ILUSTRATĪVS PĀRSKATS / VERSIJA 1.0

# Drošības izvērtējums: no secinājumiem līdz rīcībai.

Apskatiet, kā izskaidrojam konstatēto, nosakām prioritātes un plānojam turpmākās darbības. Šajā piemērā parādīta drošības izvērtējuma struktūra.

**Ilustratīvs piemērs**

Šis ir izdomāta uzņēmuma izvērtējuma paraugs ar ilustratīviem novērojumiem un ieteikumiem. Faktiskā pārskata saturs ir atkarīgs no saskaņotā izvērtējuma apjoma un pieejamās informācijas.

## Saprotams kopsavilkums vadībai.

Uzņēmums, kas izmanto IT ārpakalpojumu, vēlas izvērtēt trīs jomas: administratoru piekļuvi, drošības ierakstu pārbaudi un atbildību incidenta laikā. Paraugā katrā jomā konstatēts trūkums, ieteikta rīcība, norādīts atbildīgais un uzlabojuma pārbaudes veids.

## Šī piemēra apjoms

| | |
|---|---|
| **Piekļuve kontiem** | Administratora lomas autentifikācijas iestatījumi pakalpojumā, kas atbalsta daudzfaktoru autentifikāciju. |
| **Drošības ierakstu pārbaude** | Dokumentētā kārtība drošības ierakstu pārbaudei un konstatētā nodošanai atbildīgajiem. |
| **Saziņa incidenta laikā** | Rīcības plānā norādītais koordinators, viņa aizvietotājs un saziņas kārtība. |

Piemērā izvērtēti iestatījumi un darba kārtība. Konfigurācijas izmaiņām, ielaušanās testiem un pastāvīgai uzraudzībai nepieciešams atsevišķi saskaņots darba apjoms.

Ilustratīvie konstatējumi

SR-01 / PIEKĻUVE KONTIEM

# Administratora kontam nav ieslēgta daudzfaktoru autentifikācija

| Augsta prioritāte | Ieteiktā darbība |
|---|---|

| | |
|---|---|
| **Kas konstatēts** | Pieslēdzoties parauga administratora kontam, pietiek ar paroli, lai gan pakalpojums atbalsta daudzfaktoru autentifikāciju. |
| **Paraugā izmantotā informācija** | Parauga piekļuves politika: administratora lomai nav ieslēgta daudzfaktoru autentifikācijas prasība. |
| **Kāpēc tas ir svarīgi** | Ar nozagtu paroli varētu pietikt, lai piekļūtu administratora funkcijām. |
| **Ieteicamā rīcība** | Saskaņot izmaiņas ar IT, noteikt obligātu daudzfaktoru autentifikāciju administratoru kontiem izvērtētajā pakalpojumā un pirms ieviešanas pārbaudīt piekļuves atjaunošanas kārtību. |
| **Ieteiktais atbildīgais** | IT pakalpojumu sniedzējs ievieš izmaiņas; uzņēmuma atbildīgā persona tās apstiprina. |
| **Kā pārbaudīt uzlabojumu** | Izmantojot saskaņotu testa kontu, pārbaudīt, vai tiek prasīta daudzfaktoru autentifikācija un darbojas saskaņotā piekļuves atjaunošanas kārtība. |

