Udhëzues për qëndrim të sigurt në internet:

Higjiena kibernetike për institucionet publike dhe NVM-të

Vladan Babiq dhe Aleksandar Bratiç

Tetor 2022

DCAF Geneva Centre for Security Sector Governance

Rreth dcaf

DCAF – Qendra e Gjenevës për qeverisjen e sektorit të sigurisë i është përkushtuar përmirësimit të sigurisë së shteteve dhe njerëzve të tyre brenda kornizës së qeverisjes demokratike, sundimit të ligjit, respektimit të të drejtave të njeriut dhe barazisë gjinore. Që nga themelimi i tij në vitin 2000, DCAF ka kontribuar në krijimin e paqes dhe zhvillimit më të qëndrueshëm duke ndihmuar shtetet partnere dhe aktorët ndërkombëtarë që mbështesin këto shtete, për të përmirësuar qeverisjen e sektorit të tyre të sigurisë përmes reformave gjithëpërfshirëse dhe pjesëmarrëse. DCAF krijon produkte inovative të njohurive, promovon norma dhe praktika të mira, ofron këshilla ligjore dhe politikash dhe mbështet ndërtimin e kapaciteteve të palëve të interesuara në sektorin e sigurisë shtetërore dhe joshtetërore.

DCAF - Qendra e Gjenevës për qeverisjen e sektorit të sigurisë
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Gjenevë, Zvicër
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva
Photo credit: Shutterstock, image contributor: Illus_man
Design & layout: DTP studio

Përmbajtje

Hyrje

Ky dokument jep një pasqyrë të standardeve minimale për krijimin e sistemeve të higjienës kibernetike në institucionet publike dhe ndërmarrjet e vogla dhe të mesme (NVM). Ai paraqet masat që çdo organizatë duhet të zbatojë për të siguruar një nivel të përshtatshëm të sigurisë së informacionit për sistemet e saj informatike.

Qëllimi këtu është që të paraqitet rëndësia e higjienës kibernetike dhe të rekomandohen hapa të zbatueshëm që do të përmirësojnë sigurinë kibernetike brenda organizatës suaj.

Shkurt, higjiena e sigurisë është njësoj si larja e duarve. Kur mjeku hungarez Ignaz Semmelweis shqiptoi dy fjalët e thjeshta “lani duart” në vitin 1850, ai revolucionarizoi mjekësinë, ndonëse askush nuk e mori seriozisht në fillim. Ai vërejti se higjiena e mirë ishte e lidhur në mënyrë të pashmangshsme me shëndetin e mirë dhe me kalimin e kohës, të dhënat provuan se pastrimi parandalues i duarve reduktonte infeksionet.

Higjiena kibernetike në mënyrë të ngjashme ka të bëjë me praktikat që synojnë të parandalojnë infeksionet me malware, si dhe ndërhyrjet kibernetike dhe humbjen e të dhënave ose korruptimin, dhe të mbajnë një mjedis të shëndetshëm kibernetik. Kjo siguron shëndetin e sistemeve dhe përmirëson sigurinë kibernetike në të njëjtën mënyrë që larja rutinë e duarve ndihmon në parandalimin e përhapjes së sëmundjes.

Duke pasur parasysh se të gjitha organizatat përdorin sistemet informatike për të bërë biznes sot, të gjitha janë të ekspozuara ndaj sulmeve të ndryshme kibernetike që mund të parandalojnë funksionimin e sistemeve informatike ose të bllokojnë qasjen në të dhëna. Kështu, çdo organizatë duhet të mbrojë sistemin(sistemet) e saj dhe duhet të krijojë procedura dhe politika, si dhe të ofrojë trajnime të rregullta, për të krijuar praktika të përshtatshme të higjienës kibernetike.

Përkufizime

Janë dhënë shumë përkufizime të ndryshme të higjienës kibernetike, dhe të gjitha janë të sakta.

- Digital Guardian i referohet higjienës kibernetike si “praktikat dhe hapat që përdoruesit e kompjuterëve dhe pajisjeve të tjera marrin për të ruajtur shëndetin e sistemit dhe për të përmirësuar sigurinë në internet.”
- Kaspersky Lab thekson se higjiena kibernetike “ka të bëjë me trajnimin e vetes për të formuar zakone të mira rreth sigurisë kibernetike në mënyrë që të paraprini kërcënimet kibernetike dhe probleme të sigurisë online.”
- Revista Security përshkruan higjienën kibernetike si “sigurimi i kontrollit të plotë në mënyrë të vazhdueshme në të gjithë mjedisin tuaj.”
- Forumi i Sigurisë Kibernetike (CyberSecurity Forum) vë në dukje se higjiena kibernetike “është një term i përbashkët që i referohet praktikave më të mira dhe aktiviteteve të tjera që administratorët e sistemit kompjuterik dhe përdoruesit mund të ndërmarrin për të përmirësuar sigurinë e tyre kibernetike ndërsa përfshihen në aktivitete të përbashkëta në internet, të tilla si shfletimi në ueb, dërgimi i emailit, dërgimi i mesazheve, etj.”
- Blogu Endpoint e karakterizon higjienën kibernetike si “një grup i praktikave të zakonshme për të siguruar trajtimin e sigurt të të dhënave kritike dhe të rrjeteve. Është si higjiena personale, ku zhvilloni një rutinë aktivitetesh të vogla dhe konkrete për të parandaluar ose zbutur problemet shëndetësore.”

Me fjalë të tjera, higjiena kibernetike është një grup praktikash themelore të sigurisë që mund të merren nga i gjithë personeli për të mbrojtur veten, si dhe shëndetin e harduerit dhe softuerit personal dhe organizativ, në sistemet e bazuara në kompjuter.

Masa të përbashkëta

Higjiena e mirë kibernetike kërkon zbatimin e disa masave të përbashkëta, nga krijimi i procedurave dhe politikave të standardizuara deri në trajnime të rregullta që ndihmojnë punonjësit të kuptojnë kërcënimet

kibernetike gjithnjë në zhvillim. Natyra dhe karakteri i disa prej këtyre kërcënimeve janë përshkruar më vonë në tekst (shih kërcënimet e përbashkëta kibernetike). Por së pari, janë detajuar elementët kryesorë të një programi efektiv të higjienës kibernetike, si dhe praktikat e mira.

Analizoni sistemet dhe vendosni procedura dhe politika

Inventari i aseteve

Mbajtja e inventarit të harduerit dhe softuerit

Menaxhimi i harduerit dhe softuerit të TI-së (asetet e TI-së) mund të jetë një detyrë dërrmuese, veçanërisht nëse pajisjet dhe personeli lëvizin ose ndryshojnë vazhdimisht, por ka rëndësi thelbësore. Hardueri, softueri dhe të gjitha pajisjet e rrjetit dhe jo-rrjetit llogariten si asete për këtë qëllim.

Mbajtja e një inventari të harduerit dhe softuerit do të mbështesë procese të ndryshme në organizatën tuaj, si:

- Menaxhimi i incidenteve
- Menaxhimi i problemeve
- Menaxhimi i ndryshimeve

Dhe në këto procese, shtrohen pyetjet në vijim:

- Çfarë bën ky aset i TI-së?
- Çfarë lloj Sistemi Operativ përdor?
- Cilat aplikacione ruhen në aset?
- Çfarë është topologjia e rrjetit?
- Kush ka qasje në aset?
- Kush mban përgjegjësi për të?

Për të dhënë përgjigje, nevojitet një bazë e centralizuar informacioni. Kështu, hapi i parë në krijimin e praktikave të higjienës kibernetike është **standardizimi i inventarit të softuerit dhe harduerit**:

1. Dokumentuar qëndrimin bazë të sigurisë së organizatës
2. Duke standardizuar këtë në të gjithë organizatën bazuar në politikën dhe procedurat
3. Duke monitoruar dhe duke reaguar ndaj devijimeve
4. Duke reduktuar çdo dobësi që paraqitet nga hardueri dhe softueri

Përfitimet e mbajtjes së një inventari softuerik dhe harduerik janë shpejt të dukshme, dhe përfshijnë:

- Kontrollin e mjedisit TI
- Kontrollin e aseteve të softuerit (versioni, patch, varësia, llogaridhënia, prova e konceptit (Proof of concept - PoC))
- Kontrolli i pajisjeve harduerike (versioni, kritikaliteti, PoC, varësia)
- Administrimi efektiv
- MTTRS më e mirë (Koha mesatare për të rivendosur shërbimin)

Inventari i informacionit

Mirëmbajtja e një inventari të informacionit të ndjeshëm ose kritik

Mbrojtja e informacionit të ndjeshëm – që përfshin etiketimin, zbulimin dhe menaxhimin e duhur të tij – është jashtëzakonisht sfiduese. Mund të jetë e vështirë të kuptohet se si përdoruesit ndërveprojnë me dhe ndajnë këtë informacion. Kështu, nuk është çudi që më shumë se gjysma e të dhënave të korporatave janë 'të errëta', që do të thotë se ato nuk klasifikohen, mbrohen ose qeverisen.

Është jetike të kuptoni **peizazhin tuaj të të dhënave dhe të identifikoni të dhënat e rëndësishme në të gjithë mjedisin tuaj**. Për këtë qëllim, është e rëndësishme të krijohet një **politikë e klasifikimit të të dhënave** si hap i parë. Ekzistojnë skema të ndryshme klasifikimi që mund të përdoren sipas nevojës,

por shembulli më poshtë paraqet tre nivele:

- *Të kufizuara* – të dhëna të ndjeshme që përbëjnë një rrezik të madh nëse kompromentohen, aksesohen.
- *Konfidenciale* – Të dhëna mesatarisht të ndjeshme, të aksesueshme vetëm brenda organizatës.
- *Publike* – të dhëna jo të ndjeshme që do të shkaktonin pak ose aspak rrezik nëse do të aksesoheshin.[1]

Si hap i dytë, të dhënat duhet të jenë të koduara, veçanërisht çdo e dhënë e shënuar me një etiketë 'e kufizuar'.

Së fundi, duhet të zbatohet një **sistem i parandalimit të humbjes së të dhënave** për të zbuluar shkeljet e mundshme të të dhënave/transmetimet e eksfiltrimit të të dhënave dhe për t'i parandaluar ato duke monitoruar, zbuluar dhe bllokuar të dhënat e ndjeshme gjatë përdorimit, lëvizjes dhe pushimit.

Kjo duhet të përfshijë disa skanime dhe automatizime (për të cilat Microsoft është një mjet i mirë), dhe duhet të mbulojë:

- Depot në vend
- Aplikacionet Office
- Sajtet e SharePoint
- Exchange
- Aplikacionet cloud jo-Microsoft dhe SaaS

Vlerësimi i rreziqeve

Identifikoni rreziqet

Menaxhimi i rrezikut kërkon një kuptim të kërcënimeve me të cilat përballet organizata juaj dhe hapat që mund të ndërmerren për të parandaluar, zvogëluar ose përgatitur situata që mund të ndodhin ose jo.

Ekzistojnë tre fusha të rrezikut për sistemet e informacionit:

- **Rreziku njerëzor**, si mashtrimi, vjedhja ose gabimi njerëzor.
- **Rreziku natyror**, si përmbytjet, zjarret, apo tërmete.
- **Rreziqet teknike**, si dështimet e softuerit, harduerit ose mungesa e njohurive.

