MAAK VAN CYBERVEILIGHEID EEN PRIORITEIT VOOR JOUW KMO

Nathan Baele van Incerta

Til je cyberveiligheid naar een hoger niveau

Door de toegenomen digitalisering lopen Vlaamse bedrijven meer dan ooit het risico om gehackt te worden. Met de steun van het Agentschap Innoveren & Ondernemen (VLAIO) kan elke onderneming haar cyberveiligheid naar een hoger niveau tillen.

Ontdek in deze krantenbijlage waarom inzetten op cyberveiligheid een must is, en hoe jij jouw kmo wapent tegen een cyberaanval.

vlaio.be/cybersecurity

AGENTSCHAP INNOVEREN & ONDERNEMEN

Vlaanderen is ondernemen

Kmo's krijgen financiële steun om hun cyberveiligheid op te krikken

"BEDRIJVEN STAAN TE WEINIG STIL BIJ DE IMPACT VAN ZO'N CYBERAANVAL OP LANGE TERMIJN"

Cyberaanvallen richten financiële schade én reputatieschade op langere termijn aan bij bedrijven, en ze slaan een deuk in het vertrouwen bij klanten en leveranciers. In een digitale, geconnecteerde economie zorgen ze bovendien voor een sneeuwbaleffect. Redenen genoeg voor het Vlaams Agentschap Innoveren & Ondernemen (VLAIO) om kmo's te helpen zich te wapenen tegen cyberveiligheidsrisico's.

"Tegenover elke grote cyberaanval die de media haalt, staan tientallen aanvallen bij kleinere bedrijven", zeggen VLAIO-adviseurs Jeroen Fiers en Patrick Hauspie. "Die springen minder in het oog, maar de impact op de onderneming is minstens even groot."

Je zou denken dat elk bedrijf ondertussen wel doordrongen is van het belang van cyberveiligheid, maar dit blijkt in de praktijk vaak toch niet het geval. "Er zijn nog altijd ondernemers die het cyberveiligheidsrisico onderschatten. Dat zijn echt niet alleen de kleine kmo's. We merken dat IT-afdelingen en zeker directies nog steeds niet goed beseffen wat de mogelijke impact is van een cyberaanval. Ze denken dat het hun buur misschien kan overkomen, maar dat zij wel door de mazen van het net zullen glippen", aldus Fiers.

"Iederéén is vandaag een mogelijke prooi voor cybercriminelen", benadrukt Hauspie. "Zowel kleine kmo's als grote multinationals, in eender welke sector. We zien dat veel kmo's nog denken dat cyberaanvallen iets zijn waar alleen grote beursgenoteerde bedrijven mee te maken krijgen, zoals Picanol of vliegtuigbouwer Asco. Dat klopt niet."

De human firewall

Veel bedrijven staan niet stil bij de impact op lange termijn: de reputatieschade. "Reputatieschade is moeilijker te meten of te becijferen, maar ook moeilijker te herstellen. Een cyberaanval of een datalek zorgt voor een vertrouwensbreuk. Steeds meer leveranciers stellen cyberveiligheidseisen aan hun klanten, ze willen garanties dat hun data veilig zijn en waterdichte bescherming genieten. Bouw je niet voldoende zekerheid in, dan ga je als bedrijf klanten en opdrachten verliezen."

Die cyberveiligheid gaat verder dan een firewall, een antivirusprogramma en back-ups, voegt Hauspie eraan toe. "Je moet niet alleen de technologische kant afdekken. Er is ook een procesmatige kant. Mensen zijn één van de zwakke schakels. De ketting is maar zo sterk als de zwakste schakel. Dat is wat ze de human firewall noemen. Goede processen zijn nodig om bedrijven minder kwetsbaar te maken voor menselijke fouten. Cyberveiligheid overstijgt IT. Het is vandaag een opdracht voor élke afdeling en élke medewerker."

Ramen en deuren wagenwijd open

Jeroen Fiers botst geregeld op een aantal hardnekkige misvattingen over cyberveiligheid. "De eerste is dat bedrijven denken dat een cyberverzekering hen ontslaat van de verantwoordelijkheid om zélf nog in cyberveiligheid te investeren. Een verzekering is goed, maar ze mag geen vals gevoel van veiligheid geven. Het is niet omdat je een goede inbraakverzekering hebt dat je voortaan alle deuren en ramen laat openstaan? Bovendien vragen verzekeraars een minimaal niveau van cybersecurity beveiliging en zullen deze vereisten naar de toekomst toe wellicht nog worden aangescherpt."

"Een tweede misvatting is dat cyberveiligheid iets is dat de ITer in het bedrijf 'er even bij zal nemen'. Je kan als bedrijf zelf wel een aantal zaken aanpakken, maar cybersecurity blijft specialistenwerk. Zelfs externe IT-partners kunnen dat niet zomaar bolwerken. Een expert in cyberveiligheid hoeft niet noodzakelijk duur te zijn. Soms investeren bedrijven veel geld in nieuwe en dure firewalls, terwijl andere ingrepen misschien dringender, doeltreffender én goedkoper zijn. Experts detecteren de grootste noden en kunnen prioriteiten naar voren schuiven.

"Cybersecurity experts detecteren de grootste noden en kunnen prioriteiten naar voor schuiven."

- Jeroen Fiers,
VLAIO-adviseur

Start ook een cybersecurity verbetertraject

Via de subsidie "cybersecurity verbetertrajecten" ondersteunt VLAIO kmo's om hun cyberveiligheid naar een hoger niveau te tillen.

- ✓ **Voor kmo's in Vlaanderen**
- ✓ **Individuele begeleiding door een cybersecurity expert**
- ✓ **Subsidie komt tussen voor 45% van de kostprijs**

Meer info?
vlaio.be/cybersecurity-verbetertrajecten

Bekijk ook p 6-7 van deze bijlage voor een overzicht van alle steun.

"Iederéén is vandaag een mogelijke prooi voor cybercriminelen. Zowel kleine kmo's als grote multinationals, in eender welke sector."

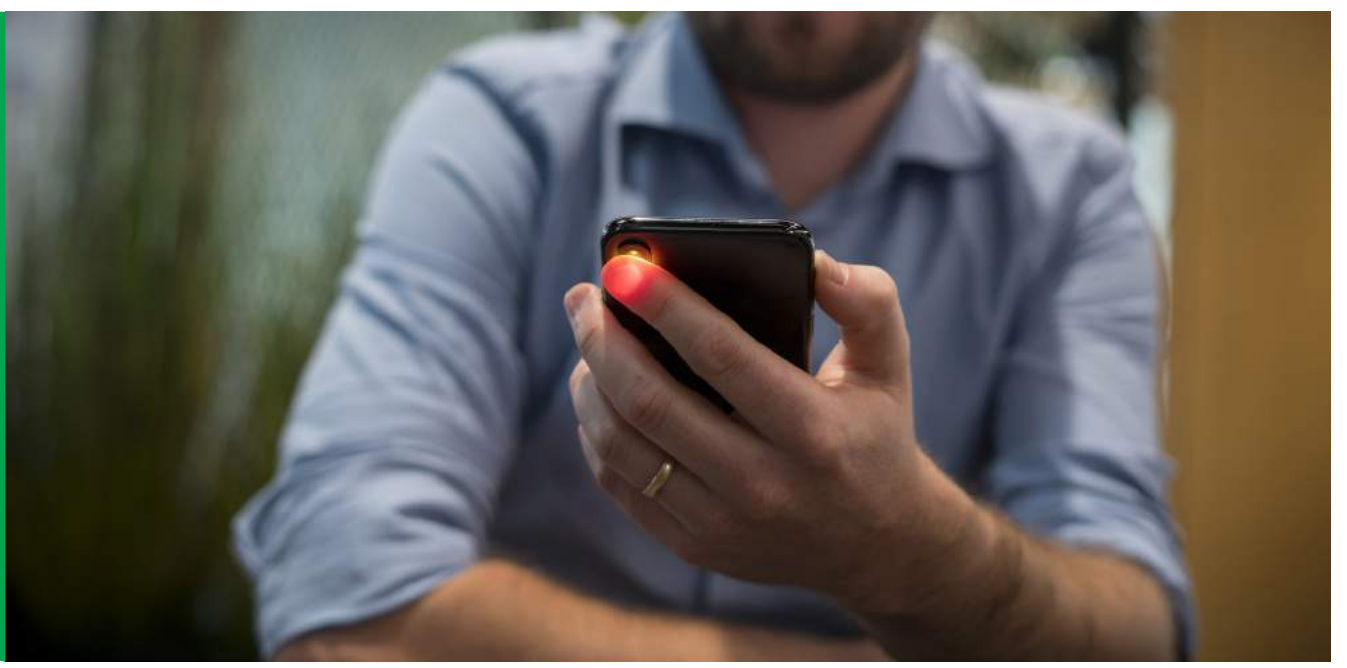
- Patrick Hauspie,
programma-adviseur cybersecurity bij VLAIO

