
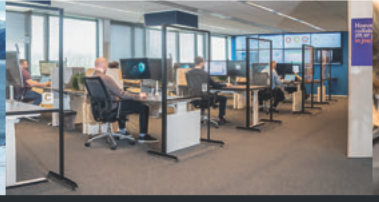

RIJNSTREEK

REGIONAAL ZAKENMAGAZINE | JAARGANG 31 | NUMMER 2 | MEI 2024

BUSINESS®

Collabite helpt het mkb bij het vergroten van de weerbaarheid tegen cyberaanvallen op hun ICT-omgeving

Hoe cyberweerbaar is jouw bedrijf?

Hoe cyberweerbaar is jouw bedrijf?

‘De gevolgen van cyber kunnen enorm zijn’

De Europese Unie heeft een verbeterde richtlijn opgesteld voor de lidstaten, de zogeheten NIS2-richtlijn, waarmee zij de weerbaarheid tegen cybercriminaliteit kunnen verhogen. De planning is dat deze richtlijn in Nederland uiterlijk in 2025 wordt omgezet in wetgeving waaraan het bedrijfsleven dan moet voldoen. Wat betekent dit voor mkb’ers en wat moeten zij concreet doen? Een interview.

Vlnr Tom Hebben (IMR Advies, Arjo Middelveld (Collabite) en Natascha van Duuren (De Clercq).

Drie bedrijven uit de regio hebben de handen ineengeslagen om het mkb te helpen bij het vergroten van hun weerbaarheid tegen cyberaanvallen op hun netwerk- en informatiesystemen. Dit zijn De Clercq Advocaten Notariaat uit Leiden, IMR Advies uit Alphen aan den Rijn en IT-bedrijf Collabite uit Bodegraven en Hillegom (voorheen Computerwacht en Joheco).

Op het kantoor van Collabite aan de N11 in Bodegraven hebben we een interview met Natascha van Duuren (partner bij De Clercq met als aandachtsgebieden IT, privacy en cybersecurity), Tom Hebben (projectadviseur informatiebeveiliging bij IMR Advies) en Arjo Middelveld, algemeen directeur van Collabite.

Waarom is het zo belangrijk dat bedrijven digitaal weerbaarder worden?

Arjo Middelveld: “We leven in een wereld die steeds digitaler wordt en waarin we steeds meer met elkaar verbonden raken. Tegelijkertijd neemt het aantal cyberaanvallen enorm toe. Het gevaar dat een organisatie hiervan het slachtoffer wordt neemt fors toe. Bijvoorbeeld door ransomware-aanvallen waarbij bestanden worden versleuteld of systemen platgelegd. Denk hierbij aan computerhacks waarbij wordt ingebroken in systemen en gegevens worden gestolen en/of openbaar gemaakt.”

Natascha van Duuren: “De gevolgen van deze vormen van criminaliteit kunnen

De Clercq Advocaten Notariaat

Het Leidse De Clercq Advocaten Notariaat, opgericht in 1850, is pionier op het gebied van IT-recht en expert op het gebied van wet- en regelgeving rond cybersecurity. Partner Natascha van Duuren geeft leiding aan het cybersecurityteam van De Clercq, dat gespecialiseerd is in privacy, compliance, aanbestedingen, IT-contractrecht en aansprakelijkheidsrecht.
Natascha van Duuren: “We helpen ondernemers om tijdig te voldoen aan alle wet- en regelgeving die op hen afkomt en hoe zij cyberrisico’s kunnen beperken. Ons team staat 24/7 klaar om bedrijven te helpen die getroffen zijn door een cyberaanval, om hen van A tot Z te begeleiden bij de afhandeling van het incident.”

criminaliteit

‘DE AANGESCHERPTE PERSOONLIJKE AANSPRAKELIJKHEID MAKEN VAN SECURITY EEN BOARDROOMKWESTIE’

enorm zijn en niet te overzien. Het kan leiden tot een ontwrichting van de economie en de samenleving. Bedrijven komen plat te liggen, waardoor de continuïteit van de bedrijfsvoering in gevaar komt. Ondernemingen kunnen hierdoor zelfs failliet gaan. Vandaar dat het belangrijk is dat bedrijven weerbaarder worden. De nieuwe strengere wetgeving die eraan komt, helpt hierbij.”

