enisa

EUROPOS SĄJUNGOS
KIBERNETINIO SAUGUMO
AGENTŪRA

Kibernetinio saugumo vadovas MVĮ

12 ŽINGSNIŲ,

KAIP APSAUGOTI SAVO VERSLĄ

COVID-19 krizė parodė, koks apskritai svarbus MVĮ yra internetas ir kompiuteriai. Siekdamos sėkmingai vystyti verslą pandemijos metu, daugelis MVĮ turėjo imtis veiklos tęstinumo priemonių, pavyzdžiui, taikyti debesijos paslaugas, tobulinti interneto paslaugas, atnaujinti savo interneto svetaines ir sudaryti sąlygas darbuotojams dirbti nuotoliniu būdu.

Šiame lankstinuke MVĮ pateikiama 12 aukšto lygio praktinių žingsnių, kaip geriau apsaugoti savo sistemas ir verslą. Šis leidinys papildo išsamesnę ENISA ataskaitą **„Kibernetinis saugumas MVĮ. Iššūkiai ir rekomendacijos“** (angl. *„Cybersecurity for SMES – Challenges and Recommendations“*).

1 KURKITE TINKAMĄ KIBERNETINIO SAUGUMO KULTŪRĄ

PRISKIRKITE VALDYMO ATSAKOMYBĘ

Tinkamas kibernetinis saugumas yra pagrindinis bet kurios MVĮ sėkmės veiksnys. Atsakomybė už šią itin svarbią funkciją turėtų būti paskirta organizacijos darbuotojui, kuris turėtų užtikrinti, kad kibernetiniam saugumui užtikrinti būtų skiriami tinkami ištekliai, pavyzdžiui, darbuotojų laikas, perkama kibernetinio saugumo programinė įranga, paslaugos ir aparatinė įranga, vykdomi darbuotojų mokymai ir kuriama veiksminga politika.

PELNYKITE DARBUOTOJŲ PRITARIMĄ

Pelnykite darbuotojų pritarimą vadovybei veiksmingai informuojant apie kibernetinį saugumą, atvirai remiant kibernetinio saugumo iniciatyvas, rengiant tinkamus mokymus darbuotojams ir teikiant jiems aiškias ir konkrečias kibernetinio saugumo politikos taisykles.

PASKELBKITE KIBERNETINIO SAUGUMO POLITIKĄ

Kibernetinio saugumo politikoje darbuotojams turėtų būti nustatytos aiškios ir konkrečios taisyklės, kaip jie turėtų elgtis naudodamiesi įmonės IRT aplinka, įranga ir paslaugomis. Šioje politikoje taip pat turėtų būti nurodytos pasekmės, su kuriomis darbuotojas gali susidurti, jei nesilaikys šių taisyklių. Politika turi būti reguliariai peržiūrima ir atnaujinama.

ATLIKITE KIBERNETINIO SAUGUMO AUDITUS

Reguliarius auditus turėtų atlikti atitinkamų žinių, įgūdžių ir patirties turintys asmenys. Auditoriai turėtų būti nepriklausomi, nesvarbu, ar tai būtų išorės rangovas, ar MVĮ vidaus auditorius, nepriklausomas nuo kasdienių IT operacijų.

NEPAMIRŠKITE DUOMENŲ APSAUGOS

Pagal ES bendrąjį duomenų apsaugos reglamentą[1] visos MVĮ, kurios tvarko arba saugo ES/EEE gyventojams priklausančius asmens duomenis, turi užtikrinti, kad būtų įdiegtos tinkamos saugumo kontrolės priemonės šiems duomenims apsaugoti. Tai apima užtikrinimą, kad visos trečiosios šalys, veikiančios MVĮ vardu, taikytų tinkamas saugumo priemones.

1 Bendrasis duomenų apsaugos reglamentas (https://ec.europa.eu/info/law/law-topic/data-protection_en).

2

ORGANIZUOKITE TINKAMUS MOKYMUS

Reguliariai organizuokite kibernetinio saugumo sąmoningumo mokymus visiems darbuotojams, kad jie galėtų atpažinti įvairias kibernetinio saugumo grėsmes ir su jomis kovoti. Šie mokymai turėtų būti pritaikyti MVĮ ir orientuoti į realias situacijas.

Organizuokite specializuotus kibernetinio saugumo mokymus asmenims, atsakingiems už kibernetinio saugumo valdymą įmonėje, siekiant užtikrinti, kad jie turėtų savo darbui reikalingų įgūdžių ir kompetencijų.

