TIS2 direktyva

Tinklo ir informacinių sistemų saugumo antroji direktyva (TIS2) įsigaliojo 2023 m. sausio 16 d. **TIS2 subjektai klasifikuojami pagal jų svarbą ir skirstomi į dvi kategorijas: kritinės svarbos ir svarbius subjektus**, kuriems bus taikomi skirtingi priežiūros režimai.

Kritinės svarbos sektoriai

- Energetika
- Transportas
- Bankų paslaugos
- Sveikatos priežiūros paslaugų tiekėjai
- Viešojo administravimo įmonės
- Informacinių paslaugų tiekėjai
- Skaitmeninės infrastruktūros paslaugų tiekėjai
- Finansų rinkos infrastuktūra
- Geriamo vandens tiekėjai
- Nuotekų valymo įmonės
- Kosminių technologijų įmonės

Svarbūs sektoriai

- Pašto ir kurjerių paslaugos
- Atliekų tvarkymas
- Cheminių medžiagų gamyba ir tiekimas
- Maisto produktų gamyba ir tiekimas
- Gamyba (elektronikos ir kt)
- Skaitmeninių paslaugų tiekimas
- Tyrimai

Kritinės svarbos įmonėms, siekiant užtikrinti veiklos tęstinumą, bus taikomas reikalavimas imtis techninių ir praktinių priemonių, kad būtų laikomasi TIS2 reikalavimų, **įskaitant reagavimą į incidentus, tiekimo grandinės saugumą, šifravimo naudojimą, pažeidžiamumų atskleidimą, tinkamą rizikos analizę, kibernetinio saugumo strategijų testavimą ir auditą bei krizių valdymo planavimą.** Kibernetinio incidento atveju šie subjektai taip pat privalės per 24 valandas pateikti pirminį pranešimą, o per 72 valandas - išsamesnę informaciją. TIS2 taip pat nustatomos baudos už reikalavimų nesilaikymą, įskaitant sertifikavimo sustabdymą ir vadovaujančias pareigas užimantiems asmenims tiesioginę atsakomybę pagal nacionalinius įstatymus.

Iš paminėtų pramonės sektorių organizacijų bus tikimasi, kad vadovybė bus atsakinga ir atskaitinga už:

- kibernetinio saugumo rizikos valdymo priemonių patvirtinimą C lygmeniu;
- rizikos valdymo priemonių įgyvendinimo savalaikę priežiūrą;
- specialių, reguliarių mokymų ir informuotumo didinimo, siekiant įgyti kibernetinio atsparumo gebėjimus ir įvertinti susijusias rizikas organizacijai, užtikrinimą;
- bet kokį organizacijos neatitikimą reikalavimams.

Pareiga informuoti ir pareiga prižiūrėti.
Visos organizacijos, kurioms taikoma TIS2 - kritinės svarbos ir svarbios, turės pradėti laikytis savo pareigos prižiūrėti infrastruktūrą. Abiejų išskirtų grupių pareigos ir atsakomybės yra vienodos; pavyzdžiui, kritinės svarbos ir svarbių subjektų valdymo organų nariai privalo išklausyti mokymus ir imtis atitinkamų techninių, praktinių ir organizacinių priemonių, norėdami suvaldyti kylančią tinklo ir informacinių sistemų saugumo riziką. Taip pat **bus reikalaujama, kad kritinės svarbos organizacijos turėtų proaktyvią pasirengimo sistemą**, kuri leistų įvertinti netinkamo valdymo poveikį net ir neįvykus incidentui. **Antrosios kategorijos - svarbių organizacijų - atitikties tikimasi reaktyviai**. Tai reiškia, kad šių organizacijų atitiktis įstatymams ir reikalavimams bus tikrinama tik įvykus incidentui. Jei atliekami veiksmai ir reikalavimų laikymasis bus įvertinti kaip nepakankami, abiejų kategorijų subjektams bus taikomos tos pačios sankcijos.

Būtinos priemonės
TIS2 direktyvoje išvardintas būtiniausių priemonių rinkinys, įskaitant rizikos analizės atlikimą ir informacinių sistemų saugumą, incidentų ir krizių valdymą, veiklos tęstinumo užtikrinimą, tiekimo grandinės saugumą, tinklo ir informacinių sistemų pirkimą ir kūrimą bei priežiūros saugumo politikos nustatymą. Taip pat rizikos valdymo priemonių veiksmingumo vertinimo politiką ir procedūras bei kriptografijos ir šifravimo naudojimą. Kritinės svarbos bei svarbūs subjektai taip pat turėtų taikyti įvairią bazinę kibernetinės saugos praktiką, pavyzdžiui, nulinio pasitikėjimo principus, programinės įrangos atnaujinimus, įrenginių konfigūraciją, tinklo segmentavimą, tapatybės ir prieigos valdymą ar naudotojų sąmoningumą, organizuoti darbuotojų mokymus ir didinti informuotumą apie kibernetines grėsmes, sukčiavimo ar socialinės inžinerijos metodus.