Waarom hebben jullie de handen ineengeslagen?
Arjo Middelveld: “We hebben een zorgplicht naar onze klanten om hen te informeren over de wetgeving die eraan komt. De wet is complex. Daarom willen we ze tijdig waarschuwen en helpen, ook omdat we weten dat mkb’ers het lastig vinden hoe met deze wet om te gaan. Onze hulp en ondersteuning omvat vanzelfsprekend een groot IT-component, maar er zijn ook juridische en organisatorische kanten aan de zaak. Daarom doen we dit samen met De Clercq en IMR Advies. Beide zijn al tien tot vijftien jaar klant. In de zomer van 2023 zijn we begonnen met het informeren van onze klanten over de NIS2-richtlijn.”

Tom Hebben: “We werken al langer met elkaar samen bij gezamenlijke klanten. Op deze manier vullen we elkaar mooi aan. Al vele jaren doen we bijvoorbeeld interne audits om klanten te helpen ISO-certificaten te halen. Ook helpen we ze bij het voldoen aan wet- en regelgeving. Zo helpen we ook Collabite bij hun certificeringstrajecten.”

Wat doen jullie concreet om ondernemers te helpen weerbaarder te worden?
Arjo Middelveld: “We hebben een gratis scan ontwikkeld waarmee we bedrijven en organisaties helpen om na te gaan hoe cyberweerbaar ze zijn en of ze voldoen aan de NIS2-richtlijn. Iedereen kan deze scan aanvragen, ook bedrijven die geen klant zijn bij Collabite. Een specialist maakt een afspraak. Die afspraak duurt ongeveer een uur, waarbij wordt besproken hoe de huidige situatie is in het bedrijf op het gebied van informatiebeveiliging. Het doel van de scan is om bewustwording te realiseren ten aanzien van de risico’s en kansen. Sinds de introductie vorig jaar hebben we de scan al zo’n tachtig keer uitgevoerd, niet alleen in onze eigen regio maar ook in de rest van Nederland. Klanten vinden het ontzettend nuttig om te doen, het levert ze een nulmeting op waarmee ze concreet verder kunnen.”

Wat gebeurt er na de scan?
Arjo Middelveld: “De scan is een goede manier om te ontdekken in welke mate de ICT-omgeving beveiligd is, wat je moet doen na een eventueel incident en hoe je zo snel mogelijk weer kunt opstarten na een incident. Na de scan krijg je een rapport waarin staat wat de risico’s zijn, uitgedrukt in een rapportcijfer tussen 1 en 10. Verder krijgen ze uitleg over de NIS2-richtlijn, actiepunten en een advies hoe men de cyberbeveiliging verder kan opschroeven. Dit kunnen technische maatregelen zijn, het opstellen van procedures voor een betere beveiliging, de juridische verplichting om incidenten te melden, informatie-uitwisseling met externe organisaties en de overheid, en toezicht op en handhaving van het naleven van de richtlijnen.”

Vraag een gratis NIS2-scan aan

Wil je weten hoe cyberweerbaar jouw bedrijf is en of je voldoet aan de regels van NIS2? Lezers van dit blad kunnen een gratis NIS2-scan aanvragen: Scan de QR-code om direct naar *www.collabite.nl/afspraak* te gaan en boek een NIS2-scan.

De scan is bedoeld voor bedrijven vanaf 15 medewerkers. Het duurt ongeveer een uur en is geheel gratis. Specialisten komen naar je toe en na afloop ontvang je een uitgebreide rapportage (9 pagina’s).