Cyberveiligheid komt onvermijdelijk met een prijskaartje. Elk jaar opnieuw, want je moet gelijke tred houden met de cybercriminelen die ook niet stilzitten en steeds inventiever worden. Laten we opnieuw de vergelijking maken met een brand: branddetectoren kosten ook geld, maar de financiële schade van een brand zal gegarandeerd een veelvoud van die investering bedragen."

VLAIO ondersteunt met de cybersecurity verbetertrajecten kmo's die een expert onder de arm nemen. Ze krijgen tot 45 procent van dat verbetertraject terugbetaald. "Elk traject bestaat uit drie stappen", legt Fiers uit. "Het begint met een analyse van de huidige situatie, gevolgd door een verbeterplan met concrete prioriteiten. Maar, en dat is heel belangrijk, we zorgen ervoor dat het daar niet stopt. Hoeveel bedrijven hebben geen plannen in de schuif liggen die ze nooit uitgevoerd hebben? We waken erover dat binnen het traject de meest prioritaire pijnpunten ook worden aangepakt. We ondersteunen geen papieren plannen, maar concrete acties die de cyberveiligheid opkrikken."

"Eén lek kan een enorme impact hebben op onze onderneming"

"We denken nooit dat het ons niet kan overkomen", zegt Jo Van der Auwera, chief compliance officer van de app FibriCheck die hartritmestoornissen detecteert. "We namen altijd al het zekere voor het onzekere. Nu brengen we onze cybersecurity naar een nog hoger niveau. Want één lek kan een enorme impact hebben op de continuïteit van onze onderneming."



> “Cybersecurity is een vereiste voor het mogen indienen van offertes en het meedingen naar overheidsopdrachten.”
>
> - Nathan Baele, security officer bij Incerta

Nathan Baele van Incerta (l) en Siebe De Roovere van Toreon (r)

Incerta kent én beperkt nu veel beter zijn cyberrisico’s

“DOOR ONZE CYBERVEILIGHEID LOPEN WE VOOR OP CONCURRENTEN”

“Welke cybersecurity-risico’s lopen we? En hoe beperken we die?” Met deze vragen stapte Nathan Baele van de kmo Incerta naar de specialisten van Toreon. “Hierdoor lopen we vandaag voor op onze concurrenten.”

Incerta volgde een cybersecurity verbetertraject. Ze lieten zich begeleiden door de cybersecurity experts van Toreon.

Wat zijn je 3 belangrijkste redenen om te investeren in cyberveiligheid?

Nathan Baele, security officer bij Incerta: “We maken en hosten eigen software. We verwerken heel wat persoonlijke data van klanten, en dat moet veilig gebeuren. Een collega van ons vertelde me gisteren over een bedrijf dat al een week plat ligt omdat cybercriminelen de data gijzelen. We willen niet dat dit ons of een klant overkomt.”

Siebe De Roovere, business unit director bij Toreon: “We bekeken de technische risico’s en werkten een lange termijnplan uit om deze aan te pakken. Incerta kent én beperkt nu veel beter zijn risico’s.”

Vragen klanten of je op een cyber- en privacyvriendelijke manier omgaat met hun data?

Baele: “Cybersecurity is een vereiste voor het mogen indienen van offertes en het meedingen naar overheidsopdrachten. Het laatste jaar sturen al onze grotere klanten lange lijsten met vereisten rond cybersecurity. Ze vragen testverslagen die bewijzen dat we kwetsbaarheden oplossen en eisen regelmatig penetratietesten.”

De Roovere: “Grote bedrijven worden verantwoordelijk gesteld voor de tekortkomingen van hun leveranciers bij eventuele datalekken. Daarom focussen ze hier steeds sterker op.”

Hoe verbetert het VLAIO-traject je cybersecurity maturiteit?

Baele: “We onderscheiden ons al een tijdje met de ISO 27001-certificering, wat de standaard is in cybersecurity. In het huidige cybersecurity verbetertraject werken we aan technische verbeteringen én aan onze gemoedsrust. Dan zijn we zeker dat onze cloudomgeving maximaal beveiligd is.”

De Roovere: “Veel ondernemingen vertrouwen op de ingebakken security van het cloudpakket dat ze gebruiken. Wat ze niet weten, is dat ze zelf de veiligheidsinstellingen scherper moeten zetten. Bijvoorbeeld in Microsoft 365. Een goedkopere licentie biedt ook minder veiligheden dan een duurdere.”

> “Hackers zijn niet geïnteresseerd in welk bedrijf ze aanvallen. Als het maar geld oplevert.”
>
> - Siebe De Roovere, business unit director bij Toreon

Wat is de meerwaarde van een externe expert?

Baele: “Vandaag kan één persoon onmogelijk alles kennen van IT. Daarom is het Toreon-team van specialisten zo belangrijk voor ons. Ieder heeft er zijn expertise. Hierdoor worden onze vragen met één telefoontje opgelost. Vroeger deden we alles zelf, en kostte ons dat soms een dag. We boeken dus een gigantische tijdswinst.”

De Roovere: “Ons team bestaat uit security generalisten en experten die heel veel weten van weinig. Alle 60 samen vormen ze een team dat alles weet. Hierdoor krijgen kmo’s de flexibiliteit om een heel team aan te kopen voor weinig geld.”

Hoe werkt deze cybersecurity-expert samen met jullie IT-partner?

Baele: “We hebben inderdaad een andere IT-partner. Maar security is niet hun business. De actiepunten uit de testen verdelen we onder hen en Toreon.”

De Roovere: “Weinig IT-providers zijn onderlegd in cybersecurity. Door het vele werk updaten ze soms ook maar om de één of meerdere maanden de software van hun klanten. Hierdoor blijven deze organisaties kwetsbaar.

Waarom investeren ook niet-IT-ondernemingen best in cybersecurity?

Baele: “Wij hebben een voorsprong op de concurrentie door een hogere cyberveiligheid. Ik kan me voorstellen dat je dit ook in andere sectoren als een troef kan uitspelen. Daarenboven sluit je door een relatief kleine investering nu het risico op grotere kosten na een hacking uit.”