Si pikënisje, vlerësimi i rrezikut përfshin caktimin e vlerës për asetet kritike, si financiare ashtu edhe të reputacionit. Kjo do t'ju ndihmojë të filloni të vlerësoni se sa shqetësuese janë kërcënimet specifike. Mënyra efektive për ta bërë këtë është duke shënuar secilin skenar – së pari, mbi gjasat e shfaqjes, dhe së dyti, mbi dëmin që do të shkaktonte shfaqja e tij.

Kjo do të bëjë që të kuptoni më mirë se ku të përqendroni përpjekjet dhe do t'ju ndihmojë të vendosni se si t'i qaseni rreziqeve, për shembull, me:

- Shmangie, kur rreziqet nuk janë një shqetësim i drejtpërdrejtë për biznesin tuaj
- Reduktim, kur rreziqet kërkojnë zbatimin e një zgjidhjeje të re sigurie
- Pranim, kur një rrezik nuk ka gjasa të ndodhë ose parandalimi i tij është përtej aftësive ekzistuese
- Transferim, kur një rrezik mund të sigurohet

Procedura e bërjes së kopjes rezerve (backup)

Krijimi i një procedure të rregullt të bërjes së kopjes rezervë (backup)

Është jashtëzakonisht e rëndësishme të keni një procedurë të bërjes së kopjes rezervë. Qëllimi është të krijohet një kopje e të dhënave që mund të rikuperohen në rast të humbjes së të dhënave – që mund të ndodh nga dështimi i harduerit ose softuerit, korruptimi i të dhënave ose ngjarjet e shkaktuara nga njeriu, të tilla si sulmet dashakeqe ose fshirja aksidentale. Një politikë e konceptuar mirë për backup, me procedura të qarta, është thelbësore dhe përfaqëson linjën e fundit të mbrojtjes për një organizatë.

Pothuajse të gjitha organizatat kanë një sistem backup. Pyetja është, a i plotëson ky sistem në mënyrë

1 https://digitalguardian.com/blog/expert-guide-securing-sensitive-data-34-experts-reveal-biggest-mistakes-companies-make-data

adekuate nevojat e organizatës suaj dhe shërbimet që ju ofroni? Është e rëndësishme të mos bëni kopje rezervë vetëm për hir të kopjes rezervë, por ta bëni këtë në mënyrë që të dhënat kryesore të mund të rikuperohen, dhe me sa më pak ndikim në punë.

Për shembull, kopjet rezervë duhet të mbulojnë punën e përditshme, por gjithashtu duhet të mundësojnë punën kur një sistem dështon. Ose, në rast fatkeqësie, të dhënat duhet të ruhen në një vend ku mund të rikuperohen.

Organizatat duhet të jenë realiste në krijimin e një rregulloreje për backup, dhe duhet të zhvillohet një plan me shkrim që detajon:

- Për cilat materiale duhet të behet kopje rezerve?
- Ku?
- Sa shpesh do të bëhen kopje rezerve?
- Kush është përgjegjës për bërjen e kopjeve rezerve?[2]

Jepni gjithmonë përparësinë më të madhe të dhënave vitale

Vendosni një orar të bërjes së kopjeve rezervë bazuar në atë se sa shumë punë organizata juaj është e gatshme të rrezikojë të humb. Mbani në mend se baza e të dhënave dhe skedarët e kontabilitetit janë asetet tuaja më kritike të të dhënave dhe duhet të ruhen para dhe pas çdo përdorimi të rëndësishëm. Për shumicën e organizatave, kjo do të thotë se çdo ditë duhet të bëhet backup të këtij lloj skedarësh. Megjithatë, organizatat jofitimprurëse që bëjnë shumë hyrje të të dhënave duhet të marrin në konsideratë të bërjen e backup-it të bazave të të dhënave të tyre pas çdo shtese të rëndësishme, edhe sikur të jetë më shumë se një herë në ditë. Skedarët kryesorë si dokumentet (në një folder 'Your Documents', për shembull) dhe skedarët e postës elektronike duhet të bëhen backup të paktën një herë në javë, ose edhe një herë në ditë.[3]

Gjithmonë testoni kopjet tuaja rezervë

Duke testuar kopjet rezervë, mund të shihni nëse ato funksionojnë siç keni menduar. Kjo ju lejon të matni se sa shpejt mund të rivendoset puna e rregullt pas një dështimi dhe të identifikoni çdo çështje që duhet të zgjidhet.

Përdor rregullin 3-2-1 për kopje rezervë

Profesionistët rekomandojnë një praktikë të tepricës rezervë të njohur si rregulli 3-2-1. Kjo përkthehet në tre kopje të të dhënave tuaja, në dy pajisje lokale (por të ndryshme) dhe në një pajisje të jashtme. Kjo qasje e bën thuajse të pamundur humbjen e të dhënave.

Në të vërtetë, ruajtja e skedarëve të rëndësishëm në një hard disk ose flash disk nuk mjafton. Hard disqet mund të prishen. Më tej, flash disqet dhe kartat SD janë të vogla dhe lehtë humben. Një sistem i mirë backup përbëhet nga kopje të shumëfishta, të mbrojtura në rast të një incidenti të paparashikuar.

Përdor backup në distancë

Backup-i jashtë organizatës ose në re (cloud) është një mënyrë efikase dhe ekonomike për t'u siguruar që të dhënat të jenë në një vend tjetër, por megjithatë të aksesueshëm.

Bëni backup shpesh dhe rregullisht

Sot, ka mjete që ju lejojnë të bëni backup automatikisht, dhe që të dyja janë të lehta për t'u konfiguruar dhe të përballueshme për nga çmimi.

Plani i reagimit ndaj incidentit

Krijoni një ekip reagimi ndaj incidenteve

Një ekip i reagimit ndaj incidenteve është një grup profesionistësh të TI-së brenda një organizate, të cilët ngarkohen me përgatitjen dhe reagimin ndaj çdo emergjence të TI-së.

Zakonisht, këta punonjës kanë formim dhe role të shumëllojshme dhe kanë aftësi teknike shtesë, që e

2 Your Organization's Backup Strategy, Articles and How-tos, techsoup.org

3 Ibid.

bën ekipin të jetë në gjendje t'u përgjigjet një sërë incidentesh të sigurisë, përfshirë shkelje ose sulm kibernetik.

Ekipi i reagimit ndaj incidenteve është zakonisht përgjegjës për zhvillimin e një plani reagimi (shih më poshtë) në mënyrë që të mund të merret një qasje metodike për të adresuar incidentet e sigurisë dhe menaxhimin e pasojave. Ekipi gjithashtu teston dhe zgjidh dobësitë e sistemit, ka praktika të forta sigurie dhe ofron mbështetje për masat e trajtimit të incidenteve.

Krijo një plan reagimi ndaj incidenteve (PRI)

PRI është një mjet i menaxhimit të rrezikut që përcakton kontrollet për të reduktuar thyerjet (breach) ose incidentet dhe përcakton se çfarë duhet të bëni nëse ndodh një thyerje. Ai do të ndihmojë në zbutjen e rrezikut, duke supozuar se organizata juaj ka një ekip reagimi ndaj incidenteve.

Është e rëndësishme të mbani mend se incidentet do të ndodhin rregullisht në çdo mjedis të ndërmarrjes. Ekipi përgjigjes do të duhet të përcaktojë se cilat incidente duhet të trajtohen menjëherë dhe cilat mund të trajtohen më vonë. **Qëllimi dhe objektivat e ekipit të përgjigjes ndaj incidenteve përcaktohen nga stafi menaxhues në PRI**.

Procedurat e përcaktuara mirë që detajojnë përgjigjet e duhura ndaj incidenteve janë të domosdoshme, veçanërisht pasi mund të ketë raste në të cilat incidentet duhet të raportohen tek autoritetet lokale, në varësi të rregulloreve që ndikojnë në industrinë tuaj. Struktura e një PRI varet nga korniza në përdorim, të tilla si ISO 28035 ose NIST (përgatitja, zbulimi dhe analiza, përmbajtja, çrrënjosja dhe rikuperimi, aktivitetet pas incidentit).

Kur ndodh një incident, duhet doemos të ndiqni PRI-në, e cila do të përcaktojë procedurat për t'iu përgjigjur llojeve të ndryshme të incidenteve.

Shumë incidente shkaktohen nga përdoruesit e brendshëm, pra është e rëndësishme që punonjësit dhe përdoruesit e tjerë të fundit të trajnohen në lidhje me sigurinë kompjuterike dhe gjithashtu të monitorohet përdorimi i tyre për të siguruar që ata nuk janë të përfshirë në veprime keqdashëse. Për ta bërë këtë, organizatat duhet:

- T'i njoftojnë përdoruesit e fundit se si të raportojnë një incident, me adresat përkatëse të emailit, portalet, linjat telefonike dhe informacionin e repartit të ndihmës.
- Të krijojnë një faqe të brendshme që përcakton detajet e nevojshme për raportimin e duhur.
- Të organizojnë trajnime vjetore të sigurisë që përfshijnë udhëzime se çfarë duhet të bëni në rast të një incidenti (raport për malware, raport për rrjedhje të të dhënave, raport për spam & phish, etj.).
- Të udhëzojnë përdoruesit e fundit të shkëpusin pajisjet nga interneti kur ndodh një incident, nëse organizata juaj nuk ka masa teknike për të kontrolluar automatikisht një host të infektuar.
- T'i udhëzojnë përdoruesit e fundit të mos kryejnë asnjë veprim pas një incidenti nëse nuk mirato-het nga ekipi përgjigjes për reagimin ndaj incidentit, në mënyrë që të ruhen provat e nevojshme për hetimin e mundshëm mjeko-ligjor.
- T'i trajnojnë përdoruesit e fundit për të ofruar sa më shumë informacion të jetë e mundur në lidhje me incidentin, duke përfshirë:
    * Çfarë ka ndodhur?
    * Ku ka ndodhur?
    * Kur ka ndodhur?
    * Kush ka qenë i përfshirë?
    * Çfarë informacioni shtesë mund të shpejtojë mbledhjen e informacionit në fazën e triazhit?

Vazhdimësia dhe rimëkëmbja nga katastrofat

Krijimi i një plani të vazhdimësisë së biznesit dhe rimëkëmbjes nga katastrofat

Ndërsa vazhdimësia e biznesit i referohet rimëkëmbjes, restaurimit dhe mirëmbajtjes së të gjithë operacionit të një organizate përballë një ngjarjeje të madhe të papritur, rimëkëmbja nga fatkeqësitë i referohet aktiviteteve specifike që kanë të bëjnë me infrastrukturën dhe të dhënat e komunikimit dhe teknologjisë.

Kur ndodh një incident i paplanifikuar, është jetike që një organizatë të mund të rifillojë punën sa më shpejt të jetë e mundur. Plani i vazhdimësisë së biznesit synon qëllimin në tërësi dhe plani i rimëkëmbjes nga katastrofat përcakton se si një organizatë mund të rikuperojë në mënyrë efikase dhe efektive qasjen në të dhënat e saj kritike dhe sistemet e teknologjisë.

