AEK
MKD-CIRT

AGJENCIA PËR KOMUNIKIME ELEKTRONIKE

QENDRA KOMBËTARE PËR PËRGJIGJE TË LIDHURA ME INCIDENTET KOMPJUTERIKE

SIGURIA KIBERNETIKE

UDHËZUES PËR NDËRMARRJE TË VOGLA DHE TË MESME

Verzioni 1.0
tetor 2019

PËRMBAJTJA

PARATHËNIE

Ky udhëzues është krijuar me qëllim për të ndihmuar bizneset, e vogla dhe të mesme të mbrohen nga sulmet kibernetike më të shpeshta.
Sektori i biznesevetë vogla, të mesme (NVMM) në tërësi është dominues në ekonominë e Republikës së Maqedonisë së Veriut.. Të dhënat më të reja tregojnë se 99,8% të bizneseve i takojnëatij grupi. Gjatë vitit 2013, 53,137 biznese ishin NVMM, nga të cilat 91,0% në vend janë ndërmarrje të vogla. NVMM janë gjithashtu punëdhënësit më të mëdhenj, duke siguruar 76.6% nga numri i përgjithshëm i punësimeve.1

Pavarësisht nëse Ju jeni pronar apo punonjës i një prej këtyre bizneseve, jeni përgjegjës i pajisjeve informatike, ose thjeshtë doni t'i siguroni pajisjet e juaja të lidhura me Internet të jenë sa më të sigurta. Brenda undhëzuesit do të gjeni këshilla se si ta përmirësoni mbrojtjen nga llojet më të shpeshta të kërcënimeve dhe krimeve kibernetike. Udhëzuesi mbulon 6 tema. Secila prej temave përmban këshilla dhe zbatimi i tyre nuk kërkon shpenzime të mëdha financiare.

Asnjë udhëzues produkt ose specialist i fushës nuk mund të garantojë mbrojten nga të gjitha llojet e sulmeve kibernetike, por ky dokument është hartuar në mënyrë që të shpjegojë disa masa për mbrojtjen e të dhënave, pajisjeve dhe reputacionin e biznesit tuaj.

MKD-CIRT (Qendra Kombëtare për Përgjigje ndaj Incidenteve Kompjuterike), si pjesë e AEK (Agjensisë për Komunikimet Elektronike), me këtë udhëzues, si dhe dokumentet dhe informacionet e tjera të publikuara periodikisht, punon në mënyrë aktive në ngritjen e vetëdijës për domethënien e sigurisë kibernetike. Misioni ynë është të sigurojmë kushte për përdorimin e sigurt të Internetit dhe veprimtarive online.

Qendra kombëtare për përgjigje të lidhura me incidente kompjuterike MKD-CIRT AEK

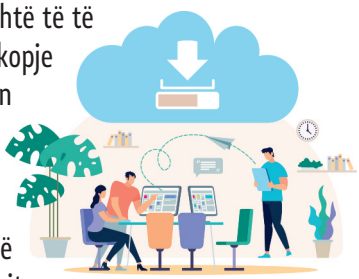
---

1) Strategjia Kombëtare për ndërmarrje të vogla dhe të mesme (2018-2023), http://economy.gov.mk/Upload/Documents/Strategija%20za%20MSP%20-%20finalna%20verzija%2003%2004%202018%20.pdf

1. KOPJE TË DYFISHTË REZERVË E TË DHËNAVE TUAJA (BACKUP)

Sipas sondazhit të fundit të MKD-CIRT-it, 50% e qytetarëve nuk bëjnë backup dhe vetëm 11% ruajnë kopje rezervë të të dhënave të rëndësishme, më së paku një herë në javë.2

Pyesni vetën cilët të dhëna janë kritike për punën tuaj? A grumbulloni dhe përpunoni të dhëna (personale) për shfrytëzuesit e shërbimeve dhe prodhimeve tuaja, ose ndoshta trajtoni porosi dhe fatura me llogari bankare. Mendoni për sa kohë mund të punoni pa të dhënave të rëndësishme.



Të gjithë ndërmarrjet duhet të bëjnë kopje të dyfishtë të të dhënave të rëndësishme dhe të sigurohen se këta kopje të dyfishtë ruhen në një vend të sigurt, përditësohen dhe të dhënat mund të ri-kthehen për ri-përdorim. Krijimi i kopjeve të dyfishtë u siguron bizneseve mundësi të vazhdojnë punën në rast të ndonjë incidenti apo ndërprerje në disponueshmërinë e të dhënave origjinale, në raste të përmbytjes, zjarrit, dëmtimit fizik ose vjedhjes së pajisjeve dhe dokumenteve. Kopjet të dyfishtë të të dhënave tuaja të cilat mund ti riktheni në mënyrë të shpejt janë një mbrojtje e mirë nga sulmet kibernetike si enkriptimi i të dhënave për përfitime financiare, shembull– „ransomver" (ang. ransomware).

KËSHILLA 1: IDENTIFIKONI TË DHËNAT PËR TË CILAT DUHET TË BËNI KOPJE TË DYFISHTË

Më së pari identifikoni të dhënat të cilat janë të rëndësishme për punën tuaj dhe pa të cilat biznesijuaj nuk do mund të funksionojë. Shpesh herë këto mund të jenë fatura, arkëtime dhe dokumente tjera me të dhëna financiare, personale dhe të ndjeshme. Bëni kopje të këtyre të dhënave në një pajisje të jashtme dhe ruani pajisjen në një vend të sigurt, larg nga pajisjet ku të dhënat dhe dokumentet origjinale janë të regjistruara.

