



EIROPAS SAVIENĪBAS  
KIBERDROŠĪBAS  
AĢENTŪRA

Kiberdrošības ceļvedis mazajiem un  
vidējiem uzņēmumiem (MVU)

12  
SOĻI

SAVA  
UZNĒMUMA  
DRŌŠĪBAS  
UZTURĒŠAN



Covid-19 krīze parādīja, cik svarīgs internets un datori kopumā ir MVU. Lai turpinātu uzņēmējdarbību pandēmijas laikā, daudziem MVU bija jāīsteno darbības pārtrauktības pasākumi, piemēram, jāievieš mākoņpakalpojumi, jāuzlabo interneta pakalpojumi, jāuzlabo savas tīmekļa vietnes un jānodrošina iespēja darbiniekiem strādāt attālināti.

Šajā brošūrā norādīts, kādi praktiski 12 soļi augstā līmenī jāspē MVU, lai labāk aizsargātu savas sistēmas un uzņēmējdarbību. Tā ir papildu publikācija līdztekus sīki izstrādātam ENISA ziņojumam **“Kiberdrošība MVU — izaicinājumi un ieteikumi”**.



# 1 IZVEIDOJIET LABU KIBERDROŠĪBAS KULTŪRU



## IECELIET ATBILDĪGO PAR PĀRVALDĪBU

Laba kiberdrošība ir jebkura MVU panākumu pamatā. Atbildība par šo būtiski svarīgo funkciju būtu jāuzņemas kādam organizācijas darbiniekam, kuram kiberdrošības nodrošināšanai būtu jāpiešķir atbilstīgi resursi, piemēram, personāls, kiberdrošības programmatūras, jāveic pakalpojumu un aparatūras iegāde, personāla apmācība un efektīvas politikas izstrāde.

## PANĀCIET DARBINIEKU IESAISTI

Panāciet darbinieku līdzdalību, efektīvi vadot komunikāciju par kiberdrošību, vadībai atklāti atbalstot kiberdrošības iniciatīvas, atbilstīgas apmācības darbiniekiem un informējot darbiniekus par skaidriem un konkrētiem noteikumiem, kas ietverti kiberdrošības politikā.





## PUBLICĒJIET KIBERDROŠĪBAS POLITIKU

Kiberdrošības politikā attiecībā uz darbiniekiem būtu jāiekļauj skaidri un konkrēti noteikumi par to, kā būtu jārikojas, izmantojot uzņēmuma IKT vidi, aprīkojumu un pakalpojumus. Šajā politikā arī jāuzsver sekas, ar kurām darbinieks varētu saskarties, ja politiku neievēro. Politika ir regulāri jāpārskata un jāatjaunina.

## VEICIET KIBERDROŠĪBAS REVĪZIJAS

Personām ar atbilstīgām zināšanām, prasmēm un pieredzi, būtu jāveic regulāras revīzijas. Revidentiem vajadzētu būt neatkarīgiem, neraugoties uz to, vai viņi ir ārpalpojumu sniedzēji vai MVU darbinieki, un tādiem, kas ikdienā neveic IT darbinieku pienākumus.

## ATCERĪETIES PAR DATU AIZSARDZĪBU

Saskaņā ar ES Vispārīgo datu aizsardzības regulu<sup>1</sup> visiem MVU, kas apstrādā vai glabā personas datus un kas pieder ES/EEZ rezidentiem, ir jānodrošina, ka ir ieviestas atbilstošas drošības kontroles, lai šos datus aizsargātu. Tas nozīmē arī pārliecināšanos par to, ka jebkuras trešās personas, kas strādā MVU vārdā, ir ieviesušas atbilstīgus drošības pasākumus.

---

<sup>1</sup> Vispārīgā datu aizsardzības regula [https://ec.europa.eu/info/law/law-topic/data-protection\\_lv](https://ec.europa.eu/info/law/law-topic/data-protection_lv)

# 2



## VEICIET ATBILSTĪGU APMĀCĪBU

Veiciet regulāras kibernetikas izpratnes apmācības visiem darbiniekiem, lai nodrošinātu, ka viņi spēj atpazīt un novērst dažādus apdraudējumus kibernetikai. Šīs apmācības būtu jāpielāgo konkrētajam MVU un jākoncentrējas uz reālām situācijām.

Veiciet specializētas kibernetikas apmācības personām, kuras ir atbildīgas par kibernetikas pārvaldību uzņēmumā, lai nodrošinātu, ka tās iegūs prasmes un kompetences, kas vajadzīgas šī darba veikšanai.



