Cybersecurity: vertrouwen in digitale tijden

Hoe wapen je je onderneming tegen steeds slimmere cybercriminelen en onzichtbare vertrouwensbreuken? Dat is één van de thema's die aan bod komen in ons Trendrapport. BDO blikt samen met trendwatcher Tom Palmaerts vooruit naar 2030. We tonen hoe Belgische ondernemingen wendbaar en vol vertrouwen de toekomst mee vorm kunnen geven. Technologie combineren met gezond verstand is hier cruciaal bij.

Cybersecurity: vertrouwen in digitale tijden

Technologie brengt ongekende mogelijkheden, maar maakt bedrijven tegelijk kwetsbaarder dan ooit. Cybercriminaliteit trekt zich niets aan van landsgrenzen en is uitgegroeid tot een dagelijkse realiteit, ook voor Belgische ondernemingen. Hackers richten zich niet enkel op multinationals, maar ook op kmo's die vaak minder beveiligd zijn. Cyberaanvallen kosten wereldwijd miljarden, maar het grootste verlies is vaak onzichtbaar en niet te becijferen: vertrouwen.

"Cyberrisico's blijven een van de meest onderschatte gevaren voor bedrijven. Ondanks de groeiende bewustwording onderschatten veel organisaties nog steeds de impact van datalekken, ransomware en gebrekkige data-integriteit. De schade blijft zelden beperkt tot financiële verliezen: ook reputatie, vertrouwen en continuïteit staan op het spel. Daarbovenop vormt slechte datakwaliteit een sluipend risico. Verkeerde of inconsistente data leiden onvermijdelijk tot foutieve beslissingen en ondermijnen het vertrouwen in systemen én leiderschap."

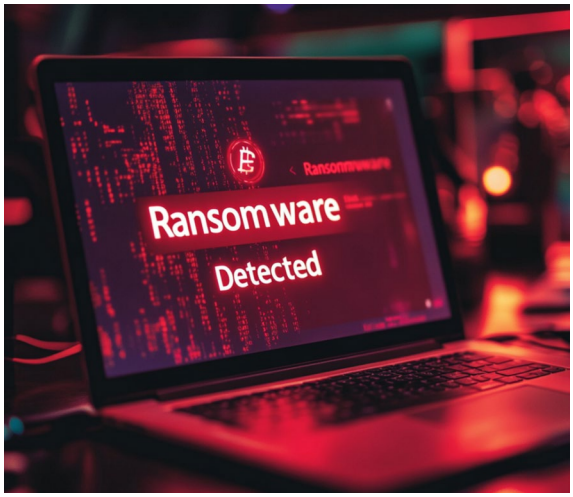
Sam Nelen, Partner Risk Advisory
BDO Belgium

MISINFORMATIE EN DESINFORMATIE

Niet elke aanval is technisch. Bedrijven worden steeds vaker geconfronteerd met desinformatiecampagnes. Soms zijn die afkomstig van concurrenten, soms van kwaadwillige actoren. Zo'n campagne kan klanten én medewerkers in verwarring brengen. Een vals bericht op sociale media of een gelekt document kan de reputatie van een onderneming binnen enkele uren beschadigen.

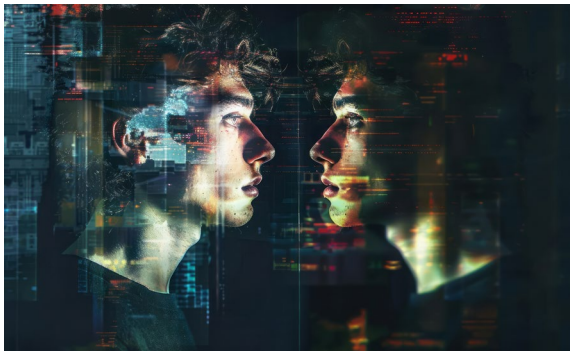
TRENDS IN CYBERHACKING

Cyberaanvallen worden complexer en verfijnder. Ransomware blijft de populairste methode: systemen worden vergrendeld en pas vrijgegeven na betaling. Maar ook supply chain-aanvallen nemen toe, waarbij hackers niet rechtstreeks een bedrijf, maar een leverancier of freelancer hacken om zo toegang te krijgen. Het toont hoe kwetsbaar netwerken zijn, de ketting is zo sterk als de zwakste schakel.



DEEPFAKES: VERTROUWEN ALS ZWAKKE PLEK

Cybercriminaliteit speelt in op ons vertrouwen. Een recent voorbeeld komt van Ferrari, waar criminelen de stem van een bestuurder nabootsten om een dringende betaling te forceren. Wat de aanval stopte, was geen ingewikkelde technologie, maar een eenvoudig stukje gezond verstand: de medewerker stelde een vraag die alleen de echte bestuurder kon beantwoorden ('Welk boek heb je me gisteren aangeraden?'). Het incident toont hoe deepfakes steeds overtuigender worden, maar ook dat waakzaamheid en kritische reflexen onze eerste verdedigingslinie blijven.



HET QUANTUM TIJDPERK

Een nieuwe dreiging ligt op de loer: quantum computing. Computers die miljoenen keer sneller rekenen zouden veel van onze huidige encryptiemethoden nutteloos maken. Hoewel het quantumtijdperk nog toekomstmuziek is, bereiden banken, overheden en technologiebedrijven zich nu al voor. Ook Belgische bedrijven doen er goed aan de ontwikkelingen op de voet te volgen en hun beveiliging stap voor stap "quantum safe" te maken.

EU CYBER RESILIENCE ACT

De EU Cyber Resilience Act verplicht bedrijven om producten en software veiliger te ontwerpen, en verantwoordelijkheid te nemen voor kwetsbaarheden. Dat klinkt als extra regelgeving, maar het creëert ook een belangrijk voordeel: meer vertrouwen bij klanten, leveranciers en investeerders. Net zoals de AI Act wil deze wet kaders en zekerheid bieden. De CRA is niet allesomvattend en de kracht ervan hangt af van handhaving, samenwerking en innovatie.

"Ondanks de snelle digitalisering blijven te veel bedrijven ter plaatse trappelen op het vlak van cybersecurity. We zien dat vooral kleinere spelers achterop hinken door gebrek aan kennis en veiligheidscultuur en door de foutieve perceptie dat zij geen interessante prooi zijn voor cybercriminelen. Dat is spelen met vuur: een hack kost niet alleen losgeld, maar ondermijnt omzet, continuïteit en concurrentiekracht. De impact is sowieso vele malen groter dan de noodzakelijke investeringen. Naast basismaatregelen zoals wachtwoordbeleid en firewalls raden we bedrijven aan een risicoanalyse, duidelijke roadmap en geavanceerde detectiemaatregelen te voorzien. De beste verdediging blijft een gelaagde aanpak."

Sam Nelen, Partner Risk Advisory
BDO Belgium

DO'S & DON'TS VOOR BEDRIJFSLEIDERS

DO'S

- Do: plan crisisoefeningen zodat teams weten wat te doen bij een hack of datalek.
- Do: screen toeleveranciers en freelancers op hun cybersecuritymaatregelen.
- Do: investeer in bewustmaking bij medewerkers, vaak is menselijk gedrag de zwakste schakel.
- Do: volg Europese initiatieven zoals de Cyber Resilience Act, die houvast bieden en het vertrouwen verhogen.

DON'TS

- Don't: denk dat je als kmo geen doelwit bent. Hackers weten dat kleinere bedrijven vaak minder goed beschermd zijn.
- Don't: vertrouw blind op technologie. Menselijke reflexen en gezond verstand blijven onmisbaar.