Prandaj, një plan i rimëkëmbjes nga katastrofat adreson në thelb dy gjëra:

- rivendosjen e sistemeve dhe teknologjisë së TI dhe komunikimit; dhe
- fitimi i qasjes së plotë në të dhëna me cilësi të mirë dhe të pastra në të cilat mbështetet organizata.

Lloji i ngjarjeve shkatërruese të paplanifikuara që mund të kërkojnë zbatimin e një plani të rimëkëmbjes nga katastrofat përfshijnë:

- Fatkeqësitë natyrore
- Luftë ose terrorizëm?
- Trazira civile
- Aksidente ose gabime njerëzore
- Krimi kibernetik

Ngjarje të tilla mund të shkaktojnë shkallë të ndryshme të shkatërrimit, duke ndikuar në:

- Një qendër të vetme të dhënash ose ndërtesë
- Një organizatë të tërë
- Sisteme lokale ose në të gjithë qytetin
- Sistemet rajonale ose kombëtare
- Sistemet globale

Një plan efektiv i rimëkëmbjes nga katastrofat që minimizon ndërprerjen duhet të marrë në konsideratë humbjet e mundshme tregtare dhe cenimin e reputacionit të organizatës dhe duhet të ndihmojë që organizata të shmangë shkeljet rregullatore ose legjislative.

Gjashtë elementë kryesorë duhet të përshkruhen në një plan të rimëkëmbjes nga katastrofat:

Një inventar i plotë i aseteve (harduer, softuer dhe të dhëna)

Ndikimet minimale të pranueshme (ulja e kohës dhe niveli i shërbimit)

Proceset dhe procedurat e rikuperimit nga fatkeqësitë e dokumenteve (SHLP-të, prioritetet e restaurimit, burimet rezervë, vërtetimi i të dhënave)

Përgjegjësitë e rimëkëmbjes nga katastrofat, si operacionale ashtu edhe autorizuese; d.m.th. kush kryen veprime të rimëkëmbjes nga katastrofat dhe kush i miraton ato.

Një plan komunikimi dhe PR (për të adresuar palët kryesore të interesit dhe rregullatorët, dhe për të mbrojtur reputacionin e një organizate)

Trajnimi (një plan nuk ka dobi nëse askush nuk di ta përdorë)

Mbroni sistemin tuaj të informacionit

Riparoni (patch) dhe përditësoni (update)

Riparoni dhe përditësoni sistemin tuaj operativ dhe softuerin e aplikacionit

Mbajtja e sistemit dhe aplikacioneve tuaja të përditësuara mund të ndihet ngandonjëherë si një shqetësim, por është shumë e rëndësishme të bëhet, për disa arsye:

- **Siguria**: përditësimet ndihmojnë në sigurimin e kompjuterit tuaj kundër sulmeve. Ndërsa zbulohen sulme të reja, identifikohen boshllëqet që kriminelët kibernetikë përdorin për të kompromentuar sistemin tuaj operativ dhe aplikacionet. Këto mangësi tejkalohen përmes përditësimeve.
- **Karakteristika të reja**: Microsoft, Apple, Android dhe të tjerë ofrojnë veçori shtesë në përditësime dhe softuerë të tjerë nga kompani të tjera ndonjëherë nuk mund të përdoren pa përditësuar më parë këto sisteme.

- **Riparime**: Jo çdo problem është për shkak të një virusi. Ndonjëherë, problemet lindin në sisteme dhe softuerë dhe thjesht duhet të riparohen. Shumë probleme që prekin përdoruesit e fundit zgjidhen me përditësime.

Pra, këshillohet të përdoren përditësimet automatike **për sistemet dhe aplikacionet**. Në këtë mënyrë, rregullimet thelbësore të sigurisë që adresojnë dobësitë e sistemit shkarkohen automatikisht.

Mbani në mend: kur shfaqet dritarja e vogël e përditësimit, mund të jetë një gjë e mirë; por megjithatë me rëndësi është të mos klikoni verbërisht.

Konfigurime të sigurta

Përdorni konfigurime të sigurta për të gjitha pajisjet dhe softuerët

Një mënyrë për të mbrojtur njerëzit dhe organizatat nga aktiviteti keqdashës është përdorimi i konfigurimeve të sigurta për pajisjet dhe softuerët. Në të njëjtën kohë, kjo përbën një sfidë të rëndësishme, duke prezantuar një nevojë pothuajse konstante për rregullime të reja të sistemit operativ, përmirësime në aplikacione dhe modifikime në rrjete. Prandaj, qëllimi parësor është të **dokumentohen të gjitha përditësimet dhe ndryshimet**, për të ofruar një pamje në konfigurimet për të gjitha sistemet.

Kur bëhen ndryshime në një aplikacion, duhet të bëhet modifikim dhe përditësim i dokumentacionit të krijuar për atë aset të veçantë. Dokumentimi i mirë duhet të mundësojë rindërtimin e një instance të tërë që nga fillimi dhe duhet të përfshijë:

- **Një regjistër të ndryshimeve** në sistemet operative dhe aplikacionet (përditësimet), modifikimet e rrjetit, instancat e reja të aplikacioneve, etj. Të gjitha këto duhet të dokumentohen dhe gjurmohen me saktësi.
- **Një listë e të gjitha aseteve** në organizatën tuaj. Çdo harduer dhe softuer duhet të identifikohet dhe dokumentohet.
- **Një bazë sigurie** për asetet. Ky është një standard minimal sigurie i rënë dakord që zbatohet për shembull për çaktivizimin e shërbimeve të panevojshme, heqjen e llogarive të vizitorëve, ekspozimin ndaj internetit publik, etj.
- **Një proces shqyrtimi dhe miratimi** që gjurmohet lehtë. Është praktikë e mirë të rishikoni konfigurimet dhe cilësimet tuaja herë pas here, pasi incidentet në mjedisin tuaj mund të ofrojnë sugjerime se çfarë duhet të modifikohet. Gjithashtu, individët nuk duhet të ndryshojnë cilësimet bazuar në nevojat e tyre, por duhet të kalojnë nëpër një proces të standardizuar miratimi.
- **Një regjistër i ndryshimeve të konfigurimit**.

Dokumentacioni duhet të përfshijë edhe:

- Diagramet e rrjeteve dhe pajisjeve, si dhe planimetrinë e qendrave të të dhënave fizike
- Parametrat e mjedisit të aplikacionit:
    * Linjat bazë të vendosura për t'u ndjekur
    * Cilësimet e Firewall, nivelet e patch, versionet OS
- Konventat dhe standardet e emërtimit, për:
    * Pajisjet (emri dhe numri i etiketës së asetit, emri i kompjuterit, vendndodhja, numri serial)
    * Rrjete (etiketimi i portit)
    * Konfigurimet e domenit (emrat e llogarisë, adresa e emailit)
- Skema IP

Për përdoruesit e fundit, konfigurimi i sigurt nënkupton:

- Heqjen dhe çaktivizimin e llogarive të panevojshme
- Ndryshimi i fjalëkalimeve të paracaktuara ose që lehtësisht qëllohen ("të dobëta")
- Heqja ose çaktivizimi i programeve të panevojshme
- Çaktivizimi i çdo karakteristike automatike që lejon ekzekutimin e skedarëve pa autorizimin e përdoruesit

Të dhëna të ndjeshme

Kriptimi i të gjitha të dhënave të ndjeshme

Kriptimi është procesi i shifrimit të informacionit në mënyrë që të mos lexohet pa një lloj çelësi. Për shembull, pronarët e të dhënave të kriptuara mund t'i çaktivizojnë ato duke përdorur një fjalëkalim, informacion biometrik ose ndonjë lloj çelësi tjetër.

Kriptimi është një element kritik i sigurisë kibernetike dhe mund të përdoret në disa mënyra për të mbajtur të dhënat konfidenciale dhe private, si në faqet e sigurta të internetit (HTTPS), në aplikacionet e sigurta të mesazheve dhe shërbimet e postës elektronike, dhe përmes rrjeteve private virtuale (VPN). Kriptimi mbron informacionin ndërsa lëviz në mënyrë aktive nga një vend në tjetrin (d.m.th. në tranzit), nga dërguesi te marrësi, dhe gjithashtu mbron informacionin ndërsa është në pushim. Nëse dikush ka qasje në një bazë të dhënash në të cilën ekziston informacioni i kriptuar, kriptimi paraqet një shtresë shtesë të sigurisë.[4]

Me fjalë të tjera, kriptimi **ndihmon në ruajtjen e informacionit të ndjeshëm dhe privat duke e bërë atë të palexueshëm për kriminelët kibernetikë**, edhe në rastin kur ata janë në gjendje të eksfiltrojnë atë informacion.

Njohja e informacionit të ndjeshëm në mjedisin tuaj unik që duhet të kodohet është jetike, por zakonisht kjo përfshin, ndër të tjera:

- Informacion personalisht të identifikueshëm
- Të dhëna financiare
- Të dhëna të sigurimit shëndetësor
- Numra të kartave të kredisë

Lufta kundër softuerit keqdashës (malware)

Përdodrni softuer anti-malware

Malware ose softuer keqdashës është çdo program i dizajnuar për të kryer funksione të padëshiruara ose të dëmshme që godasin kompjuterët, serverët dhe rrjetet. Softueri anti-malware pra është pjesë e domosdoshme e një pako sigurie.

Vite më parë, kompanitë e sigurisë kibernetike u përpoqën të krijonin një zgjidhje universale anti-virus që mund të adresonte të gjitha nevojat tona në një produkt. Megjithatë, kjo nuk është më efektive, sepse kriminelët kibernetikë kanë evoluar. Kërcënimet që ato përbëjnë po bëhen gjithnjë e më të sofistikuara, duke bërë që kompanitë të zhvillojnë programe të posaçme anti-malware.

Është e rëndësishme të kuptohet se të gjitha viruset janë malware, por jo të gjitha malware janë viruse. Një virus kompjuterik përhapet nga përdoruesi në përdorues duke u vetë-replikuar, dhe programet anti-virus identifikojnë kërcënime të njohura duke zbuluar nënshkrime unike. Por skanuesit modernë të malware përdorin zbulimin heuristik, i cili mund në mënyrë proaktive të kërkojë kodin keqdashës.

Zgjidhjet anti-malware do të bllokojnë shumicën e programeve keqdashëse dhe potencialisht të padëshiruara dhe do të skanojnë të dhënat hyrëse për të parandaluar ekzekutimin e programeve keqdashëse në një pajisje, ndryshimin e cilësimeve ose ngarkimin e programeve shtesë të kompromentuara. Ata gjithashtu pengojnë përdoruesit të vizitojnë faqet e internetit që njihen si shpërndarëse të kodev keqdashëse (në sulmet phishing dhe ransomware).

