EUROOPA LIIDU KÜBERTURVALISUSE AMET

Küberturvalisuse juhend VKEdele

12 SAMMU

TEIE ETTEVÕTTE KAITSMISEKS

COVID-19 kriis näitas, kui tähtsad on VKEdele internet ja arvutid üldiselt. Et olla pandeemia ajal edukas, pidid paljud VKEd võtma ettevõtte toimepidevuse meetmeid, näiteks võeti kasutusele pilveteenused, täiustati oma veebiteenuseid, uuendati veebisaite ja võimaldati personalil teha kaugtööd.

Sellel teabelehel soovitatakse VKEdele kõrgemal tasandil rakendatavat 12 praktilist sammu, mille abil paremini kaitsta oma süsteeme ja ettevõtet. Teabeleht kuulub üksikasjalikuma ENISA aruande **„Cybersecurity for SMES – Challenges and Recommendations“** (VKEde küberturvalisus – väljakutsed ja soovitused) juurde.

1 LOOGE HEA KÜBERTURVALISU SE KULTUUR

NIMETAGE VASTUTAV ISIK

Heal tasemel küberturvalisus on tähtis iga VKE jätkuva edu tagamisel. Organisatsioonis tuleks selle ülitähtsa ülesande täitmiseks nimetada vastutav isik, kes peaks tagama, et küberturvalisuse valdkonnas on olemas asjakohased ressursid, nagu töötajate aeg, soetatud küberturvalisuse tark- ja riistvara ja teenused, personalikoolitused ning väljatöötatud toimivad põhimõtted.

VÕITKE TÖÖTAJATE TOETUS

Töötajate toetuse saamiseks peaks juhtkond jagama tulemuslikult küberturvalisust käsitlevat teavet, toetama avalikult küberturvalisuse algatusi, korraldama töötajatele asjakohaseid koolitusi ning esitama töötajatele küberturvalisuse põhimõtetes nimetatud selged ja konkreetsed eeskirjad.

AVALDAGE KÜBERTURVALISUSE PÕHIMÕTTED

Küberturvalisuse põhimõtetes tuleks esitada töötajale selged ja konkreetsed eeskirjad selle kohta, millist käitumist nendelt oodatakse, kui nad kasutavad ettevõtte IKT-keskkonda, -seadmeid ja -teenuseid. Põhimõtetes tuleks ka rõhutada võimalikke tagajärgi töötajatele, kui nad põhimõtteid eiravad. Põhimõtted tuleb korrapäraselt läbi vaadata ja neid uuendada.

KORRALDAGE KÜBERTURVALISUSE AUDITEID

Asjakohaste teadmiste, oskuste ja kogemusega isikud peaksid läbi viima korrapäraseid auditeid. Nii väljastpoolt kaasatud lepingulised audiitorid kui ka VKE siseaudiitorid peaksid olema sõltumatud, sealhulgas igapäevastest IT-toimingutest.

PÖÖRAKE TÄHELEPANU ANDMEKAITSELE

ELi isikuandmete kaitse üldmääruse[1] alusel peab ELi/EMP elanike isikuandmeid töötlev või säilitav VKE tagama, et nende andmete kaitsmiseks on võetud nõuetekohased turvakontrollimeetmed. Seejuures tuleb tagada, et nõuetekohased turvameetmed on võtnud ka VKE nimel töötav kolmas isik.

[1] Isikuandmete kaitse üldmäärus
https://ec.europa.eu/info/law/law-topic/data-protection_et

2

KORRALDAGE ASJAKOHASEI D KOOLITUSI

Korraldage kõigile töötajatele regulaarseid küberturvalisust puudutavaid koolitusi, et nad tunneksid erinevaid küberohte ja oskaksid nendega toime tulla. Need koolitused peaksid olema VKEdele kohandatud ja keskenduma elulistele olukordadele.