# 3

## NODROŠINIET EFEKTĪVU TREŠO PERSONU PĀRVALDĪBU

Nodrošiniet, lai visi pakalpojumu sniedzēji, jo īpaši tie, kuriem ir piekļuve sensitīviem datiem un/vai sistēmām, tiktu aktīvi pārvaldīti un atbilst saskaņotajiem drošības līmeņiem. Pakalpojumu sniedzēju atbilstību šīm drošības prasībām būtu jāregulē līgumsaistībās.

# 4



## IZSTRĀDĀJIET PLĀNU, KĀ REAGĒT INCIDENTA GADĪJUMĀ

Izstrādājiēt oficiālu plānu, kā reagēt uz incidentiem, kurā būtu dokumentētas skaidras pamatnostādnes, ieņemamie amati un pienākumi, lai nodrošinātu, ka uz visiem ar drošību saistītajiem incidentiem tiktu reagēts savlaicīgi, profesionāli un atbilstīgi. Lai ātri reagētu uz apdraudējumiem drošībai, izpētiet rīkus, ar kuriem varētu uzraudzīt un izveidot brīdinājumus, ja notiek aizdomīgas darbības vai drošības pārkāpumi.

# 5 DROŠĀ PIEKLUVE SISTĒMĀM

Mudiniēt ikvienu parolē izmantot ieejas frāzi, kas sastāv no vismaz trim nejauši izvēlētiem vienkāršiem vārdiem, apvienotiem teikumā, tādējādi nodrošinot gan ļoti vieglu atcerēšanos, gan labu drošību. Ja izvēlaties tipisku paroli,

- izdomājiēt to pietiekami garu, izmantojiēt mazos un lielos burtus, iespējams, arī ciparus un īpašās rakstzīmes;
- izvairīties no viegli uzminamiem vārdiem, piemēram, "parole", burtiem vai cipariem tādā secībā kā, piemēram, "abc" vai "123";
- neizmantojiēt personisko informāciju, ko var atrast tiešsaistē.

Un neatkarīgi no tā, vai izmantojāt ieejas frāzes vai paroles,

- nelietojiēt tās citur;
- nekopīgojiēt tās ar kolēģiem;
- iespējojiēt daudzfaktoru autentifikāciju;
- izmantojiēt īpašu parolu pārvaldības rīku.



# 6

## PADARIET IERĪCES DROŠAS



Galvenais kiberdrošības programmas solis ir personāla izmantoto ierīču — galddatoru, klēpj datoru, planšētdatoru vai viedtālruni — izmantošanas drošība.

### LIECIET IELĀPUS PROGRAMMATŪRĀM UN ATJAUNINIET TĀS

Ideālā gadījumā izmantojot centralizētu platformu ielāpu pārvaldīšanai. MVU ļoti ieteicams:

- regulāri atjaunināt visu programmatūru;
- kur vien iespējams, iespējot automātiskus atjauninājumus;
- identificēt programmatūru un aparāturu, kuru atjauninājumi jāveic manuāli;
- ņemt vērā mobilās un lietu internetu veidojošās ierīces.

### ANTIVĪRUSU RISINĀJUMS

Visu veidu ierīcēs būtu jāievieš un regulāri jāatjaunina centralizēti pārvaldīts pretvirusu risinājums, lai nodrošinātu tā nepārtrauktu efektivitāti. Turklāt neuzstādi pirātisku programmatūru, jo tajā var atrasties ļaunatūra.

## IZMANTOJIET E-PASTA UN TĪMEKĻA AIZSARDZĪBAS RĪKUS

Izmantojiet risinājumus, kas bloķē surogātpastus, e-pasta ziņojumus, kas satur saites uz ļaunprātīgām tīmekļa vietnēm, e-pasta ziņojumus, kas satur ļaunprātīgus pielikumus, piemēram, vīrusus, un pikšķerēšanas e-pasta ziņojumus.

### ŠIFRĒŠANA

Aizsargājiet datus, tos šifrējot. MVU būtu jānodrošina, lai mobilajās ierīcēs, piemēram, klēpj datoros, viedtālrunos un planšētdatoros, saglabātie dati tiktu šifrēti. Ja dati tiek pārsūtīti, izmantojot publiskos tīklus, piemēram, viesnīcu vai lidostu WiFi tīklus, pārliecinieties, vai dati tiek šifrēti, izmantojot virtuālo privāto tīklu (VPT) vai piekļūstot vietnēm, izmantojot drošus savienojumus, izmantojot SSL/TLS datu pārraides protokolu. Jānodrošina, ka to vietnēs tiek izmantota piemērota šifrēšanas tehnoloģija, lai aizsargātu klientu datus, tiem ceļojot pa internetu.