Përtej kësaj, softueri anti-malware ofron:

- Mbrojtje në kohë reale
- Skanime të inicializimit
- Skanime të pajisjeve të jashtme
- Mbrojtje e informacionit të ndjeshëm
- Mbrojtje nga spam dhe vjedhje të identitetit

4 Should I Encrypt Sensitive Files on My Computer?, Experian

Mure mbrojtëse (Firewalls)

Përdor muret mbrojtëse

Muret mbrojtëse sigurojnë mbrojtje kundër sulmeve kibernetike duke ndihmuar në ruajtjen e kompjuterëve dhe rrjeteve. Muret mbrojtëse mund të jenë softuer ose harduer, në pajisje ose në një rrjet, por të gjitha funksionojnë në të njëjtën mënyrë duke inspektuar trafikun dhe duke bllokuar paketat e padëshiruara.

Një mur mbrojtës do të ulë ndjeshëm rrezikun për individët dhe organizatat. Organizatat që nuk përdorin mure mbrojtëse thjesht e bëjnë punën e kriminelëve kibernetikë më të lehtë, duke u lejuar atyre qasje të mundshme në sisteme dhe skedarë si dhe mundësinë për të përhapur përmbajtje keqdashëse. Prandaj, një mur mbrojtës i konfiguruar, mirëmbajtur dhe monitoruar siç duhet është çelësi për të mbrojtur të dhënat, rrjetin dhe pajisjet tuaja.

Ndër të tjera, një firewall ju ndihmon të siguroni veten nga:

- Regjistrime në distancë
- Rrëmbim të seancave të emailit
- Dobësitë e aplikacioneve dhe SO
- Ndalimin e shërbimeve (DoS)
- e-mail bomba
- Makro keqdashëse

Rrjete WI-FI

Mbroni rrjetet tuaja WI-FI

Rrjetet WI-FI duhet të jenë të sigurta, të koduara dhe të fshehura:

- **Duhet të ndizet kriptimi i rrjetit WI-FI**. Kriptimi është thelbësor për sigurinë. Prandaj, ruteri juaj duhet të mbështesë kriptimin WPA2, dhe duhet të zëvendësohet nëse nuk e mundëson këtë.
- **Mbani softuerin të përditësuar me përditësimet dhe riparimet (patches)**.
- Vendndodhja e ruterëve duhet parë si çështje sigurie. Shpesh, njerëzit nuk janë në dijeni se një ruter i vendosur pranë një dere ose dritareje rrit mundësinë që një sinjal WI-FI të kapet nga dikush me qëllim të keq. Për të përmirësuar sigurinë e WI-FI, **është më mirë të vendosni ruterin sa më afër qendrës së zyrës tuaj që të jetë e mundur**, pasi kjo do të reduktojë mundësinë që hakerat të mund të lidhen me rrjetin tuaj.
- **Aktivizoni filtrimin e adresave MAC** për të kontrolluar pajisjet që kanë qasje në rrjetin tuaj.
- **Çaktivizoni administrimin në distancë**.
- **Krijoni një rrjet të veçantë WI-FI për klientët**, për të shmangur qasjen e tyre në rrjetin tuaj të brendshëm.

Rregullimet e shfletuesit të internetit (web browsing)

Konfiguro cilësimet e sigurisë së shfletuesit të internetit

Shfletuesit e internetit ekzistojnë pothuajse në të gjitha pajisjet. Meqenëse ato përdoren shumë në jetën e përditshme, është jetike t'i konfiguroni ato në mënyrë të sigurt, veçanërisht pasi ato zakonisht përdoren me cilësimet e paracaktuara.

Shfletuesit e internetit përfaqësojnë një objektiv të rëndësishëm të sulmit për t'u shfrytëzuar nga kriminelët kibernetikë dhe një shfletues i pasigurt mund t'i lërë përdoruesit ose organizatat të hapur për instalimin e përmbajtjeve keqdashëse pa dijeninë e përdoruesit. Në disa raste, kjo mund të çojë në humbjen e kontrollit mbi një pajisje, përdorimin e informacionit të një përdoruesi ose edhe përdorimin e një pajisjeje për të sulmuar të tjerët.

Çdo shfletues i internetit (Firefox, Chrome, DuckDuckGo, Brave, etj.) duhet të sigurohet. Duke vepruar kështu, sigurohuni që të:

- **Aktivizoni përditësimet automatike**. Ky **hap vendimtar** do të mbrojë organizatën tuaj kundër dobësive të shumta të zbuluara çdo ditë. Kjo është një pjesë thelbësore e higjienës së duhur kiber-

netike të shfletuesit tuaj të internetit dhe do t'ju ndihmojë të qëndroni të sigurt.

- **Bllokoni njoftimet pop-up, shtojcat plugin dhe faqet e phishing**. Shumica e e njoftimeve pop-ups janë reklama, të cilat mund të infektohen me përmbajtje keqdashëse; dhe njihen për nga implikimet që kanë për rrezikun e sigurisë.
- **Mos ruani fjalëkalimet**. Ky zakon nuk rekomandohet sepse, nëse një shfletues është i kompromentuar, e njëjta ndodh edhe me kredencialet e ruajtura.
- **Çaktivizo kukit e palëve të treta**.
- **Ç'instalo çdo zgjerim (extension) të papërdorur të shfletuesit**.
- **Përditëso rregullisht çdo zgjerim që përdoret**.

Zgjedhja personale gjithashtu luan një rol në sigurinë e shfletuesit, të tilla si qasja e përdoruesve në uebfaqet **https në vend të uebfaqeve http**.

Pajisje mobile

Siguroni pajisjet mobile

Pajisjet mobile mund të paraqesin sfida të mëdha sigurie dhe menaxhimi, veçanërisht nëse mbajnë informacion konfidencial ose mund të futen në një rrjet organizate.

Për të menaxhuar përdorimin e pajisjeve mobile, organizatat duhet t'u kërkojnë përdoruesve:

- pajisje për mbrojtjen e fjalëkalimeve;
- të kriptojnë të gjitha të dhënat; dhe
- të instalojnë aplikacione sigurie që parandalojnë vjedhjen e informacionit kur një telefon përdor rrjetet publike.

Organizatat gjithashtu duhet të:

- Vendosni procedurat e raportimit për pajisjet e humbura ose të vjedhura.
- Konfiguroni pajisjet për t'u bllokuar automatikisht pas një periudhe të caktuar kohe.

Pajisjet e Internetit të gjërave (IoT)

Pajisje të sigurta IoT

Rëndësia e rritjeve të teknologjisë në jetën tonë ka nxitur "Internetin e gjërave", ose IoT. Kjo do të thotë se një numër i madh pajisjesh janë të lidhura me internetin përmes sensorëve IoT që i lejojnë ata të mbledhin të dhëna në kohë reale dhe t'i shpërndajnë ato. Duke mbledhur të dhëna nga sistemet fizike dhe virtuale, IoT është një "hapësirë sulmuese" e konsiderueshme për sulmuesit kibernetikë, nëse nuk është siguruar siç duhet.

Sigurimi i një rrjeti IoT nënkupton sigurimin e pajisjeve para se ato të bashkohen me rrjetin. Për ta bërë këtë:

- Ndrysho fjalëkalimet standarde
- Përdorni fjalëkalime të forta
- Përditësoni softuerin në pajisje (gjithmonë verifikoni përditësimet e disponueshme nga faqet e internetit të prodhuesit para se t'i aplikoni në pajisje)
- Kriptoni dhe autentifikoni pajisjet
- Ndryshoni cilësimet e paracaktuara të privatësisë
- Ndryshoni cilësimet standarde
- Siguroni rrjetin tuaj dhe WI-FI
- Krijoni një rrjet vizitorësh

Siguria fizike

Kujdesuni për sigurinë fizike të pajisjeve, sidomos të pajisjeve celulare

Siguria fizike është po aq e rëndësishme sa edhe siguria kibernetike. Nëse një hajdut vjedh një laptop

ose pajisje celulare, humbja e parë është vetë pajisja, por nëse hajduti është në gjendje të hyjë në informacion në një pajisje, i gjithë informacioni mund të jetë në rrezik. Ekziston gjithashtu mundësia që të aksesohet edhe informacion tjetër duke përdorur të dhënat e ruajtura në këto pajisje, përfshirë detajet e ndjeshme të llogarisë së organizatës ose klientit – siç janë fjalëkalimet ose informacioni i kartës së kreditit – në të cilat nuk duhet të kenë akses individë të paautorizuar.[5]

Për të mbrojtur veten dhe të tjerët në organizatën tuaj:

- Siguroni pajisjen tuaj me një fjalëkalim dhe zbatoni autentikimin me dy faktorë (2FA)
- Mbani gjërat me vlerë me vete gjatë gjithë kohës dhe mos i lini kurrë pajisjet pa mbikëqyrje, veçanërisht kur udhëtoni

Qasje në distancë

Nëse organizata juaj përdor qasje në distancë, ajo duhet të jetë e sigurt, e kriptuar dhe e fshehur. Në këtë drejtim duhet:

- Të siguroheni se të gjitha programet e aksesit në distancë të jenë të rregulluara dhe të përditësuara.
- Të kufizohet qasja në distancë nga vendndodhje të dyshimta gjeografike ose adresa IP.
- Të kufizpohet aksesi në distancë i punonjësve vetëm në sistemet dhe kompjuterët që u nevojiten për të bërë punën e tyre.
- Të kërkohen fjalëkalime të forta për të fituar qasje në distancë.
- Të aktivizohet autentifikimit me shumë faktorë, nëse është e mundur.
- Të mundësohet monitorimi dhe lajmërimi për të alarmuar për sulme të dyshuara apo veprimtari të dyshimta.

Zbatoni praktikat e mira

Fjalëkalime

Çdo organizatë duhet të ketë një politikë fjalëkalimesh për të siguruar që fjalëkalimet komplekse dhe të veçanta të përdoren dhe të ndryshohen rregullisht. Fjalëkalimet paraqesin linjën e parë të mbrojtjes kundër qasjes së paautorizuar.

Një rregullore fjalëkalimi është e nevojshme për të shmangur disa nga dobësitë më të zakonshme, siç janë:

- Zakoni i përdoruesve për të ruajtur fjalëkalimet në shënime, skedarë teksti ose dokumente të tjera të pambrojtura që mund të aksesohen lehtësisht nga kriminelët kibernetikë.
- Tendenca e përdoruesve për të ruajtur fjalëkalimet në shfletues, e cila paraqet një tjetër objektiv për kriminelët kibernetikë.
- Fjalëkalime që përfshijnë informacione personale që merren lehtësisht në internet.
- Përdorimi i vetëm një fjalëkalimi për llogari të shumëfishta.
- Ndarja e fjalëkalimeve me kolegët ose përmes emailit, mesazheve SMS ose platformave të tjera (kjo vlen në veçanti nëse fjalëkalimet nuk ndryshohen rregullisht).

Mënyra më e lehtë për të ndryshuar ose zbutur sjelljen e përdoruesve në lidhje me fjalëkalimet është përdorimi i **menaxherit të fjalëkalimeve**. Kjo lejon krijimin e fjalëkalimeve komplekse për llogari të ndryshme, të gjitha të koduara dhe të ruajtura, kështu që përdoruesit duhet të memorizojnë vetëm një fjalëkalim kryesor për të hyrë në kasafortën e tyre të fjalëkalimeve. Një menaxher fjalëkalimesh ndihmon përdoruesit të gjenerojnë fjalëkalime dhe tregon se sa i fortë është një fjalëkalim, dhe gjithashtu mund të njoftojë përdoruesit për shkeljet e sigurisë që përfshijnë emailin e tyre dhe të tjera.

