ideve të reja dhe metodave të shkencave sociale janë gjithashtu vlerat thelbësore të qendrës. Çdo vit, QKSS publikon raporte të shumta, analiza të politikave dhe përmbledhje të politikave për çështjet që kanë të bëjnë me sigurinë. QKSS gjithashtu organizon më shumë se 200 ngjarje publike duke përfshirë konferenca, tryeza dhe debate, ligjërata në Kosovë, ku një pjesë e tyre organizohen në bashkëpunim me partnerë rajonalë dhe ndërkombëtarë.

Një gamë e gjerë aktivitetesh përfshijnë hulumtimin, ngritjen e kapaciteteve, ngritjen e ndërgjegjësimit dhe avokimin. Puna e QKSS-së mbulon një gamë të gjerë temash, duke përfshirë por pa u kufizuar në: reformën dhe zhvillimin e sektorit të sigurisë, identifikimin dhe analizimin e rreziqeve të sigurisë që lidhen me ekstremizmin, radikalizmin dhe krimin e organizuar, politikën e jashtme dhe bashkëpunimi rajonal, dhe vlerësimin e sundimit të ligjit në Kosovë. Këtë vit QKSS shënoi 15 vjetorin e themelimit. Për më tepër detaje rreth QKSS, mund të referoheni tek:

qkss.org
securitybarometer.qkss.org

@KCSSQKSS
#KCSSQKSS

ISBN 978-9951-842-08-2