Saistītās vadlīnijas

CIS Control 6: Access Control Management

Ilustratīvie konstatējumi

SR-02 / DROŠĪBAS IERAKSTI

# Nav noteikts atbildīgais par drošības ierakstu pārbaudi

| Vidēja prioritāte | Ieteiktā darbība |
|---|---|

| | |
|---|---|
| **Kas konstatēts** | Parauga IT vidē drošības ieraksti tiek uzkrāti, taču darba kārtībā nav noteikts, kurš tos pārbauda. |
| **Paraugā izmantotā informācija** | Parauga uzraudzības kārtība: nav norādīts pārbaudītājs, pārbaudes biežums vai persona, kurai nodot konstatēto. |
| **Kāpēc tas ir svarīgi** | Būtiska aktivitāte var palikt nepārbaudīta, un komandai var nebūt skaidrs, kurš lemj par turpmāko rīcību. |
| **Ieteicamā rīcība** | Noteikt atbildīgo, pārbaudāmos ierakstus un brīdinājumus, kā arī saskaņot pārbaudes biežumu un saziņas kontaktus. |
| **Ieteiktais atbildīgais** | Uzņēmuma atbildīgā persona saskaņo pienākumus ar IT pakalpojumu sniedzēju un drošības partneri. |
| **Kā pārbaudīt uzlabojumu** | Izveidot nekaitīgu, iepriekš saskaņotu testa notikumu un pārbaudīt, vai tas tiek reģistrēts, izvērtēts un nodots atbildīgajiem atbilstoši noteiktajai kārtībai. |

Saistītās vadlīnijas

CIS Control 8: Audit Log Management

Ilustratīvie konstatējumi

SR-03 / GATAVĪBA INCIDENTIEM

# Incidenta plānā norādīts tikai viens IT kontakts

| Vidēja prioritāte | Ieteiktā darbība |
|---|---|

| | |
|---|---|
| **Kas konstatēts** | Parauga rīcības plānā norādīts ierastais IT kontakts, bet nav paredzēts aizvietotājs vai alternatīvs saziņas veids. |
| **Paraugā izmantotā informācija** | Parauga kontaktu sarakstā norādīta viena IT kontaktpersona. Aizvietošanas kārtība nav aprakstīta. |
| **Kāpēc tas ir svarīgi** | Ja kontaktpersona nav sasniedzama, var aizkavēties lēmumu pieņemšana un iespējamā incidenta ierobežošana. |
| **Ieteicamā rīcība** | Norīkot koordinatoru un viņa aizvietotāju, vienoties par alternatīvu saziņas kanālu un precizēt, kurš drīkst apstiprināt reaģēšanas darbības. |
| **Ieteiktais atbildīgais** | Vadība un IT pakalpojumu sniedzējs vienojas par lomām, kontaktiem un lēmumu pieņemšanas pilnvarām. |
| **Kā pārbaudīt uzlabojumu** | Izspēlēt īsu situāciju, kurā ierastais kontakts nav sasniedzams. Fiksēt neatbildētos jautājumus un noteikt atbildīgos par turpmākajiem darbiem. |

Saistītās vadlīnijas

CIS Control 17: Incident Response Management

Turpmākā rīcība un avoti

# No secinājumiem līdz saskaņotiem darbiem.

| | |
|---|---|
| **Apstiprināt prioritātes** | Pārrunāt secinājumus ar vadību un IT, ņemot vērā ietekmi uz uzņēmumu un darbu savstarpējo saistību. |
| **Saskaņot izmaiņas** | Pirms ieviešanas noteikt darbu apjomu, pilnvaras, atbildību un izmaksas. |
| **Pārbaudīt un dokumentēt** | Pārbaudīt veiktās izmaiņas un fiksēt rezultātu, atlikušos riskus un turpmākos darbus. |

Secinājumus varat izmantot kopā ar savu IT pakalpojumu sniedzēju. Ieviešanas atbalstu un pastāvīgu uzraudzību saskaņojam atsevišķi.

## Piemērā izmantotās vadlīnijas

Ieteikumi saistīti ar tālāk norādītajām CIS kontrolēm. Paraugs aptver atsevišķas tēmas, nevis pilnu kontroļu izvērtējumu.

**CIS Control 6: Access Control Management**
https://cas.docs.cisecurity.org/en/latest/source/Controls6/

**CIS Control 8: Audit Log Management**
https://cas.docs.cisecurity.org/en/latest/source/Controls8/

**CIS Control 17: Incident Response Management**
https://cas.docs.cisecurity.org/en/latest/source/Controls17/

Parauga prioritātes noteiktas atbilstoši izdomātajai situācijai. Faktiskā izvērtējumā tās nosaka pēc informācijas pārbaudes, ņemot vērā ietekmi uz uzņēmumu.

**Pārrunāt izvērtējumu**