NIS2 direktīvas atbilstības ietekme uz uzņēmuma konkurētspēju 1/19/25

Direktore IT konsultāciju nodaļā, PwC Latvija
Dr.dat. Baiba Apine

NIS2 (Network and Information Security Directive) ir Eiropas Savienības direktīva, kuras mērķis ir stiprināt kiberdrošību visā ES, īpaši attiecībā uz kritisko infrastruktūru un būtiskiem pakalpojumiem. Latvijā šī direktīva ir transponēta nacionālajā likumdošanā, pieņemot Nacionālo kiberdrošības likumu (NCL). Šobrīd uzņēmumiem būtu jābūt skaidrībai par savu statusu (ir vai nav NCL subjekts) un jāreģistrējas līdz 2025. gada 1. aprīlim Nacionālajā kiberdrošības centrā (NKC). Organizācijām ir jāieceļ kiberdrošības vadītājs un jāiesniedz pirmais pašvērtējuma ziņojums līdz šī gada 1. oktobrim un jāsāk ziņot par kiberdrošības incidentiem no šī gada 1. jūlija.

PwC rīkotajā Digitālās uzticamības – 2025 aptaujā piedalījās vairāk nekā 4000 uzņēmumu un informācijas tehnoloģiju vadītāju no 77 valstīm, akcentējot kiberdrošību. Tikai 2% vadītāju uzskatīja, ka viņu uzņēmumi ir veikuši pietiekamus kibernoturības pasākumus. Mazāk nekā 50% respondentu norādīja, ka viņu kiberdrošības vadītāji ir iesaistīti stratēģiskajā plānošanā un uzņēmuma vadības ziņojumu sagatavošanā. Tas skaidri norāda, ka kiberdrošībā praksē runāšanas ir vairāk nekā darīšanas.

NIS2 direktīvas mērķis ir ar likuma spēku likt aptuveni 100 000 uzņēmumu ES stiprināt kibernoturību, stiprināt kiberdrošības vadītāja lomu uzņēmumā un mazināt draudus. Latvijā NCL attiektos uz aptuveni 1500 uzņēmumiem, šobrīd reģistrācija NKC uzsākta aptuveni 600 uzņēmumiem.

NIS2 un NCL ieviešana noteikti nav solis birokrātijas mazināšanas virzienā. Prasību ieviešana palielinās administratīvo slogu uzņēmumiem, jo būs nepieciešama kiberrisku politika, procedūras incidentu identificēšanai un ziņošanai, kā arī nepārtrauktas darbības nodrošināšanas plāns. Tomēr likums liek mainīt uzņēmumu vadītāju attieksmi pret kiberdrošību. NIS2 prasību realizācija uzlabos kibernoturību, tomēr negarantēs pilnīgu aizsardzību pret incidentiem. Piemēram, incidentu reakcijas un darbības nepārtrauktības plāni palīdz uzņēmumiem ātri atgūties no kiberdraudiem. Uzņēmumi būs labāk pozicionēti partnerībai un piekļuvei ES tirgum, uzlabojot to sistēmu aizsardzību, samazinot dārgu datu noplūžu un dīkstāves risku, kā arī veicinot klientu lojalitāti.

Atbilstība NIS2 direktīvas prasībām ir būtisks solis uzņēmumu kiberdrošības stiprināšanā, un tās ieviešana prasa visu iesaistīto pušu aktīvu līdzdalību. Lai gan administratīvais slogs var radīt grūtības, uzņēmumi, kas būs veiksmīgi īstenojuši NIS2 direktīvas prasības, būs labāk sagatavoti nākotnes kiberdraudiem un spēs saglabāt konkurētspēju ES tirgū.