isse

SECURITY. ENGINEERED.

UZŅĒMUMA DROŠĪBAS PĀRBAUDE

# Ziemeļu birojs. Skaidrs skatījums uz drošību.

**SIA ZIEMEĻU BIROJS · DEMONSTRĀCIJAS UZŅĒMUMS**

Ierobežota apjoma profesionālā pārbaude. Visi uzņēmuma dati un konstatējumi šajā dokumentā ir fiktīvi.

VERSIJA 1.0 · 2026-11-15 · info@isse.lv

08 LAPPUSES

DEMONSTRĀCIJA · NAV REĀLA KLIENTA ZIŅOJUMS

02 · VADĪBAS KOPSAVILKUMS

# Prioritātes ir skaidras.

**2**
AUGSTAS PRIORITĀTES

a u
uzl

**4**
IETEICAMI UZLABOJUMI

**8**
BEZ KONSTATĒTAS PROBLĒMAS

## SVARĪGĀKIE NĀKAMIE SOĻI

ISSE-001

### Nepilnīgs daudzfaktoru autentifikācijas pārklājums

Ieslēgt MFA visiem lietotājiem, sākot ar e-pastu un attālināto piekļuvi. Atļaut izņēmumu tikai laika ierobežotā, dokumentētā gadījumā.

ISSE-002

### Bijušā darbinieka piekļuves prasa papildu pārbaudi

Pārbaudīt aktīvās sesijas, grupas, koplietojamos resursus, VPN, paroļu pārvaldnieku un fizisko piekļuvi. Dokumentēt pabeigtās darbības.

ISSE-003

### DMARC konfigurēts tikai uzraudzībai

Pārskatīt DMARC atskaites un visus leģitīmos sūtītājus. Pēc pārbaudes pakāpeniski pāriet uz p=quarantine vai p=reject.

## KONTROLES BEZ KONSTATĒTAS PROBLĒMAS

- Administratoru kontu skaits ir ierobežots un ikdienas konti netiek izmantoti administrēšanai.
- Paroļu pārvaldnieks tiek izmantots, un koplietoto piekļuvju saraksts ir pieejams IT nodrošinātājam.
- SPF ieraksts ir atrasts, un nav vairāku savstarpēji pretrunīgu ierakstu.
- DKIM parakstīšana tiek izmantota vismaz primārajai Microsoft 365 pasta plūsmai.
- Darbinieku piekļuves grupām ir nozīmēts īpašnieks.
- Darba datoru operētājsistēmu atjauninājumi tiek centralizēti uzraudzīti.

Šis nav vienots drošības procents. Rezultāts atspoguļo tikai konkrētā apjoma pārbaudi un pieejamos pierādījumus.

03 · PĀRBAUDES APJOMS

# Kas pārbaudīts un kas nav.

Pārbaudes mērķis ir sniegt skaidru un izmantojamu pirmo priekšstatu, nevis apliecināt visaptverošu atbilstību vai drošību.

| | |
|---|---|
| **TEHNISKI PĀRBAUDĪTS** | Publiskie DNS ieraksti, DMARC politika un demonstrācijas Microsoft 365 konfigurācijas izraksts. |
| **KLIENTA SNIEGTA INFORMĀCIJA** | Darbinieku skaits, procesi, ierīču pārvaldība, piekļuves atsaukšana un rezerves kopiju prakse. |
| **NAV PĀRBAUDĪTS** | Visas ierīces, klientu datu saturs, iekšējie serveri, ziņu piegāde un faktiskā lietotāju pieredze. |
| **NEATTIECAS** | Kontroles, kurām demonstrācijas videi nav atbilstoša objekta vai kuras nav saskaņotas apjomā. |

## IEROBEŽOJUMI

- Laika ziņā ierobežota attālināta pārbaude; mērķa apjoms ir 90 minūtes.
- Nav pilns audits, penetrācijas tests, visu ierīču apskate vai regulatīvās atbilstības sertifikācija.
- Ziņojums atspoguļo konkrētu laika momentu; vide un apdraudējumi laika gaitā mainās.
- Trūkst pierādījumu nozīmē “nav pārbaudīts”, nevis automātiski “nav droši”.