De Roovere: “Ik krijg vaak telefoon van een bedrijfsleider die veel wil betalen om de hacking op te lossen. Voorkomen is steeds beter dan genezen. Hackers zijn niet geïnteresseerd in welk bedrijf ze aanvallen. Als het maar geld oplevert. Ze scannen constant en automatisch op internet naar zwak beveiligde organisaties. Zo worden ook eenmanszaken en kleine kmo’s uit alle sectoren gehackt.”

Incerta

- Ontwikkelaar en leverancier van bedrijfssoftware
- Focust op processen met betrekking tot veiligheid, kwaliteit en milieu
- Geeft zelf het goede voorbeeld met ISO27001 en ISO9001
- Investeert in cybersecurity, en volgde een cybersecurity verbetertraject

Agoria, Sirris en VLAIO dagen Vlaamse kmo’s uit

“DURF JE AF TE VRAGEN WAT DE IMPACT VAN EEN CYBERAANVAL OP JE KMO IS”

Hoe lang draait je onderneming nog verder als je IT-systeem uitvalt? Het antwoord op deze vraag toont welke impact een cyberaanval kan hebben.

“Als ik vraag naar wat er gebeurt eens IT onbereikbaar wordt, krijg ik gevarieerde antwoorden”, ervaart Patrick Coomans, expert cybersecurity, innovatie en entrepreneurship voor Agoria en Sirris. “Gemiddeld zeggen bedrijfsleiders dat na vier uur tot twee dagen alles stilvalt. Geen productie, geen verkoop, geen omzet,... alleen maar kosten.”

Om Vlaamse kmo’s dit leed te besparen, sensibiliseren en informeren hij en Patrick Hauspie, programma-adviseur cybersecurity bij VLAIO, ondernemingen rond cybersecurity. In dit interview bundelen ze hun expertise en aanbod aan kmo’s.

Waarom is cybersecurity ook iets voor niet-IT-ondernemingen?

Patrick Hauspie: “Bestaan er nog ondernemingen die geen IT in huis hebben? Ook een landbouwer heeft zijn computer nodig, een bakkerij, loodgieter, architectenbureau, groepspraktijk van tandartsen... Kmo’s beseffen vaak niet hoe afhankelijk ze zijn van computers, software, netwerken en IT-tools.”

Patrick Coomans: “Iedereen kent wel iemand die gehackt is geweest of geld is verloren aan cybercriminelen. Kmo’s hangen dit niet aan de grote klok. Maar als ik na een opleiding of presentatie vraag wie er al schade leed door een cyberaanval, steekt één op de drie de hand op.”

Welke vragen stellen ondernemingen?

Coomans: “Wij krijgen weinig vragen omdat kmo’s denken dat zij nooit het slachtoffer van internetcriminelen worden. Want wat hebben hackers nu bij hen te zoeken? Wel, het zijn geen hackers meer. Het zijn professionele criminelen die een opportuniteit zien en grijpen. Zonder doelgericht één bedrijf aan te vallen, zoeken ze kwetsbaarheden. Die verkopen ze verder aan iemand die er geld uitslaat. Dit ecosysteem werkt helaas zeer goed.”

Hoe weet een kmo dat die zich beter moet wapenen?

Coomans: “Iedereen die ik de vrij beschikbare hacking tools en het dark web toon, is geshockeerd. Ze ontdekken dat er heel gevoelige data openbaar circuleert en beseffen dat databeveiliging cruciaal is.”

Hauspie: “We begrijpen dat iedereen zijn handen vol heeft. Maar al op een halve dag kan je de ernst begrijpen met zeven eenvoudige vragen.”

Hoeveel kost een dag stilstand?

Stel dat je kmo het slachtoffer zou worden van een cyberaanval. Welke schade zou je dan leiden? Schrijf de antwoorden neer en bespreek ze op directieniveau.

1. Hoe lang draait je bedrijf verder eens IT onbereikbaar wordt?
2. Hoeveel kost een dag stilstand?
3. Heb je contracten met boeteclausules?
4. Hoeveel aan boetes zou je moeten betalen als klantgegevens gestolen worden?
5. Hoeveel zou het kosten om te herstarten en de gehackte data en systemen te herstellen?
6. Hoeveel van je huidige klanten zullen niet meer bij je kopen na een hacking?
7. Werk je voor ondernemingen die het cyberrisico van de samenwerking willen inschatten via cybersecurity-vragenlijsten?

Dit kan een kmo toch niet alleen oplossen?

Hauspie: “Je hoeft dit niet alleen te doen. Het netwerk van dienstverleners verbonden aan VLAIO staat klaar om bedrijven te informeren, te adviseren, te coachen en te verwijzen naar de juiste partners. Je kan onder meer een grondige doorlichting laten doen én laten subsidiëren via de cybersecurity verbetertrajecten.”

Coomans: “Deze kansen snel grijpen is de boodschap. Want cybersecurity is als de fundering van je huis. Zonder fundering zakt je mooie huis weg. Als je de fundering vooraf aanlegt, valt de kostprijs mee. Maar als je ze pas steekt als het huis er al staat, is het enorm duur. Weet dat je vroeg of laat een inhaalbeweging moet doen. Ik heb al gezien dat iemand ontdekt dat zijn product niet cyberveilig was... net voor de lancering. Ze verloren een jaar om een veilige versie 2.0 te maken.”

“Vanuit VLAIO verwijzen we door naar heldere informatie, advies en subsidies.”

- Patrick Hauspie,
programma-adviseur cybersecurity bij VLAIO

Op welke dienstverlening kunnen bedrijven rekenen?

Hauspie: “Vanuit VLAIO verwijzen we door naar websites waarop heldere informatie te vinden is over cybersecurity, zoals bijvoorbeeld digitaletoekomst.be van VLAIO of safeonweb.be van het Centrum voor Cybersecurity België. Daarenboven bekijken we subsidies en verwijzen we je door naar advies en begeleiding, opleidingen. Ook via onze partners uit het VLAIO Netwerk kunnen bedrijven informatie, advies en begeleiding inwinnen. Zo brengen UNIZO, Voka en Confederatie Bouw toegankelijke informatie, workshops en advies naar hun leden.”

Coomans: “Agoria en Sirris hebben als trekkers van het industriepartnerschap een horizontaal aanbod voor bedrijfsleiders en algemene profielen waarin ze leren wat elk bedrijf moet doen. ‘Cybersecurity in 30 stappen’ is hierin een populaire workshop. Ons verticaal aanbod voor specialisten is gericht op clusters van risicoprofielen, bijvoorbeeld voor de maakindustrie of ontwikkelaars. Aanvullend hieraan stellen we directies voor om ons in te huren voor een korte presentatie over cybersecurity.”

Ontdek het aanbod van VLAIO en dienstverleners als Agoria, Sirris, Voka, UNIZO en Confederatie Bouw of via vlaio.be/expertisedatabank, thema ‘digitalisering’.

"CYBERSECURITY GEEFT ONS EEN STERKERE REPUTATIE EN MARKTPOSITIE"

Cybersecurity is vandaag een uniek verkoopargument. Ook Remedus wint nieuwe klanten dankzij zijn focus op het veilig beheren van data. "De aandacht voor databeveiliging geeft ons een meer betrouwbare reputatie en sterkere marktpositie."

"Wij zijn toeleverancier van ziekenhuizen en farmabedrijven, vertelt Peter van Vooren, head of digital transformation bij Remedus. "Als wij in commerciële gesprekken aantonen dat wij cybersecurity professioneel aanpakken, spreekt dat in ons voordeel. Zo was het een belangrijk punt in ons eerste buitenlands contract."