3

UŽTIKRINKITE VEIKSMINGĄ TREČIŲJŲ ŠALIŲ VALDYMĄ

Užtikrinkite, kad visi pardavėjai, ypač tie, kurie turi prieigą prie neskelbtinų duomenų ir (arba) sistemų, būtų aktyviai valdomi ir atitiktų sutartus saugumo lygius. Turėtų būti įgyvendinami sutartiniai susitarimai, kuriais būtų reglamentuojama, kaip pardavėjai laikosi tų saugumo reikalavimų.

4

PARENKITE REAGAVIMO Į INCIDENTUS PLANĄ

Parenkite oficialų reagavimo į incidentus planą, kuriame būtų pateiktos dokumentais pagrįstos aiškios gairės, vaidmenys ir atsakomybė, siekiant užtikrinti, kad į visus kibernetinius incidentus būtų reaguojama laiku, profesionaliai ir tinkamai. Siekiant greitai reaguoti į grėsmes saugumui, ištirkite priemones, kuriomis būtų galima stebėti ir kurti įspėjimus, kai vykdoma įtartina veikla ar saugumo pažeidimai.

5 APSAUGOKITE PRIEIGĄ PRIE SISTEMŲ

Raginkite visus naudoti slaptafrazę – bent trijų atsitiktinų paprastų žodžių, sujungtų į frazę, rinkinį, kuris būtų lengvai įsimenamas ir saugus. Jei pasirinksite paprastą slaptažodį:

- Jis turi būti ilgas, sudarytas iš mažųjų ir didžiųjų raidžių, galbūt taip pat skaičių ir specialiųjų ženklų.
- Venkite akivaizdžių slaptažodžių, tokių kaip „slaptažodis“, raidžių ar skaičių sekų, pavyzdžiui, „abc“ ir „123“.
- Venkite naudoti asmeninę informaciją, kurią galima rasti internete.

Ir nesvarbu, naudojate slaptafrazes, ar slaptažodžius

- Niekur kitur jų nenaudokite.
- Nesidalykite jais su kolegomis.
- Įjunkite dvielementį tapatumo nustatymą.
- Naudokite specialią slaptažodžių tvarkyklę.

6

APSAUGOKIT E ĮRENGINIUS

Vienas iš pagrindinių kibernetinio saugumo programos žingsnių yra užtikrinti darbuotojų naudojamų įrenginių – stalinių, knyginių ir planšetinių kompiuterių ar išmaniųjų telefonų – saugumą.

PROGRAMINĖ ĮRANGA TURI BŪTI TAISOMA IR ATNAUJINAMA

Geriausia naudoti centralizuotą platformą pataisoms valdyti. MVĮ labai rekomenduojama:

- Reguliariai atnaujinti visą savo programinę įrangą.
- Kai tik įmanoma, įjungti automatinius atnaujinimus.
- Nustatyti, kuri programinė ir aparatinė įranga turi būti atnaujinama rankiniu būdu.
- Atsižvelgti į mobiliuosius ir daiktų interneto įrenginius.

ANTIVIRUSINĖ PROGRAMA

Centralizuotai valdoma antivirusinė programa turėtų būti įdiegta ir atnaujinama visų tipų įrenginiuose, kad būtų užtikrintas nuolatinis jos veiksmingumas. Be to, nediekite piratinės programinės įrangos, nes joje gali būti kenkimo programinės įrangos.

NAUDOKITE EL. PAŠTO IR SAITYNO APSAUGOS PRIEMONES

Naudokite priemones, skirtas nepageidaujamiems el. laiškams, el. laiškams su nuorodomis į kenkėjiškas svetaines, el. laiškams su kenkėjiškais priedais, pvz., virusais, ir apgaulingiems el. laiškams blokuoti.

ŠIFRAVIMAS

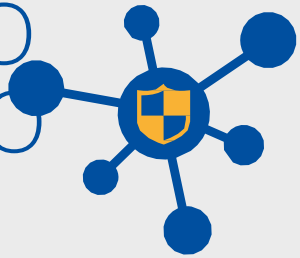
Apsaugokite duomenis juos užšifruodami. MVĮ turėtų užtikrinti, kad mobiliuosiuose įrenginiuose, pavyzdžiui, knyginiuose kompiuteriuose, išmaniuosiuose telefonuose ir planšetiniuose kompiuteriuose, saugomi duomenys būtų užšifruoti. Jei duomenys perduodami viešaisiais tinklais, pvz., viešbučių ar oro uostų „WiFi“ tinklais, užtikrinkite, kad jie būtų užšifruoti – naudokite virtualųjį privatųjį tinklą (VPN) arba prie interneto svetainių junkitės saugiais ryšiais, naudodami SSL/TLS protokolą. MVĮ turi užtikrinti, kad jų interneto svetainėse būtų naudojama tinkama šifravimo technologija, skirta klientų duomenims jiems keliaujant internetu apsaugoti.