‘CYBERINCIDENTEN STAAN IN DE TOP-DRIE VAN RISICO’S DIE BEDRIJVEN LOPEN, DAAROP ANTICIPEREN IS EEN KERNTAAK VAN DIRECTIES EN BESTUURDERS’

IMR Advies

Al bijna 30 jaar ondersteunt en adviseert IMR bedrijven bij het halen en houden van certificaten, het voldoen aan wet- en regelgeving en het trainen van medewerkers.

Projectadviseur Tom Hebben: “Ons team van professionals denkt en werkt mee om organisaties te verbeteren. Dit varieert van het opstellen van procedures en documenten tot begeleiding bij de implementatie van normen, certificaten en het voldoen aan Nederlandse en Europese wetgeving voor kwaliteit, arbeidsomstandigheden, veiligheid, informatiebeveiliging, maatschappelijk verantwoord ondernemen en milieu.”

In relatie tot de NIS2-richtlijn kan IMR helpen bij het beschermen van informatiesystemen en het beschermen van organisaties tegen informatiebeveiligingsrisico’s, uiteenlopend van het starten van een securityscan, risicoanalyses en businessimpactanalyses, opstellen van gedragsregels, implementeren van bedrijfscontinuïteitsplannen tot het behalen van een ISO 27001-certificaat voor informatiebeveiliging.

Voor wie is de scan bedoeld?
Arjo Middelveld: “Wij adviseren alle bedrijven vanaf 15 medewerkers om een scan te doen. NIS2 geldt voor grote en middelgrote bedrijven in vitale sectoren zoals energie, water, transport, financiën, infrastructuur, zorg, ICT en overheid. Bedrijven die onder de NIS2-wetgeving vallen, zijn verplicht om passende beveiligingsmaatregelen te nemen. Zo is het bijvoorbeeld nodig om software bij te werken, cyberaanvallen te melden en risicobeoordelingen uit te voeren. Om af te dwingen dat dit ook daadwerkelijk gebeurt, kunnen bestuurders van bedrijven zelfs persoonlijk aansprakelijk worden gesteld inclusief boetes en schorsingen.”

Natascha van Duuren: “Bedrijven die onder de NIS2-wet vallen, zijn bovendien verplicht om te checken of ook hun leveranciers aan de nieuwe strengere regels voldoen. Je kunt dus ook indirect te maken krijgen met NIS2, doordat klanten strengere eisen gaan stellen op het gebied van cybersecurity. Dit plus de aangescherpte persoonlijke aansprakelijkheid maken van security een boardroomkwestie. Cyberincidenten staan in de top-drie van risico’s die bedrijven lopen. Daarop anticiperen is een kerntaak van directies en bestuurders.” ■

Computerwacht + Joheco = Collabite

Joheco en Computerwacht werken al een tijd samen. Daarom hebben ze nu samen een nieuwe naam: Collabite. ICT-oplossingen en service zoals gebruikelijk, maar dan in een nieuw jasje.

De nieuwe naam Collabite staat voor collaborate, het Engelse woord voor samenwerken. Samenwerken tussen de twee bedrijven onderling en vooral ook samenwerken met hun klanten, zoals bij invoering van de NIS2-richtlijn. De nieuwe naam staat ook voor de wereld van bits en bytes en voor het vastbijten in ICT-vraagstukken (vandaar de ‘hapjes’ uit de i en de t van Collabite). De Engelse naam staat daarnaast symbool voor het internationale karakter van het bedrijf, van de business en van de klanten die vaak wereldwijd actief zijn.

De ruim tachtig medewerkers blijven opereren vanuit de twee bestaande locaties in Bodegraven en Hillegom voor klanten door heel Nederland en daarbuiten, als onderdeel van de landelijk opererende Futureproof Group.

member of Futureproof group

Collabite Bodegraven
Klipperaak 101
2411 ND Bodegraven
0172 235835
www.collabite.nl

Collabite Hillegom
Ampèrestraat 6b
2181 HB Hillgom
0252 240190
www.collabite.nl