De eigen applicatie Remecare verzamelt en deelt gegevens van patiënten met het specialistisch ziekenhuisteam en met de eerstelijnsactoren zoals huisarts, thuisverpleegkundige en apotheker.

Het is net deze applicatie die hen al jaren drukt op het belang van cybersecurity. "Door de vele verhalen van gehackte bedrijven in de pers kreeg dit thema een extra boost in het bedrijf. Want wij willen nooit een cyberincident meemaken", zegt Peter. In zijn zoektocht naar een grotere cybersecurity maturiteit vond hij het cybersecurity verbetertraject van VLAIO. Hij koos CRANUM uit de negen door VLAIO geselecteerde externe specialisten.

Ook beveiliging tegen brand

Remecare verwerkt uiterst gevoelige gegevens van ziekenhuizen, farmabedrijven en patiënten. Al vindt de dienstenleverancier uit Aartselaar cybersecurity belangrijk voor elke onderneming. "Elk bedrijf dat vandaag gegevens elektronisch verwerkt en zijn operaties baseert op data uit computersystemen, valt stil als deze gegevens verdwijnen of onbereikbaar worden. Dat moeten ook bedrijven beseffen die denken dat ze nooit het slachtoffer zullen worden van cybercriminelen. Ook een medewerker kan bepaalde zaken saboteren. Ook een brand of natuurramp kunnen de serverruimte verwoesten", zegt Peter hierover.

"Om op dat moment businesscontinuïteit te verzekeren, moet je een oplossing klaar hebben. Want een incident valt nooit te voorzien. Komt die er en staan je processen op punt, dan is een snellere heropstart mogelijk", zegt Koen Mathijs, business unit director bij CRANIUM.

Peter van Vooren, head of digital transformation bij Remedus

"Dit is ook voor bedrijven die denken dat ze nooit het slachtoffer worden van cybercriminelen."

- Peter van Vooren, head of digital transformation bij Remedus

Verder bouwen op bestaande oplossingen

Sommige oplossingen voor cybersecurityrisico's zijn best eenvoudig, weet Koen: "Een back-up is onmisbaar. Best is dat je dit back-upproces meteen automatiseert. Dat kan eenvoudig via de meeste backup-oplossingen en antivirussoftware. Als wij kmo's adviseren, zoeken wij steeds een oplossing die de IT-aanbieder van de kmo al in zijn portfolio heeft."

Zoals veel kmo's heeft Remedus al cybersecurity-oplossingen in huis. "Onze klanten verwachten dat wij gegevens op een veilige manier behandelen. Ook onze eerste klant in het buitenland vroeg hierover garanties. Maar omdat we als kmo niet alle kennis in huis hebben, werken we samen met CRANIUM aan het optimaliseren van de oplossingen, het formaliseren en documenteren van ons cybersecurityproces."

Technologie volstaat niet

Jaar na jaar ziet Peter de cybercriminelen slimmer worden. Hij probeert de deur voor hen toe te houden: "Technologie alleen volstaat hier niet. Cybersecurity vereist ook een continue aandacht van ons personeel." "Daarom leiden wij ook het personeel op binnen het cybersecurity verbetertraject. Zij zijn vaak de achilleshiel bij cyberaanvallen, de toegangspoort voor hackers", legt Koen uit.

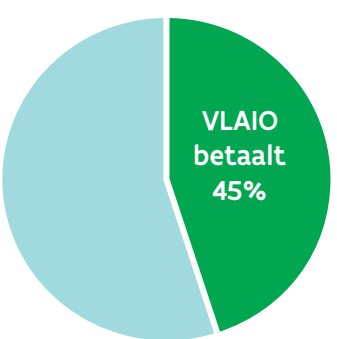
"Het cybersecurity verbetertraject hielp ons om gemakkelijker een externe expert te kiezen die in nauwe samenwerking met onze IT-partner het volledige proces aanpakt. De selectie van VLAIO gaf ons vertrouwen in CRANIUM. Bovendien verliep het interne beslissingsproces gemakkelijker omdat VLAIO een deel subsidieert", zegt Peter.

Remedus

- **Dienstenleverancier voor thuiszorg**
- **Koppelt ziekenhuizen, zorgverleners en patiënten via de app Remecare**
- **Investeert in cybersecurity, en volgde een cybersecurity verbetertraject**

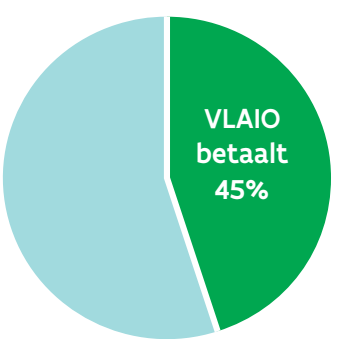
VRAAG SUBSIDIES VOOR JOUW CYBERSECURITY

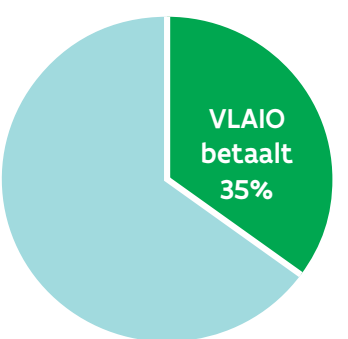
Investeren in cybersecurity is nu fors goedkoper via de cybersecurity verbetertrajecten voor kmo's en de kmo-portefeuille van VLAIO.



Cybersecurity verbetertrajecten

kleine en middelgrote ondernemingen
VLAIO betaalt 45%
Trajecten vanaf € 15.000





Kmo-portefeuille voor advies en opleiding

kleine ondernemingen
VLAIO betaalt 45%
Maximum steun: € 7.500 (incl. btw)

middelgrote ondernemingen
VLAIO betaalt 35%
Maximum steun: € 7.500 (incl. btw)

Meer info? vlaio.be/cybersecurity-verbetertrajecten en vlaio.be/kmo-portefeuille

Vind hier financiële steun, advies en begeleiding

INVESTEREN IN CYBERSECURITY DOE JE NIET ALLEEN!

Denk je aan investeren in cybersecurity? De return on investment is helemaal voor jou en je onderneming! Jouw onderneming is beter beschermd bij een cyberaanval. Maar de investering? Die doe je niet alleen! Ontdek hier welke financiële steun je hierbij kan helpen. Maak ook kennis met interessante advies- en begeleidingstrajecten die het VLAIO Netwerk aanbiedt.

FINANCIËLE STEUN

Kmo-portefeuille voor advies en opleiding cybersecurity

Wil je jouw personeel opleiden rond cybersecurity? Of zoek je kwaliteitsvol advies om een cybersecurityplan op te stellen? Sinds kort kan je voor beperktere cybersecurity trajecten beroep doen op de kmo-portefeuille. Je krijgt als kleine of middelgrote onderneming een hoger steunpercentage voor het inkopen van advies en opleiding rond cybersecurity.

VOOR WIE?

Vlaamse kmo's of beoefenaars van vrije beroepen.

VOOR WAT?

Voor de aankoop van diensten die de kwaliteit van je onderneming verbeteren. Concreet zijn dat opleidingen en adviesdiensten die je helpen met het cybersecurityplan van je bedrijf.

HOEVEEL SUBSIDIE?

Voor cybersecurity krijgen kleine ondernemingen een hogere tussenkomst van 45%. Middelgrote ondernemingen: 35%. Tot maximaal 7.500 euro per jaar.