Nëse organizata juaj nuk përdor një menaxher fjalëkalimesh, ja disa **këshilla për krijimin e një politike fjalëkalimesh**:

5 https://www.cisa.gov/uscert/ncas/tips/ST04-017

- **Fjalëkalimet më të gjata janë më të mira** sepse kërkojnë më shumë kohë për t'u zbërthyer. Fjalëkalimet duhet të përmbajnë minimum 12 karakterë.
- **Kompleksiteti është çelësi**! Fjalëkalimet duhet të përfshijnë simbole, një kombinim të shkronjave të vogla dhe të mëdha, dhe numrave. Dhe pastaj duhet të shifrohen.
- **Përdorni fjalë pa kuptim** dhe shmangni parashikueshmërinë. Në rastin indeal, fjalëkalimet nuk duhet të përfshijnë fjalë që mund të gjenden në fjalorë (në çfarëdo gjuhë).
- **Fjalkalimet le të jenë unike**. Rregulli në çdo organizatë duhet të jetë: një llogari, një fjalëkalim.

Është gjithashtu e rëndësishme të ndryshoni **fjalëkalimet e paracaktuar** para se t'ua jepni pajisjet punonjësve, për të shmangur rreziqet që kanë të bëjnë me mundësinë e ekspozimit ndaj hakerave ose ndonjë shkelje tjetër të madhe.

Autentifikim me shumë faktorë

Përdorni autentifikimin me shumë faktorë sa herë që është e mundur

Ka tre mënyra që një kompjuter, ose sistem, të identifikojë një përdorues. Mund të kërkojë diçka që një përdorues e di, është ose e ka. Këta janë tre faktorët e autentifikimit. Standardi i artë për verifikimin e identitetit është një autentifikim me shumë faktorë që përdor të paktën dy nga këta faktorë.

Ideja është që dy fjalëkalime të ndryshme nuk janë shumë më të mira se një, por dy faktorë janë të ndryshëm. Kjo është arsyeja pse një tërheqje parash nga një bankomat kërkon vërtetim me dy faktorë: diçka që një person ka (një kartë bankomati), dhe diçka që një person e din (PIN-in).

Përdorimi vetëm i fjalëkalimeve nuk është i sigurt, pasi hakerat kanë zhvilluar metoda të panumërta gjatë viteve për të vjedhur kredencialet e nevojshme për të fituar qasje të paautorizuar në llogaritë private. E vërteta e trishtë është se pothuajse 90% e incidenteve të tilla mund të bllokohen me përdorimin e autentifikimit me shumë faktorë.

Organizatat duhet të zbatojnë autentifikimin me dy faktorë (2FA) për përdoruesit kudo që është e mundur:
- për të mbrojtur përdoruesit nga vjedhja e identitetit nëpërmjet një fjalëkalimi të vjedhur.
- për të mbrojtur organizatat nga fjalëkalimet e dobëta të punonjësve.
- për të zbutur përdorimin e pajisjeve të pamenaxhuara, veçanërisht me rritjen e shkallës së punës nga shtëpia gjatë pandemisë covid.
- për të rritur efektivitetin e masave të tjera të sigurisë.
- për të ndihmuar organizatat të ruajnë përputhshmërinë.

Llogari

Përdorni llogari të kufizuara për punë të rregullta dhe të përditshme

Llogaritë duhet të trajtohen me kujdes, pasi shpërdorimi i llogarisë mund të çojë në humbjen e informacionit, reputacionit dhe parave të organizatës.

Ekzistojnë dy lloje të llogarive: Përdoruesi dhe Administratori Standard.

Një llogari e përdoruesit standard është:
- më e përshtatshme për detyrat e përditshme (përdorimi i aplikacioneve, shfletimi i uebit);
- e konfiguruar për të mbrojtur sistemin tuaj nga sulmet e dukshme; dhe
- nuk i lejon përdoruesit të bëjnë ndryshime që prekin të gjithë ata që përdorin një kompjuter.

Llogaritë të përdoruesit standard kanë më pak fleksibilitet se llogaritë e Administratorit. Por, nga ana tjetër, malueri i instaluar nën një llogari të përdoruesit standard mund të dëmtoj pak kedarët e sistemit. Kjo për shkak se sulmuesit që fitojnë qasje në një llogari të Përdoruesit Standard mund të hyjnë vetëm në skedarët e atij përdoruesi. Në këtë drejtim, kufizimet në llogaritë të përdoruesit standard janë në favor të një organizate nëse një program kundërshtar ose keqdashës fiton qasje.[6]

6 Why You Shouldn't Use an Admin Account as Your Main Account, Make Tech Easier

Qasja e punonjësve

Qasja e punonjësve duhet të jetë e kufizuar në mënyrë që asnjë punonjës të mos mund të hyjë në të gjitha sistemet e të dhënave

Rekomandohet që asnjë punonjësi të mos i jepet qasje në të gjitha sistemet e të dhënave. Punonjësve duhet t'u jepet qasje vetëm në sistemet specifike të të dhënave që u nevojiten për të bërë punët e tyre.

Mos lejoni punonjësit të instalojnë softuer pa leje

Punonjësit nuk duhet të jenë kurrë në gjendje të instalojnë softuer pa leje.

Regjistrimi (Logging)

Ruajtja e regjistrimit

Nga pikëpamja e sigurisë, një log vepron si një alarm kur diçka e keqe po ndodh. Rishikimi i rregullt i log-ve mund të ndihmojë në identifikimin e sulmeve keqdashëse në sistemin tuaj.

Në të vërtetë, një log që është i lehtë për t'u aksesuar dhe përfshin informacion vendimtar që mund të përmbajë një sistem informatik ose kompjuterik. Regjistrimi do të ndihmojë me:

- Zbulimin e gabimeve të sistemit (debugging)
- Ndjekjen e gabimeve
- Zgjidhjen e problemeve të punës
- Kontabilitetin
- Auditimin
- Sigurinë

Në mënyrë të dukshme, skedarët e regjistrit mund të përdoren gjithashtu për të ruajtur pajtueshmërinë rregullatore. Shumë organizata duhet të pajtohen me rregullore të ndryshme që kërkojnë një auditim të aktiviteteve, duke përfshirë sigurimin e llogarive të përdoruesve ose qasjen në sistemet financiare.

Çështja më e madhe lidhur me regjistrimin është mungesa e mbikqyrjes. Duhet të kuptohet se çfarë duhet të regjistrohet, bazuar në praktikat më të mira, dhe të rishikohen regjistrat çdo ditë në kërkim të gabimeve, anomalive ose aktivitetit të dyshimtë. Megjithatë, regjistrimi i tepërt nuk është i dobishëm, pasi krijon shumë "zhurmë" dhe kërkon më shumë kapacitet ruajtjeje. Prandaj, disa aktivitete mund të kenë nevojë për këtë më tepër se të tjera.

Ndërgjegjësimi për sigurinë kibernetike

KËRCËNIME TË ZAKONSHME KIBERNETIKE

Sulmi kibernetik është një përpjekje keqdashëse dhe e qëllimshme nga një individ ose organizatë për të shkelur sistemin e informacionit të një individi ose organizate tjetër. Zakonisht, sulmuesi kërkon një lloj përfitimi nga prishja e rrjetit të objektivit. Organizatat përballen me një mori kërcënimesh kibernetike dhe sulmuesit përdorin një shumëllojshmëri strategjish për të tentuar apo kryer sulme.

Sulmet e inxhinjerisë sociale

Sulmet e inxhinierisë sociale mashtrojnë dhe manipulojnë objektivat, për të marrë informacion ose për të fituar qasje në kompjuterët e tyre. Ky lloj sulmi mbështetet në ndërveprimin njerëzor dhe zakonisht përfshin manipulimin e një përdoruesi në mënyrë që ata të shkelin procedurat e sigurisë dhe praktikat më të mira për të fituar qasje të paautorizuar në sisteme ose të ndajnë informacione të ndjeshme.

Në sulmet e inxhinierisë sociale, kriminelët kibernetikë fshehin identitetet dhe motivet e tyre të vërteta, duke e paraqitur veten si individë të besueshëm. Sulmi pastaj ekzekutohet duke mashtruar përdoruesit

që të klikojnë lidhjet keqdashëse ose duke fituar fizikisht qasje në një kompjuter.

Phishing

Shumica e sulmeve kibernetike fillojnë me një email phishing. Phishing është një lloj sulmi i inxhinierisë sociale në të cilin kriminelët kibernetikë mashtrojnë viktimat për të dorëzuar informacion të ndjeshëm ose për të instaluar malware.

Edhe pse masat teknike të sigurisë vazhdojnë të përmirësohen, phishing mbetet një nga mënyrat më të lira dhe më të lehta për kriminelët kibernetikë për të fituar qasje në informacion të ndjeshëm dhe personal. Përdoruesit thjesht duhet të klikojnë në një link dhe siguria e tyre mund të rrezikohet në atë masë që ata mund të bëhen viktima të vjedhjes së identitetit. Përdoruesit gjithashtu mund të kompromentojnë informacionin e tyre personal, kredencialet e hyrjes (emrat e përdoruesve dhe fjalëkalimet) dhe informacionin financiar (numrat e kartës së kreditit) nëse klikojnë linkun.

Shpesh, sulmuesit e arrijnë këtë përmes emaileve keqdashëse që duket se janë nga burime të besueshme. Por nganjëherë, ata përdorin edhe metoda të tjera.

Si funksionon phishing-u?

Shumica e fushatave phishing përdorin një nga dy metodat themelore:

1. **Bashkëngjitje keqdashëse** në emaile, të cilat zakonisht kanë përshkrim alarmuese si 'FATURA'. Kur hapen, këto shtojca instalojnë malware në pajisjen e një përdoruesi.
2. **Lidhje me faqe keqdashëse të internetit** që shpesh janë klone të faqeve të ligjshme. Lundrimi në uebfaqe mund të shkaktojë shkarkimin e malware, ose faqja e hyrjes në uebfaqe mund të përmbajë skedare që vjedhin kredencialet.[7]

Llojet e sulmeve të phishing

Spear Phishing

Spear phishing është një sulm keqdashës i email-it që synon një organizatë apo individ të caktuar, duke ndjekur qasje të paautorizuar në informacione të ndjeshme. Tentativat spear phishing nuk ka të ngjarë të ekzekutohen nga sulmues të rastit, por nga kriminelë kibernetik në kërkim të përfitimeve financiare ose informacioneve të tjera të vlefshme.[8]

Në një sulm spear phishing, një email dërgohet nga një burim i besueshëm por çon në një faqe interneti të rreme me malware. Këto emaile priren të përdorin mjete kreative për të tërhequr vëmendjen e përdoruesve.

Spear phishing është shumë më efektive se sulmet e tjera phishing, por kërkon që nga kriminelët kibernetik të shpenzojnë kohë dhe burime duke ndërmarrë kërkime para sulmit, pasi ata do të jenë më të suksesshëm në qoftë se njohin objektivin e tyre para se të nisë një sulm.