04 · KONSTATĒJUMI UN IETEIKUMI

# Kas prasa uzmanību un kāpēc.

ISSE-001

TEHNISKI PĀRBAUDĪTS · NEKAVĒJOTIES

## Nepilnīgs daudzfaktoru autentifikācijas pārklājums

IDENTITĀTES UN KONTU DROŠĪBA · HIGH

KONSTATĒJUMS

Demonstrācijas datu kopā MFA ir iespējota administratoriem, bet ne visiem e-pasta un attālinātās piekļuves lietotājiem. Palikuši vismaz divi lietotāju konti ar vienu faktoru.

IETEIKUMS

Ieslēgt MFA visiem lietotājiem, sākot ar e-pastu un attālināto piekļuvi. Atļaut izņēmumu tikai laika ierobežotā, dokumentētā gadījumā.

IETEKME

Viena nozagta parole var ļaut piekļūt pastkastei vai attālinātajai videi. Tas var novest pie klientu datu atklāšanas, krāpnieciskām ziņām un viltotiem maksājumiem.

TEHNISKĀ DETAĻA

Pārbaudīt Microsoft Entra pieteikšanās metodes un uzņēmējpiekļuves politiku. Pārliecināties, ka vecā autentifikācija netiek izmantota kā faktiskas aizsardzības apvedceļš.

ATBILDĪGAIS: IT nodrošinātājs ar uzņēmuma vadītāja apstiprinājumu

ISSE-002

KLIENTA SNIEGTA INFORMĀCIJA · NEKAVĒJOTIES

## Bijušā darbinieka piekļuves prasa papildu pārbaudi

PIEKĻUVES PĀRVALDĪBA · HIGH

KONSTATĒJUMS

Klienta vides aprakstā norādīts, ka darbinieks aizgāja pirms sešām nedēļām. E-pasts tika bloķēts, bet koplietotās mapes un paroļu pārvaldnieka piekļuves atsaukšana nav dokumentēta.

IETEIKUMS

Pārbaudīt aktīvās sesijas, grupas, koplietojamos resursus, VPN, paroļu pārvaldnieku un fizisko piekļuvi. Dokumentēt pabeigtās darbības.

IETEKME

Neatsaukta piekļuve var saglabāties neredzamā veidā un radīt konfidencialitātes vai datu integritātes risku.

TEHNISKĀ DETAĻA

Salīdzināt lietotāja tiešās un grupu tiesības ar apstiprinātu piekļuves matricu. Pārbaudīt arī OneDrive un SharePoint ārējās koplietošanas saites.

ATBILDĪGAIS: IT nodrošinātājs un personāla funkcija

ISSE-003

TEHNISKI PĀRBAUDĪTS · 7 DIENU LAIKĀ

## DMARC konfigurēts tikai uzraudzībai

E-PASTA DROŠĪBA · MEDIUM

KONSTATĒJUMS

Publiskajā DNS ir viens DMARC ieraksts ar politiku p=none. SPF un DKIM demonstrācijas datos ir konfigurēti, bet tie netiek pārbaudīti ar faktisku ziņas autentifikāciju.

IETEIKUMS

Pārskatīt DMARC atskaites un visus leģitīmos sūtītājus. Pēc pārbaudes pakāpeniski pāriet uz p=quarantine vai p=reject.

IETEKME

Uzraudzības politika sniedz redzamību, bet lietotāju pastkastēs pati par sevi neaptur domēna vārdā viltotas ziņas.

TEHNISKĀ DETAĻA

Iekļaut CRM, rēķinu sistēmu, mājaslapas kontaktformu un citus sūtītājus. Pirms politikas maiņas pārbaudīt SPF un DKIM alignment.