Cybersecurity verbetertrajecten

Wil je de cyberveiligheid van je onderneming op een duurzame manier verbeteren? Krijg je graag meer vat op de kwetsbaarheden van je bedrijf? Heb je nog geen strategie om de cyberveiligheid van je onderneming te verhogen? Dan is een cybersecurity verbetertraject iets voor jou! De negen door VLAIO geselecteerde dienstverleners ondersteunen kmo's bij het duurzaam versterken van hun cyberveiligheid.
Nieuw is het lightpakket. Om nog meer kmo's te stimuleren om van cyberveiligheid een prioriteit te maken, bieden we nu ook een instapversie aan. Als kmo betaal je hiermee - na tussenkomst - zo'n 10.000 euro minder dan bij het standaardpakket.

VOOR WIE?

- **Lightpakket**: Voor kmo's die hun eerste stappen zetten op vlak van cyberveiligheid en/of kmo's met een minder complexe IT/OT-omgeving.
- **Standaardpakket**: Voor kmo's met een business kritische hoeveelheid aan IT-architectuur, software of verbonden IoT-systemen.

VOOR WAT?

Om extern advies en begeleiding in te kopen waarmee je de cyberveiligheid van jouw bedrijf versterkt. Je kiest een door VLAIO geselecteerde dienstverlener. Deze werkt samen met jou aan een grondige (technische) analyse, de opmaak van een actieplan en het oplossen van de prioritaire veiligheidsproblemen.

HOEVEEL SUBSIDIE?

- **Lightpakket**: 45% steun op trajecten tussen de 15.000 en 20.000 euro (excl. btw)
- **Standaardpakket**: 45% steun op trajecten tussen de 15.000 en 50.000 euro (excl. btw).

Innovatiesteun voor onderzoek & ontwikkeling

Koester je plannen om een innovatieve vernieuwing te realiseren en wens je hierbij aandacht te schenken aan de cyberveiligheidsaspecten? Is je bedrijf bezig met het uitbouwen of het versterken van de onderzoeks- en ontwikkelingsactiviteiten rond cybersecurity, digitalisering en/of artificiële intelligentie? Via een ontwikkelings- of onderzoeksproject krijg je van VLAIO een financieel duwtje in de rug.

VOOR WIE?

Ondernemingen, non-profitorganisaties en publiekrechtelijke organisaties die een nieuwe technologie ontwikkelen waarvoor nieuwe kennis nodig is, die processen of diensten doordacht verbeteren, een prototype bouwen of een pilootfase doorlopen.

VOOR WAT?

Voor personeels- en andere kosten gerelateerd aan het project.

HOEVEEL SUBSIDIE?

25 tot 60% van de projectbegroting met minimum 25.000 euro en maximaal 3 miljoen euro.
Ook wordt jaarlijks een thematische ICON-oproep rond cybersecurity georganiseerd. Met de CS-ICON-projecten wil VLAIO de brug slaan tussen onderzoeksresultaten op vlak van cybersecurity en toepassingen hiervan in het Vlaamse bedrijfsleven.

“De masterclass “Cyberveilig in 30 stappen” van Agoria was een goede gelegenheid om te kijken of er dingen zijn die we nog niét doen. Ze heeft ons ook geholpen om ons beleid rond cyberveiligheid te vertalen naar onze klanten.”

- Jeroen Van Hautte,
CTO & CPO TechWolf

ADVIES & BEGELEIDING

Experten uit het VLAIO Netwerk

Weet je niet goed hoe te starten met een betere cyberveiligheid en/of wil je zelf meer te weten komen over wat cyberveiligheid inhoudt? Zoek je advies, coaching of een lerend netwerk van bedrijven die voor dezelfde uitdagingen staan? Wend je dan tot de partners uit het VLAIO Netwerk. Zij sensibiliseren, adviseren en informeren ondernemers over het belang van cyberveiligheid. Ze voorzien coaching en begeleiding rond de aanpak van cyberveiligheid in de eigen onderneming. Je kan bij hen terecht voor infosessies, masterclasses, workshops, opleidingen, netwerking, begeleiding...

Blikopener hogescholen

Zoek je praktisch toepasbare kennis en projecten rond artificiële intelligentie en cybersecurity? Via het project Blikopener verspreiden 10 Vlaamse hogescholen hun kennis naar bedrijven, non-profit organisaties, gemeenten, steden, OCMW's en onderwijsinstellingen. Elke ondernemer, starter of prestarter die via praktijkgericht onderzoek een oplossing zoekt voor een concreet probleem, kan bij dit platform aankloppen. Blikopener organiseert eerstelijnsadvies, ondersteunt je bij de vraagarticulatie van het probleem en brengt je in contact met een aantal geschikte partijen om oplossingen te ontwikkelen.

“Als kmo hebben we niet alle kennis in huis. Bij het cybersecurity verbetertraject van VLAIO vonden we een externe expert die in nauwe samenwerking met onze IT-partner het volledige proces aanpakt.”

- Peter van Vooren,
Head of digital transformation bij Remedus

Proeftuin Innovatieve cyberbeveiliging voor industrie 4.0

Maakt je bedrijf gebruik van data- en geconnecteerde machines? Dan is beveiliging een must! De proeftuin Innovatieve cyberbeveiliging voor industriële bedrijven in de maakindustrie creëert demo's voor bedrijven die willen werken aan een doordacht cyberveiligheidsbeleid. Hier ontdek je alle do's en don'ts op het vlak van cyberbeveiliging. Inclusief de laatste nieuwe trends op basis van artificiële intelligentie. Ook organiseert deze proeftuin workshops, infosessies en demo's op maat van verschillende doelgroepen.

VLAIO bedrijfsadviseurs

Heb je ambitieuze digitaliseringsplannen en wil je het aspect cyberveiligheid hierbij niet uit het oog verliezen? Dan helpen de VLAIO bedrijfsadviseurs deze waar te maken. Zij gidsen je naar de juiste kennis, partners en financiële hefbomen en brengen je in contact met cybersecurity-knowhow die specifiek voor jouw bedrijf relevant is. Denk aan private aanbieders, kennisinstellingen strategische - en collectieve onderzoekscentra en intermediaire organisaties zoals Voka, UNIZO, Agoria,...

Scan de QR-code! En vind meer info online

Scan! En start vandaag nog je traject naar meer cyberveiligheid. Online vind je makkelijk de begeleiding of financiële steun die past bij jouw onderneming. Scan de QR-code en scrol door het aanbod van VLAIO en het VLAIO Netwerk.

Jouw plan voor meer cyberveiligheid

EERSTE HULP BIJ EEN CYBERAANVAL

Stel: jouw kmo wordt aangevallen door cybercriminelen. Wat doe je? Hoe stop je de cyberaanval zo snel mogelijk? Dit 7-stappenplan helpt je op weg. Het plan is gebaseerd op advies van het Centrum voor Cybersecurity België.

STAP 1

Waarschuw iedereen

Zorg ervoor dat je in het cyberplan van jouw onderneming een collega aanduidt die verantwoordelijk is om als eerste actie te ondernemen bij een cyberaanval. Die collega brengt meteen iedereen die jouw IT-systemen beheert op de hoogte van de infectie, zodat alle aangetaste computers en servers van het netwerk ontkoppeld kunnen worden. Ontkoppel ook externe harde schijven om verdere infectie te voorkomen. Opgelet! Schakel de computers niet uit. Wie dat wel doet, kan belangrijke data verliezen die nodig zijn om de aanval te stoppen.

STAP 2

Zoek de oorzaak

Probeer vervolgens zo snel mogelijk te begrijpen waar de aanval vandaan komt. Stel jezelf of je collega's de volgende vragen:

- Heeft een medewerker op een link in een e-mail geklikt?
- Zijn het besturingssysteem, de applicaties of andere software niet up-to-date?
- Heeft iemand bewust of onbewust een virus geïnstalleerd?