## IEVIESIET IERĪČU MOBILO PĀRVALDĪBU

Atvieglojot darbinieku attālināto darbu, daudzi MVU ļauj darbiniekiem izmantot pašiem piederošus klēpj datorus, planšet datorus un/vai viedtālrunus. Tas rada vairākas ar drošību saistītas problēmas attiecībā uz sensitīviem uzņēmējdarbības datiem, kas tiek glabāti šajās ierīcēs. Viens veids, kā pārvaldīt šo risku, ir izmantot mobilo ierīču pārvaldības (*MDM*) risinājumu, kas ļauj MVU:

- kontrolēt, kurām ierīcēm ir atļauts piekļūt to sistēmām un pakalpojumiem;
- nodrošināt, ka ierīcē ir uzstādīta atjaunināta pretvīrusu programmatūra;
- noteikt, vai ierīce ir šifrēta;
- apstiprināt, ka ierīcē ir uzstādīti atjaunināti programmatūras ielāpi;
- panākt, ka ierīci aizsargā PIN un/vai parole;
- Attālināti izdzēsiet no ierīces visus MVU datus, ja ierīces īpašnieks ziņo, ka tā ir pazaudēta vai nozagta, vai ja ierīces īpašnieka darba attiecības ar MVU ir beigušas.

# 7 PADARIET DROŠU SAVU TĪKLU



## IZMANTOJIET UGUNSMĪRUS

Uguns mūri pārvalda tīklā ienākošās un no tā izejošās informācijas plūsmu un ir būtisks instruments MVU sistēmu aizsardzībai. Uguns mūri būtu jāizvieto, lai aizsargātu visas būtiski svarīgās sistēmas, jo īpaši uguns mūrīs jāizmanto, lai aizsargātu MVU tīklu no interneta.

## PĀRSKATIET ATTĀLINĀTAS PIEEJAS RISINĀJUMUS

MVU būtu regulāri jāpārskata visi attālinātās piekļuves rīki, lai nodrošinātu to drošumu, jo īpaši:

- jāpārlicinās, vai visai attālinātās piekļuves programmatūrai ir ielāpi un tā ir atjaunināta;
- jāierobežo attālinātā piekļuve no aizdomīgām ģeogrāfiskām vietām vai noteiktām IP adresēm;
- jāierobežo darbinieku attālinātā piekļuve, nodrošinot to tikai tām sistēmām un datoriem, kas vajadzīgi viņu darbam;
- attālinātajai piekļuvei jāizmanto neuzlaužamas paroles un, ja iespējams, jāiespējo daudzfaktoru autentifikācija;
- jāpārlicinās, vai ir iespējota uzraudzības un brīdināšanas sistēma, lai brīdinātu par iespējamiem uzbrukumiem vai neparastām aizdomīgām darbībām.



# 8 UZLABOJIET FIZISKO DROŠĪBU

Visur, kur atrodas svarīga informācija, būtu jāveic atbilstīga fiziskā kontrole. Piemēram, uzņēmuma klēpj datoru vai viedtālruni nedrīkst atstāt bez uzraudzības automašīnas aizmugurējā sēdekli. Ikreiz, kad lietotājs atiet no sava datora, tas būtu jābloķē. Pretējā gadījumā jāiespējo automātiskās bloķēšanas funkcija jebkurā ierīcē, kas tiek izmantota uzņēmējdarbības nolūkos. Arī sensitīvos drukātos dokumentus nedrīkst atstāt bez uzraudzības un, kad tie netiek izmantoti, tie ir jāuzglabā drošā vietā.



# 9 DROŠI DUBLĒJUMI

Lai varētu atjaunot pamata datus, būtu jā saglabā dublējumi, jo tie ir efektīvs veids, kā atgūties no tādām katastrofām kā izspiedējvīrusa uzbrukums. Būtu jāpieņem šādi noteikumi attiecībā uz dublēšanu:

- dublēšana jāveic regulāri un, ja iespējams, automatizēti,
- dublēšana jāveic atsevišķi no MVU ražošanas vides,
- dublētie dati ir jāšifrē, jo īpaši ja tie ir paredzēti pārvietošanai no vienas vietas uz citu,
- jāpārbauda spēja regulāri atjaunot datus no dublējumiem. Ideālā gadījumā būtu jāveic regulāra pilnīgas atjaunošanas pārbaude no sākuma līdz beigām.