ĮDIEKITE MOBILIŲJŲ ĮRENGINIŲ VALDYMĄ

Sudarydamos sąlygas darbuotojams dirbti nuotoliniu būdu, daugelis MVĮ leidžia jiems naudotis savo knyginiais ir planšetiniais kompiuteriais ir (arba) išmaniaisiais telefonais. Tai kelia saugumo problemų, susijusių su tuose įrenginiuose saugomais neskelbtinais verslo duomenimis. Vienas iš būdų valdyti šią riziką – taikyti mobiliųjų įrenginių valdymą, leidžiantį MVĮ:

- Kontroliuoti, kokiems įrenginiams leidžiama naudotis jų sistemomis ir paslaugomis.
- Užtikrinti, kad įrenginyje įdiegta naujausia antivirusinė programa.
- Nustatyti, ar įrenginys yra užšifruotas.
- Patikrinti, ar įrenginyje įdiegtos naujausios programinės įrangos pataisos.
- Užtikrinti, kad įrenginys būtų apsaugotas PIN kodu ir (arba) slaptažodžiu.
- Nuotoliniu būdu ištrinti visus MVĮ duomenis iš įrenginio, jei jo savininkas praneštų, kad įrenginys yra pamestas ar pavogtas, arba jei prietaiso savininko darbo santykiai su MVĮ nutrūktų.

7 APSAUGOKITE SAVO TINKLĄ



NAUDOKITE UŽKARDAS

Užkardos valdo į tinklą patenkantį ir iš jo išeinantį srautą ir yra labai svarbi MVĮ sistemų apsaugos priemonė. Užkardos turėtų būti įdiegtos siekiant apsaugoti visas svarbiausias sistemas, visų pirma užkarda turėtų būti naudojama norint apsaugoti MVĮ tinklą nuo interneto.

PERŽIŪRĖKITE NUOTOLINĖS PRIEIGOS SPRENDIMUS

MVĮ turėtų reguliariai peržiūrėti visas nuotolinės prieigos priemones, kad užtikrintų jų saugumą, visų pirma:

- Užtikrintų, kad visa nuotolinės prieigos programinė įranga yra taisoma ir atnaujinama.
- Apribotų nuotolinę prieigą prisijungimams iš įtartinų geografinių vietovių arba tam tikrų IP adresų.
- Apribotų darbuotojų nuotolinę prieigą tik prie jų darbui reikalingų sistemų ir kompiuterių.
- Užtikrintų patikimus nuotolinės prieigos slaptažodžius ir, jei įmanoma, įjungtų dvielementį tapatumo nustatymą.
- Užtikrintų, kad būtų įjungta stebėjimo ir įspėjimo funkcija, pranešanti apie įtariamas atakas ar neįprastą įtartiną veiklą.

8 GERINKITE FIZINĮ SAUGUMĄ

Visur, kur saugoma svarbi informacija, turėtų būti taikomos tinkamos fizinės kontrolės priemonės. Pavyzdžiui, negalima įmonės knyginio kompiuterio ar išmaniojo telefono palikti be priežiūros ant galinės automobilio sėdynės. Kiekvieną kartą, kai naudotojas atsitraukia nuo kompiuterio, jis turėtų jį užrakinti. Priešingu atveju įjunkite automatinio užsirakinimo funkciją visuose įrenginiuose, naudojamuose verslo tikslais. Slapto pobūdžio spausdintų dokumentų taip pat negalima palikti be priežiūros, o nenaudojamus reikia saugiai laikyti.