STAP 3

Ruim de infectie op

Zoek naar sporen, doe bijvoorbeeld een virusscan. Ga ook na of hetzelfde incident op alle andere systemen in je IT-omgeving voorkomt. Vind je bijvoorbeeld software die externe toegang geeft, maar die niemand in je team installeerde? Dan check je of deze ook op andere computers of servers staat.

Als je gevonden hebt waar de infectie vandaan komt, voer dan een virusscan uit. Doe vervolgens een update van de besturingssystemen en software op alle systemen in je netwerk.

STAP 4

Herstart vanuit back-up

Het is risicovol om geïnfecteerde systemen terug aan het netwerk te hangen. Als de infectie zich nog verder kan verspreiden, zoals bij ransomware, doe je dit beter niet.

Een volledige herinstallatie en herstart van geïnfecteerde systemen is vaak nodig. Herinstalleer de laatste versie van de software. Let op! Als je geen back-up maakte van alle bestanden ben je jouw bestanden kwijt na een herinstallatie.

STAP 5

Verander wachtwoorden

Controleer vervolgens de toegangen. Cybercriminelen gebruiken soms oude accounts met zwakke wachtwoorden om binnen te geraken. Bekijk zeker welke gebruikers toegang hebben tot de clouddiensten waarop je organisatie een abonnement heeft. Het is belangrijk om alle accounts na te kijken en eventueel toegang te weigeren. Verander de wachtwoorden van alle accounts. Hiervoor gebruik je best een wachtwoordmanager.

STAP 6

Monitor je omgeving

Is de aanval gestopt? Wees nu extra waakzaam en hou je IT-omgeving continu in de gaten. Als je merkt dat de aanval opnieuw start, is de infectie niet volledig verwijderd.

STAP 7

Verwittig de autoriteiten

Als het incident ernstig is, meld dit dan bij de autoriteiten. Doe zo snel mogelijk aangifte bij de lokale politie. Geef vervolgens het nummer van het proces-verbaal door aan je bank en je verzekeraar. Vul ook een uitgebreid invulformulier van de het federale Computer Emergency Response Team - kortweg de CERT - in. Zo zijn de diensten die in België onderzoek doen naar cybercriminaliteit meteen en gedetailleerd op de hoogte.

> “Kmo’s zien cybersecurity vaak als een kost. Maar ze kunnen het ook als een investering bekijken.”
>
> **- Vincent Naessens, cybersecurity-expert KU Leuven**

Fotocredit © Frank Toussaint

Trends in cybersecurity

4 VRAGEN AAN CYBERSECURITY-EXPERT VINCENT NAESSENS (KU LEUVEN)

Phishing, malware en kwetsbaarheden in websites zijn veel voorkomende oorzaken van cybersecurity-incidenten bij kmo’s. “Nieuwe trends maken kmo’s extra kwetsbaar”, weet cybersecurity-expert aan de KU Leuven, Vincent Naessens.

“Een architect vertelde me onlangs dat al zijn bestanden versleuteld waren”, zegt Vincent Naessens, cybersecurity-expert en auteur van De Cyber Arena. “Hij moest losgeld in bitcoins betalen om weer toegang te krijgen tot zijn data. Iets voordien vertelde mijn elektricien dat zijn klantgegevens gestolen waren. Al zijn klanten ontvingen phishingmails.”

De twee voorbeelden tonen aan dat elke kmo getroffen kan worden door cybercriminelen. En dat phishing maar één van de mogelijke wapens is van hackers.

Wat zijn vandaag de grootste cybergevaren voor kmo’s?

Vincent Naessens: “Phishing staat op één in Europees onderzoek bij kmo’s (nvdr. Enisa-onderzoek, juni 2021). Bij 41 procent van de aanvallen ligt phishing aan de oorsprong. 40 procent vindt zijn oorzaak in slecht beveiligde websites. 39 procent in malware. Als we de gevaren optellen, komen we uit boven de 100 procent. Dat komt omdat cybercriminelen een combinatie van strategieën inzetten. Zo kan phishing een hefboom zijn om malware te installeren of paswoorden te ontfutselen. Hackers laten wormen over het internet zwerven die willekeurig netwerken scannen van bedrijven. De zwakste schakels vallen door de mand.”

Welke nieuwe trends vergroten het gevaar?

Naessens: “Op kantoor en de fabrieksvloer worden steeds meer apparaten van externe fabrikanten aan internet gekoppeld: camera’s, sensoren, machines, luchtkwaliteitsmeters… Zo kunnen machineparken en kantoorruimtes op afstand gemonitord worden. Dat is handig, maar door het koppelen van die toestellen aan je IT-netwerk kunnen bijkomende zwakke toegangspunten ontstaan.

Omdat de apparaten beheerd worden door externe fabrikanten, heb je vaak weinig controle op hoe deze toestellen worden onderhouden, beveiligd en geüpdatet. Net hetzelfde met cloudoplossingen die medewerkers op eigen houtje gebruiken. Dit is de zogenaamde ‘shadow-IT’, zoals Dropbox en persoonlijke OneDrives. Mensen plaatsen er gevoelige data in… en vergroten zo de kans op datalekken.”

Hoe vermijd je cyberaanvallen?

Naessens: “Het goede nieuws is dat veel kmo’s minder attractieve doelwitten zijn en daardoor minder in het vizier komen van de zwaarbewapende cybercriminelen. Vergelijk het met inbraken en ramkraken. Het inbreken in een bank is lucratiever dan in een woning. Maar tegelijkertijd kunnen criminelen wel even van een ondermaats beveiligde woning profiteren voor een snelle inbraak.
Het toepassen van een haalbaar beveiligingsbeleid helpt veel kmo’s al vooruit.”

Cybersecurity kost toch vooral geld?

Naessens: “Kmo’s zien security inderdaad als een kost. Maar ze kunnen het ook als een investering bekijken. Vandaag zijn ze bereid om extra uit te geven aan oplossingen die duurzaam of energievriendelijker zijn.

Wanneer ze ook een beetje meer uitgeven aan veilige hard- en software en het uitrollen van een degelijk veiligheidsbeleid voorkomen ze veel problemen. Zo kunnen ze nieuwe camera’s selecteren op beeldkwaliteit, prijs én cyberveiligheid. Idem voor smartphones, netwerksystemen,… Daarenboven subsidieert de overheid verbeteringen op vlak van cybersecurity, waardoor de kost voor kmo’s gevoelig minder wordt.”

WAT IS PHISHING?

Phishing is een vorm van internetfraude waarbij een cybercrimineel probeert gevoelige informatie of geld van jou te stelen. Dit gebeurt via valse e-mails of steeds vaker via sms. Deze vorm van sms-phishing heet smishing. De oplichter kan je ook bellen. Dan spreken we over vishing, ofwel phishing via voice.

De berichten hebben één doel: je laten doorklikken naar een valse website die een perfecte kopie is van deze van je bank, de overheid of andere vertrouwde instantie. Daar ontvreemden ze je gebruikersnaam, wachtwoord, kredietkaartnummer, bankcodes, geld…

Let op voor deze 5 kenmerken

1. **Phishingberichten komen meestal onverwacht.**
2. **De taal is dwingend of wil je nieuwsgierig maken.**
3. **De mails beginnen met een vage aanspreektitel of je e-mailadres als aanspreking.**
4. **De afzender is een onbekend of foutief e-mailadres.**
5. **Er staat een link in de mail.**

Wil je phishing melden?

