lmt biznesam

Pārliecinies, ka tava uzņēmuma **IT vide ir sakārtota**

Vadītājam nav jāzina IT tehniskās detaļas, bet viņam jāprot uzdot pareizos jautājumus, lai saprastu, vai uzņēmuma digitālā vide ir sakārtota. Biznesam augot, haotisks IT sāk kavēt darbu – rodas dīkstāves, drošības riski, tiek kavēts darba process.

Pareizi jautājumi palīdz vadītājam laikus pamanīt kritiskus "sarkanos karogus" kā arī vidēji kritiskas pazīmes , lai pārliecinātos, ka IT ir atbalsts biznesam, nevis tikai problēmu dzēšana.

Rezervē laiku sarunai! Kopā soli pa solim iziesim cauri testam, lai definētu galvenās IT prioritātes un nākamos soļus, kas palīdzēs ieviest sistēmu un kārtību tava uzņēmuma IT infrastruktūrā.

Pieteikties

1. Pārredzamība

Vadītāja kompetencē

1. Vai ir skaidri noteikts, kurām personām ir piekļuve datiem?

Kā pārbaudīt:

- [ ] Ir pieejams saraksts (piem., Excel vai SharePoint), kurā norādīts, kuriem darbiniekiem ir piekļuve konkrētām mapēm

2. Vai eksistē IT dokumentu mape? Vai ir dokumentēta tīkla shēma un pieejas dati?

Kā pārbaudīt:

- [ ] Fiziska vai digitāla (šajā gadījumā – ar ierobežotu piekļuvi) mape, kurā glabājas PDF, Visio vai Draw.io dokuments ar šādu informāciju:
  - iekārtu nosaukumi
  - IP adreses
  - shēma "kur kas pieslēdzas"
  - paroļu glabāšanas vieta (drošs paroļu glabāšanas rīks, nevis, piem., Excel bez paroles)

3. Vai domēns ir reģistrēts uz uzņēmumu?

Kā pārbaudīt:

- [ ] https://www.nic.lv/whois/ (domēniem ar .lv) vai https://whois.eurid.eu/ (domēniem ar .eu)
- [ ] Maksājumi tiek veikti tieši domēnu reģistratūrai, nevis IT uzturētājam

4. Vai ir saraksts par visām IT iekārtām un lietotājiem?

Kā pārbaudīt:

- [ ] Excel vai SharePoint saraksts, kurā jābūt šādai informācijai:
  - dators
  - lietotājs
  - datora pirkuma datums
  - garantijas termiņš

5. Vai jūs saņemat regulārus IT pārskatus (notikumi, darbinieku problēmas utt.)?

Kā pārbaudīt:

- [ ] Mēneša vai kvartāla atskaites piemērs
- [ ] Atskaitē tiek uzskaitīti: incidenti, licences, risks, rekomendācijas

IT speciālista kompetencē

6. Kur ir dokumentācija par IT sistēmām un vai tā tiek atjaunota?

Pierādījums:

- [ ] Pārzina centrālo dokumentu vietu (SharePoint, OneDrive vai kādu citu dokumentu vietu)
- [ ] Dokumentiem jābūt ar pēdējā atjauninājuma datumu

7. Cik ātri iespējams atjaunot darbu?

Pierādījums:

- [ ] Dokuments, kur aprakstīts, cik ilgā laikā sistēmu var atjaunot pēc incidenta

2. Atbildība

Vadītāja kompetencē

8. Vai ir skaidra datu uzglabāšanas politika?

Kā pārbaudīt:

- [ ] Dokuments (PDF vai Word, 1–2 lpp.), kurā definēts, kur un kādi dati glabājas (pašu serverī, OneDrive, SharePoint, Google Drive utt.)

IT speciālista kompetencē

9. Kāds ir process darba attiecību izbeigšanas gadījumā?

Pierādījums:

- [ ] Dokuments "Offboarding procedure"
- [ ] E-pasta pierādījums, ka darba attiecību izbeigšanas gadījumā pieejas ir aizvērtas vienas dienas laikā

10. Vai ir izveidots saraksts ar lietotājiem (kontiem), kuriem ir administratora tiesības?

Pierādījums:

- [ ] Eksports no Active Directory/Microsoft 365 admin centra – fails ar atjaunināšanas datumu
- [ ] Saraksts

3. Procesi

Vadītāja kompetencē

11. Vai eksistē incidentu (pazūd dators, uzlaušana) plāns?

Kā pārbaudīt:

- [ ] Aprakstīta plāna esamība

12. Vai darbinieki ir apmācīti, kas jādara, saņemot aizdomīgu e-pastu?

Kā pārbaudīt:

- [ ] Apmācību žurnāls (Excel vai LMS)
- [ ] Darbinieku testa rezultāti (ja ir simulācijas)

IT speciālista kompetencē

13. Kā tiek kontrolēta programmu izmantošana? Vai ir atļauto/aizliegto programmu saraksts (piem., torrenti, nestandarta antivīrusi utt.)?