Korraldage teie ettevõttes küberturvalisuse eest vastutavatele isikutele küberturvalisuse erikoolitusi, et neil oleksid oma töö tegemiseks vajalikud oskused ja pädevused.

3

TAGAGE TOIMIV KOLMANDATE ISIKUTE HALDAMINE

Tagage, et kõiki teenuseosutajaid, eriti neid, kellel on juurdepääs tundlikele andmetele ja/või süsteemidele, hallatakse aktiivselt ning nad vastavad kokkulepitud turvatasemele. Sõlmida tuleks lepingujärgsed kokkulepped, et reguleerida turvanõuete täitmist teenuseosutajate poolt.

4

TÖÖTAGE VÄLJA INTSIDENTIDELE REAGEERIMISE KAVA

Töötage välja ametlik intsidentidele reageerimise kava, milles on dokumenteeritud selged juhised, rollid ja kohustused, mis tagavad, et kõigile intsidentidele reageeritakse õigel ajal, professionaalselt ja nõuetekohaselt. Küberohtudele kiiresti reageerimiseks valige vahendid, mis jälgivad ja loovad kahtlasest tegevusest ja turvarikkumistest teavitavaid hoiatusi.

5 TAGAGE JUURDEPÄÄS SÜSTEEMIDELE

Soovitage kõigil kasutada paroolina fraasi, mis koosneb vähemalt kolmest juhuslikult valitud levinud sõnast, mis jäävad väga hästi meelde ja tagavad ühtlasi turvalisuse. Kui valite tavalise salasõna:

- veenduge, et see oleks pikk, sisaldaks suur- ja väiketähti, võimaluse korral ka numbreid ja sümboleid.
- Vältige kergesti äraarvatavaid paroole, nagu „salasõna“, ning tähe - või numbrikombinatsioone, nagu „abc“ ja „123“.
- Ärge kasutage internetis kättesaadavat isiklikku teavet.

Nii salafraaside kui ka salasõnade kasutamisel veenduge järgmises:

- ärge kasutage neid mujal;
- ärge jagage neid kolleegidega;
- kasutage mitmeastmelist autentimist;
- kasutage paroolihaldurit.

6

TURVALISED SEADMED

Küberturvalisuse programmis on tähtis etapp töötajate kasutatavate seadmete, nagu laua-, süle- ja tahvelarvutite või nutitelefonide turvalisuse tagamine.

PAIGAKE JA UUENDAGE TARKVARA KORRAPÄRASELT

Paikamiseks on kõige parem kasutada keskset platvormi. On väga soovitatav, et VKEd:

- uuendaksid korrapäraselt kogu oma tarkvara;
- lülitaksid võimaluse korral alati sisse automaatsed uuendused;
- teeksid kindlaks, milline tark- ja riistvara vajab manuaalset uuendamist;
- pööraksid tähelepanu mobiilseadmete ja esemevõrguseadmete turvalisusele.

VIIRUSETÕRJE

Igat liiki seadmetes tuleks kasutusele võtta keskselt hallatav viirusetõrjelahendus ja seda korrapäraselt uuendada, et tagada selle jätkuv tõhusus. Lisaks hoiduge piraattarkvara paigaldamisest, sest see võib sisaldada pahavara.

VÕTKE KASUTUSELE E-POSTI JA VEEBI KAITSEVAHENDID

Võtke kasutusele lahendused, mille abil blokeerida rämpsposti, pahatahtlike veebisaitide linke ja pahatahtlikke manuseid, näiteks viiruseid sisaldavaid e-kirju ning andmepüügi e-kirju.