Whale Phishing/Whaling

Whale Phishing është e ngjashme me spear phishing, me disa dallime të dukshme. Ndërsa spear phishing zakonisht është e drejtuar ndaj anëtarëve të një grupi, whale phishing është i fokusuar në një individ specifik - zakonisht 'peshku më i madh' në një organizatë të synuar ose një individ me pasuri ose fuqi të konsiderueshme.

Vishing

Vishing, ose "voice phishing", përfshin manipulimin e njerëzve përmes telefonit. Sulmuesit joshin një objektiv që të zbulojë një informacion të ndjeshëm në një tentativë për të përdorur këto të dhëna për përfitimin e tyre, zakonisht për të përfituar financiarisht.

7 What is phishing? Everything you need to know, IT Governance UK

8 ypes of Cyber Threat in 2019, IT Governance USA

Smishing

Termi smishing i referohet sms phishing, dhe përfshin një mesazh tekst në vend të një email-i. Në përgjithësi, shënjestrat marrin një mesazh mashtrues që i detyron t'i japin informacione personale ose financiare një agjencie qeveritare, banke ose kompanie tjetër të ligjshme.

Sulmuesit që përdorin smishing shpesh kërkojnë informacione personale ose bankare të llogarisë, të tilla si kredencialet e llogarisë, numrat e kartës së kreditit dhe numrat e identifikimit. Pastaj, ata e përdorin këtë informacion për të kryer sulme të ndryshme, duke përfshirë mashtrimet financiare, dhuratat ose mbështetjen e klientëve.

Si të parandalohen sulmet phishing

Në Email: mësoni të shikoni me kujdes email-et, veçanërisht nëse përmbajnë bashkëngjitje dhe lidhje web

Edukoni punonjësit se si të njohin tentativat për phishing dhe të raportojnë takimet e dyshuara. Ja disa shenja që tregojnë se një email mund të jetë keqdashës:

- **Gabime drejtshkrimore dhe gramatikore**. Kompanitë ose organizatat profesionale zakonisht kanë një staf editorial për t'u siguruar që klientët të marrin përmbajtje emaili të cilësisë së lartë dhe profesionale. Nëse një mesazh email është i mbushur me gabime, ka shumë më shumë të ngjarë të jetë një mashtrim.
- **Link-e të dyshimta**. Përdoruesit kurrë nuk duhet të klikojnë ndonjë link në një mesazh e-mail që dyshojnë se mund të jetë keqdashës. Një mënyrë e testimit të legjitimitetit të një linku është që të vendos miun – pa klikuar –mbi link-un, për të parë nëse adresa përputhet me informacionin në mesazh.
- **Bashkëngjitje të dyshimta**. Nëse një përdorues merr një email me një bashkëngjitje, ose nga dikush që nuk e njeh ose nga dikush që nuk e priste të dërgonte një link, duhet të reflektojë nëse mund të jetë një tentativë për phishing. Kështillohet që të mos hapen kurrë bashkëngjitjet derisa të verifikohet autenticiteti i tyre. Për shkak se ka mënyra të shumta që sulmuesit t'i mashtrojnë marrësit që të besojnë se një skedar i bashkangjitur është legjitim, është e rëndësishme që përdoruesit të dinë se:
    * nuk mund t'i besohet ikonës të lidhur me një bashkëngjitje pa verifikim tjetër.
    * Duhet të kenë kujdes nga shtesat e kombinuara të skedarëve, të tilla si 'pdf.exe', 'rar.exe', ose 'txt.hta'.
    * Mënyra më e mirë e veprimit, nëse keni dyshim, është të kontaktoni personin i cili në mënyrë të vazhdueshme ka dërguar mesazhin e email-it në fjalë, për t'i kërkuar atyre të konfirmojnë se email-i dhe bashkëngjitja janë të ligjshme.
- **Mesazhe detyruese**. Këto emaile kanë për qëllim të shkaktojnë ndjenjë paniku ose presioni, për të gjeneruar një përgjigje të shpejtë dhe të pamenduar nga marrësi. Për shembull: 'Duhet të përgjigjesh deri në fund të ditës!' Ose, të thuhet se marrësi mund të përballet me ndëshkime financiare të mundshme nëse nuk përgjigjet.
- **Mashtrim** (**spoofing**) E-mailat spoofing përdorin lidhje të dyshimta që duket se lidhen me faqet e internetit të ligjshme ose kompanitë dhe mund të shfaqin dritare të ligjshme pop-up, por që i shpien përdoruesit në faqet mashtruese. Një formë e spoofing përdor uebsajte të ndryshuara që ngjajnë shumë me emrat e uebsajteve të njohura të kompanisë, të tilla si 'www.micorsoft.com' ose 'www.mircosoft.com'.
- **Mospërputhje** (**mismatching**). Marrësi duhet të dyshojë nëse teksti i një lidhjeje dhe URL nuk përputhen, ose nëse emri, firma dhe URL e dërguesit nuk përputhen.[9]

WI-FI Publik: Kujdes kur përdorni rrjetet publike WI-FI

Jemi të rrethuar nga rrjetet publike WI-FI në hotele, qendra tregtare, kafene, aeroporte, etj. Shumë prej nesh e kanë zakonin e keq të lidhen me këto rrjete pa menduar për sigurinë. Megjithatë, ato përbëjnë rreziqe të vërteta sigurie dhe duhen përdorur me kujdes.

9 Protecting against coronavirus themed phishing attacks, microsoft.com

Problemi më i madh i sigurisë me WI-FI publik është se përdoruesit nuk e dinë se kush drejton rrjetin ose kush tjetër është duke e ndarë rrjetin.

Prandaj, organizatat duhet:

- **T'i trajnojnë punonjësit mbi rreziqet e përdorimit të WI-FI publik**.
- **Të pamundësojnë aksesin e punonjësve në të dhënat e ndjeshme gjatë përdorimit të WI-FI publik**.
- **T'i udhëzojnë punonjësit të lidhen vetëm me rrjetet e besuara**.
- **T'i pamundësojnë punonjësit të lidhen me faqet e mbrojtura me fjalëkalim kur përdorin WI-FI publike**.

Duhet të merren parasysh opsione të tjera në vend të WI-FI-së publike. Telefon mund të shërbejë si një hotspot i lëvizshëm, për shembull, duke lejuar pronarin e pajisjes të kontrollojë rrjetin dhe kush e përdor atë. Nëse duhet të përdoret WI-FI publik, mund të përdoret një VPN për të koduar çdo të dhënë që dërgohet me WI-FI, e cila i fsheh këto të dhëna nga kushdo që "është" në të njëjtin rrjet.

Kompromet imi i e-mailit të biznesit (Business Email Compromise)

Kompromet imi i emailit të biznesit (BEC) është lloj mashtrimi që synon kompanitë të cilat kryejnë transferta parash dhe kanë furnizues jashtë vendit. Llogaritë elektronike të korporatave ose të drejtuesve të disponueshme publikisht, ose të punonjësve të nivelit të lartë që merren me financë ose janë të përfshirë në transfertet elektronike të parave, janë të mashtruar ose të kompromet uar nëpërmjet programeve për incizimin e rahjeve të tastierës (key loggers) ose sulmeve phishing për të kryer transferime mashtruese. Kjo mund të sjellë humbje prej qindra mijë dollarësh.[10]

Shkarkime në kalim (Drive-By Downloads)

Në një sulm të shkarkimit në kalim, shkarkimet e skripteve keqdashëse përfundojnë në një kompjuter ose pajisje tjetër pa dijeninë e përdoruesit, duke e ekspozuar përdoruesin ndaj kërcënimeve kibernetike të ndryshme. Kjo mund të ndodhë në çdo pajisje që drejton çdo sistem operativ dhe zakonisht ndodh kur një përdorues lundron dhe shfleton një faqe interneti të kompromet uar.

Sulmet njeriu në mes (Man in the middle MITM)

Një sulm MITM ndodh kur një kriminel kibernetik futet fshehurazi midis pajisjeve, ose midis një pajisjeje dhe një rrjeti WI-FI të pasigurt, për të kapur komunikimet që pastaj mund të lexohen dhe/ose modifikohen. Në rast të tillë, përdoruesi mund t'ia kalojë pa dashje kredencialet ose informacione të tjera një krimineli kibernetik.

Sulme USB Drop

Në një sulm USB Drop, një pajisje USB që përmban kod keqdashës është i lidhur në një kompjuter.

Zakonisht, kërcënimi kibernetik nga ky lloj sulmi është malware ose virus. Infeksioni nëpërmjet një USB mund të jetë si i qëllimshëm, ashtu edhe i paqëllimshëm, në varësi të malware-it në fjalë.

Do ishte mirë që organizatat të mos i besonin teknologjisë USB të vjetëruar, dhe të përdorin fuqinë e rrjeteve dixhitale të siguruara duke përdorur ruajtjen në cloud.

Malware

Malware është një term i përgjithshëm që përdoret për të përcaktuar çdo fajl ose program që ka për qëllim të dëmtojë ose të prishë një kompjuter. Kjo përfshin:

- **Softuer Botnet** i projektuar për të infektuar një numër të madh të pajisjeve të lidhura në internet.

10 https://www.trendmicro.com/vinfo/hk/security/definition/business-email-compromise-(bec)

Disa botnet përbëjnë shumë pajisje, ku secila përdor një sasi relativisht të vogël të fuqisë përpunuese. Kjo mund ta bëjë të vështirë zbulimin e këtij lloji malware, madje edhe gjatë ndodhjes së botnet-it.

- **Sulmet Ransomware** kriptojnë informacionin e përdoruesit dhe kërkojnë pagesë në këmbim të çelësit të dekriptimit, për të rikthyer informacionin. Megjithatë, pagimi i shpërblesës nuk garanton rikthimin e të dhënave të kriptuara.
- **Spyware** përdoret për të monitoruar në mënyrë të paligjshme aktivitetin kompjuterik të një përdoruesi dhe për të korrur të dhënat personale.
- **Trojan-ët** shfaqen si softuer legjitim por kryejnë aktivitet keqdashës kur ekzekutohen.
- **Viruset dhe krimbat** janë kod keqdashës të instaluar pa dijeninë e përdoruesit. Viruset mund të shumëfishohen dhe të përhapen në kompjuterë të tjerë duke u lidhur me skedarë të tjerë kompjuterikë. Krimbat janë gjithashtu vetë-replikuese, por nuk kanë nevojë të bashkëngjiten në një program tjetër për ta bërë këtë.[11]

Sulmi DoS/DDoS

Një sulm i Mohimit të Shërbimit të Shpërndarë (DDoS) është një sulm kibernetik në të cilin sulmuesi përmbyt një server me trafik interneti për të penguar qasjen e përdoruesit në shërbimet dhe faqet e lidhura online.