Pierādījums:

- [ ] Aizliegto/atļauto programmu saraksts dokumentā

4. Kvalitāte

Vadītāja kompetencē

14. Vai regulāri saņem IT pārskatus ar incidentiem, riskiem un nākamajiem soļiem?

Kā pārbaudīt:

- [ ] Mēneša vai kvartāla atskaites piemērs
- [ ] Atskaitē tiek uzskaitīti: incidenti, licences, risks, rekomendācijas

15. Vai tīkla iekārtas un vadi izskatās sakārtoti, nevis kā "sprādziens makaronu fabrikā"?

Kā pārbaudīt:

- [ ] Vizuāla apskate – iekārtām jābūt marķētām (tīkla iekārtas, pieslēguma vietas, barošanas bloki), vadi nedrīkst būt mudžeklī

IT speciālista kompetencē

16. Vai rezerves kopijas tiešām strādā?

Pierādījums:

- [ ] Atjaunošanas testa protokols ar datumu

17. Vai serveriem un kritiskajām iekārtām ir UPS (nepārtrauktās barošanas avots)?

Pierādījums:

- [ ] Foto vai vizuāla apskate, ka UPS tiešām ir
- [ ] UPS (vai akumulatoru) vecums – ražotāji rekomendē nepārsniegt 3–5 gadus

18. Kad pēdējoreiz veikta UPS akumulatoru pārbaude?

Pierādījums:

- [ ] Servisa akts, e-pasta apliecinājums ar pārbaudes datumu, izmantoto tehnisko rīku (ja ir) atskaite

5. Drošība

Vadītāja kompetencē

19. Vai kritiskajās vidēs (piem., e-pasts, failu koplietošana, CRM, grāmatvedības uzskaite u.c.) ir ieslēgta divu faktoru autorizācija (2FA)?

Kā pārbaudīt:

- [ ] Pieslēdzoties kritiskajām vidēm, parādās 2FA prasība
- [ ] Administrēšanas pārskatā IT var uzrādīt "2FA enabled users"

20. Vai viesiem tiek nodrošināts atsevišķs Wi-Fi?

Pierādījums:

- [ ] Pieejams atsevišķs Wi-Fi tīkls (SSID) "Guest", "Visitors" vai taml.

21. Vai darbinieku datoriem nav pielīmētas paroles?

Kā pārbaudīt:

- [ ] Vizuāla apskate (jebkura pielīmēta parole = sarkanais karogs)

22. Kiberdrošības apmācības.

Kā pārbaudīt:

- [ ] Apmācību žurnāls (Excel vai LMS)
- [ ] Darbinieku testa rezultāti (ja ir simulācijas)

IT speciālista kompetencē

23. Vai rezerves kopijas atrodas citā ēkā vai mākonī?

Pierādījums:

- [ ] Ekrānšāviņš vai konfigurācijas apraksts
- [ ] Ja ir tikai lokālā kopija = sarkanais karogs

24. Kāda ir paroļu politika (garums, obligātie simboli, mainīšanas biežums)?

Pierādījums:

- [ ] Ekrānšāviņš no Microsoft 365/AD Password Policy
- [ ] Apraksts

6. Attīstība

Vadītāja kompetencē

25. Vai ir 6–12 mēnešu IT attīstības plāns? Kas šobrīd ir lielākais IT risks uzņēmumā?

Kā pārbaudīt:

- [ ] PDF, PowerPoint vai Word dokuments ar prioritātēm un budžetu
- [ ] Plāns ir datēts

26. Vai IT funkcionē "ugunsgrēka režīmā"?

Kā pārbaudīt:

- [ ] Vai tiek saņemti ieteikumi, e-pasta rekomendācijas, uzlabojumi
- [ ] Novērtējums "0 ieteikumi pēdējo 6 mēnešu laikā" = problēma

27. Kāds ir šobrīd lielākais IT risks uzņēmumā? Un vai ir skaidrs kā to novērst, mazināt?

Kā pārbaudīt:

- [ ] Risku saraksts un to novērtējums
- [ ] Plāns risku novēršanai

Ātrais "sarkano karogu" saraksts

Problēma	Pierādījums
Haoss vados un iekārtās	Redzams foto, video vai apskates laikā
Neviens nezina, kam ir administratora tiesības	Nav darbinieku saraksta, kam ir administratora tiesības
Nav divu faktoru autorizācijas (2FA)	Sistēma ļauj pieslēgties tikai ar lietotājvārdu un paroli
Nav skaidrs, kur glabājas dati	Nav datu politikas dokumenta
Nav inventāra un tīkla shēmu	Nav dokumentācijas vai tā netiek atjaunota vismaz 12 mēnešu intervālā
Rezerves kopijas nav testētas	Nav atjaunošanas testa protokola
Domēns nav reģistrēts uz uzņēmuma vārda	Informācija no WHOIS (nic.lv vai citās vietnēs), domēna rēķinus maksā kāds cits, nevis uzņēmums
Netiek slēgtas pieejas darbiniekiem, ar kuriem izbeigtas darba attiecības	Nav "offboarding" pierakstu un saraksts ar aktīvajiem lietotājiem

Ja vismaz uz trim no šiem jautājumiem nav dokumentētu atbilžu,
IT pārvaldība uzņēmumā nav sakārtota – sistēma kaut kā funkcionē bez skaidras vīzijas un kontroles.

Pieteikties konsultācijai