



NIS2 atbilstības ceļvedis un nepieciešamās kiberdrošības ieviešanas ceļa karte

GATAVĪBA NIS2 DIREKTĪVAI un KIBERDROŠĪBAS LIKUMAM: MAZĀK RAIŽU, VAIRĀK DROŠĪBAS!

60 IZAICINĀJUMI

IEGUVUMI

Laika trūkums un stress

Nodrošināt atbilstību NIS2 direktīvas prasībām var būt laikietilpīgs uzdevums. Satraukumu rada NIS2 iekļautie sodi un sankcijas vadībai.



Pārliecības un zināšanu trūkums

Pārliecības trūkums, lai pilnībā izprastu savas tehnoloģiskās un kiberdrošības situācijas atbilstību NIS2 prasībām.



Neskaidri soļi un izmaksas

Neskaidrība par to, kādas izmaiņas un finanšu līdzekļi ir nepieciešami, lai nodrošinātu atbilstību NIS2 prasībām. Risks veikt investīcijas neefektīvos, novecojušos vai dārgi uzturamos rīkos.



Vairāk laika un mazāk stresa

Procesu racionalizēšana atbilstoši kiberdrošības labākajai praksei un ekspertu atbalsta sniegšana, lai optimizētu procesu uzlabošanu. Atbilstības savlaicīga ieviešana mazina sodu riskus.

Skaidra ceļa karte un izpratne

Organizācijas infrastruktūras atbilstības izvērtēšana NIS2 prasībām. Izmantojot esošo, nokļūt pie atbilstības ar jums maksimāli pielāgotām nepieciešamajām izmaiņām.

Optimālas izmaksas un investīciju caurskatāmība

Ieteikumi par nepieciešamajām darbībām, ieguldījumiem tehnoloģijās un ar to saistītajām izmaksām, lai efektīvi un, saglabājot izmaksu caurskatāmību, nodrošinātu atbilstību vismaz minimālajām NIS2 prasībām.

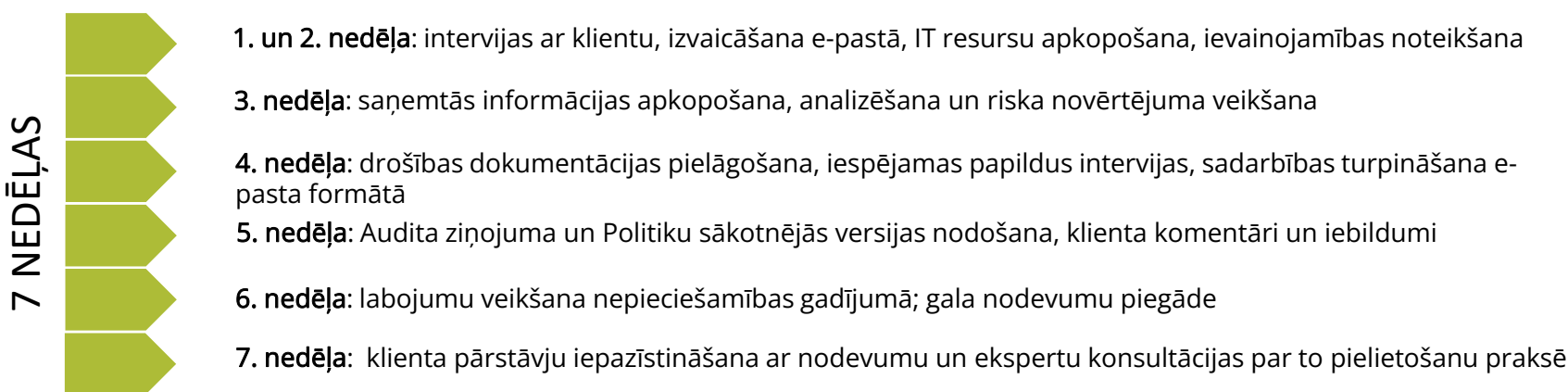
MŪSU RISINĀJUMS

Mūsu pakalpojums "NIS2 atbilstības ceļvedis un kiberdrošības riska novērtējums" pamatojas uz Nacionālā Kiberdrošības likuma, NIS2 direktīvas un Zero Trust ietvara prasībām un rekomendācijām, kas ietver intervijas un automatizētu rīku izmantošanu, lai:

- ātri un efektīvi ieviestu mūsdienu kiberdraudiem atbilstošus risinājumus;
- samazinātu jums stresu par atbilstības NIS2 un partneru prasībām nodrošināšanu;
- piedāvātu skaidru nākotnes ceļa karti kiberdrošas IT infrastruktūras izveidei ar minimāliem ieguldījumiem.

Mēs ne tikai palīdzēsim nodrošināt atbilstību NIS2 direktīvai dokumentācijas līmenī, bet arī veicam visaptverošu jūsu tehniskās infrastruktūras kiberdrošības stāvokļa novērtējumu.

PROJEKTA GRAFIKS ~ 2 mēneši



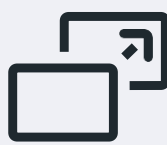
JŪSU ORGANIZĀCIJAS IT UN KIBERDROŠĪBAS PĀRVALDĪBAS PROCESI TIKS VIENLĪDZĪGI IZVĒRTĒTI 5 JOMĀS



Identitātes pārvaldība



Ierīces



Tīkls / vide



Lietojumprogrammas



Datu pārvaldība

NODEVUMI

- 1** Audita ziņojums. Kopsavilkums. Organizācijas pašreizējās kiberdrošības situācijas augsta līmeņa izvērtējums. Saraksts ar svarīgākajiem uzdevumiem, kas jāizpilda, lai nodrošinātu atbilstību minimālajām NIS2 direktīvas prasībām.
- 2** Audita ziņojums. Konkrētas rekomendācijas noteiktajās jomās, lai organizācijas varētu koriģēt savu drošības situāciju vienmērīgi visos IT pārvaldības un tehnoloģiju virzienos:
 - identitātes;
 - ierīces;
 - infrastruktūra;
 - aplikācijas un programmatūra;
 - dati.
- 3** Audita ziņojums. Saraksts ar rekomendācijām par nepieciešamajām izmaiņām IT drošības politikā un IT pārvaldības procedūrās, lai esošos procesus pielāgotu labākajai kiberdrošības praksei, Zero Trust modeļa ieteikumiem un NIS2 direktīvas prasībām.
- 4** Ievainojamību saraksts iekštīklā un ārtīklā. Infrastruktūras ievainojamības risku noteikšana izmantojot nozares standartu — Nessus Professional rīku.
- 5** Papildus politikas dokumenti. Nepieciešamības gadījumā, nodrošināsim jums trūkstošās politikas sagataves.
- 6** Kiberdrošības izpratnes apmācība darbiniekiem — apmācību ierakstā vai tiešsaistes platformā (Zoom, Teams)
- 7** Ekspertu konsultācijas. Tehniskas diskusijas klātienē vai tiešsaistē ar mūsu ekspertiem par secinājumiem un stratēģiju atbilstības nodrošināšanai.
- 8** Prezentācija (tiešsaistē) vadībai.