Një sulm DDoS është një nën kategori e sulmit më të përgjithshëm Mohimi i shërbimit (Denial-of-Service (DoS)). Në një sulm DoS, sulmuesi përdor një lidhje të vetme interneti për të bombarduar një objektiv me kërkesa të rreme ose për të provuar dhe shfrytëzuar një dobësi të sigurisë kibernetike. DDoS është kështu më e madhe në shkallë, duke përdorur mijëra (madje miliona) pajisje të lidhura për të përmbushur qëllimin e saj. Ky vëllim i madh i pajisjeve e bën DDoS shumë më të vështirë për të luftuar.[12]

Ekzistojnë tri lloje të përgjithshme të sulmeve DDoS:

- **Sulme volumetrike**: Në këtë lloj klasik të sulmit DDoS, metodat për të gjeneruar volume masive të trafikut për të përmbytur tërësisht uebsajtin, duke krijuar një bllokim trafiku që e bën të pamundur që trafiku legjitim të qarkullojë në ose jashtë uebsajtit të synuar.
- **Sulme protokolli**: Këto sulme janë të dizajnuara për të shterur kapacitetin e përpunimit të burimeve të infrastrukturës së rrjetit si serverat, muret mbrojtëse, dhe balancuesit e ngarkesës duke vënë në shënjestër komunikimin e protokollit Shtresa 3 dhe Shtresa 4 me kërkesa dashakeqe të lidhjes.
- **Sulmet e aplikacioneve**: Ndër sulmet më të sofistikuara DDoS, këto sulme shfrytëzojnë dobësitë në shtresën e aplikacioneve – Shtresën 7 – duke hapur lidhje dhe duke filluar kërkesat e procesit dhe transaksioneve që konsumojnë burime të fundme si hapësira e diskut dhe memoria në dispozicion.[13]

Trajnime të rregullta

Për **të rritur ndërgjegjësimin rreth kërcënimeve kibernetike dhe sigurisë së informacionit**, trajnimi i ndërgjegjësimit për sigurinë është një nga elementët më të rëndësishëm të higjienës kibernetike që mund të zbatohet nga çdo organizatë, për të mësuar punonjësit se si të shmangin, identifikojnë, dhe raportojnë kërcënimet potenciale.

Regjistrimi i stafit në një kurs të fuqishëm trajnimi për ndërgjegjësimin e sigurisë është një nga masat proaktive që organizatat mund të marrin për të shmangur sulmet kibernetike. Pa llogaritur këtë element njerëzor, dera e organizatës suaj mbetet e hapur për kërcëmnimet kibernetike.

Trajnimi i ndërgjegjësimit për sigurinë ndihmon në rritjen e njohurive të përdoruesve rreth kërcënimeve potenciale, të cilat:

- reduktojnë rrezikun;

11 Types of Cyber Threat in 2019, IT Governance USA

12 https://www.fortinet.com/resources/cyberglossary/ddos-attack

13 https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained

- pengojnë kohën e mosaktivitetit;
- përmirësojnë besimin e punonjësve; dhe
- forcojnë besimin e klientit.

Pra, trajnimi i ndërgjegjësimit për sigurinë është jetësor për sigurinë e efektshme kibernetike dhe higjienën kibernetike. Dhe me kalimin e kohës, trajnimet vjetore të ndërgjegjësimit për sigurinë mund të ndryshojnë kulturën e sigurisë kibernetike në organizatën tuaj. Këto trajnime duhet të përfshijnë informacion të paktën në lidhje me:

- Informacionin e ndjeshëm: çfarë është dhe si t'i bësh ballë
- Si t'i njohësh email-et phishing
- Si të përdoren pajisjet e kompanisë
- Si të raportohen incidentet
- Çfarë të bëni në rast emergjence që ndikon në sistemet kompjuterike dhe informatike
- Si t'i trajtojmë informacionet personalisht të identifikueshme (PII)
- Higjiena bazë kibernetike: çfarë është dhe si ta zbatojmë atë

Trajnimet e zgjeruara duhet të fokusohen në përmbajtje, materiale mbështetëse, testime phish, metrikë, raportim dhe sondazhe.

Programe të suksesshme të trajnimit të ndërgjegjësimit të sigurisë:

- Edukoni dhe mbështetni punonjësit pa i shkurajuar ose pa i turpëruar.
- Mos u përqëndroni vetëm në fushatat e phishing (qëllimi është që punonjësit të mësojnë të njohin dhe raportojnë kërcënime në kohë reale, të cilat marrin forma të shumta që vazhdimisht ndryshojnë).
- Shmangni përsëritjen e të njëjtës përmbajtje dhe përpiquni t'i pajisni punonjësit me informacion të ri në çdo trajnim.
- Përfshini materialin që lidhet edhe me jetën private të punonjësve, pasi kjo personalizon përmbajtjen dhe mund t'i bëjë punonjësit më të gatshëm për të dëgjuar.

Rekomandohet që rezultatet e trajnimeve – pozitive ose negative – të mbeten brenda organizatës dhe të mos ndahen me palët e interesit.

Përmbledhje

Pothuajse të gjitha sulmet kibernetike përfitojnë nga kushtet që bien nën ombrellën e higjienës së dobët kibernetike. Kjo përfshin riparime të humbura, konfigurime të këqija dhe ndërgjegjësim të dobët të përdoruesve. Një mungesë e vazhdueshme e higjienës kibernetike është pra një nga kërcënimet më të mëdha që mund të vijnë nga brenda një organizate. Për të nxitur higjienën e mirë kibernetike në të gjithë organizatën tuaj:

- Ofroni punonjësve trajnim të mjaftueshëm për të identifikuar dhe raportuar aktivitetet e dyshimta kibernetike.
- Sigurohuni që të gjitha serverat, kompjuterët e punës, telefonat celular dhe pajisjet e tjera që përdorin punonjësit të marrin përditësime të shpeshta sigurie.
- Zbatoni politikë të fortë të menaxhimit të aksesit të sistemit që kërkon autentifikim shumë-faktorësh sa herë që është e mundur dhe standarde strikte fjalëkalimi.
- Investoni në sisteme dhe zgjidhje që mundësojnë dukshmëri të qartë dhe qasje të kontrollit granular në të gjithë infrastrukturën e rrjetit të organizatës.

Ndërsa mund të duket se kompleksiteti do të ishte armiku i krimit kibernetik, ai është në fakt armiku i vetë sigurisë kibernetike. Në një botë dixhitale të ndërlikuar dhe dinamike, mbrojtja më e mirë në të vërtetë është të ktheheni tek bazat.

Për të përmirësuar dhe rritur higjienën kibernetike, nuk mjafton që një organizatë thjesht t'u ofrojë shembuj punonjësve dhe të theksojë rrezikun e pasigurisë kibernetike. Në çdo organizatë, higjiena kibernetike duhet të përcaktohet në mënyrë specifike dhe pastaj të mbështetet nëpërmjet metrikave dhe edukimit.

Një kornizë sigurie është një pikënisje e madhe, por ajo duhet të jetë:

- Me madhësinë e duhur për nevojat tuaja organizative
- Në përputhje me kërkesat tuaja unike rregulluese
- E plotësuar nga stërvitja që është në dispozicion dhe e përballueshme për organizatën tuaj
- E mirëmbajtur/përsëritshme me burimet tuaja organizative
- Në mbështetje të objektivave tuaja të biznesit dhe të punës

Konkluzione

Në fund të fundit, zakonet e këqija kibernetike – ose higjiena e dobët kibernetike – janë shkaku i sulmeve më të suksesshme kibernetike. Prandaj është kaq e rëndësishme që organizatat të zhvillojnë një kulturë të mirë të higjienës kibernetike. Por masat e rekomanduara në këtë Udhëzues, edhe pse paraqiten kryesisht nga pikëpamja e sigurisë organizative, janë të zbatueshme si për organizatat ashtu edhe për individët. Organizatat duhet të kërkojnë që punonjësit të zbatojnë zakonet e higjienës kibernetike edhe në shtëpi. Në fund të fundit, zakonet e mira të higjienës kibernetike që praktikohen në shtëpi, ka edhe më shumë të ngjarë të praktikohen në punë. Për më tepër, ne jemi të gjithë më të sigurt në botën kibernetike kur kultura e higjienës kibernetike shtrihet edhe në hapësirën personale edhe në atë profesionale.

Referenca

ENISA: Review of Cyber Hygiene practices https://www.enisa.europa.eu/publications/cyber-hygiene

Centre for Cyber Security Belgium: Cyber security guide for SME https://ccb.belgium.be/sites/default/files/CCB-EN%20-C.pdf

ANSSI: Guideline for a healthy information system https://www.ssi.gouv.fr/uploads/2013/01/guideline-for-a-healthy-information-system-in-42-measures_v2.pdf

CPME-ANSSI: Guide Des Bonnes Pratiques De L'informatique https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

NIST: Small business information security: the fundamentals https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

CISA: Cyber Essentials Starter Kit https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf

CMU SEI: Cyber Hygiene: 11 Essential Practices https://insights.sei.cmu.edu/blog/cyber-hygiene-11-essential-practices/

Canadian Centre for Cyber Security: Cyber Hygiene https://cyber.gc.ca/en/guidance/cyber-hygiene

Kaspersky: Good cyber hygiene habits to help you stay safe online https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

ANSSI: 40 Essential measures for a healthy network https://www.ssi.gouv.fr/uploads/2013/01/guide_hygiene_v1-2-1_en.pdf

US House of Representatives: Promoting Good Cyber Hygiene Act of 2017 https://www.congress.gov/115/bills/hr3010/BILLS-115hr3010ih.pdf

NCSC NL: Cyber Hygiene in the Netherlands https://english.ncsc.nl/research/research-results/cyber-hygiene-in-the-netherlands

NIST NCCoE: Critical Cybersecurity Hygiene: Patching the Enterprise https://www.nccoe.nist.gov/projects/critical-cybersecurity-hygiene-patching-enterprise

CISA: Cyber Hygiene Services https://www.cisa.gov/cyber-hygiene-services

CYBER4Dev: Cyber Security Hygiene/Awareness https://cyber4dev.eu/cyber-security-hygiene-awareness/

[16] eGA: What is Cyber Hygiene? https://ega.ee/blog_post/podcast-what-is-cyber-hygiene/