# 10

## IESAISTIETIES MĀKONĪ

Lai gan mākoņrisinājumi piedāvā daudzas priekšrocības, tie rada dažus unikālus riskus, kas MVU būtu jāapsver pirms izvēlēties mākoņpakalpojumu sniedzēju. ENISA ir publicējusi "Mākoņu drošības rokasgrāmatu MVU"<sup>2</sup>, kuru MVU būtu jāņem vērā, veicot datu migrāciju uz mākonī.

Izvēloties mākoņpakalpojumu sniedzēju, MVU būtu jāpārlicinās, ka tas nepārkāpj normatīvos aktus, uzglabājot datus, jo īpaši personas datus, ārpus ES/EEZ. Piemēram, ES VDAR ir pieprasīts, lai ES/EEZ iedzīvotāju personas dati netiktu uzglabāti vai pārsūtīti ārpus ES/EEZ, ja vien nav ievēroti īpaši nosacījumi.

---

<sup>2</sup> <https://www.enisa.europa.eu/about-enisa/about/lv>



# 11

## PADARIET DROŠAS TIEŠSAISTES VIETAS

Ir būtiski, lai MVU nodrošinātu savu tiešsaistes vietņu drošu konfigurēšanu un uzturēšanu un visu personas datu vai finanšu informācijas, piemēram, kredītkaršu datu, pienācīgu aizsardzību. Tas nozīmē regulāru drošības pārbaūžu veikšanu vietnēs, lai konstatētu iespējamus trūkumus drošības ziņā, un regulāras pārbaudes, lai nodrošinātu vietnes pareizu uzturēšanu un atjaunināšanu.



## MEKLĒJIET UN KOPĪGOJIET INFORMĀCIJU

Efektīvs līdzeklis cīņā pret kibernetiskiem uzbrukumiem ir informācijas kopīgošana. Informācijas kopīgošana saistībā ar kibernetiskiem uzbrukumiem ir svarīga MVU, lai labāk izprastu riskus, ar kuriem tie saskaras. Pastāv lielāka ticamība, ka uzņēmumi, kas būs uzzinājuši par kibernetiskās drošības problēmām un to, kā šīs problēmas tika pārvarētas, no sev līdzīgiem uzņēmumiem, drīzāk veiks pasākumus savu sistēmu aizsardzībai, nekā tad, ja tie līdzīgu informāciju būtu uzzinājuši no visiem nozares pārstāvjiem adresētiem ziņojumiem vai kibernetiskās drošības apsekojumiem.



EIROPAS SAVIENĪBAS  
KIBERDROŠĪBAS  
AGENTŪRA

## PAR ENISA

Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) ir Savienības aģentūra, kuras mērķis ir panākt vienādi augsta līmeņa kiberdrošību visā Eiropā. Eiropas Savienības Kiberdrošības aģentūra, kas dibināta 2004. gadā un nostiprināta ar ES Kiberdrošības aktu, sniedz ieguldījumu ES kiberdrošības politikā, stiprina IKT produktu, pakalpojumu un procesu uzticamību ar kiberdrošības sertifikācijas shēmām, sadarbojas ar dalībvalstīm un ES struktūrām un palīdz Eiropai sagatavoties nākotnes izaicinājumiem kiberdrošības jomā. Kopīgojot zināšanas, veidojot spējas un veicinot izpratni, aģentūra sadarbojas ar savām galvenajām ieinteresētajām personām, lai vairotu uzticību savienotajai ekonomikai, palielinātu Savienības infrastruktūras noturību un, visbeidzot, garantētu Eiropas sabiedrībai un iedzīvotājiem digitālo drošību. Plašāku informāciju skatiet vietnē [www.enisa.europa.eu](http://www.enisa.europa.eu).

## ENISA

Eiropas Savienības Kiberdrošības aģentūra

### Birojs Atēnās

Ethnikis  
Antistaseos 72 & Agame  
mnonos 14,  
Chalandri 15231, Attiki,  
Grieķija

[enisa.europa.eu](http://enisa.europa.eu)

### Birojs Hēraklejā

95 Nikolaou Plastira  
700 13 Vassilika Vouton,  
Heraklion, Grieķija