2)2) Raporti i sondazhës së opinionit publik për zbatimin e masave të sigurisë së Internetit, https://mkd-cirt. mk/2019/07/30/izveshtaj-od-ispituvanje-na-javnoto-mislenje-za-primena-na-merki-za-bezbednost-na-internet/

KËSHILLA 2: RUANI KOPJEN REZERVE SA MË LARG VENDIT TË PUNËS

Pavarësisht se kopja është e regjistruar në USB, disk të jashtëm apokompjuter të veçantë, kufizoni qasjen në to në atë menyrë që:

- kopjet dytësore të mos aksesohen nga të gjithë, por vetëm nga personeli i autorizuar.
- pajisjet në të cilët janë të regjistruara, nuk duhet të jenë gjatë gjithë kohëstë lidhura (fizikisht ose nëpërmjet rrjetit lokal kompjuterik) me pajisjet në të cilën gjenden të dhënat origjinale

Nëse pajisja për ruajtje ose magazinim, ku është e regjistruar kopja dytësoreështë e lidhur gjatë gjithë kohësnë rrjetin lokal kompjuterik, në rast të infektimit me „ransomver" ose lloj tjetër softueri („malver", ang. malware), mund të afektohet automatikisht dhe pajisja sektondare në të njëjtën mënyrëtë njejtën softueri automatikisht mund të transferohet te pajisja për magazinim.

Kjo do të thotë se çdo kopje sekondare mund të infektohet, duke ju lënë pa kopje të pastër sekondare nga e cila mund të ri-ktheni të dhënat.

KËSHILLA 3: MAGAZINIMI I TË DHËNAVE NË RE (CLOUD)

Ka të ngjarë që ju përdorni shërbime për magazinim të të dhënave në re (cloud) çdo ditë. Nëse nuk përdorni serverin tuaj të postës elektronike, mesazhet tuaja elektronike tashmë janë në „re" dhe janë të regjistruara në një server jashtë organizatës. Shumë shpesh kontaktet e regjistruara në telefonin celular në mënyrë automatike regjistrohen në re (cloud), ashtu sikur edhe kopja e komunikimit nëpërmjet aplikacionet si Viber, Messenger ose WhatsApp.

Shërbimi i magazinimit të të dhënave në re (cloud) do të thotë që ofruesi i shërbimeve i ruan të dhënave juaja në infrastrukturën e tij nëpërmjet Internetit. Në atë mënyrë, të dhënat janë fizikisht të ndara nga vendndodhja juaj dhe sigurohet magazinimi i të dhënave dhe ofrimi i shërbimeve ueb pa qënë nevoja

të investoni në pajisje të shtrenjta. Përfitimi shtesë është niveli i lartë i qasjes. Shumica nga ofruesit e shërbimeve për magazinimin dhe ruajtjene të dhënave në re ofrojnë një hapësirë falas të kufizuar për magazinimin dhe ruajtjen e të dhënave, e cila mund të rritet me pagesë shtesë.

KËSHILLA 4: BËRJA BEKAP (ang. BACKUP) SI AKTIVITET I JUAJ I PËRDITSHËM

Zgjidhjet për magazinimin dhe ruajtjen nëpërmjet rrjetit ose në re mundësojnë përditësim automatik të kopjeve të dyfishtë, pa patur njohuri të mëparshme ose teknika të përparuara. Përditësimiautomatik të kopjeve të dyfishtë kurson kohë dhe Ju garanton se çdoherë do të i keni verzionet e përditësuara të dokumenteve tuaja.

Shumë nga këto zgjidhje janë të lehta për t'u instaluar dhe të përballueshme kur bëhet fjalë për çmimin duke marrë parasysh mbrojtjen e të dhënave të rëndësishme që ofrojnë. Analizoni se sa kapacitet Ju nevojitet për magazinimin e kopjes dyfishtë për të dhënat e rëndësishme, pavarësisht nëse do ta bëni magazinimin në re ose në disk të jashtëm. Duke zgjedhur menyra e regjistrimit ose shënimit të të dhënave tuaja, është shumë e rëndësishme të përcaktoni kohën maksimale për kthimin e të dhënave të cilat biznesi juaj mund të mbijetojë. Përdorni këtë informacion si një kriter shtesë në zgjedhjen e metodës së ruajtjes së kopjeve sekondaretë të dhënave.

2. MBROTJA NGA SOFTUERI MALICIOZ

Softueri keqbërës (i njohur si „malver" - ang. malware) është softuer që mund ta dëmtojë biznesit tuaj nëpërmjet fshirjes së të dhënave të rëndësishme, keqpërdorim të pajisjeve tuaja për sulme dhe shantazh nëpërmjet mbylljes apo kodimit të dokumenteve, siç ishte dukuria e mëhershme e WannaCry dhe NonPetya. Forma më e njohur e softuerit keqbërës janë virusët, programe të cilat vetë-kopjojnë (replikojnë) dhe e infektojnë softuerin legjitim.

Vijojnë 5 këshilla të thjeshta për zbatim, të cilat mund të ndihmojnë në mbrojtjen nga softueri malicioz dhe parandalimi i dëmtimit të punës së organizatës tuaj.

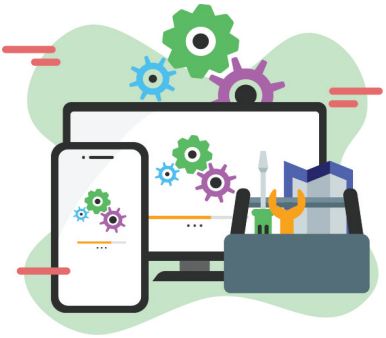
KËSHILLA 1: SOFTUER ANTIVIRUS VAZHDIMISHT AKTIV DHE I PËRDITËSUAR

Softueri antivirus i cili shpesh herë përfshihet falas në sistemet operative të njohura, duhet të përdoret në të gjithë kompjuterët, laptopët, tabletët dhe smartfonët. Ka të ngjarë që kompjuteri dhe pajisja juaj celulare tashmë kanë mbrojtje antivirus të softuerit që vjen me pajisjen, por zakonisht programet falas ofrojnë mbrojtje minimale. Megjithatë, konsideroni blerjen e zgjidhjeve tregtare të licencuara për mbrojtje antivirus, të cilat do të përmirësojnë sigurinë e pajisjeve dhe organizatës Suaj.

KËSHILLA 2: AKTIVIZONI Programet apo Sistemet Firewall (FIREWALL)

Zgjidhjet Firewall krijojnë një zonë neutrale midis rrjetit kompjuterik të brendshëm dhe rrjeteve të jashtme siç është Interneti. Sistemet më të njohura operative përfshijnë një program firewall falas, i cili është shumë i lehtë për aktivizim dhe rekomandohet të jetë i aktivizuar vazhdimisht.

KËSHILLA 3: MOS I LEJONI PUNONJËSIT TË SHKARKOJNË APLIKACIONE TË DYSHIMTA



Në pajisjet kompjuterike duhen lejuar për tu shkarkuar apo instaluar programe apo aplikacioni vetëm nga dyqanet online të autorizuar dhe certifikuar nga prodhuesi, i sistemit operativ (për telefonat celulare dhe tabletët është Google

Play Store ose Apple App Store). Këto aplikacione kontrollohen nga ana e prodhuesit të sistemit operativ për nivelin e sigurisëtë caktuar të mbrojtjes nga softueri keqdashësqë mund të shkaktojë dëme. Duhet të parandalohet shkarkimi dhe instalimi i aplikacioneve të palëve të treta, nga shitësit / burimet e panjohura, ose programet pirate, pasi nuk janë testuar dhe shpesh përmbajnë viruse ose kod tjetër keqdashës.

Vetëm në raste të veçanta vendosni shfrytëzim e llogarive të përdoruesve me të drejta „administrative". Llogaritë e punonjësit për qasje në pajisje dhe të dhëna të organizatës duhet të kenë vetëm qasje e mjaftueshme për të kryer rolin e tyre, me leje shtesë (d.m.th. për administratorët) të dhëna vetëm për ata qëkanë nevojë për to. Kur krijohen llogaritë administrative, duhet të përdoren vetëm për atë detyrë të veçantë, ndërsa për detyra të përditshme pune përdoren llogaritë standarde të përdoruesve. Mos lejoni punonjësit t'i kryejnë detyrat e përditshme pune në pajisjen kompjuterike me të drejta administratorike.

KËSHILLA 4: MIRËMBANI PAJISJEN INFORMATIKE TË PËRDITËSUAR (INSTALIMI NË KOHË I - TË ARNUAR - PATCHING DHE PËRDITËSIM - UPDATING)

Për pajisjet informatike (kompjuterë, laptopë, telefona celulare dhe tableta), sigurohuni që softueri dhe firmvaeri janë gjithnjë të përditësuara me versionet më të fundit nga prodhuesit dhe furnitorët përkatës. Aplikimi i këtyre përditësimeve (një proces i njohur si instalim i arnave ose „peçing" - ang. patching) është një nga gjërat më të rëndësishme që mund të bëni për përmirësimin e sigurisë së pajisjeve. Sistemet operative, aplikacionet, telefonat celularë dhe tabletët duhet të vendosen në „përditësim automatik" gjithmonë kur ka mundësi.

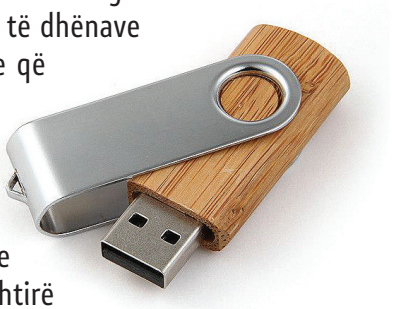
Kur përfundon mbështetja zyrtare e përditësimeve e cila e ofron prodhuesi i pajisjes ose aplikacionit, duhet të merrni parasysh rreziqet e përdorimit të mëtejshëm të asaj pajisje ose softueri pasi që dobësitë

e zbuluara rishtas nuk do të riparohen me arnime nga ana e prodhuesit, gjë që do të rrisë ndjeshmërinë dhe vulnerabilitetin ndaj sulmeve dhe do të rrisë rrezikun gjatë punës.

Pas përfundimit të mbështetjes zyrtare të prodhuesve për pajisjet dhe softuerin që përdorni, konsideroni mundësinë e zëvendësimit të pajisjeve me të reja.

KËSHILLA 5: KONTROLLI GJATË PËRDORIMIT TË MEMORISË SË JASHTME - USB

Pajisjet e memorieve të jashtme USB përdoren në menyrë masive për transferim të skedarëve dhe të dhënave midis organizatave dhe njerëzve. Për cënim të sigurisë së të dhënave të një oganizate është e mjaftueshme që vetëm një përdorues i pakujdesshëm të lidhë pa dashje një pajisje të infektuar (disk USB që përmban softuer malicioz). Meqë ato shpërdahen lirisht dhe shpesh përdoren për qëllime private dhe zyrtare, është shumë e vështirë të gjurmohet se çka përmbajnë konkretisht, ku ishin dhe kush i ka përdorurato. Mund të zvogëloni mundësinë e infektimit prej këtyre pajisjeve duke:



- bllokuar/ndaluar lidhjen në portat fizike USB për shumicën e punonjësve;
- përdorur programe antivirus, të cilat do të kontrollojnë përmbajtjen e pajisjes çdo herë kur pajisja memorike do të lidhet me kompjuterin;
- kufizuar që vetëm pajisjet e miratuara të përdoren brenda kompanisë suaj - dhe askund tjetër;

Bëni këto rregulla pjesë të procedurës së përdorimit të pranueshëm të pajisjeve IT të organizatës suaj. Edukoni punonjësit për transferimin e skedarëve me email ose duke përdorur shërbime të ruajtjes në re.

3. MBROTJA NGA SULMET FISHING

Në një sulm tipik fishing (sulm joshës), mashtruesit (ang – scammers) dërgojnë porosi të rreme për mijëra njerëz, duke kërkuar informacione sensitive (siç janë të dhënat bankare) ose përmbajnë linqe të faqeve të rrezikshme web. Të njejtat mund t'ju mashtrojnë që të dërgoni para, t'ju vjedhin detaje për qëllim shitje ose mund të kenë motive politike ose ideologjike për qasje në informacionet e organizatës suaj.

Mesazhet Fishing po bëhen më të sofistikuara dhe mund tët'i mashtrojnë edhe përdoruesit më të kujdesshëm. Ka më shumë të ngjarë të përballoni me sulme fishing. Më poshtë janë disa këshilla që mund të ndihmojnë në identifikimin e sulmeve fishing, por duhet të jeni të vetëdijshëm se ekziston një kufi në atë që mund të prisni nga ana e përdoruesve.

KËSHILLË 1: KËSHILLA TË SIGURISË PËR LLOGARITË PËRDORUESE TË PUNONJËSIT

Gjatë konfigurimit të llogarivetë përdoruesve për punonjësit tuaj duhet të zbatoni parimin „sa më pak privilegje të nevojshme"– punonjësit të kenë privilegje dhe qasje në pajisje dhe dokumente në një nivel të mjaftueshëm për të kryer detyrat e tyreme sukses dhe në kohë. Privilegjet e tepërta dhe të panevojshme rrisin rrezikun e një sulm të suksesshëm fishing.

Sigurohuni që punonjësit nuk përdorin llogari me të drejta administratorinë pajisjet të lidhura me Internet gjatë kryerjes së detyrave të përditshme. Llogaria e përdoruesit administrativ është një llogari që ju lejon të bëni ndryshime të cilat do të ndikojnë te përdoruesit e tjerë. Administratorët mund t'i ndryshojnë përshtatjet e sigurisë, të instalojnë softuer dhe harduer dhe t'i përdorin të gjithë skedarët në kompjuterin / pajisjen. Nëse sulmuesi merr qasje në një llogari të përdoruesitme privilegje administrative, dëmi i organizatës mund të jetë i madh.

Përdorni autetintik me 2 faktorë (ang. 2FA – two factor authentication) në llogaritë tuaja të rëndësishme, siç është emaili. Kjo domethënë se edhe në qoftë se sulmuesi arrin të marrë fjalëkalimet tuaja, ai ende nuk do të jetë në gjendje të hyjë në atë llogari se përveç fjalëkalimit, atij dot'i duhet p.sh. gjithashtu edhe kodin i cili do të merrni në celularin tuaj.

KËSHILLA 2: MENDONI PËR PYETJEN SI TA ORGANIZONI PUNËN TUAJ

Konsideroni mënyrat me të cilat dikush mund të sulmojë organizatën tuaj dhe sigurohuni që punonjësit tuaj t'i kuptojnë mënyrat e zakonshme të punës (veçanërisht në lidhje me bashkëpunim me organizata të tjera), në mënyrë që të edukohen t'i vërejnë kërkesat që nuk janë të zakonshme. Mashtrimit të zakonshëm përfshin dërgim e një faturë për një shërbim që nuk e keni përdorur, kështu që kur do të hapni shtojcën (attachment), softueri malicioz instalohet automatikisht në kompjuterin tuaj pa dijeninë tuaj.

Një mënyrë tjetër për mashtrimin e punonjësit është transferimi i parave në llogari të pakontrolluara ose dorëzimi i informacioneve sensitive duke dërguar një përgjigje me dukje autentike të postës elektronike.

Mendoni për praktikat tuaja të zakonshme dhe në çfarë menyrë mund të ndihmoni këto përpjekje të kenë një shans më të ulët të suksesit. Për shembull:

- A e dinë punonjësitsi të veprojnë në rast të kërkesave të pazakonta, kujt t'i paraqesin dhe ku mund të marrin ndihmë?
- Pyesni veten nëse dikush i cili paraqitet si një person i rëndësishëm (klient ose menaxher) përmes email duhet të kontrollohet (ose të verifikohet identiteti i tij në një mënyrë tjetër, për shembull me konfirmim të dërguar me një mesazh SMS) para se të ndërmarretnjë veprim i caktuar siç është pagesa e parave, dërgimi i informacionit të rëndësishëm etj.

- A i kuptoni marrëdhëniet tuaja të zakonshme të biznesit? Mashtruesit shpesh dërgojnë mesazhe fishing nga organizata të mëdha (siç janë bankat) me shpresën se disa prej pranuesve të postës elektronike do të kenë një lidhje me atë organizatë. Nëse merrni një email nga një organizatë me të cilën nuk keni lidhje, trajtojeni atë me dyshim dhe kujdes. Njoftoni menjëherë superiorin ose personi përgjegjës për sektorit IT brenda organizatës.
- Mendoni në çfarë menyrë mund t'itrajnoni dhe mbështesni punonjësit tuaj për të njohur ose vërejtur kërkesa të dyshimta ose thjesht kërkesa të pazakonta, edhe nëse ato duken se janë nga persona të rëndësishëm. Të ketë besim për pyetjen „a është ky mesazh autentike?"mund të jetë dallimi mes ruajtjes së sigurisë së kompanisë ose një gabimi që mund t'ju kushtojë shtrenjtë.

KËSHILLA 3: SHENJA FISHING NË MESAZHET

Hamendësimi se punonjësit tuaj arrijnë të indentifikojnë dhe t'i fshijnë të gjitha fishing mesazhet është e pamundur. Sidoqoftë, punonjësit të arsimuar dhe të trajnuar t'i paraqesin mesazhet të dyshimta janë mbrojtja më e mirë për organizatën tuaj kundër sulmeve fishing. Në vijim ka disa shenja për identifikimin e sulmeve për të cilat punonjësit duhet të edukohen:

- Shumë sulme fishing vijnë nga vende të huaja dhe shpesh herë drejtshkrimi, gramatika dhe shenjat e pikësimit të tekstit në mesazhet janë shumë dobëta dhe bëhen nëpermjet përdorimit të shërbimeve të automatizuara të përkthimit të tekstit, siç është Google translate. Disa sulmues do të përpiqen të krijojnë mesazhe që janë shumë të ngjashme me mesazhet zyrtare duke përfshirë logot dhe grafikat e ngjashme me tuajat ose kompanitë me të cilat punoni. Detaisht shikoni mesazhin e shenjave për falsifikim.
- Nëse në titullin e mesazhit ju drejtohen me adresën tuaj të email-it ose shkruan „të ndëruar", „koleg" ose është përdorur një term të ngjajshëm gjenerik, kjo mund të jetë shenjë se dërguesi nuk ju njeh dhe mesazhi ndoshta është dërguar për mashtrim fishing.

- Kini dyshim në mesazhet ku në tekstet kërkohet nga ju të veproni shpejt. Kini dyshim nëse në mesazhet ka fjalë të tipit „dërgoni këto detaje brenda 24h" ose „Ju jeni viktimë e krimit, klikoni këtu menjëherë".
- Keni kujdes me mesazhe të cilla në shikim të parë duken siç të janë dërguar nga një person i rangut të lartë të organizatës suaj, me kërkesë për pagesa të shpejta në llogari të caktuara bankare. Sigurohuni që e njihni adresëne email-it nga e cila dërgohet mesazhi apo thjesht është e ngjashme me adresat që i përdorni shpesh për komunikim. Kontrolloni saktësinë e kësaj llogarie bankare dhe nëse me të vërtetë i përket kompanisë që njihni, që keni punuar me të dhe keni ndërtuar besim në të kaluarën. Kërkoni vërtetim nëpërmjet SMS-së ose një kanali tjetër komunikimi për vërtetësinë e kërkesës.
- Mos iu përgjigjni email-ave, SMS-ve, Viber ose WhatsApp mesazheve në të cilat ju ofrohen para ose trashëgimi nga vende të huaja, të dërguara nga njerëz dhe adresa e email-it që nuk i njihni, ose mesazhe ku ju ofrohen qasje në informacione të fshehura ose kompromet uese në Internet.
- Mos iu përgjigjni email-ave që ju shantazhojnë me postimin e informacione dhe fotografi kompromet uese nëse nuk pagoni në monedhë Bitcoin, për të cila pretendohet se janë të dërguara nga adresa juaj e email-it. Shumë shpesh, këto kërcënime janë të rreme dhe vetëm duken sikur të ishin dërguara nga adresa juaj e email-it. Kërkoni ndihmë nga personi ose institucioni përgjegjë spër komunikimin tuaj me email, me qëllim që të identifikoni adresën e vërtetë të email-it nga i cili është dërguar mesazhi dhe i cili është maskuar për t'u duket i njëjtë me adresën tuaj të email-it.

KËSHILLA 4: PARAQITNI TË GJITHA SULMETFISHING

Edukoni punonjësit t'i njoftojnë TË GJITHA mesazhe të dyshimta. Pas njoftimit, nëse dyshoni se jeni objektiv i një sulmi fishing, merrni masa urgjente për skanimin e pajisjeve për ekzistencën e mundshme e softuerit malicioz

(malver) dhe siguroni ndryshim të rregullt të fjalëkalimeve tuaja.

Mos prisni qëpunonjësit t'i njohin të gjitha përpjekje për sulmet fishing. Inkurajoni ata t'i paraqiten të gjitha gabime gjatë punës dhe sigurojeni ata që nuk do të ndëshkohen për hapjen e një bashkangjitje tënjë mesazhi email pa dashje. Mos i ndëshkoni punonjësit nëse janë të mashtruar. Kërcënimet me dënim mund të shkurajojnëpunonjësit t'i paraqiten përpjekjet e ardhshme për fishing mashtrime. Në atë mënyrë mund të shkaktohet më shumë dëme në biznesin tuaj.

Nëse dyshoni se organizata juaj është objekt ose viktimë e mashtrimit online ose në internet, (ransomware) ose një sulm fishing, duhet ta raportoni këtë në Ministrinë e Punëve të Brendshme në stacionin më të afërt të Policisë ose nëpërmjet telefonit. Gjithashtu mund të lajmëroni në MKD-CIRT, duke plotësuar formularin në dispozicion në faqen tonë të internetit https://mkd-cirt.mk ose me email në info@mkd-cirt.mkdhe në këtë rast MKD-CIRT do t'Ju dërgojë udhëzime për të trajtuar sulmin e paraqitur dhe sipas nevojës do të dërgojë mesazhin në MPB.

4. FJALËKALIME DHE QASJE

Kur u pyetën nëse keni një fjalëkalim për pajisjet që përdorni, 75% e përdoruesve të pajisjeve dixhitale që përdorin Internetin në vend u përgjigjën se përdorin fjalëkalime. Edukimi i punonjësit rreth rëndësisë së përdorimit të fjalëkalimeve si mbrojtje e tyre parësore ka rëndësi të veçantë. Laptopët, kompjuterët, tabletët dhe smart telefonat tuaj mund të përmbajnë të dhëna kritike për biznesin, të dhëna personale të klientëve tuaj dhe detaje të llogarive në internet që ju qaseni. Me përdorimin e fjalëkalimeve siguroni nivelin më të ulët të mbrojtjes për hyrje në të dhënat tuaja, parandalohet qasjen dhe përdorimin e paautorizuar. Vijojnë këshilla për përdorimin e fjalëkalimeve me qëllim siguri më të madhe.

KËSHILLA 1: ATY KU ËSHTË E NEVOJSHME PËRDORNI MBROJTJE I QASJES SË TË DHËNAVE ME FJALËKALIME

Pavarësisht nëse bëhet fjalë për një kompjuter, telefon, tablet apo shërbim online, vendosni një fjalëkalim për kufizimi i qasjes në këto pajisje dhe shërbime nëse ato përmbajnë të dhëna të ndjeshme ose të rëndësishme për biznesin tuaj. Përveç fjalëkalimeve, duhet të siguroni qasjen me mbrojtje shtesë kudo ku është e mundshme, p.sh. duke përdorur PIN (ang. Personal Identification Number) shenja gishti ose fytyre, si mënyra vërtetimishtesë.

Sigurohuni që pajisjet IT siç janë kompjuteri dhe laptopi përdorin enkriptim ose shifrimim e të dhënave të regjistruara në të. Një shembull i kësaj është BitLocker për Windows dhe FileVault për macOS. Aktivizoni enkriptimin përpara se të fillojë të përdoretkompjuteri juaj. Pyetni IT personat përgjegjës për mirëmbajtjen e pajisjeve t'ju aktivizojnë këtë opsion.

KËSHILLA 2: PËRDORNI FJALËKALIME TË FORTA

Nëse jeni përgjegjës për politikat e përdorimit të pajisjeveIT brenda organizatës suaj, sigurohuni që punonjësit të dinë në çfarë menyrë të krijojnë fjalëkalime të forta, të cilat do të jenë të lehta për t'u kujtuar, por në të njejtën kohë të vështira për t'u zbuluar nga kriminelët. Praktika më e zakonshme është gjatësia e fjalëkalimeve me të paktën 8 karaktere dhe të përmbajë tre nga katër grupet e shenjave (shkronja të vogla, shkronja të mëdha, numra dhe shenja speciale).

Sigurohuni që çdo përdorues të këtë qasje personale në sistemet përkatëse dhe nivelin e qasjes së dhënë është gjithmonë në nivelin më të ulët të nevojshëm për përfundimin e punës së vetë.

KËSHILLA 3: PËRDORNI VËRTETIM ME DY FAKTORË PËR LLOGARITË „E RËNDËSISHME"

Sipas sondazhit të fundit të MKD-CIRT, 70% e përdoruesve të Internetit në vend nuk përdorin vërtetim me dy faktorë. Nëse ju jepet mundësia të përdorni vërtetim me dy faktorë (i njohur gjithashtu si 2FA - ang. „two factor

authentication") duhet ta shfrytëzoni të njejtën për ndonjë nga llogaritë tuaja. Kjo e përmirëson më tej sigurinë e organizatës. 2FA kërkon dy metoda të ndryshme për „vërtetimin" e identitetin tuaj përpara se të keni mundësi të përdorni një shërbim të veçantë, zakonisht një fjalëkalim plus një metodë tjetër. Ky mund të jetë një kod, i dërguar në smartfonin juaj (ose kod i cili është prodhuar nga një token për shërbime bankare) që duhet të vendosni përkrah fjalëkalimit tuaj.

KËSHILLA 4: NDIHMONI PUNONJËSIT JUAJ TË PËRBALLËN ME NUMËR TË MADHË FJALËKALIMESH

Punonjësit tashmë kanë më shumë fjalëkalime për t'u mbajtur mend për nevojat zyrtare dhe ato private. Për t'i ardhur ne ndihmë, insistoni në qasje me fjalëkalim vetëm për shërbimet që i duhen me të vërtetë. Praktika e ndryshimit të fjalëkalimeve periodike tashmë është braktisur. Fjalëkalimet duhet të ndryshohen kur dyshoni se detajet e qasjes në të rrezikohen gjatë përdorimit të një shërbimi të veçantë.

Sigurohuni ruajtjen e sigurt të fjalëkalimeve. Punonjësit mund t'i regjistrojnë fjalëkalimet për llogaritë të rëndësishme (si posta elektronike dhe bankare) dhe t'i ruajnë ato në menyrë të sigurt (por jo në pajisjen që e përdorin). Meqë punonjësit mund t'i harrojnë fjalëkalimet e tyre, sigurohuni sedo të kenë munësi t'i rivendosin fjalëkalimet e tyre në një mënyrë të thjeshtë dhe të shpejtë. Nëse keni mundësi brenda organizatës suaj, përdorni të a.q. menaxherë për fjalëkalime (ang. password managers). Këto janë vegla softuerike të cilat mund të krijojnë dhe të ruajnë fjalëkalime për shumë shërbime në një vend, deri te të cilat mund të arrihet përmes një fjalëkalim master/kryesor. Fjalëkalimi kryesor duhet të jetë mjaft kompleks, për shembull duhet të përdorët një frazë metre fjalë të rastit dhetë ketë gjatësia totale prej të paktën 8 karaktere, si edhe të përmban karaktere nga tre grupet e mëposhtme: shkronja të mëdha, shkronja të vogla, numra dhe karaktere të veçanta.

KËSHILLA 5: NDRYSHONI TË GJITHA FJALËKALIME STANDARDE (DEFAULT)

Një gabim i zakonshëm është të mos ndryshohen fjalëkalimet standarde të vendosura nga prodhuesit që vijnë me smartfonët, laptopët, ruterët

të rrjetit dhe lloje të tjera të pajisjeve aktive kompjuterike dhe të rrjetit. Ndryshoni të gjitha fjalëkalime standarde para se punonjësit të fillojnë t'i përdorin ato. Kryeni kontrolle të rregullta periodike të pajisjeve dhe aplikacioneve për të siguroheni se fjalëkalimet standarde janë të ndryshuar.

5. TELEFONA, TABLETA DHE PAJISJE SMART

Realiteti është se telefonat celularë zyrtarë dhe tabletët shpesh herë përdoren për qëllime private, jashtë kohës dhe hapësirës së punës. Gjithashtu, shumë organizata e lejojnë përdorimin e pajisjeve celulare private për qëllime zyrtare. Vijojnë këshilla dhe rekomandime për përdorimin e sigurt të këtyre pajisjeve në organizatën tuaj.

KËSHILLA 1: AKTIVIZONI MBROJTJE PËR QASJE ME FJALËKALIM

Një PIN kod ose fjalëkalim kompleks përballë atyre të thjeshtëve që mund lehtësisht të nxirren nga profilet e rrjetet tuaj social, mund t'i parandalojë kriminelët të hyjnë në pajisjen tuaj celular. Sot, shumica nga këto pajisje përfshijnë njohje e gjurmëve të gishtërinjve për hyrje në pajisjen, pa pasur nevojë për fjalëkalim. Nëse këto karakteristika janë të disponueshme por nuk janë të mundësuara paraprakisht, praktikoni aktivim dhe përdorim për të njejtat.

KËSHILLA 2: SIGUROHUNI QË PAJISJET TË HUMBURA OSE TË VJEDHURA MUND T'I NDJEKNI, MBYLLNI OSE FSHINI

Tabletat ose telefonat e punonjësit ka të ngjarë të vidhen (ose të humbasin) kur janë jashtë zyrës ose shtëpisë. Për fat të mirë, shumica e pajisjeve përfshijnë vegla ueb falas që në rast të humbjes së pajisjes mund t'i përdorni për të ndjekur vendndodhjen e pajisjes së kyçur, mbyllja nga distanca e pajisjes, si edhe fshirja nga distanca e të dhënave.

Këto vegla mund t'i përdorni për pajisjet tuaja personale dhe zyrtare. Menaxhimi i një numër të madh të pajisjeve celulare bëhet përmes të a.q. „mobile device menagment software" për të cilin më shumë informacione mund të gjeni në Internet.