**Heb je een verdachte e-mail of een verdacht bericht ontvangen?
Stuur het door naar verdacht@safeonweb.be.
Check safeonweb.be voor meer info.**

Cybersecurity-raamwerk

STELT JOUW BEDRIJF DE JUISTE PRIORITEITEN?

Stelt jouw bedrijf de juiste prioriteiten op het vlak van cyberveiligheid? Pak je de meest urgente cybersecurity-uitdagingen aan? Het Raamwerk Cybersecurity van KU Leuven geeft overzicht.

Om het spoor binnen cybersecurity niet bijster te raken, ontwikkelden de specialisten van het Departement Computerwetenschappen van de KU Leuven het cybersecurity-raamwerk. Dit structureert uitdagingen volgens 5 cybersecurity categorieën. Gebruik het als checklist om je cybersecurityprioriteiten te bepalen.

1 TECHNOLOGIEDOMEINEN

De nieuwste technologie is in staat om bedrijven behoorlijk te beveiligen. Denk onder meer aan netwerk- en serverbeveiliging, endpoint-beveiliging en beveiliging van het web en mobiele applicaties.

2 GEBRUIKERS, AUTHENTICATIE EN TOEGANG

Evalueer wie toegang heeft tot applicaties en het netwerk. Beperk deze toegang zo sterk mogelijk. Ook sterke wachtwoorden en tweestapsverificatie zijn cruciaal.

3 NIEUWE DIGITALE PRODUCTEN EN DIENSTEN

Cybersecurity moet van in het begin ingebouwd worden in nieuwe soft- en hardware. Klanten zullen dit als een troef ervaren.

4 OPLEIDING EN JE ORGANISATIE WEERBAAR MAKEN

Met technologie alleen red je het niet. Maak personeel weerbaar door hen op te leiden, spreek een cybersecurity gedragscode af, benoem een verantwoordelijke en informeer alle betrokkenen regelmatig.

5 VOORBEREIDING OP INCIDENTEN

Evalueer de capaciteit op het vlak van detectie en respons. Laat een risicoanalyse uitvoeren. Check en test back-ups.

"Cyberrisico's zijn niet opgelost door het kopen van een technische oplossing", zegt Koen Simoens, COO van Sentiance dat sensordata uit je smartphone omzet in inzichten.

"Cybersecurity moet je wel met je hele team uitwerken volgens je cultuur en organisatie. Dit maatwerk vonden wij bij CRANIUM, via het cybersecurity verbetertraject van VLAIO. Zo worden wij nog beter en efficiënter in het beveiligen van de privacy van onze klanten."

"Wij kopen niet zomaar een oplossing. Cybersecurity is maatwerk."

- Koen Simoens, COO van Sentiance

Bedrijf ‘Phished’ test en traint je medewerkers

STUUR JE EIGEN MEDEWERKERS PHISHINGMAILS

Cybercriminelen mikken steeds op je zwakste schakel: je website, je digitaal netwerk, je software, je productiemachines, of... je mensen. Gelukkig kan je mensen trainen tegen het gevaar. Het Leuvense bedrijf Phished stuurt in opdracht van werkgevers phishingmails uit om de alertheid van werknemers te testen.

Gestart vanuit concreet probleem

Als organisaties voor het eerst bij Phished aankloppen, klikt de helft van de medewerkers op de phishingmails die ze uitsturen. Na een jaar is dat minder dan 5%. Arnout Van de Meulebroucke kreeg het idee voor zijn eigen bedrijf bij zijn vorige werkgever: “Ik zette er een bewustzijnscampagne op rond phishing. Ik kon kiezen uit veel tools, maar ze waren duur en tijdsintensief. Dat kon beter.” Daarop begon Arnout te bouwen in zijn vrije tijd. “Ik wilde het testen en trainen van medewerkers voor phishing automatiseren en personaliseren. De proof of concept introduceerde ik bij bevriende bedrijven. Al snel sprongen andere bedrijven mee op de kar.”

“VLAIO heeft eerder dit jaar onze verdere groei mee ondersteund via een ontwikkelingsproject.“

- Arnout Van de Meulebroucke, CEO van Phished

Businessplan 3x overtroffen

Sindsdien gaat het hard. Phished test en traint twee jaar na de opstart drie keer zoveel mensen dan Arnout had voorzien in zijn businessplan. Vanuit het hoofdkwartier in Leuven en het nieuwe kantoor in Londen bedient Phished meer dan 600 bedrijven in heel Europa en zet het partnerships op tot in Japan, Singapore, Zuid-Afrika en Canada. Eind oktober opende de Vlaamse cybersecurity-specialist een kantoor in New York om de Amerikaanse markt aan te boren.

Beter dan cybercriminelen

Wat is nu net uniek aan de tool van Phished? Arnout legt uit: “Op vlak van thema’s en professionaliteit van onze gepersonaliseerde phishingmails lopen we voor op concurrenten en cybercriminelen”. Ze spelen in op events als het EK en mailen zogezegd uit naam van een collega of een bekend bedrijf. De berichten worden geschreven door native speakers in de tien talen van de verschillende klanten.”

Met dank aan artificiële intelligentie

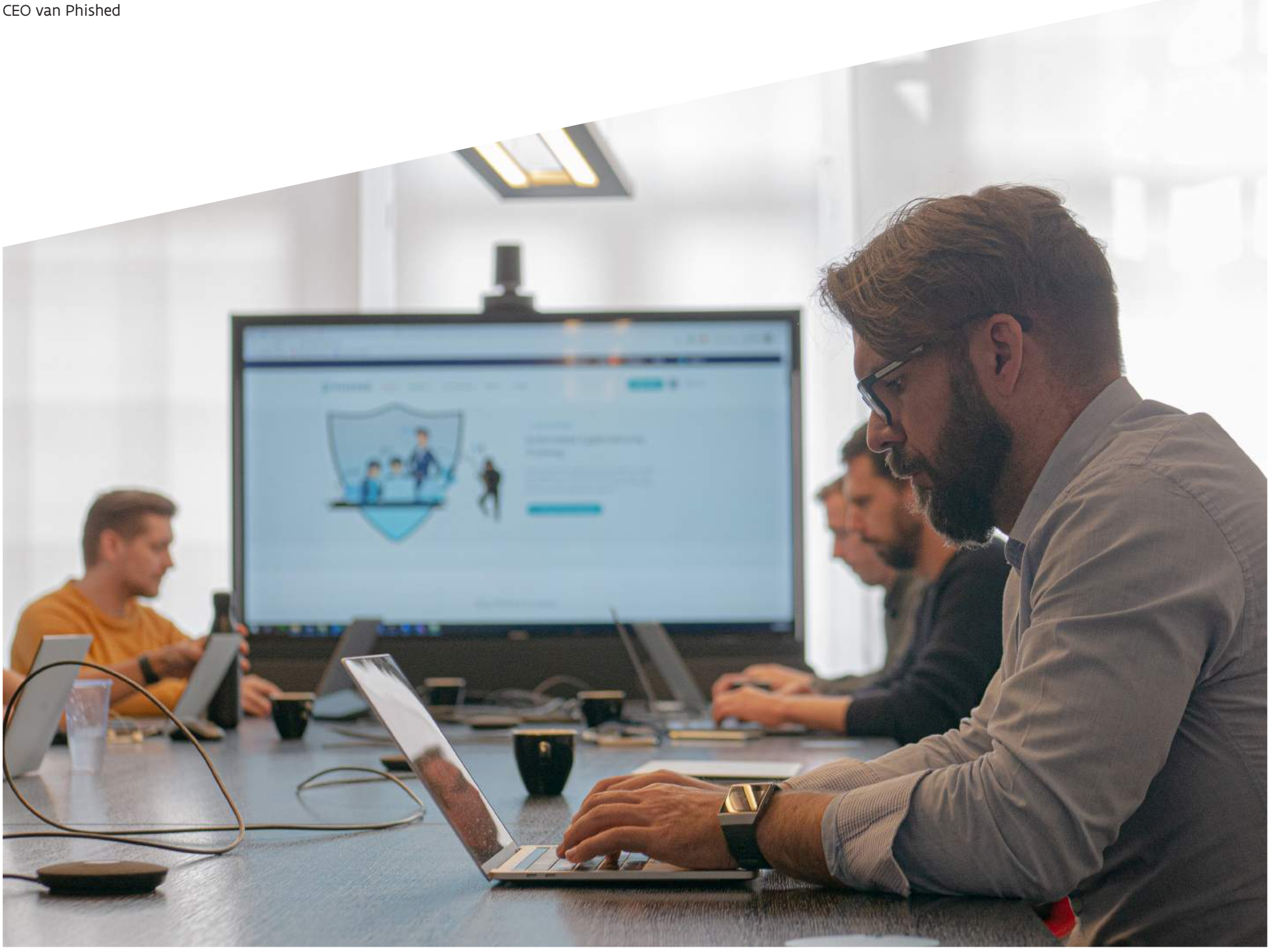
De valse phishingmails van Phished worden automatisch uitgestuurd en opgevolgd. Om dit automatisch en toch gepersonaliseerd te laten verlopen, wordt artificiële intelligentie (AI) ingeschakeld. Arnout verklaart: “AI helpt ons om gebruikers in te schatten. Zo meet het bijvoorbeeld of een marketingmanager een phishingmail rond Google Data Studio opent, hoe lang die erdoor scrolt, hoe lang het duurt voordat die klikt... Op basis van deze data krijgt elke unieke ontvanger een ID en wordt die gekoppeld aan een groep ID’s waarvan we voorspellen dat die gelijkaardig reageert. Gelinkte ID’s worden vervolgens op dezelfde manier getest en opgeleid.”

