primend

CISOaaS – Informācijas drošības līmeņa novērtēšana un attīstība

CISO kā pakalpojums | Uzņēmuma informācijas drošības līmeņa novērtēšana un uzlabošana

Kāpēc daudzos mazos un vidējos uzņēmumos, un pat dažos lielajos uzņēmumos nav galvenā informācijas drošības speciālista (CISO) uz pilnu slodzi?

- Ikdienas darba apjoms nav tik liels.
- Šāda eksperta nodarbināšana uz pilnu slodzi nav rentabla.

Kā Tavam uzņēmumam var palīdzēt Primend galvenais informācijas drošības speciālists?

- Sniedzot norādījumus, kā aizsargāt uzņēmumu no dažādiem kiberdraudiem.
- Palīdzot nodrošināt atbilstību noteikumiem un standartiem.
- Atbalstot uzņēmumu informācijas drošības pasākumu uzlabošanā.

Primend informācijas drošības speciālists vai nu pilda šī amata lomu uzņēmumā kā ārējs eksperts vai arī konsultē par informācijas drošību atbildīgo uzņēmuma štata darbinieku, sniedzot nepieciešamās zināšanas un pieredzi.

Ar ko sākt informācijas drošības līmeņa novērtēšanu?

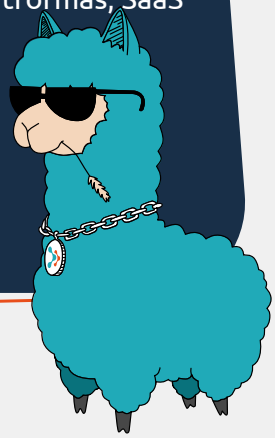
Pirmkārt, ir nepieciešams iegūt visaptverošu pārskatu par dažādām uzņēmumā izmantotajām informācijas sistēmām un lietotnēm, kā arī lomām, procesiem un citām tehnoloģijām, saskaņā ar uzņēmuma biznesa stratēģiju.

Veiktā novērtējuma rezultātā tiek sagatavots kopsavilkums, identificējot nākamos veicamos soļus un saskaņojot prioritātes, kas uzņēmumam nodrošinās maksimālos ieguvumus.

Drošības līmeņa novērtējuma posmi:

- Sarunas ar uzņēmuma vadību un procesā iesaistītajiem darbiniekiem.
- Sarunas ar nozīmīgiem partneriem, IT arhitektūras analīze un integrācija.
- Datortīklu topoloģijas analīze – novērtējot, vai tīkli ir atbilstoši aizsargāti, segmentēti utt.
- IT infrastruktūras vispārīga analīze.
- Datu atjaunošanas plānu un satura dublēšanas politikas analīze, kā arī biznesa risku novērtēšana, balstoties uz RPO/RTO.
- Lietojumprogrammu analīze (iekšējās izstrādes, mājas lapas, e-komercijas platformas, SaaS pakalpojumi).
- Kopsavilkuma ziņojuma sastādīšana un attīstības priekšlikumu izstrāde.

Atkarībā no uzņēmuma lieluma un sarežģītības šis process parasti aizņem apmēram 1-3 mēnešus. Efektīva gala rezultāta saņemšanai ļoti būtiska ir sekmīga abu pušu sadarbība.



Informācijas drošības līmeņa novērtējuma atskaite un kopsavilkums atvieglo lēmuma pieņemšanas procesu, ļaujot identificēt kritiskos aspektus, kuru risināmi nekavējoties, un jomas, kurās uzlabojumus var veikt pakāpeniski.

Potenciālās nākamās darbības:

- Informācijas drošības stratēģiju, mērķu un metrikas noteikšana, pamatojoties uz uzņēmuma biznesa stratēģiju.
- Informācijas drošības risku analīzes veikšana.
- Nepieciešamo informācijas drošības risinājumu plānošana, ieviešana un pārvaldība.
- Informācijas drošības politiku, noteikumu un vadlīniju izstrāde un uzturēšana.
- Nepārtrauktas informācijas drošības uzlabošanas plāna izstrāde un īstenošana.
- Uzņēmuma darbinieku izpratnes veidošana par informācijas drošību, kā arī apmācību nodrošināšana.

Fināla versija veicamo uzdevumu sarakstam vienmēr ir atkarīga no specifiskajām uzņēmuma vēlmēm un vajadzībām, un vienošanās par to notiek pakalpojuma pasūtīšanas procesā. Galvenā informācijas drošības speciālista pakalpojumus var iegādāties gan uz konkrēta projekta termiņu, gan kā ikmēneša pakalpojumu.

Sazinies ar mums
Dace Rostoka | IT biznesa konsultante
dace.rostoka@primend.com

primend

bm certification
ISO 9001
ISO 27001
System certification