KRÜPTIMINE

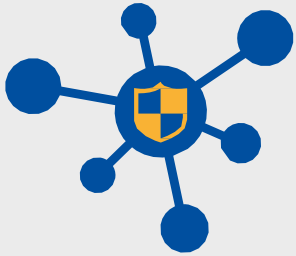
Kaitske andmeid nende krüptimisega. VKEd peaksid tagama, et mobiilsetes seadmetes, nagu süle- ja tahvelarvutites ning nutitelefonides säilitatavad andmed on krüptitud. Avalike võrkude, näiteks hotellide või lennujaamade WiFi-võrkude kaudu edastatavate andmete puhul tagage, et andmed on krüptitud, kasutades kas virtuaalset privaatvõrku (VPN) või külastades veebisaite üle turvalise ühenduse SSL/TLS-protokolliga. Tagage, et teie veebisaitidel kasutatakse asjakohast krüptimistehnoloogiat, et kaitsta interneti teel edastatavaid kliendiandmeid.

RAKENDAGE MOBIILSEADMETE HALDUST

Võimaldades personalil teha kaugtööd, lubavad paljud VKEd töötajatel kasutada isiklikke süle- ja/või tahvelarvuteid ja/või nutitelefone. See tekitab palju turvariske seoses nendes seadmetes säilitatavate tundlike ettevõtlusandmetega. Üks viis selle riski ohjamiseks on mobiilseadmete haldus (Mobile Device Management, MDM), mis võimaldab VKEdel:

- kontrollida, mis seadmetel lubatakse juurde pääseda ettevõtte süsteemidele ja teenustele;
- tagada, et seadmesse on paigaldatud uuendatud viirusetõrje tarkvara;
- teha kindlaks, kas seade on krüptitud;
- kinnitada, kas seadmesse on paigaldatud uuendatud tarkvarapaigad;
- nõuda, et seade oleks kaitstud PIN -koodi ja/või parooliga;
- kaugkustutada VKE andmed seadmest, kui seadme omanik teatab selle kadumisest või vargusest või kui seadme omanik lõpetab töösuhte VKEga.

7 KAITSKE OMA VÕRKU



KASUTAGE TULEMÜÜRE

Tulemüürid haldavad võrku sisenevat ja sellest väljuvat liiklust ning on hädavajalikud VKEde süsteemide kaitsmiseks. Tulemüüre tuleks kasutada kõigi hädavajalike süsteemide kaitsmiseks, eelkõige VKE võrgu kaitsmiseks interneti eest.

VAADAKE ÜLE KAUGHALDUSE LAHENDUSED

VKEd peaksid korrapäraselt üle vaatama kaughalduse vahendid, et tagada nende turvalisus. Eelkõige tuleks:

- tagada, et kogu kaughalduse tarkvara on paigatud ja uuendatud;
- piirata kaughaldust, mis pärineb kahtlustäratavatest geograafilistest asukohtadest või teatud IP-aadressidelt;
- lubada töötajatele kaugpääsu ainult süsteemidesse ja arvutitesse, mida nad vajavad oma töö tegemiseks;
- nõuda kaughalduse jaoks tugevaid paroole ja võimaluse korral kasutada mitmeastmelist autentimist;
- tagada, et seire ja hoiatused on sisse lülitatud, et hoiatada arvatava rünnaku või ebatavalise kahtlustäratava tegevuse eest.

8 SUURENDAGE FÜÜSILIST JULGEOLEKUT

Tähtsa teabe säilitamise korral tuleks alati tagada nõuetekohane füüsiline kontroll. Näiteks ettevõtte sülearvutit või nutitelefoni ei tohiks jätta järelevalveta auto tagaistmele. Iga kord arvutist eemaldudes peaks kasutaja selle lukustama. Lülitage igas ettevõtte eesmärkidel kasutatavas seadmes sisse automaatlukustuse funktsioon. Lisaks ei tohiks jätta järelevalveta tundliku sisuga prinditud dokumente; kui dokumente parasjagu ei kasutata, tuleb need turvaliselt ära panna.