Pranešimai
TIS2 direktyvoje pranešimui apie kibernetines atakas numatytas „dviejų etapų metodas“. Pirmuoju pranešimu siekiama apriboti galimą incidento plitimą ir sudaryti sąlygas subjektams kreiptis pagalbos. Jis yra privalomas - reikalingas atsakingų institucijų informavimui apie įvykusį incidentą. Antrasis pranešimas turi būti daug išsamesnis. Jo paskirtis - susipažinti su sėkmingos atakos priežastimis ir pasimokyti iš ankstesnių klaidų.
1. Pirmasis pranešimas. Pirmasis pranešimas, kuriame, jei įmanoma, nurodoma, ar incidentas įvyko dėl neteisėtos ar piktavališkos veikos, turi būti nedelsiant pateiktas kompetentingai institucijai arba atitinkamam nacionaliniam CISR visais atvejais per 24 valandas nuo sužinojimo apie incidentą. Ši nuostata apibrėžia griežtai būtiną informaciją. Per 72 valandas nuo pirmojo pranešimo pateikimo nukentėjęs subjektas taip pat turi pateikti atnaujintą informaciją ir pirminį vertinimą, kuriame išsamiau aprašoma ataka ir taikomos priemonės. Subjektui paprašius, galima gauti gaires dėl galimų poveikio mažinimo priemonių įgyvendinimo ir, jei reikia, papildomą techninę pagalbą. Kriminalinio incidento atveju paveiktas subjektas taip pat gauna gaires, kaip pranešti apie incidentą teisėsaugos institucijoms.
2. Antras pranešimas. Per vieną mėnesį nuo pirmo pranešimo pateikimo turi būti pateikta galutinė ataskaita, kurioje: a) išsamiai aprašytas incidentas, jo rimtumas ir pasekmės, b) grėsmės rūšis arba priežastis, galėjusi sukelti incidentą, ir c) taikytos ir taikomos poveikio mažinimo priemonės.

Vykdymo užtikrinimo priemonės

Kompetentingos institucijos turės įgaliojimus abiejų tipų subjektams taikyti patikrinimus vietoje ir ne vietoje vykdomą ex-post priežiūrą, kurią atlieka kvalifikuoti specialistai, tikslinį saugumo auditą, saugumo skenavimą, prašymus leisti susipažinti su duomenimis, dokumentais ir informacija, taip pat prašymus pateikti kibernetinio saugumo politikos įgyvendinimo įrodymus, pavyzdžiui, kvalifikuoto auditoriaus atlikto saugumo audito rezultatus ir atitinkamus pagrindžiančius įrodymus. Nustačiusios pažeidimą kompetentingos institucijos gali pa-sinaudoti tolesniais vykdymo užtikrinimo įgaliojimais, pavyzdžiui, įspėti, pateikti instrukcijas, duoti nurodymus subjektams nutraukti veiklą, kuria pažeidžiama direktyva, nurodyti subjektams informuoti fizinius ar juridinius asmenis, kuriems gali turėti įtakos netinkamas elgesys, arba net paviešinti informaciją. Jei šios priemonės nepadeda ištaisyti padėties, kompetentingos institucijos gali laikinai sustabdyti subjekto veiklą ir organizacijos vadovo, vykdančio vyriausiojo vadovo arba atstovaujamojo teisinio lygmens pareigas, veiklą.

Sankcijos

TIS2 direktyva nustatoma nuosekli sankcijų sistema visoje Europos Sąjungoje, sudarant minimalų administracinių sankcijų už kibernetinio saugumo rizikos valdymo ir pranešimų teikimo įpareigojimų pažeidimus sąrašą. Šios sankcijos apima privalomus nurodymus, saugumo audito rekomendacijų įgyvendinimą, saugumo priemonių suderinimą su TIS2 reikalavimais ir administracines baudas. Kalbant apie administracines nuobaudas, naujojoje Tinklų ir informacinių sistemų saugumo direktyvoje išskiriami kritinės svarbos ir svarbūs subjektai.

Valstybės narės turi suteikti atitinkamoms institucijoms galimybę skirti dideles baudas. TIS2 direktyvoje reikalaujama, kad valstybės narės numatytų tam tikro dydžio administracines baudas, visų pirma ne mažesnes kaip 10 000 000 EUR arba 2 % visos praėjusių finansinių metų pasaulinės metinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė. Kalbant apie svarbius subjektus, TIS2 direktyvoje reikalaujama, kad valstybės narės numatytų ne mažesnę kaip 7 000 000 EUR baudą arba ne mažesnę kaip 1,4 % visos praėjusių finansinių metų pasaulinės metinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė.

Naudodamosi vykdymo užtikrinimo įgaliojimais, kompetentingos institucijos turėtų tinkamai atsižvelgti į konkrečias kiekvieno atvejo aplinkybes, pavyzdžiui, pažeidimo pobūdį, sunkumą ir trukmę, padarytą žalą ar patirtus nuostolius, taip pat į tyčinį ar neatsargų pažeidimo pobūdį.