Innovatief dankzij VLAIO

Sinds januari 2021 ondersteunt VLAIO Phished via een **ontwikkelingsproject**. Met deze steun verbetert de scale-up zijn phishingmails. Bedrijfsadviseur Bas Sturm begeleidde Phished bij het opstellen van het dossier. “Ons idee was wel innovatief, maar complex en niet goed uitgelegd”, herinnert Arnout zich. “Bas hielp het concreet maken en helder uitleggen. Tegelijkertijd verbeterde hij ons idee door ons uit te dagen via de VLAIO-werkpakketten. Zowel de uitwerking als het overzicht verbeterden fors.”

“Na één jaar training klikt minder dan 5% op phishingmails. Voordien klikte nog 50% op gevaarlijke links.”

- Arnout Van de Meulebroucke, CEO van Phished



Maak nu je plan tegen hackers

10 TIPS OM EEN CYBERAANVAL TE VOORKOMEN

Cybercriminelen vallen continu Vlaamse bedrijven aan. Voorkom dat jouw onderneming ook slachtoffer wordt. Maak een plan met deze 10 actiepunten voor een verhoogde beveiliging tegen hackers.

Het aantal Vlaamse bedrijven dat slachtoffer is van hackers loopt fors op. Toch kan je een cyberaanval voorkomen. Hoe? In dit artikel sommen we 10 actiepunten op van het Centrum voor Cybersecurity België. Aarzel niet om bij het uitvoeren van deze acties beroep te doen op externe expertise!

1 Schrijf een beveiligingsplan

Je moet de strijd op verschillende fronten voeren. Deze actieterreinen breng je samen in één strategisch actieplan voor je organisatie. Stel dit plan op in nauw overleg met leidinggevenden uit verschillende diensten. Deze zijn verantwoordelijk voor de veiligheid van informatie en moeten daarvoor organisatorische doelstellingen en ambities bepalen.

2 Inventariseer de IT-infrastructuur

Weet je vandaag welke machines, toestellen en mobiele apparaten er verbonden zijn met je bedrijfsnetwerk? Wie heeft toegang tot de software? Wie logt in op deze apparaten of bedient deze? Inventariseer de volledige IT-infrastructuur, inclusief de mobiele en private toestellen van medewerkers wanneer ze hiermee mailen, surfen of online werken voor je onderneming.

3 Update alle software

Softwarefabrikanten updaten voortdurend hun programma's. Ze verbeteren hun systemen en dichten zo ontdekte lekken. Haal deze updates binnen van zodra je er melding van krijgt of kies voor automatische updates.

4 Neem back-ups

Maak dagelijks een back-up van je belangrijke gegevens en software. Bewaar deze back-up op een fysiek andere plaats of vertrouw dit back-uppen toe aan een leverancier van cloud-back-upoplossingen. Kies daarbij voor een volledig automatische dienst. Zelfs wanneer je alle gegevens kwijt bent, is het mogelijk weer op te starten met deze back-up.

5 Splits het netwerk

Splits je netwerk in verschillende deelnetwerken. Cruciale diensten zoals productie, sales en logistiek mogen nooit direct aan elkaar gekoppeld zijn. Deze netwerksegmentatie vermijdt dat virussen zich ongehinderd verspreiden. Geef ook cloudtoepassingen een aparte sectie.

6 Scherm de toegang af

Vroeger volstonden robuuste firewalls rondom bedrijven. Vandaag is een meer slimme en flexibele beveiliging nodig die vlot digitaal werken mogelijk maakt, ook via mobiele en private toestellen. Denk aan antivirusprogramma's, next generation firewalls, beveiligingsoplossingen voor je cloudtoepassingen en all-in securitypacks.

7 Check je leveranciers

Steeds meer ondernemers, kmo's en grote organisaties vertrouwen op clouddiensten. Maar ook tussen bedrijven worden data uitgewisseld. Weet je hoe betrouwbaar je leveranciers zijn? Analyseer hun beveiliging. Check hoe gegevens met de leverancier uitgewisseld worden én eis de beste bescherming voor je data.

8 Beveilig je website

Vraag je webmaster naar het beveiligingssysteem dat bij het content management systeem van je website past. Voor websites van kleinere ondernemingen kan een eenvoudige plug-in volstaan.

9 Leid je mensen op

Technisch mag je onderneming uiterst beveiligd zijn, uiteindelijk is deze beveiliging zo sterk als de zwakste schakel. Bij cybercrimes blijken mensen vaak deze zwakste schakel te zijn. Eén verkeerde klik kan de deur voor hackers wijd openzetten. Organiseer cyberopleidingen. Informeer je mensen over alle mogelijke gevaren. Spreek vervolgens een eenvoudige gedragscode af.

10 Verbeter continu

Zoals cybercriminelen steeds slimmer te werk gaan, moet je je onderneming ook alsmaar intelligenter beveiligen. Evalueer en verbeter daarbij voortdurend. Neem hiervoor een specialist onder de arm en informeer naar ondersteunende maatregelen.

Heel wat werk op de plank maar je staat er niet alleen voor!

Op blz. 6-7 ontdek je op welke financiële steun je beroep kan doen en ook welke interessante advies- en begeleidingstrajecten het VLAIO Netwerk aanbiedt. Je cybersecurity versterken doe je echt niet alleen!

vlaio.be/cybersecurity

Verantwoordelijke uitgever: VLAIO