Shtojcë: lista kontrolluese e praktikave të mira

ANALIZONI SISTEMET DHE VENDOSNI PROCEDURAT DHE POLITIKAT		
Kategoria	**Praktikat e mira**	**Palët përkatëse të interest**
Inventari i harduerit dhe softuerit	- Mbani inventar të harduerit dhe softuerit - Standardizoni inventarin e programeve dhe pajisjeve	Institucionet Publike dhe NVM-të
Inventari i informacionit të ndjeshëm ose kritik	- Mbani një inventar të informacionit të ndjeshëm ose kritik - Kuptoni peizazhin e të dhënave dhe identifikoni të dhëna të rëndësishme në të gjithë mjedisin tuaj - Krijoni një politikë klasifikimi të të dhënave - Kriptoni të dhënat, veçanërisht të dhënat e klasifikuara si "të kufizuara" - Zbatoni një sistem të parandalimit të humbjes së të dhënave	Institucionet Publike dhe NVM-të
Analiza e riskut	- Identifikoni rreziqet • rreziku njerëzor {mashtrimi, vjedhja ose gabimi njerëzor). • rreziqet natyrore (përmbytjet, zjarret, tërmetet, etj.) • rreziqet teknike (dështimet e softuerit, hardueri ose mungesa e njohurive). - Shmangni rrezikun – nëse nuk është një shqetësim i drejtpërdrejtë për biznesin tuaj - Reduktoni rrezikun - duke zbatuar zgjidhje të reja sigurie - Pranoni rrezikun – nëse nuk ka gjasa të ndodhë ose është përtej aftësive aktuale të organizatës suaj - Transferoni rrezikun - nëpërmjet sigurimit	Institucionet Publike dhe NVM-të
Procedurat e bërjes së kopjeve rezerve (backup)	- Vendosni një procedurë të rregullt të bërjes së kopjeve rezerve - Jini realist në krijimin e një politike për backup, dhe zhvilloni një plan me shkrim që përcakton: • Prej cilat materiale duhet të bëhet kopje rezervë? • Ku bëhet kopja rezervë? • Sa shpesh do të bëhet kopja rezervë? • Kush është përgjegjës për bërjen e kopjes rezervë? - Gjithmonë jepini përparësinë të dhënave më të rëndësishme - Gjithmonë testoni sistemin e bërjes së kopjeve - Aplikoni rregullën 3-2-1 - Përdorni ruajtjen në distancë/cloud - Bëni përditësime të shpeshta dhe të rregullta	Institucionet Publike dhe NVM-të
Përgjigje ndaj incidentit	- Create an incident response plan or IRP - When an incident occurs, it is critical the IRP is followed	Institucionet Publike
Vazhdimësia e biznesit dhe rikuperimi pas fatkeqësive	- Vendosni vazhdimësinë e biznesit dhe planet e rikuperimit pas fatkeqësive	Institucionet Publike

MBRONI SISTEMIN TUAJ INFORMATIK		
Sistemi operativ dhe programi i aplikacionit	- Riparoni dhe përditësoni sistemin tuaj operativ dhe softuerin e aplikacionit, për: • Siguri • Karakteristika të reja • Rregullime - Aktivizoni përditësimet automatike për të dy sistemet dhe aplikacionet	Institucionet Publike dhe NVM-të
Siguroni konfigurimet	- Përdorni konfigurime të sigurta për të gjitha pajisjet dhe softuerët - Dokumentoni të gjitha përditësimet dhe ndryshimet • Regjistroni ndryshimet vazhdimisht • Vendosni një bazë sigurie • Zbatoni një proces shqyrtimi dhe miratimi • Regjistroni ndryshimet e konfigurimit	Institucionet Publike dhe NVM-të
Të dhëna të ndjeshme	- Kriptoni i të gjitha të dhënave të ndjeshme - Kriptimi ndihmon ruajtjen e informacionit të ndjeshëm dhe privat duke e bërë atë të palexueshëm për kriminelët kibernetikë, pasi mund të aksesohet vetëm me një çelës	Institucionet Publike dhe NVM-të
Softuer anti-malware	- Përdorni softuer anti-malware - Zgjidhjet anti-malware do të bllokojnë shumicën e programeve keqdashëse dhe potencialisht të padëshiruara	Institucionet Publike dhe NVM-të
Mur mbrojtës (Firewalls)	- Përdorni mure mbrojtëse, në mënyrë që të: • bllokoni shumicën e programeve keqdashëse dhe potencialisht të padëshiruara • parandaloni ekzekutimin e programeve keqdashëse në një pajisje • parandaloni që programet keqdashëse të ndryshojnë cilësimet • parandaloni softuerin keqdashës nga ngarkimi i softuerit shtesë të kompromentuar	Institucionet Publike dhe NVM-të
Rrjete WI-FI	- Mbroni rrjetet WI-FI - Përdorni kriptimin e rrjetit WI-FI - Përditësoni dhe riparoni softuerin. - Vendosni ruterët WI-FI sa më afër qendrës së organizatës suaj - Aktivizoni filtrimin e adresës MAK - Çaktivizoni administrimin në distancë - Krijoni një rrjet të veçantë WI-FI për vizitorët	Institucionet Publike dhe NVM-të
Cilësimet e shfletuesit të internetit	- Konfiguroni rregullimet e sigurisë së shfletuesit të internetit universalisht - Bllokoni njoftimet pop-up, shtojcat plugin dhe faqet e phishing - Mos lejoni ruajtjen e fjalëkalimeve - Çaktivizoni kukit e palëve të treta - Deinstaloni zgjerime që nuk përdoren - Përditësoni rregullisht zgjerimet që përdoren - Nxisni përdoruesit të hyjnë në uebfaqe HTTPS në vend të uebfaqeve http	Institucionet Publike dhe NVM-të
Pajisjet mobile	- Kërkoni që përdoruesit të: • Mbrojnë pajisjet me fjalkalim • Kriptoni të dhënat • Instaloni aplikacione të sigurisë për të parandaluar kriminelët kibernetikë nga vjedhja e informacionit ndërsa pajisja është e lidhur me rrjetet publike • Konfiguroni pajisjen për t'u kyçur automatikisht - Vendosni procedurat e raportimit për pajisjet e humbura ose të vjedhura	Institucionet Publike dhe NVM-të
Pajisje IoT	- Siguroni pajisjet IoT: • duke ndryshuar fjalkalimet të parapërcaktuara • duke përdorur fjalëkalime të forta • duke përditësuar softuerin e pajisjes rregullisht • duke kriptuar dhe autentifikuar pajisjet • duke ndryshuar cilësimet e paracaktuara të privatësisë • duke ndryshuar cilësimet standarde • duke siguruar që rrjeti i organizatës dhe WI-FI janë të siguruara • duke krijuar rrjet vizitorësh • duke verifikuar gjithmonë përditësimet e disponueshme në faqen e internetit të prodhuesit para se t'i aplikoni në pajisjet tuaja.	Institucionet Publike dhe NVM-të
Siguria fizike e pajisjeve	- Kujdesuni për sigurinë fizike të pajisjeve, veçanërisht pajisjeve celulare: • Duke mbrojtur pajisjet me fjalëkalime të forta • Duke mbajtur përdoruesit/pronarët sendet me vlerë me vete gjatë gjithë kohës	Institucionet Publike dhe NVM-të

<table>
<tr><td>Qasje në distancë</td><td>- Sigurohuni që të gjitha programet e aksesit në distancë të jenë të riparuara (patched) dhe të përditësuara
- Kufizoni qasjen në distancë nga vende të dyshimta gjeografike ose adresa të caktuara IP
- Kufizoni qasjen në distancë të punonjësve vetëm në sistemet dhe kompjuterët që ata kanë nevojë për të bërë punën e tyre
- Zbatoni fjalëkalime të forta për qasje në distancë
- Aktivizoni vërtetimin me shumë faktorë nëse është e mundur
- Sigurohuni që monitorimi dhe lajmërimi të jetë mundësuar për të paralajmëruar për sulme të dyshuara ose aktivitet të dyshimtë</td><td>Institucionet Publike dhe NVM-të</td></tr>
<tr><td colspan="3">ZBATONI PRAKTIKAT E MIRA</td></tr>
<tr><td>Fjalëkalime</td><td>- Fjalëkalimet më të gjata janë më të mira
- Kompleksiteti është çelësi! Kërkoni simbole, shkronja të vogla dhe të mëdha, dhe numra
- Përdorni fjalë pa kuptim dhe shmangni parashikueshmërinë
- Të gjitha fjalëkalimet le të jenë unike
- Ndryshoni të gjitha fjalëkalimet e paracaktuara</td><td>Institucionet Publike dhe NVM-të</td></tr>
<tr><td>Autentikimi me shumë faktorë</td><td>- Përdor autentikimin me shumë faktorë sa herë që është e mundur
- Përdorni dy nga tre faktorët e autentikimit - diçka që një përdorues e di, është, ose e ka</td><td>Institucionet Publike dhe NVM-të</td></tr>
<tr><td>Llogaritë</td><td>- Përdorni llogari të kufizuara (Përdoruesi Standard) për qëllime të rregullta dhe të përditshme
- Krijoni llogari të përdoruesit standard dhe administrative për qëllime të ndryshme</td><td>Institucionet Publike dhe NVM-të</td></tr>
<tr><td>Qasja e punonjësve</td><td>- Mos i jepni asnjë punonjësi të vetëm qasje në të gjitha sistemet e të dhënave
- Punonjësve t'u jepet qasje vetëm në sistemet që ata kanë nevojë për të bërë punën e tyre
- Mos u jepni punonjësve mundësi për të instaluar softuer pa leje</td><td>Institucionet Publike dhe NVM-të</td></tr>
<tr><td>Regjistrimi (logging)</td><td>- Bëni regjistrim të vazhdueshëm
- Sigurohuni që të kuptoni se cilat regjistrime janë të nevojshme bazuar në praktikat më të mira dhe rishikojini ato çdo ditë për të gjetur gabime, anomali ose aktivitete të dyshimta</td><td>Institucionet Publike</td></tr>
<tr><td colspan="3">NDËRGJEGJËSIMI PËR SIGURINË KIBERNETIKE</td></tr>
<tr><td>Kërcënimet e zakonshme kibernetike</td><td>LLOJI I KËRCËNIMIT KIBERNETIK

- Inxhinieri Sociale
- Sulme Phishing
• Spear Phishing
• Whale Phishing/Whaling
• Vishing
• Smishing
- Kompromet imi i e-mailit të biznesit (Business Email Compromise)
- Shkarkime në kalim (Drive-By Downloads)
- Sulme MITM
- Sulm USB drop
- Malware
• Softuer Botnet
• Sulm me Ransomware
• Spyware
• Trojan
• Viruset dhe krimbat
- Sulme DoS/DDoS
• Volumetrik
• Protokoll
• Aplikacion</td><td>REKOMANDIME

- EMAILET: Kujdes me emailet, sidomos nëse ato përmbajnë bashkëngjitje dhe lidhje web. Kërkoni:
• Gabime drejtshkrimore dhe gramatikore
• Lidhje të dyshimta
• Bashkëngjitje të dyshimta
• Gjuhë kërcënuese
• Mashtrim (spoofing)
• Adresa të ndryshuara
• Mospërputhje
- RRJETE PUBLIKE WI-FI: Gjithmonë bëni kujdes kur lidheni me rrjetet publike WI-FI:
• Duke shmangur futjen në të dhëna të ndjeshme
• Duke u lidhur me rrjete të besueshme
• Duke mos u lidhur automatikisht</td><td>Institucionet Publike dhe NVM-të</td></tr>
<tr><td>Trajnime të rregullta</td><td colspan="2">- Rritja e ndërgjegjësimit në lidhje me kërcënimet kibernetike dhe sigurinë e informacionit përmes trajnimeve vjetore ose më të shpeshta
- Një kurs i fuqishëm trajnimi për ndërgjegjësimin e sigurisë duhet të mbulojë:
• Informacion i ndjeshëm: çfarë është dhe si t'i trajtoni ato
• Si të njihet emaili phish
• Si të përdoret pajisja e kompanisë?
• Si të raportohen incidentet
• Çfarë duhet të bëni në rast emergjence që ndikon në sistemet kompjuterike dhe të informacionit?
• Si të trajtohet informacioni personal i identifikueshëm (PII)</td><td>Institucionet Publike dhe NVM-të</td></tr>
</table>

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva