

Küberturvalisuse ABC

Olulised põhitõed küberohutuse tagamiseks

Paroolid puust ja punaseks

Digitaalses maailmas on kõige tavalisemaks kasutaja tuvastamise viisiks salasõnad. Turvaliste ja meeldejäävate salasõnade genereerimine on paras peavalu, eriti kui kasutatavaid keskkondi on kümneid, kui mitte sadu. Seetõttu kiputaksegi minema lihtsama vastupanu teed ning kasutatakse lihtsaid paroole või sama salasõna mitmes erinevas kohas.

Turvaline parool on pikk

Hea parool ei tohi olla lihtne ega kergesti ära arvatav. Turvaline parool peaks olema vähemalt 12 tähemärki või veel pikem. Kindlasti peaks ta sisaldama nii suuri kui väikseid tähti, numbreid ning sümbboleid. Lühike parool on haavatavam nn “toore jõu” (inglise keeles brute force) rünnakuga, kus parooli üritatakse ära arvata lihtsalt erinevaid kombinatsioone järjest läbi proovides.

Näiteks 8-kohalise parooli murdmise võtab aega 40 minutit, 12-kohalise parooli murdmise aga tuhandeid aastaid.

Kasuta paroolihaldurit

Turvalisuse ja mugavuse huvides soovitame kasutada paroolihaldurit nagu 1Password, Bitwarden või Dashlane. Paroolihaldurid on programmid, äpid ja veebilehitseja lisad, mis genereerivad keerulisi salasõnu ning salvestavad need krüpteeritult turvalisse serverisse. Edaspidi pead meeles pidama ainult ühte salasõna, millega paroolihaldurisse siseneda. Pane tähele, et laadid halduri alla ainult ametlikult kodulehelt. Kindlasti soovitame halduril aktiveerida ka mitmeastmelise autentimise.

Ära salvesta paroole veebilehitsejasse, neid ei hoita seal turvaliselt!



Kas minu parooli on häkitud?

haveibeenpwned.com andmebaasist saad kontrollida, kas mõne e-posti aadressiga seotud konto on kuskilt lekkinud. Sealt saad endale ka teavituse tellida, juhuks kui sinu e-post peaks tulevikus mõnda paroolilekkesse sattuma.





**Millest koosneb
ettevõtte
küberturvalisuse
baastase?**

Küberturvalisuse teemad on paljudele võõrad ja tunduvad seetõttu millegi väga kauge ja keerukana. Tegelikuses ei ole see mingi raketiteadus ning küberturvalisuse baastaseme saavutamine on pelgalt otsustamise küsimus. Alusta kohe!

Erinevaid teemasid on üsna palju ja lihtsuse huvides oleme jaganud need üheksasse kategooriasse, mis jagunevad omakorda alateemadeks. Olenemata ettevõtte suurusest või tegevusvaldkonnast on teemad samad, aga vahendid nendega tegelemiseks võivad olla erinevad.

Kasutajate teadlikkus

- ✓ **Koolitused** – üks küberturbe alustaladest. Koolitused on päriselt olulised, et töötajad oskaks ohte märgata ja neist hoiduda. Enamik ründeid saab alguse just massilise õngitsemise käigus saadud klikkidest.
- ✓ **Korrad ja kokkulepped** – igas ettevõttes tasub sõlmida kokkuleppeid, kuidas asju tehakse. Näiteks ülekandeid tehakse ainult partneri lepingus märgitud arvelduskontole ja kontonumbri muutmiseks on vaja sõlmida digitaalselt allkirjastatud lepingu lisa.
- ✓ **Infomaterjalid** – kõik need korrad, kokkulepped ja muud olulised teemad tuleb töötajateni viia. Tihti on otsused tehtud, aga töötajad ei tea asjast midagi.

Töökohaseadmete turvalisus

- ✓ **Seadmete haldus** – oluline on jälgida, et seadmete tarkvara oleks alati uuendatud.
- ✓ **Andmete krüpteerimine** – siis ei juhtu valedesse kättesse sattunud seadme puhul sama andmetega.
- ✓ **Andmete varundamine** – et seadme kadumine või mitte töötamine ei põhjustaks andmete kadu.
- ✓ **Seadmete hankimine ja utiliseerimine** – seade tuleb osta usaldusväärselt partnerilt, et sinna poleks juba eos pahavara sisse pandud. Samuti utiliseeri seade korrektselt, et andmed hiljem uut elu ei leiaks.
- ✓ **Pahavara kaitse** – eksimine on inimlik, aga kui kasutaja kasvõi kogemata vale linki klikib või halvaloomulise faili avab, tõkestab ohu tarkvara.



Juurdepääsud

- ✓ **Mitmetasandiline autentimine** – nii ei piisa sisse logimiseks ainult ühest teadmisest (näiteks parool) vaid on vaja ka täiendavat faktorit, näiteks ligipääsu telefonile või võtmele, sõrmejälge, geograafilist asukohta vmt.
- ✓ **Paroolihaldurid** – kõik on kuulnud, et parool peab olema tugev ja ühte parooli ei tohi korduvkasutada, aga kuidas need kümned erinevad paroolid meelde jätta ning neid ka perioodiliselt vahetada? Siin tuleb appi paroolihaldur.





Serverite turvalisus

Sarnaselt töökohaseadmetele peavad ka serverid olema õigesti hallatud, paigutatud, varundatud, hangitud ja utiliseeritud. Kuid lisaks veel:

- ✓ **Serveri pahavarakaitse** – tasub kasutada spetsiaalselt serverile mõeldud pahavarakaitset, mis on oluliselt efektiivsem ja võimekam.
- ✓ **Serverite majutus** – server peab olema igal ajal kättesaadav neile, kellel on vaja sellele ligi pääseda ning kättesaamatu kõigile teistele. Kui organisatsioonil endal serveriruumi ei ole, võiks servereid majutada mõne teenusepakkuja juures, mitte piltlikult öeldes kellegi laua all.

Rakenduste turvalisus

- ✓ **Rakenduste haldus** – turvalisuse huvides peavad rakendused olema aktiivselt hallatud, s.o administreeritud, ajakohaselt uuendatud jne.
- ✓ **Rakenduste disain** – täpselt nagu hindame rakenduste valikul efektiivsust ja kuluoptimaalsust, tasub tähele panna, et turvameetmed oleks lihtsalt rakendatavad.
- ✓ **Andmete varundus** – hoolitse selle eest, et andmed oleks pidevalt varundatud.

Ülevaade ja kontroll

- ✓ **Kasutajate õigused süsteemides** – igaüks võiks ligi pääseda süsteemidele, kuhu tal on vaja ligi pääseda ja ei tohiks pääseda sinna, kuhu vaja pole. Organisatsioonil peaks olema selge protsess ligipääsude haldamiseks, et ei ununeks näiteks lahkunud töötajatelt ligipääsude eemaldamine.
- ✓ **IT-süsteemide monitooring** – aitab silma peal hoida nii turvalisusel kui ressurssidel. Näiteks võib andmetarbimise järsk kasv viidata küberründele. Samas on hea teada, milline on süsteemi võimekus, selle varu ja millal oleks aeg seda suurendada.
- ✓ **Turvanõrkuste kontroll** – kõike, mis on võrku ühendatud, skaneeritakse väljast pidevalt turvanõrkuste suhtes. Mõistlik on seda ka ise teha ja olla teadlik, mis välja paistab ehk piltlikult öeldes kontrollida, kas lahti on mõni uks või aken, mis peaks kinni olema. Mõned aknad peavadki lahti olema ja see on äriiline risk – lihtsalt need riskid peavad olema teadlikult võetud.



Võrkude turvalisus

- ✓ **Võrguseadmete hankimine ja utiliseerimine** – sarnaselt teistele seadmetele hangi neid ainult usaldusväärse partneri käest.
- ✓ **Võrguseadmete haldus** – ka võrguseadmed vajavad uuendusi, patchimist, konfigureerimist ja varundamist.
- ✓ **Wifi** – eralda organisatsioonisisene turvaline võrk ja loo eraldi wifi-võrgud külalistele.
- ✓ **Tootmisvõrkude turvalisus** – ärikriitiline osa, mis jäetakse tihti tähelepanuta.

Füüsiline turve

Ära lase ise pahalasi tuppa! Jälgi hoolega, et töötõendita võõrad majja ei pääseks. Muidu võib keegi ettevõtte sisevõrku isikliku seadme ühendada või oma USB-pulgaga kontoris olevat seadet pahavaraga „rikastada“. Pane tähele, et nii serverid kui võrguseadmed oleks mitme luku taga ja füüsiliselt pääseks neile ligi vaid autoriseeritud inimesed.





Valmisolek ootamatusteks

Küberturbe intsidendi tekkimise tõenäosust saab vähendada, aga võimalus jääb alati. Intsidendi lahendamine on mõistlik jätta professionaalide hooleks, kellel on vajalikud oskused ja kogemused. Ise guugeldades lahendama hakates võib olukorra hoopis hullemaks muuta. Ennetavalt peaks olema tehtud vähemalt kaks kokkulepet:

- ✓ Ettevõtte töötaja peab teadma, mida teha. Kui arvuti või tööjaam hakkab ühtäkki Bitcoine küsima, siis kelle poole pöörduda? Probleemist pilt teha ja sotsiaalmeediasse postitada ei ole ilmselt kõige parem mõte. Ettevõttes peab olema kokku lepitud vastutav isik ning kõik töötajad peavad seda teadma. See vastutav isik ei pea olema küberturbe ekspert, aga tal peab olema teada, mida selles olukorras teha.
- ✓ Ettevõtte töötaja peab teadma, mida küberintsidendi kahtluse korral teha. Vastutaval isikul peab olema partner, kelle poole pöörduda ja kes aitab olukorda lahendada. Intsidendi ajal on juba hilja hakata partnerit otsima – siis on iga minut loetud. Börsiettevõtte puhul oleks hea, kui lisaks tehnilisele partnerile oleks teada ka PR-partner ning juriidiline partner, sest õige kommunikatsioon on samuti lahenduse võti.





**3 lugu elust
enesest,
kuidas
igapäevastes
olukordades
varitseb
küberrisk**

01 Lood elust enesest

Uus film

Ühel ilusal päeval oli kinodesse jõudmas uus ja põnev film. Veebis pakuti huvilistele võimalust filmi tasuta vaadata, selleks tuli vaid luua konto filmide jagamise keskkonda.

Kasutaja tegi omale konto enda Gmaili aadressi ja selle sama parooliga, mida Gmailis postkastis kasutas. Tulemusena sai ta juurdepääsu leheküljele, kust nägi sedasama treilerit, mida filmitootja kodulehel.

Mis toimus aga sellel ajal, kui kasutaja klipiga tutvus?

Pahalased avastasid, et parooliga pääseb Gmaili kontole ligi.

Nad otsisid postkastist kirju, mis olid seotud uue konto loomise või olemasoleva konto parooli muutmisega (näiteks Facebook, LinkedIn jt). Muu hulgas leiti ka kasutaja töökoha e-posti aadressi parooli andmed, millega said pahalased juurdepääsu tööpostkasti.

Selgus, et kasutaja väljastab tööl regulaarselt arveid. Pahalased asusid kasutaja nimel arveid saatma, täpselt samas summas, mida kasutaja saatis ja täpselt sama teenuse eest. Muudeti vaid pangaarve, kuhu raha peaks laekuma. Tulemusena tasusid paljud ettevõtted arve valele kontole, segadust kui palju ning kaotatud raha samuti.

Mis oleks sellise juhtumi ära hoidnud?

- ✓ Kui kasutaja ei kasutaks sama parooli mitmes kohas.
- ✓ Mitmetasandiline autentimine – kui sisselogimiseks ei piisaks vaid parooli teadmise.

02 Lood elust enesest

Sülearvuti autos

Kasutaja läks trenni ning jättis sülearvuti spordikeskuse juurde autosse. Tagasi tulles ootas ees katkise aknaga auto – sülearvuti oli varastatud. Esimese hooga mõtles kasutaja, et arvuti oligi vana ning nüüd saab ehk kindlustuse abiga uue.

Paari tunni pärast helises aga kasutaja telefon ja talle pakuti tema sülearvutis olevaid andmeid tagasi müüa – hinnaks 10 000 eurot. Kui kasutaja neid ei soovi, lubati need müüa kolmandatele isikutele. Kasutaja võttis ühendust tuttava IT-spetsialistiga ja arutas olukorra läbi. Tulemus:

- | | |
|--|--|
| ✓ sülearvutis olevad andmed ei olnud varundatud ehk kasutaja kaotaks enda andmed; | isikuandmeid; |
| ✓ sülearvutis olevad andmed ei olnud krüpteeritud, ehk on suvalise isiku poolt lihtsasti loetavad; | ✓ sülearvutis oli omajagu isiklikke pilte, mida üldsusega jagada ei tahaks; |
| ✓ sülearvutis olid töötajate töölepingud, mis sisaldasid ka | ✓ sülearvutis olid ettevõtte finantsandmeid kajastavad Excelid, kirjavahetused, ettevõtte turundusplaan ning enamuse klientide andmed (GDPR!). |

Kasutaja otsustas andmed tagasi osta, et ettevõtte saaks tööd jätkata ning vältida andmete soovimatut levikut. Andmeid selle tulemusena teadaolevalt ei levitatud, aga ettevõtte neid tagasi ka ei saanud.

Mis oleks sellise juhtumi ära hoidnud?

- ✓ Kövaketta krüpteerimine;
- ✓ Andmete varundamine.

03 Lood elust enesest

Hommik laeval

Ühel ilusal argipäeva hommikul sõidab praam Hiiumaalt mandrile. Kõikjal sagivad ning vadistavad rõõmsad puhkajad, töölesõitjad ja muud reisijad.

Kuid mida märkaks turvaekspert?

- ✓ Üks seltskond jagab omavahel rõõmsalt värskeid reisipilte – kõik kopeerivad enda pildid mä lupulgale, seejärel kopeeritakse pildid igaühe arvutisse.
- ✓ Kõrvallauas istuv naisterahvas jätab arvuti sisselogituna lauale ja läheb kohvi tooma.
- ✓ Inimesed logivad erinevatesse keskkondadesse, arvuti ekraan ja klaviatuur kõigile näha, ilma mitmeastmelist autentimist kasutamata.
- ✓ Üks seltskond kurdab teisele, et laeva wifi on aeglane ja saab vastu soovitusel kasutada laeva teisi wifi-võrke.

Mis on pildil valesti?

Kui mõni pahalane tahaks inimeste kasutajanimed ja paroole hankida, piisaks lihtsalt mobiiltelefoniga kasutaja filmimisest. Sealt näeks nii seda, kuhu kasutaja andmed sisestas, kui seda, mida ta sisestas. Sama info saaks kätte näiteks laeva turvakaamerate. Ilma mitmeastmelise autentimiseta saab pahalane kasutajakontosid kohe kasutama hakata.

Automaatne turvarisk on ka suvalisse wifi-võrku ühendumine, sest kasutajat võidakse rünnata selle võrgu kaudu. Enamasti on väga keeruline veenduda, et pakutav wifi-võrk on turvaline. Pahatihti on võimatu tuvastada isegi seda, kes võrku pakub.

Ka mälupulga kasutamine, eriti selle erinevate arvutite vahel jagamine, on turvarisk. Mälupulk võib sisaldada viiruseid ja pahavara isegi siis, kui kasutaja näeb, et mälupulk on tühi. Kirjeldatud viisil mälupulga kasutamist võib võrrelda sellega, kui poe eest võetakse kasutatud mask eest ja jagatakse seda sõpradega, kes selle kõik järgemööda ette panevad.



Lukustamata arvuti juurest ei tohiks kunagi lahkuda. Arvuti võidakse varastada ja andmed sealt ära kopeerida, samuti võidakse arvutisse pahavara kopeerida või võib keegi lihtsalt nalja teha ja kõik sinu Facebooki sõbrad sulle homseks külla kutsuda.

Kuidas avalikus kohas targalt käituda?

- ✓ Kasuta arvutit nii, et sinu tegevus oleks võõraste pilkude ja kaamerasilma eest kaitstud.
- ✓ Ära kasuta wifi-võrke, kui sa ei ole nende turvalisuses kindel, eelista mobiilset andmesidet (4G või 5G).
- ✓ Ära kasuta mälupulka!
- ✓ Kui arvuti juurest lahkud, siis lukusta alati arvuti (Mac: Control + command + Q; Windows: Windows + L).





7 küberhügieeni põhitõde

1. Kasuta kõigi olulisemate teenuste puhul (e-post, sotsiaalmeedia jms) mitmetasemelist autentimist

Ka kõige keerulisem parool võib süsteemist välja lekkida.

Kui kasutad sama parooli ka mujal, võib pahalane selle abil ka muudesse veebikeskkondadesse sisse logida. Siin tuleb appi mitmetasandiline autentimine. Mitmetasandiline autentimine on protsess, mis käivitub pärast salasõna sisestamist ja tuvastab näiteks SMSi, e-posti või nutitelefoni rakendusega, et veebilehele logib sisse ikka õige inimene. Näiteks saadetakse registreerimisel märgitud telefoninumbrile või e-posti aadressile salajane kood, mis tuleb sisselogimisel sisestada.

2. Krüpteeri oma kõvaketas

Kõvaketta krüpteerimine tagab andmete kaitse ka siis, kui arvuti kaob või varastatakse, mida tavaline parooliga sisselogimine ei tee. Windowsi (BitLocker) ning MacOSi (FileVault) operatsioonisüsteeme kasutaval arvutil saab terve arvuti kõvaketta krüpteerida ning ning kasutaja jaoks muutub vaid see, et arvuti küsib käivitamisel täiendavalt parooli.

3. Hoia seadmed ja tarkvara uuendatuna või lase seda teha automaatselt

Enamus seadmeid ning tarkvara püüab end regulaarselt uuendada ning ehkki selline pidev uuendamine võib tunduda tüütu, on oluline uuendused siiski esimesel võimalusel paigaldada. Uuendused sisaldavad enamasti ka turvauuendusi, sest tarkvarades leitakse ohtlikke vigu, mille kaudu võivad pahalased sind ja sinu andmeid ohustada. Riskide vähendamiseks on kõige lihtsam kõik pakutavad uuendused kohe paigaldada.

Seega järgmine kord, kui arvuti käivitamisel jälle uuendusi laadima hakkab, võta seda kui hetke iseendale – nii aja mahavõtmise kui turvalisuse mõttes.

4. Ära hoia mune ühes korvis – tee varukoopiaid ja kasuta pilveteenuseid

Arvesta alati võimalusega, et sinu arvuti või telefoniga võib midagi juhtuda – seade võib kaduma minna, vette kukkuda või lihtsalt töötamise lõpetada. Kui antud seade on ainuke koht, kus asuvad sinu olulised dokumendid või fotod, võivad need kaduda koos seadmega. Pilveteenuste kasutamine lisab andmete säilitamisel nii mugavust kui ka turvalisust.

5. Avalikus kohas või liikvel olles ole eriti hoolas

- ✓ Enamik avalikke wifi-võrke on krüpteerimata. See tähendab, et ükskõik milline teine samasse võrku ühendatud seade saab pealt kuulata kogu sinu internetiliiklust ja tegevust. Kui kasutad wifi-võrku kohvikus, kaubanduskeskuses või restoranis, võib suvaline võõras täpselt jälgida, mida sa teed – tal on võimalus internetiliiklust näha, muuta või üldse sinuna esineda. Hea soovitus on avalikke wifi-võrke mitte kasutada ja selle asemel kasutada telefoni hotspot'i.
- ✓ Kui avalikus kohas arvutisse või veebiteenusesse kasutajanime ja parooli trükid, jälgi ümbrust. Veendu, et sinu selja taga ei oleks uudistavaid silmi või filmivat kaamerat, mille salvestuselt on hõlbus ka keerukamaid paroole tuvastada. Pane tähele ka turvakaameraid! Võimalusel vali töötamiseks istekoht seljaga vastu seina.
- ✓ Kui lahkud oma seadme juurest, siis veendu alati, et lukustad ekraani – lukustamata on sinu andmed ja seadmed täiesti kaitseta.

6. Kasuta ainult usaldusväärsetest allikatest pärit tarkvara (Google Play, AppStore, ametlikud tarkvaratootjad) ning väldi failivahetuskeskkondadest tarkvara allalaadimist

Lihtne viis enda nutitelefoni või arvuti pahavaraga nakatamiseks on tarkvara allalaadimine tundmatutest allikatest – näiteks otsides veebist või failivahetusplatvormidelt tasuliste tarkvarade tasuta versioone.

Sageli on sellistesse tarkvaradesse või tarkvara „tasuta aktiveerimise“ vahenditesse lisatud ka pahavara, mis annab pahalastele ligipääsu sinu seadmele või lekitab sinu andmeid.

Kindlaim viis sellise olukorra vältimiseks on hankida tarkvara ainult ametlike allikate kaudu või kasutades sisseehitatud rakenduste poode, milles pakutav tarkvara on juba kontrollitud.

7. Pea meeles, et arvuti ja telefon võiks olla sama personaalne kui hambahari – ja tööarvuti võiks olla vaid töötegemiseks

Kaugtöö puhul on esile kerkinud uus turvarisk – tööandja ei saa alati kontrollida, milliseid seadmeid töö tegemiseks kasutatakse. Ettevõtte võib anda küll turvalise arvuti, aga vahel on kodus e-posti vaatamiseks mugavam kasutada abikaasa sülearvutit või ühist tahvelarvutit. Nii on ka teistel pereliikmetel juurdepääs töökirjadele või failidele.

Veelgi keerukam on olukord siis, kui tööarvutist jäetakse välja logimata ning pereliikmed kasutavad ettevõtte arvutit enda asjade tegemiseks. Sellega võivad aga realiseeruda kõikvõimalikud eelkirjeldatud riskid pahavaraga nakatumiseks või andmete lekkimiseks. Soovitame hoolega läbi mõelda, milliseid seadmeid kasutatakse kodus töö tegemiseks ja kindlasti luua neisse eraldi kasutajakontod, et välistada kõrvaliste inimeste ligipääs olulistele andmetele.





Kati

Mati

Külaised





**Mida küberkaitse
teenuste ja
toodete valikul
silmas pidada?**



1. Tootja

Küberkaitses mängib olulist rolli kasutajate kaitsmine otse seal, kus nad toimetavad, s.o seadmetes ja rakendustes (mitte nt ainult ettevõtte võrgus). Valida tasub tootja, kelle põhifookus on küberkaitse – kellel on selles pikaajaline kogemus ning globaalne ülevaade rünnakutest, ohtudest ja uuest pahavarast.

Telia on valinud endale partneriks Trend Micro. Trend Micro on küberturbe globaalne liider, tegutseb valdkonnas juba 35 aastat ning keskendub ainult küberturbe toodete ja teenuste pakkumisele.

2. Kaitse tööjaamas

Tänapäeval tehakse tööd kodust, kohvikust, lennujaamast jm, mistõttu peab tööjaamas toimuv olema hästi kaitstud ning toimuvast peab olema hea ülevaade.

Tööjaama kaitse miinimumtase võiks olla järgmine:

- ✓ Andmebaas konkreetsetest teadaolevatest küberohtudest (nt pahavaraga veebilehed, failid jmt);
- ✓ Masinõpe uue ja tundmatu pahavara tuvastamiseks;
- ✓ Käitumismustri analüüs, et tõkestada kahtlased tegevused tööjaamas;
- ✓ Veebikaitse pahavara linkide avamise tõkestamiseks otse tööjaamas;
- ✓ Väliste seadmete kontroll tundmatute andmekandjate kasutamise tõkestamiseks;
- ✓ XDR (laiendatud ohutuvastus ja -kõrvaldus) tööjaamas toimuva pidevaks jälgimiseks, automaatseks intsidendi tuvastamiseks ja sellele reageerimiseks.

3. Kaitse rakendustes (e-post, failijagamisteenused, suhtlusrakendused)

Kuna töötajad kasutavad töötegemiseks ka isiklikke seadmeid, peab kaitse olema ka rakendustel, mitte üksnes tööandja seadmetel. Näiteks saab enamus kasutajatele suunatud rünnetest alguse e-postist. Seega väga oluline on puhastada e-post:

- ✓ rämpspostist
- ✓ pahavarast
- ✓ õngitsuskirjadest
- ✓ petuskeemidest

Üha rohkem kasutatakse erinevaid failijagamisteenused nagu OneDrive, Sharepoint Dropbox, Box, Google Drive jt. Ka need rakendused tuleb võtta kontrolli alla ning puhastada tuntud ja tundmatust pahavarast, et see ei saaks ettevõtte sees levima minna.



XDR-tehnoloogia jälgib pidevalt tööjaamu ja rakendusi ning tuvastab ja tõkestab automaatselt intsidente. Samuti annab see konsolideeritud ülevaate erinevatest kihtidest (e-post, rakendused, tööjaamad) ja annab edasisi soovitusi ohu kõrvaldamiseks.

4. Teenus

Kõik eelnev võib kõlada nii, nagu peaks iga ettevõtte poole kohaga IT-valdkonnale pühenduma või tööle palkama terve meeskonna küberturbspetsialiste. Õnneks ei ole see siiski nii. Appi tõttab Telia oma küberturbeteenustega. Keskendu oma põhitegevusele ja jätta küberturve spetsialistide hooleks.

Telia käest saad turvalise ja testitud Trend Micro lahenduse koos vajalike toetavate lahendustega, et pakkuda sinu ettevõttele maksimaalset kaitset. Soovi korral saad Telia küberturbe spetsialistide abiga lahendusele teha täiendavaid seadistusi.

Kui mõni küberohu intsident peaks siiski aset leidma, on Telia kogenud spetsialistid kohe käepärast olukorra lahendamisel ning aitavad toimunut ka analüüsida, et tulevikus taolisi ohte veel paremini vältida.





**Mida teha, kui
küberturbe
intsident siiski
juhtub?**



Küberturbe intsidendi juhtumist ei saa kunagi lõpuni välistada ning see võib juhtuda iga ettevõttega. Saab vaid vähendada tõenäosust ja valmistada end võimalikult hästi ette. Valmisolek annab vajalikud tööriistad probleemiga tegelemiseks ning aitab vähendada intsidendi mõju ja kaasnevat kahju.

Mida teha selleks, et valmis olla:

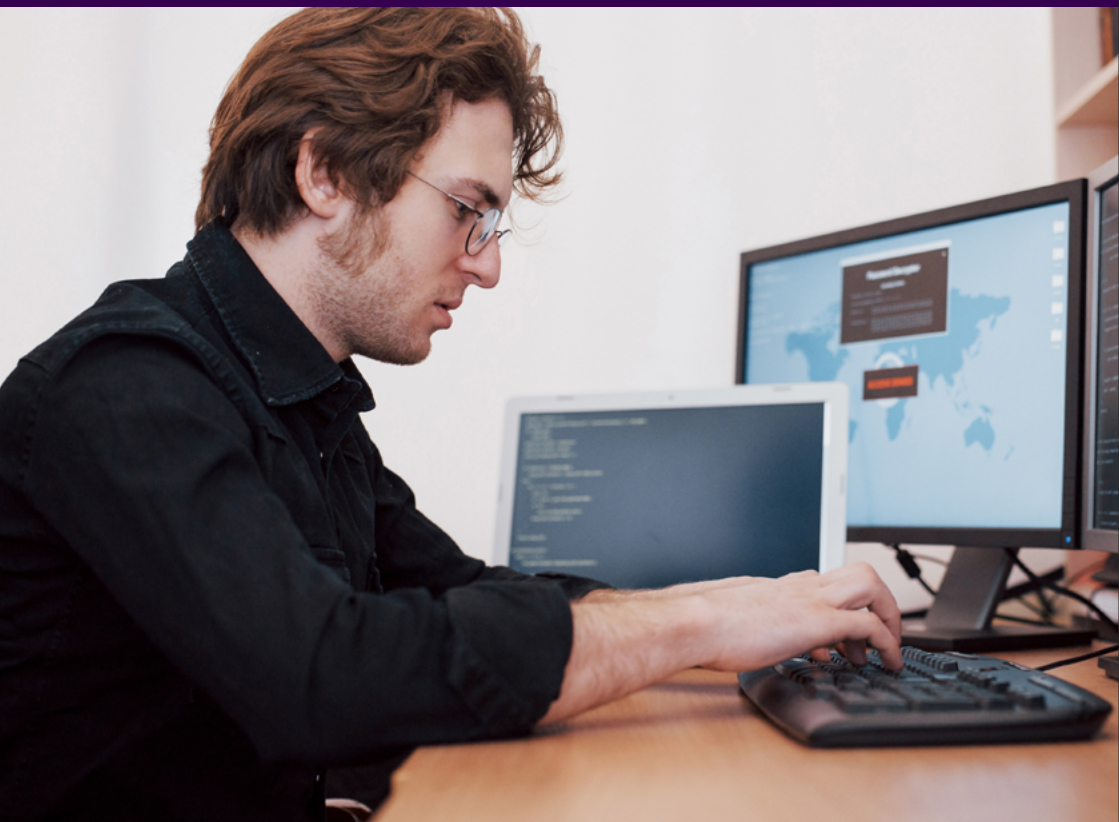
- ✓ Koolita oma inimesi - koolitusel omandavad inimesed elementaarsed kübermaailma oskused selleks, et mitte panna ennast ja teisi ohtu ning oskuse käituda juhul kui küberturbe intsident on juhtunud.
- ✓ Kasuta keerulisi paroole, ära kasuta ühte parooli mitmes kohas ja muuda seda regulaarselt. Parim lahendus on paroolihalduri kasutamine.
- ✓ Kasuta võimalusel mitmetasemelist kasutaja tuvastamist ehk autentimist.
- ✓ Lepi ettevõttes kokku selged infoturbega seotud käitumisreeglid nii igapäevaseks tegevuseks kui selleks puhuks, kui juhtub küberturbe intsident.
- ✓ Halda enda seadmeid ja uuenda regulaarselt seadmetes olevat tarkvara.
- ✓ Varunda enda seadmetes olevat tarkvara.
- ✓ Krüpteeri enda arvuti kõvaketas.



- ✓ Kasuta arvuti ja serveri küberkaitse tooteid.
- ✓ Säilita seadmete logi. Seda on väga vaja juhul, kui küberturbe intsident on juba juhtunud.
- ✓ Vaata üle seadmete turvanõrkused. Selles on suureks abiks turvanõrkuste skaneerimise lahendused.
- ✓ Jälgi toimuvat. Kasuta erinevaid tööriistu, mis annavad ülevaate nii võrgus, serveris kui töökohaseadmes toimuvast.
- ✓ Vaata üle kasutajate õigused infosüsteemides. Ülearused õigused suurendavad küberturbe intsidendi tekkimise riski.
- ✓ Leia partner juhuks, kui juhtub halvim. Küberturbe intsidendi lahendamine vajab tihti väga spetsiifilist kompetentsi – kompetentsi, mida ettevõtte igapäevaselt ei vaja.

Kõiki neid tegevusi saab teha Telia abiga, loe lähemalt <https://www.telia.ee/ari/it-teenused/turvalisus/kuberturvalisus>







**Kuidas käituda,
kui intsident on
juba juhtunud?**



Intsidendi lahendamine on mõistlik jätta professionaalide hooleks, kellel on vajalikud kompetentsid ja kogemused.

Oskamatu tegutsemine võib olukorda hoopis hullemaks ajada, samuti võib hävineda info, mis aitaks intsidenti lahendada. Kõik see tähendab ettevõttele veelgi suuremat kahju (aeg, raha, mainekahju).

Abi saamise kokkulepped peaks olema sõlmitud juba enne intsidenti toimumist. Nii saad abi vajadusel võimalikult kiiresti ega raiska väärtuslikku aega selle otsimisele. Telia kogenud ja oskuslikud spetsialistid on sinust alati vaid ühe telefonikõne kaugusel.

Telia küberintsidendi abi teenus sisaldab:

- ✓ Telia küberturbemeeskonna abi intsidendi lahendamisel;
- ✓ Reageerimist kokkulepitud aja jooksul;
- ✓ Intsidendi lahendamise koordineerimist;
- ✓ Vajadusel suhtlust kolmandate osapooltega (näiteks CERT-EE)
- ✓ Kokkuvõtet intsidendist;
- ✓ Soovitusi edaspidiseks.

Teenus annab sulle meelerahu:

- ✓ Saad olla kindel, et intsidendi lahendamiseks ja koordineerimiseks vajalik kompetents on alati olemas. Abi on vaid telefonikõne kaugusel.
- ✓ Tead täpselt, kes ja millal appi tuleb ning ei pea hakkama abi otsima siis, kui tekib hädavajadus.
- ✓ Reageerimise tingimused lepime eelnevalt kokku.
- ✓ Oskame vältida vigu, mis võivad intsidendi tagajärjed veel halvemaks muuta.

Soovid rohkem teada: <https://www.telia.ee/ari/it-teenused/turvalisus/kuberintsidendi-abi/>



