

CISOaaS – informacijos saugumo brandos lygio įvertinimas ir tobulinimas

CISO-as-a-Service – organizacijos informacijos saugumo brandos lygio vertinimas ir tobulinimas



Kodėl daugelis mažų, vidutinių ir net kai kurios didesnės įmonės neturi vyriausiojo informacijos saugos pareigūno (CISO), dirbančio pilnu etatu?

- Nėra pakankamai darbo, kurį būtų galima dirbti visą darbo dieną.
- Įdarbinti ekspertą pilnu etatu gali būti ekonomiškai neefektyvu.

Kuo „Primend“ vyriausiojo informacijos saugos pareigūno paslauga gali jums padėti?

- Konsultacijos, kaip apsaugoti įmonę nuo įvairių kibernetinių grėsmių.
- Pagalba prisitaikant prie privalomų taisyklių ir standartų.
- Pagalba įmonei žengiant konkrečius žingsnius informacijos saugumui užtikrinti.

„Primend“, kaip iš šalies samdomas informacijos saugos pareigūnas (angl., CISO-as-a-Service) atlieka įmonėje vyriausiojo informacijos saugos pareigūno pareigas, jei įmonė tokio darbuotojo neturi, arba padeda už informacijos saugą atsakingam įmonės darbuotojui atlikti savo pareigas, suteikdamas jam reikiamų žinių ir patirties.

Nuo ko pradėti informacijos saugumo brandos vertinimą?

Pirma, būtina išsamiai peržiūrėti įvairias informacines sistemas ir programas, vaidmenis, procesus ir kitas naudojamas technologijas, pagrįstas įmonės verslo strategija.

Atlikus brandos vertinimą, parengiama santrauka, kurioje aprašyti tolesni žingsniai ir prioritetai, siekiant didžiausios naudos organizacijai.

Brandos vertinimo etapai:

- pokalbiai su organizacijos vadovybe ir svarbiausiais darbuotojais;
- pokalbiai su svarbiais partneriais, IT architektūros analizė ir integracijos;
- kompiuterių tinklo topologijos analizė – įvertinama, ar tinklai tinkamai apsaugoti, segmentuoti ir pan.;
- bendra IT infrastruktūros analizė;
- atkūrimo planų ir atsarginių kopijų politikos analizė, verslo rizikos įvertinimas, susijęs su (RPO) ir (RTO);
- taikomųjų programų (vidinių kūrinių, interneto svetainių, e. prekybos platformų, SaaS paslaugų) analizė;
- apibendrinamosios ataskaitos parengimas kartu su plėtros pasiūlymais.

Priklausomai nuo organizacijos dydžio ir kompleksiško, šis procesas paprastai trunka 1-3 mėnesius ir, žinoma, reikalauja sklandaus organizacijos bendradarbiavimo.



Remiantis informacijos saugumo brandos įvertinimo ataskaita, galima nuspręsti, kokius veiksmus ir pasiūlymus būtina atlikti nedelsiant, o kokius galima išdėstyti ilgesniu laikotarpiu.

Galimi tolimesni veiksmai:

- informacijos saugumo strategijų, tikslų ir rodiklių nustatymas, remiantis įmonės verslo strategija;
- informacijos saugumo srities rizikos analizė;
- būtinų informacijos saugumo sprendimų planavimas, diegimas ir valdymas;
- informacijos saugumo politikos, taisyklių ir gairių kūrimas ir priežiūra;
- nuolatinio informacijos saugumo tobulinimo plano kūrimas ir įgyvendinimas;
- įmonės darbuotojų informuotumo apie informacijos saugą didinimas ir mokymai.

Galutinis užduočių sąrašas visada priklauso nuo konkrečių įmonės norų ir poreikių ir gali būti suderinamas paslaugų užsakymo metu. Vyriausiojo informacijos saugos pareigūno paslaugą galima užsakyti kaip projektą arba kaip mėnesinę paslaugą.

Daugiau informacijos:

Tadas Jankauskas | Pardavimo vadovas
tadas.jankauskas@primend.com