ATBILDĪGAIS: IT nodrošinātājs

05 · KONSTATĒJUMI UN IETEIKUMI

# Kas prasa uzmanību un kāpēc.

ISSE-004 KLIENTA SNIEGTA INFORMĀCIJA · 30 DIENU LAIKĀ

## Datu atjaunošanas pārbaude nav dokumentēta

REZERVES KOPIJAS · MEDIUM

KONSTATĒJUMS

Klienta sniegtā informācija apstiprina automātisku Microsoft 365 un ierīču kopēšanu. Nav pierādījumu par vismaz viena faila reālu atjaunošanas testu vai fiksētu atjaunošanas laiku.

IETEIKUMS

Veikt kontrolētu atjaunošanas testu atsevišķā vietā, pārbaudīt saturu un pierakstīt faktisko ilgumu, problēmas un nākamo pārbaudes datumu.

IETEKME

Kopēšanas statuss vien neparāda, vai datus var atjaunot pieņemamā laikā un vai kopiju nevar izdzēst ar uzlauztu administratora kontu.

TEHNISKĀ DETAĻA

Pārbaudīt arī nemainīgu saglabāšanu, atsevišķu piekļuves modeli un aizsardzību pret dzēšanu ar administratīvo tiesību starpniecību.

ATBILDĪGAIS: IT nodrošinātājs ar uzņēmuma atbildīgās personas līdzdalību

ISSE-005 KLIENTA SNIEGTA INFORMĀCIJA · 30 DIENU LAIKĀ

## Diska šifrēšanas statuss netiek vienmērīgi pārbaudīts

DARBA IERĪCES · MEDIUM

KONSTATĒJUMS

Windows ierīcēm šifrēšana tiek pieminēta kā ieslēgta, bet macOS ierīču FileVault statuss un atjaunošanas atslēgu pārvaldība nav apstiprināta.

IETEIKUMS

Pārbaudīt visus pārnēsājamos datorus neatkarīgi no operētājsistēmas un centralizēt atjaunošanas atslēgu pārvaldību.

IETEKME

Pazaudēta nešifrēta ierīce var atklāt klientu failus un saglabātos pieteikšanās datus.

TEHNISKĀ DETAĻA

Pārliecināties, ka FileVault un BitLocker statuss tiek pārraudzīts no pārvaldības risinājuma, nevis tikai datora lietotāja ekrāna.

ATBILDĪGAIS: IT nodrošinātājs

ISSE-006 KLIENTA SNIEGTA INFORMĀCIJA · 90 DIENU LAIKĀ

## Drošības norādes darbiniekiem nav dokumentētas

DARBINIEKU IZPRATNE · LOW

KONSTATĒJUMS

Jaunajiem darbiniekiem tiek mutiski izskaidrota pieteikšanās un datu glabāšana. Nav vienota materiāla vai pieraksta, kas apstiprinātu apmācības saņemšanu.

IETEIKUMS

Sagatavot īsu praktisku materiālu, iekļaut to uzņemšanas procesā un atkārtot galvenos scenārijus vismaz reizi gadā.

IETEKME

Atšķirīga izpratne par aizdomīgu e-pastu un maksājumu pārbaudi var palielināt viltotu rēķinu un kļūdainas koplietošanas risku.

TEHNISKĀ DETAĻA

Norādīt ziņošanas e-pastu vai IT atbalsta kontaktu un pārbaudīt, vai viena testa ziņa tiek savlaicīgi pamanīta un apstrādāta.

ATBILDĪGAIS: Uzņēmuma vadība kopā ar IT nodrošinātāju

06 · RĪCĪBAS PLĀNS

# Secība, kas ir izpildāma.

Dažas darbības var veikt uzņēmums vai esošais IT sniedzējs. Citas var prasīt skaidru tehnisko lēmumu vai ārēju palīdzību.

## NEKAVĒJOTIES

ISSE-001 · Pabeigt MFA pārklājumu e-pastam un attālinātajai piekļuvei.
ISSE-002 · Atsaukt visas bijušā darbinieka atlikušās sesijas un piekļuves.