9 APSAUGOKITE ATSARGINES KOPIJAS

Kad būtų galima atkurti svarbiausią informaciją, turėtų būti išsaugotos atsarginės kopijos, nes jos yra veiksmingas būdas atsigauti po tokių įvykių kaip išpirkos reikalaujančios programinės įrangos išpuolis. Turėtų būti taikomos šios atsarginio kopijavimo taisyklės:

- atsarginis kopijavimas turi būti atliekamas reguliariai ir, kai įmanoma, automatizuotai,
- atsarginės kopijos turi būti saugomos atskirai nuo MVĮ gamybinės aplinkos,
- atsarginės kopijos turi būti užšifruotos, ypač jei jos bus perkeliamos iš vienos vietos į kitą,
- turi būti tikrinama galimybė reguliariai atkurti duomenis iš atsarginių kopijų. Geriausia būtų reguliariai atlikti viso atkūrimo proceso nuo pradžios iki pabaigos bandymą.

10 NAUDOKITĖS DEBESIJOS PASLAUGOMIS

Nors debesijos paslaugomis grindžiami sprendimai turi daug privalumų, jie kelia tam tikrą ypatingą riziką, į kurią MVĮ turėtų atsižvelgti prieš pradėdamos bendradarbiauti su debesijos paslaugų teikėju. ENISA paskelbė MVĮ skirtą debesijos saugumo vadovą (angl. *„Cloud Security Guide for SMEs"*[2]), kuriuo MVĮ turėtų remtis pereidamos prie naudojimosi debesijos paslaugomis.

Rinkdamosi debesijos paslaugų teikėją, MVĮ turėtų užtikrinti, kad jis, saugodamas duomenis, ypač asmens duomenis už ES/EEE ribų, nepažeidžia jokių teisės aktų ar reglamentų. Pavyzdžiui, ES Bendrajame duomenų apsaugos reglamente (BDAR) reikalaujama, kad ES/EEE gyventojų asmens duomenys nebūtų saugomi ar perduodami už ES/EEE ribų, išskyrus labai konkrečias sąlygas.

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

11 APSAUGOKITE INTERNETO SVETAINES

Labai svarbu, kad MVĮ užtikrintų, kad jų interneto svetainės būtų sukonfigūruotos ir tvarkomos saugiai ir kad visi asmens ar finansiniai duomenys, pavyzdžiui, kredito kortelių duomenys, būtų tinkamai apsaugoti. Tam reikės reguliariai atlikti svetainių saugumo bandymus, kad būtų nustatyti galimi saugumo trūkumai, ir reguliariai atlikti peržiūras, siekiant užtikrinti, kad svetainė būtų tinkamai prižiūrima ir atnaujinama.

12 IEŠKOKITE INFORMACIJOS IR JA DALYKITĖS

Veiksminga kovos su kibernetiniais nusikaltimais priemonė yra dalijimasis informacija. Dalijimasis su kibernetiniais nusikaltimais susijusia informacija yra itin svarbus veiksnys MVĮ, kad jos geriau suprastų joms kylančią riziką. Įmonės, iš kolegų išgirdusios apie kibernetinio saugumo sunkumus ir jų įveikimo būdus, dažniau imsis priemonių savo sistemoms apsaugoti, nei sužinojusios panašią informaciją, pateiktą sektoriaus ataskaitose ar kibernetinio saugumo tyrimų tyrimuose.

EUROPOS SĄJUNGOS
KIBERNETINIO
SAUGUMO AGENTŪRA

APIE ENISA

Europos Sąjungos kibernetinio saugumo agentūra (ENISA) yra Sąjungos agentūra, kurios tikslas – siekti aukšto bendro kibernetinio saugumo lygio visoje Europoje. Europos Sąjungos kibernetinio saugumo agentūra, įkurta 2004 ir sustiprinta ES kibernetinio saugumo aktu, prisideda prie ES kibernetinės politikos, didina IRT produktų, paslaugų ir procesų, kuriuose naudojamos kibernetinio saugumo sertifikavimo schemos, patikimumą, bendradarbiauja su valstybėmis narėmis ir ES įstaigomis ir padeda Europai pasirengti būsimiems kibernetiniams iššūkiams. Dalydamasi žiniomis, stiprindama gebėjimus ir didindama informuotumą, agentūra kartu su savo pagrindiniais suinteresuotaisiais subjektais siekia stiprinti pasitikėjimą susieta ekonomika, didinti Sąjungos infrastruktūros atsparumą ir, galiausiai, užtikrinti Europos visuomenės ir piliečių skaitmeninį saugumą. Daugiau informacijos rasite svetainėje www.enisa.europa.eu.

ENISA

Europos Sąjungos kibernetinio saugumo agentūra

Biuras Atėnuose
Ethnikis Antistaseos 72 &
Agamemnonos 14,
halandris 15231, Atika,
Graikija

Biuras Heraklione
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklionas, Graikija

enisa.europa.eu