Asigurarile Cyber devin un instrument-cheie de conformare pentru companii, protectie financiara si rezilienta (broker)

Asigurarile Cyber s-au transformat dintr-o optiune de protectie într-o componenta critica a strategiei de gestionare a riscului si de continuitate a afacerii, în conditiile în care nicio organizatie nu este imuna la riscurile cibernetice, sustin reprezentantii Leader Team Broker.

Potrivit unui comunicat remis spre publicare, Directiva NIS2 transforma securitatea cibernetica într-o obligatie strategica.

"Asigurarile Cyber devin un instrument-cheie de conformare, protectie financiara si rezilienta. Într-o economie aproape complet digitalizata, în care companiile din toate sectoarele beneficiaza de oportunitati extinse de dezvoltare, discutia despre riscurile cibernetice si vulnerabilitatile asociate este mai relevanta ca oricând. În prezent, nicio organizatie nu este imuna la riscurile cibernetice, iar asigurarile - si în special politele Cyber - s-au transformat dintr-o optiune de protectie într-o componenta critica a strategiei de gestionare a riscului si de continuitate a afacerii.În contextul în care un singur incident poate afecta semnificativ activitatea sau reputatia unei organizatii, nevoia unor masuri de protectie avansate este imperativa", precizeaza reprezentantii brokerului corporate de asigurari din România si Europa.

Conform sursei citate, în completarea solutiilor tehnice de securitate informatica vin asigurarile, care nu mai sunt percepute ca un cost suplimentar, ci ca un element esential, parte a strategiei de dezvoltare a oricarei companii, indiferent de domeniul în care activeaza.

La nivelul UE, Directiv a NIS2 impune companiilor din sectoarele esentiale noi cerinte, care transforma securitatea digitala dintr-o optiune tehnologica într-o obligatie strategica de business, iar asigurarile Cyber devin un instrument esential de conformare, protectie financiara si rezilienta operationala, se arata în comunicat.

În cadrul conferintei-dezbatere "Cyber Insurance & NIS2 - Reglementare, risc si raspundere în era digitala", organizate de Leader Team Broker de asigurare au participat experti în securitate cibernetica si asigurari, din România si din strainatate, iar discutiile s-au concentrat pe explicarea noilor cerinte legislative.

Totodata, discutiile au vizat si identificarea de solutii concrete pentru companiile românesti afectate de noua Directiva NIS2, punând în prim-plan modul în care asigurarile Cyber pot deveni un pilon strategic de protectie si rezilienta în era digitala.

La finalul anului 2024, România a facut un pas major în directia consolidarii securitatii cibernetice, prin transpunerea Directivei europene NIS2 în legislatia nationala, mii de companii din domenii strategice precum energie, transporturi, sanatate, infrastructura digitala, productie industriala, apa, servicii IT, administratie publica sau telecomunicatii intrând sub incidenta noilor reguli, se mai precizeaza în comunicat.

"Într-o economie tot mai digitalizata, securitatea cibernetica nu mai este o optiune, ci o necesitate strategica. Vorbim despre o noua cultura organizationala în care securitatea IT devine parte integranta din strategia de afaceri. Directiva NIS2 nu este doar o lege, este o schimbare de paradigma, care ne reaminteste ca protejarea infrastructurii digitale si a datelor este esentiala pentru continuitatea oricarei afaceri. În acest context, si asigurarile Cyber au evoluat firesc si s-au transformat din simple instrumente financiare în solutii complete de management al riscului. Ele ofera nu doar despagubire, ci si sprijin concret în momentul producerii unui incident cibernetic: acces la specialisti IT, juridici, specialisti în comunicare si la planuri rapide de raspuns rapide. Prin produsele

dezvoltate de Leader Team Broker, ajutam companiile sa fie mai reziliente, mai pregatite si mai protejate. Iar investitia într-o polita Cyber nu este doar o masura de conformare cu NIS2, ci un pas esential catre siguranta, încredere si stabilitate pe termen lung", a declarat Alexandra Elena Durbaca, CEO Leader Team Insurance Broker, citat în comunicat.

Conform sursei citate, o singura bresa de securitate poate bloca o companie zile întregi, iar costurile de refacere, notificare, consultanta, PR si eventualele despagubiri pot depasi usor câteva sute de mii de euro.

În lipsa unei asigurari, o afacere poate ajunge în colaps. În context, asigurarea Cyber nu mai este privita ca un produs de nisa, 2025 marcând momentul în care aceasta polita specializata devine un instrument de supravietuire corporativa, se mai precizeaza în document.

"Impactul financiar, operational si reputational al unui singur incident poate fi major - de la atacuri ransomware care blocheaza activitatea zile întregi, pâna la brese de securitate care expun informatii sensibile si atrag sanctiuni din partea autoritatilor. Astazi, companiile au la dispozitie o gama variata de solutii de asigurare cibernetica, menite sa le protejeze împotriva consecintelor financiare si operationale ale unui incident de securitate. O polita Cyber completa acopera, de regula, costurile de raspuns la incidente, întreruperea activitatii, restaurarea datelor, atacurile ransomware, precum si raspunderea fata de terti, cum ar fi bresele de date sau sanctiunile impuse de autoritati. Valoarea reala a unei astfel de asigurari consta însa si în sprijinul operational imediat: acces 24/7 la echipe specializate de experti IT, juristi, specialisti în comunicare de criza si recuperare, care pot interveni rapid pentru a limita daunele", a apreciat Georgia Dicker, expert în Cyber Insurance pentru UK&UE CFC Underwriting - Lloyd's of London.

Potrivit acestuia, organizatiile ar trebui sa adopte o abordare proactiva si sa combine protectia oferita de asigurare cu masuri de preventie solide: autentificare multifactor (MFA), actualizari regulate ale sistemelor, instruirea angajatilor si planuri clare de raspuns la incidente.

"Nicio companie nu poate elimina complet riscul cibernetic, însa printr-o combinatie între rezilienta cibernetica si protectie financiara, se poate reduce semnificativ impactul atacurilor si se poate asigura o revenire rapida dupa un incident major", a adaugat Georgia Dicker.

Companiile care intra sub incidenta Directivei NIS2 trebuie sa demonstreze ca detin politici de guvernanta cibernetica, controale de acces riguroase, procese clare de management al riscurilor si planuri de continuitate a activitatii.

"De asemenea, sunt obligate sa notifice incidentele majore în termen de 24 de ore, sa furnizeze un raport detaliat în 72 de ore si un raport final într-o luna. Neîndeplinirea cerintelor poate aduce sanctiuni severe - pâna la 10 milioane de euro sau 2% din cifra de afaceri globala pentru entitatile esentiale", se mai precizeaza în comunicat.

Leader Team Broker este un broker corporate de asigurari din România si Europa, cu o experienta de peste 19 ani în consultanta de risc si solutii de asigurare dedicate companiilor, care ofera solutii personalizate pentru companii mici, medii si mari, adaptate nevoilor specifice ale fiecarui domeniu de activitate.