KËSHILLA 3: PËRDITËSIM I RREGULLT DHE NË KOHË I PAJISJEVE

Është shumë e rëndësishme që pajisjet të jenë gjithnjë të përditësuara. Prodhuesve të sistemeve operative si Android ose iOS rregullisht publikojnë përditësime kritike të sigurisë. Pajisjet duhet të vendosen gjithmonë në përditësim automatik. Edukoni punonjësit për rëndësinë e përditësimit në kohë dhe nëse është e nevojshme, u shpjegoni atyre se si ta bëjnë atë. Në momentin kur prodhuesi i pajisjes ndalon mbështetjen dhe lëshimin e përditësimeve të reja kritike për lloj të caktuar të pajisjeve, mendoni t'i zëvendësoni ato me të reja.

KËSHILLA 4: PËRDITËSIM I RREGULLT DHE NË KOHË I APLIKACIONIT

Gjithashtu si sistemet operative të pajisjeve të organizatës suaj, të gjitha aplikacionet që i keni instaluar duhet të përditësohen rregullisht me perditesimeve te kodit (ang. patches) nga ana e prodhuesve të softuerëve. Këto përditësime jo vetëm që do të shtojnë funksione të reja, por gjithashtu do të rregullojnë çdo dobësi sigurie të zbuluar. Sigurohuni që punonjësit të dinë kur janë gati përditësimet, si t'i instalojnëato dhe shpjegoni rëndësinë për zbatimin e përditësimeve të menjëhershme.

KËSHILLA 5: MOS U LIDHNI NË WI-FI HOTSPOTE TË PANJOHURA

Problemi me përdorimin e hotspotetWi-Fi të hapura ose publike siç janë ato në hotelet dhe restorantet është se nuk e dini kush e kontrollon hotspotin. Nëse lidheni me hotspote të tilla, rrezikoni qasje të padëshirueshme në dokumentet tuaja dhe në atë që e punoni, si edhe qasje tek të dhënat tuaja të ndjeshme siç janë emri i përdoruesit

dhe fjalëkalimi, ose shifrat për hyrje në faqet bankare online ose rrjetet sociale. Masat paraprake më të thjeshta janë: mos u lidhni në internet duke përdorur hotspote të panjohura dhe në vend të kësaj përdorni rrjetin tuaj celular 3G ose 4G, që tashmë ka masa sigurie. Përdorni „tethering" (kur pajisjet tuaja të tjera, si laptopët, e shpërndajnë 3G/4G lidhjen tuaj të telefonit celular), ose një pajisje USB wireless për lidhje pa tel (ang. dongle) nga rrjeti juaj celular. Një masë shtesë është përdorimi i rrjeteve virtuale private (ang. VPN) për enkriptimine të dhënave para se të dërgohen përmes Internetit.

6. INCIDENTE KIBERNETIKE (SAJBER, ANG. CYBER)

Një incident kibernetik është qasje e paautorizuar (ose përpjekje për qasje) në sistemet IT të një organizate. Kjo i përfshin sulmet keqbërëse, qëllimi i të cilave është vjedhja e të dhënave, shantazhet ose keqpërdorimi i të dhënave tuaja dhe sistemet IT ose shkaktimi i një dëmi. Shembuj të incidenteve kibernetike janë mohimi i shërbimit (ang. Denial of Service - DoS), një sulm që e bën disponueshmërinë e shërbimeve tuaja të pamundur dhe e ndërpret funksionimi tuaj normal, si edhe sulmet me„ransomver". Dëmtimet fizike, katastrofat natyrore ose vjedhjet gjithashtu mund të jenë shkaqe për incidentet. Trajtimi i incidentit është një proces i cili i mbulon hapat të mëposhtme.

HAPI 1: BËHUNI GATI PËR INCIDENT

Kjo fazë i referohet rezistencës ose qëndrueshmërisë suaj ndaj incidenteve dhe e përfshin identifikimin e të dhënave dhe sistemeve të rëndësishme për organizatën që janë kritike për funksionimin e saj. Duhet ruajtje e rregullt i një kopje sekondare të këtyre të dhënave që do të ruhet në një vend të sigurt, Plan efektiv për menaxhimi i rreziqeve dhe Plan për vazhdimësi e funksionimit të binznesit dhe rimëkëmbja nga fakteqësitë ose katastrofat brenda organizatës Suaj. Më shumë informata mbi vlerësimin e rreziqet mund të gjeni duke kërkuar në Internet dhe në faqen e internetit të qendrës MKD-CIRT. Është e këshillueshme që të keni procedura të dokumentuara për menaxhimin e sistemet IT që janë thelbësore

për shërbimet dhe punën tuaj. Shembuj janë sistemet e e-postës dhe ueb faqja juaj në internet, kontabiliteti dhe puna arkivuese. Menaxhimi efektiv i rreziqeve dhe zbatimi i suksesshëm i planit të rimkëmbjes pas incidenteve nënkupton se do të keni persona të identifikuar që janë përgjegjës për sistemet kritike IT, të cilët do të luajnë role të rëndësishme gjatë realizimit të planeve, qofshin ata të punonjësit tuaj ose pjesë e një organizate të jashtme me të cilën keni marrëveshje.

Krijoni një Plan për incidente. Mendoni se çfarë do të ndodhte nëse papritmas nuk keni qasje në sistemet kritike ose të dhënave të identifikuara më parë. Bëhuni një listë të sistemeve të nënrënditura sipas përparësisë së bazuar në të kuptuarit e asaj që është e rëndësishme, në mënyrë që të mos ketë ndërprerje të punës, sepse çfarë po merrni për mbrojtje është shumë e rëndësishme.

HAPI 2: IDENTIFIKIMI I NJË INCIDENTI KIBERNETIK

Disa nga shenjatse ka ndodhur një incident kibernetik ose incidenti po ndodhet në momentin janë: kompjuterët po punojnë ngadalë, merrni email mesazhe me shantazhe, kur punonjësit nuk mund të hyjnë në llogaritë dhe dokumentet e tyre ose nëse persona të tjerë ju njoftojnë se marrin email-e të çuditshme të dërguara nga adresat tuaja.

Nëse dyshoni se ka ndodhur njëincident kibernetik, hapi tjetër është të zbuloni saktësisht se çfarë ka ndodhur. Në një çështje të tillë, mundt'Ju ndihmojnë përgjigjet e pyetjeve kush dhe kur ka paraqitur një problem, cilat shërbime dhe sisteme janë të përfshira me problemin, cilat të dhëna janë fshirë ose janë të paarritshme (nëse ka të tilla), kur keni mësuar për së pari për problemin, si edhe cilat pjesë të punës të organizatës janë përfshirë.

HAPI 3: NDËRPRERJE DHE ZGJIDHJE TË INCIDENTIT

Gjëja e parë që duhet të bëni është të kontrolloni aktivitetin e mbrojtjes antivirus, i cili mund t'Ju japë informacion mbi llojin e incidentit dhe shtrirjen e dëmit. Nëse nuk mund ta bëni këtë vetë, punësoni një ekspert të

jashtëm për rishikimin e atë që ka ndodhur. Përdorni informata që i keni mbledhur me qëllim që të kërkoni këshilla në Internet nga burime të besueshme. Për tejkalimin e disa probleme të caktuara, mund të gjeni udhëzime në Internet.

Zgjidhja e incidentit nënkupton qasje e sërishme të shërbimeve, sistemeve dhe informacioneve që nuk ishin të disponueshme për shkak të këtij incidenti. Personat që i mirëmbajnë sistemet IT luajnë një rol kryesor në këtë aktivitet. Këta persona duhet t'Ju japin informacion të saktë për llojin e incidentit dhe shtrirjene tij, si dhe të sugjerojnë dhe të zbatojnë veprime të përshtatshme për tejkalimin e incidentit. Në varësi të llojit të incidentit që e keni, kjo mund të përfshijë pastrim i pajisjeve të infektuara, ndryshim i fjalëkalimeve, kopjim i të dhënave, instalim i përditësimeve dhe arnime në sistemet operative dhe aplikacioneve.

HAPI 4: NJOFTIM PËR INCIDENTIN DHE SHPËRNDARJA E INFORMACIONEVE

Kur do të zgjidhet incidenti kibernetik, mund të jetë e detyrueshme të njoftoni ndonjë institucion ose rregullator për incidentin dhe dëmin e pësuar. Mos harroni se sulmet kibernetike, qasja e paautorizuar në sistemet IT dhe vjedhja ose shkatërrimi i të dhënave dhe mjeteve janë vepra penale. Ruani të gjitha informacionet e incidenteve të tilla, si informacionet e hyrjes dhe skedarët të ndryshuara. Tejkaloni paragjykimet se është e turpshme të raportoni një sulm që ju ka ndodhur. Raportimi dhe shkëmbimi i informacionit me kolegët dhe palët e tjera të interesit do të parandalojë të ndodhë i njëjti incident në një organizatë tjetër. Nëse me incidentin, në çfarëdo mënyrejanë kompromet uar të dhëna në lidhje me klientët tuaj, punonjësit ose bashkëpuntorët, duhet t'i njoftoni atosa më shpejt.

Njoftoni incidentin në MKD-CIRT dhe kërkoni të shpërndahet informacioni me organizatat e tjera. MKD-CIRT,sipas kërksën tuaj, do të anonimojë informacionin përpara se të ndajë të njejtën dhe do t'Ju mbrojë si njoftues. Më shumë rreth njoftim të incidenteve në MKD-CIRT do të gjeni në faqen e internetit të qendrës. Sa më shumë njerëz njoftojnë

aq më shumë ka të ngjarë që shkelësit të arrestohen, akuzohen dhe dënohen. Nëse incidenti ka ndikim të ndjeshëm në biznesin tuaj, konsideroni të kërkoni ndihmë juridike.

HAPI 5: MËSONI NGA INCIDENTIT

Pas një incidenti, është e rëndësishme të rishikoni atë që ka ndodhur dhe të mësoni nga gabimet e zbuluara. Atëherë duhet të ndërmerrni masa për tejkalimin e mangësive të identifikuara, duke zvogëluar në këtë menyrë mundësinë e ndodhjes së një dukurie të ngjashme përsëri dhe në të njejtën kohë do të rrisni qëndrueshmërinë e organizatës suaj.

Nëse është e nevojshme, rishikoni planet dhe rivlerësoni rreziqet. Për shembull, nëse jeni viktimë e një sulmi me fjalëkalim, ndoshta do të ketë nevojë të krijoni një politikë të re për fjalëkalime, të siguroni trajnime të reja ose të siguroni ruajtje fizike të sigurt për fjalëkalimeve (ose aplikacioneve për menaxhimin e fjalëkalimit) të punonjësit tuaj.

Nëse personat të jashtëm janë përgjegjës për mirëmbajtjen e sistemeve IT në kuadër të organizatës Suaj, revidoni marrëveshjet e mirëmbajtjes, me qëllim që koha e përgjigjeve dhe rimëkëmbjës të përputhet me kohën maksimale të pranueshme në të cilën shërbimet tuaja mund të jenë të padisponueshme.

Botues:	Agjencia për komunikime elektronike
Përgatitur nga:	Qendra Kombëtare e Reagimit të incidenteve kompjuterike MKD-CIRT
Praktikimi dhe korrigjimi:	Ema Gjorova
Shtyp:	GLOBAL Komunikacii
Sasi:	1.000 kopje

SIGURIA KIBERNETIKE

UDHËZUES PËR NDËRMARRJE TË VOGLA DHE TË MESME

SHKURTIMISHT...

- BENI RREGULLISHT BEKAP (ANG. BACKUP) TË TË DHËNAVE TË RËNDËSISHME
- PËRDORNI MBROJTJE ANTIVIRUSE DHE SOFTUER LEGAL
- PËR TRANSMETIM TË DOKUMENTEVE PËRDORNI POSTË ELEKTRONIKE DHE SHËRBIMET E RE-SË NË VEND TË USB
- PËRDORNI SISTEMET FIREWALL (ANG. FIREWALL) MIDIS RRJETIT LOKAL DHE INTERNETIT
- EDUKONI PUNONJËSIT T'I NJOHIN MASHTRIMET FISHING DHE TË RAPORTOJNË INCIDENTE

Më shumë informata dhe këshilla mbi sigurinë kibernetike mund të gjeni në faqen e internetit të Qendrës Kombëtare për përgjigje në incidente kompjuterike MKD-CIRT http://mkd-cirt.mk

Dërgoni pyetje dhe njoftime të incidenteve në info@mkd-cirt.mk ose 02/3091232