## 7 DIENU LAIKĀ

ISSE-003 · Pārskatīt DMARC atskaites un apstiprināt leģitīmos sūtītājus.
Pārbaudīt MFA lietotāju atbalsta procesu pēc ieviešanas.

## 30 DIENU LAIKĀ

ISSE-004 · Veikt un dokumentēt pirmo atjaunošanas testu.
ISSE-005 · Centralizēt BitLocker un FileVault statusa un atslēgu pārvaldību.

## 90 DIENU LAIKĀ

ISSE-006 · Ieviest praktisku darbinieku drošības pamācību.
Atkārtoti pārskatīt atvērtos konstatējumus un piekļuves matricu.

**ATKĀRTĪBAS UN PĀRSKATS**

Pēc MFA ieviešanas pārbaudiet lietotāju atbalsta procesu. Pirms DMARC stingrākas politikas pabeidziet sūtītāju sarakstu. Pirms atjaunošanas testa apstipriniet, kurš drīkst piekļūt kopijām un kurš apstiprina rezultātu.

07 · NEOBLIGĀTI IEVIEŠANAS SOĻI

# Palīdzība ir izvēle, nevis nosacījums.

Cenas tiek apstiprinātas tikai pēc apjoma un vides izvērtēšanas. Šie soļi nav saistošs piedāvājums un prasa atsevišķu rakstisku vienošanos.

01

## MFA un kontu piekļuves sakārtošana

Cena pēc apjoma saskaņošanas

Pieteikšanās metožu pārskats, MFA pārklājums, administratoru kontu pārbaude un īsa izmaiņu dokumentācija.

Aptuveni 3–4 stundas

Iespējama papildu licences nepieciešamība atkarībā no izvēlētās metodes.

02

## E-pasta autentifikācijas pilnveide

Cena pēc apjoma saskaņošanas

Sūtītāju pārbaude, SPF un DKIM korekcijas, DMARC monitoringa pārskats un stingrākas politikas ieviešanas plāns.

Aptuveni 3–5 stundas

Parasti bez papildu licences.

03

## Rezerves kopiju atjaunošanas darbnīca

Cena pēc apjoma saskaņošanas

Viens kontrolēts atjaunošanas tests, rezultātu pieraksts, nepilnību saraksts un nākamā pārbaudes procesa izveide.

Aptuveni 3–4 stundas

Atkarīgs no esošā rezerves kopiju risinājuma.

Esošais IT sniedzējs var veikt jebkuru ieteikumu, ja tam ir atbilstošas tiesības un kompetence. ISSE iesaiste nav nepieciešama, lai rīcības plāns būtu izmantojams.

08 · NĀKAMIE SOĻI

# Lēmumi paliek jūsu pusē.

Ziņojums ir paredzēts sarunai ar uzņēmuma vadību un IT sniedzēju. Prioritātes var pielāgot faktiskajai ietekmei, pieejamajai palīdzībai un vides atkarībām.

## NĀKAMIE SOĻI

- Apstipriniet divu augsto prioritāšu darbību atbildīgo.
- Vienojieties par DMARC sūtītāju sarakstu.
- Ieplānojiet pārbaudītu datu atjaunošanu.
- Atkārtoti pārskatiet vaļējos konstatējumus pēc 90 dienām.

## IEROBEŽOJUMI

- Nav pilns audits vai penetrācijas tests.
- Nav atbilstības sertifikācija.
- Nav visu ierīču vai klientu datu pārbaude.
- Ziņojums atspoguļo konkrētu laika momentu.

**KONFIDENCIALITĀTE**

Reāla klienta ziņojuma sagatavošanai jāizmanto tikai apstiprināti dati, ierobežota piekļuve un atsevišķa privātā datu vide. Šis publiskais paraugs nesatur klientu pierādījumus vai pieteikšanās informāciju.

## NODERĪGI MATERIĀLI

isse.lv/bezmaksas-rikki · isse.lv/zinasanu-centrs

**info@isse.lv · +371 24 421 133**