9 LOOGE VARUKOOPIAD

Et tähtsat teavet oleks võimalik taastada, tuleks luua varukoopiad. Varundamine on tõhus viis õnnetustest, näiteks lunavara rünnakust taastumiseks. Rakendada tuleks järgmisi varundamisnõudeid:

- varundamine on korrapärane ja võimaluse korral automatiseeritud;
- varukoopiaid säilitatakse eraldi VKE tootmiskeskkonnast;
- varukoopiad krüptitakse, eriti juhul, kui neid kavatsetakse viia ühest kohast teise;
- testitakse suutlikkust taastada korrapäraselt andmeid varukoopiatest. Kõige parem oleks teha korrapäraselt algusest lõpuni täieliku taastamise teste.

10

KASUTAGE PILVE

Kuigi pilvepõhistel lahendustel on palju eeliseid, kaasnevad nendega ka mõned eriomased riskid, mida VKEd peaksid enne pilveteenuse ostmist arvesse võtma. ENISA on avaldanud juhendi „Cloud Security Guide for SMEs“[2] (Pilvandmetöötluse turvalisuse juhend VKEdele), millega VKEd peaksid pilve kolimisel tutvuma.

Pilveteenuse osutajat valides peaksid VKEd veenduma, et ta ei riku ühtki õigusnormi andmete ja eriti isikuandmete säilitamisega väljaspool ELi/EMP-d. Näiteks nõutakse ELi isikuandmete kaitse üldmääruses, et ELi/EMP elanike isikuandmeid tohib säilitada väljaspool ELi/EMP-d või edastada väljapoole ELi/EMP-d ainult rangetel eritingimustel.

[2] https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 TURVALISED VEEBISAIDID

On oluline, et VKEd tagaksid oma veebisaitide turvalise seadistuse ja halduse ning et isiku- või finantsandmeid, näiteks krediitkaardi andmeid, kaitstaks nõuetekohaselt. See hõlmab veebisaitide korrapäraseid turvateste võimalike turvanõrkuste tuvastamiseks ja saitide korrapärast läbivaatamist, et tagada nende nõuetekohane haldus ja uuendamine.

12 OTSIGE JA JAGAGE TEAVET

Küberkuritegevuse vastases võitluses on tõhus vahend teabe jagamine. Küberkuritegevusega seotud teabe jagamine aitab VKEdel oma riske märksa paremini mõista. Ettevõtjad, kes kuulevad küberturvalisusega seotud probleemidest ja nende ületamisest teistelt ettevõtjatelt, võtavad suurema tõenäosusega meetmeid oma süsteemide kaitsmiseks kui ettevõtjad, kes vaid loevad sarnastest aspektidest oma tegevusvaldkonna aruannetest või küberturvalisuse uuringutest.

EUROOPA LIIDU KÜBERTURVALISUSE AMET

ENISA
Euroopa Liidu Küberturvalisuse Amet (ENISA) on Euroopa Liidu asutus, mille eesmärk on saavutada küberturvalisuse ühtlane kõrge tase kogu Euroopas. 2004. aastal asutatud ning ELi küberturvalisuse määrusega tugevdatud Euroopa Liidu Küberturvalisuse Amet osaleb ELi küberpoliitikas, suurendab IKT-toodete, -teenuste ja -protsesside usaldusväärsust küberturvalisuse sertifitseerimiskavade abil, teeb koostööd liikmesriikide ja ELi organitega ning aitab Euroopal valmistuda tuleviku küberprobleemideks. Jagades teadmisi, suurendades võimekust ja teadlikkust teeb amet koostööd peamiste sidusrühmadega, et tugevdada usaldust sidusmajanduse vastu, edendada Euroopa Liidu taristu säilenõtkust ning tagada kokkuvõttes Euroopa ühiskonna ja kodanike digitaalne turvalisus. Lisateave: www.enisa.europa.eu.

ENISA
Euroopa Liidu Küberturvalisuse Amet

Ateena büroo
Ethnikis Antistaseos 72 ja
Agamemnonos 14,
Chalandri 15231, Atika, Kreeka

Heraklioni büroo
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Kreeka

enisa.europa.eu