PERSMEDEDELING

KABINET VAN DE VLAAMSE MINISTER VAN ECONOMIE, INNOVATIE, WERK, SOCIALE ECONOMIE EN LANDBOUW

4 op de 10 ondernemingen beschikt over procedures om adequaat op een cyberincident te reageren

Driekwart van de Vlaamse ondernemingen meent dat hun onderneming goed beschermd is tegen cyberaanvallen. Dat staat in schril contrast met de hoeveelheid ondernemingen die over voldoende procedures beschikt om adequaat op een cyberincident te reageren, zo blijkt uit de resultaten van de tweede Cybersecurity-barometer, een bevraging over de maturiteit inzake cybersecurity bij Vlaamse ondernemingen. Vlaams minister van Economie en Innovatie Jo Brouns: *'De wereld van cybersecurity verandert en evolueert constant. Er is nog veel werk aan de winkel.'*

In opdracht van het Departement Economie, Werk en Innovatie werd de tweede Cybersecurity-barometer opgemaakt. Aan de hand van een bevraging waaraan maar liefst 2367 Vlaamse ondernemingen meewerkten werd hierbij voor de tweede maal de stand van zaken geschetst over de staat van cybersecurity bij Vlaamse ondernemingen. Vlaams minister van Economie en Innovatie Jo Brouns: *'Er is nog veel werk aan de winkel. De mogelijkheden om digitale beveiliging te organiseren evolueert constant – net zoals de mogelijkheden voor criminelen constant evolueren. Ik roep onze ondernemingen op om volop gebruik te maken van het aanbod dat we via VLAIO aanbieden. Vlaanderen is een absolute topregio inzake innovatie. Data is onze belangrijkste grondstof, die moeten we adequaat beschermen.'*

Nood aan meer cybersecurity

Een grondig cybersecurity-beleid vereist grote inspanningen. Vlaamse bedrijven die technische maatregelen namen, bleken vooral beheersprocedures te implementeren om zich effectief te beschermen tegen cyberaanvallen – denk daarbij aan toegangsbeheer of identificatiemanagement. Net geen drie kwart van alle ondernemingen zet hierop in. Ook hebben zo'n 60% van de ondernemingen procedures om te herstellen van cyberaanvallen, zoals herstel via back-ups, herinstallatie van systemen en het wijzigen van wachtwoorden. Ondernemingen zetten echter veel minder in op procedures om cyberaanvallen te detecteren (bijvoorbeeld continue monitoring van veiligheidsrisico's) (49,7% van de bevraagden), gevoelige databronnen of kritieke bedrijfsprocessen die mogelijk doelwit zijn bij een mogelijke cyberaanval te identificeren (40,7%), en tot slot er adequaat op te reageren (bijvoorbeeld aan de hand van incidentanalyse of crisiscommunicatie) (37,0%). Bovendien geeft slechts 1 op 5 van de bedrijven aan dat het beschikt over een uitgewerkt cybersecurity-plan.

Vlaamse ondernemingen beperken zich nog steeds vaak tot relatieve basistoepassingen inzake technische maatregelen. Zelfs vrij elementaire toepassingen, zoals regelmatige software-updates, een systematisch beleid rond back-ups, toegangsbeheer van het ondernemingsnetwerk en sterke paswoordauthenticatie worden nog niet door alle bedrijven toegepast. Meer geavanceerde technische maatregelen zoals ICT-veiligheidstesten, of encryptietechnieken voor data, documenten of e-mails worden maar door een minderheid van de bedrijven gebruikt.

Tot slot voorziet slechts een derde van alle Vlaamse ondernemingen opleidingen of activiteiten rond cyberveiligheid voor medewerkers. Dit aantal blijft laag, terwijl 57% van de ondernemingen wel zelf aangeeft dat een gebrek aan bewustzijn bij de werknemers een belangrijk obstakel bij de invoer en het gebruik van cybersecurity-maatregelen vormt.

Met sensibilisering versterken we de Vlaamse economie

De resultaten van deze meting tonen aan dat er nog steeds een grote nood is aan een actief beleid dat ondernemingen verder stimuleert en ondersteunt om hun cyberveiligheid te verbeteren. *'Bedrijven die pas nadenken over te ondernemen acties wanneer het cyberincident reeds heeft plaatsgevonden, dreigen hopeloos achter de feiten aan te lopen'*, zegt minister Brouns.

Samen met actoren uit het VLAIO-netwerk wordt daarom een mix aan activiteiten voorzien om ondernemingen te sensibiliseren en te informeren over de noodzaak en de mogelijkheden om een volwaardig cybersecurity-beleid uit te stippelen. Met Cybsersecurity-verbetertrajecten wordt daarbovenop ook directe financiële steun gegeven aan kmo's die extern advies en begeleiding willen inkopen om hun beleid te versterken.

'In het volledige aanbod van VLAIO zal ook de 'secure by design'-toets een grotere rol spelen.' Hiermee wordt digitale veiligheid een toetssteen die steeds wordt meegenomen in de afweging voor de toekenning van subsidies aan ondernemingen. *'Zo sensibiliseren we ondernemingen om steeds, van meet af aan, cyberveiligheid mee te nemen in de toekomstplannen'*, concludeert minister Brouns.

Voor Jolyce Demely, Algemeen Directeur van Agoria Vlaanderen, toont deze nieuwe CS-barometer aan dat er nog meer moet worden ingezet op sensibilisering. *'Uit de barometer blijkt dat maar liefst 13,5% van de Vlaamse bedrijven het afgelopen jaar slachtoffer werd van een cyberaanval, een percentage dat waarschijnlijk zelfs een onderschatting is. Toch geven bedrijven aan dat ze onvoldoende het nut inzien van cybersecurity of dat hieraan te weinig prioriteit wordt gegeven. Dat moét anders. Een cyberaanval heeft namelijk verregaande gevolgen en het blijft nodig om élke werknemer, ook het management, te wijzen op het belang van een robuuste cyberveiligheid. We doen dit vandaag al, onder meer via Cyberstart, een programma in samenwerking met VLAIO, met advies en tips en tricks om tot een praktisch actie- en implementatieplan te komen rond cybersecurity.'*

Contactgegevens
Dennis Rombauts, persverantwoordelijke kabinet Brouns, 0474/92.80.90