Cybersecurity Accelerator Program (CSAP)

Versneld naar een veilige digitale transformatie met Inetum-Realdolmen

inetum realdolmen
Positive digital flow

Organisaties plukken stilaan de vruchten van de digitale transformatie waarop ze de voorbije jaren hebben ingezet. Die noodzakelijke transformatie verliep bij de ene organisatie al iets vlotter en sneller dan bij de andere. Maar verliep ze ook altijd even veilig?

In het jongste jaarlijkse prioriteitenonderzoek van Beltug, de grootste vereniging voor CIO's en IT-beslissingsnemers in België, stond security in elk geval met stip bovenaan de agenda. Het **bewustzijn** – en misschien ook wel de bezorgdheid? – rond het belang en de impact van security blijft met andere woorden groot.

Een andere gebruikersenquête van Beltug geeft daarenboven aan dat ook de investeringen in **beveiligingsproducten** de jongste jaren op peil bleven. Oplossingen voor antivirus (81%), gegevensback-up (66%) en firewall-bescherming (64%) kwamen als populairste aankopen tevoorschijn. Daarmee blijft de top drie onveranderd ten opzichte van 2020. Twee derde (64%) van de door Beltug ondervraagde bedrijven verwacht dat die investeringen ook in 2023 zullen aanhouden. Een op de vier respondenten ziet ze zelfs nog toenemen, waarbij een meerderheid (60%) de aanschaf van bijkomende beveiligingsoplossingen vooropstelt.

Security gaat echter om **veel meer dan producten alleen**. En helaas durft daar het spreekwoordelijke schoentje nog wel eens te knellen.

> "Bedrijfsleiders stellen nieuwe prioriteiten, zoals IT-beveiligingsstrategieën, gegevensbeheer en gebruikersbewustzijn."
>
> Danielle Jacobs, Beltug

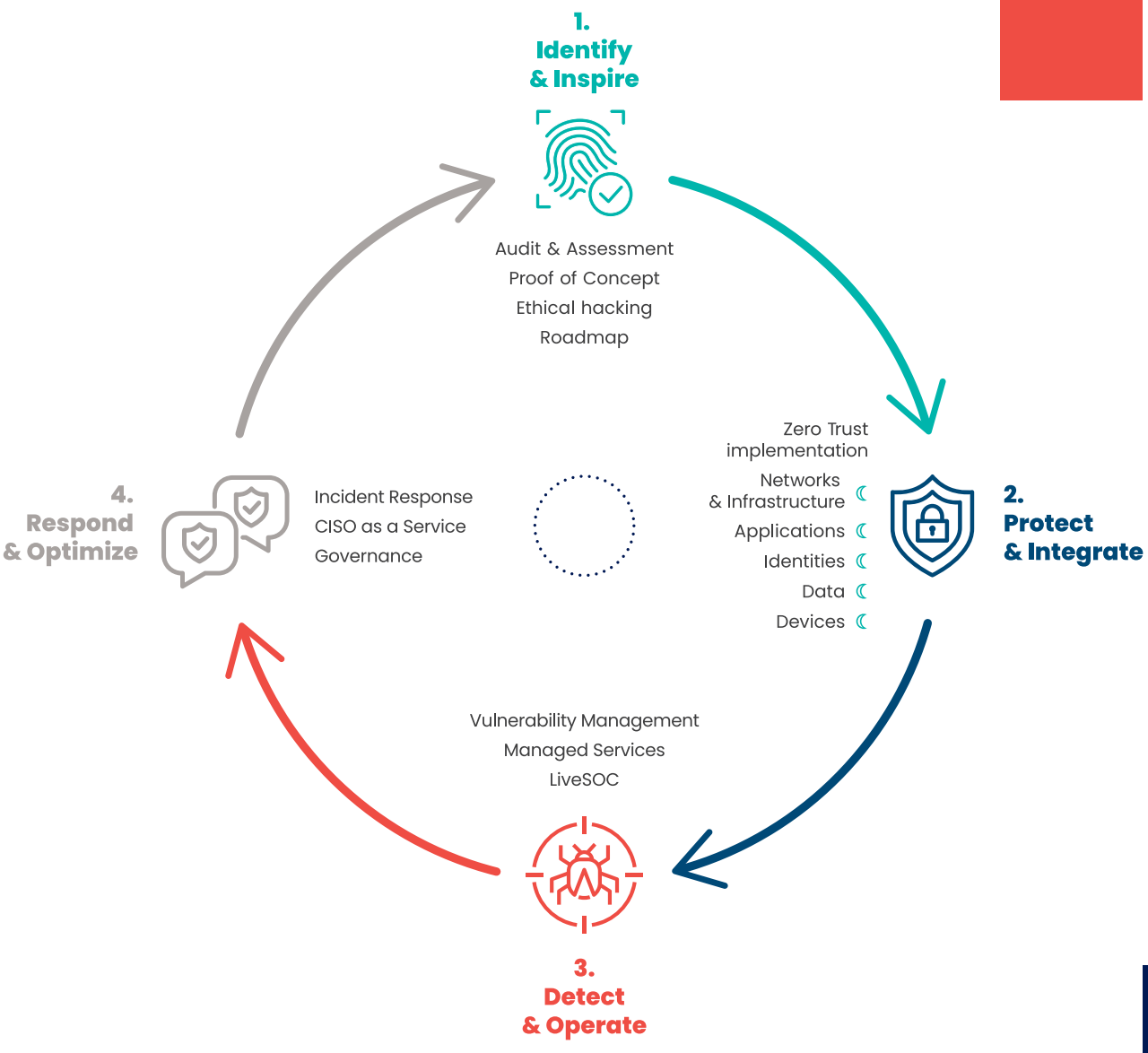
CSAP: uw garantie op een veilige digitale versnelling

Niet voor niets is de grootste bezorgdheid van Belgische CIO's, volgens het jaarlijkse prioriteitenonderzoek van Beltug, het omlijnen en uitvoeren van een duidelijke **visie** rond cybersecurity in hun bedrijf (46%). Ook uitdagingen rond de **security-architectuur** (39%) en het verhogen van de **betrokkenheid van mensen** binnen de organisatie (38%) staan hoog op de prioriteitenlijst.

Al die belangrijke, onmisbare aspecten van IT-beveiliging, die niet direct aan producten en soms niet eens aan technologie gerelateerd zijn, verdienen evenzeer uw aandacht. Om ervoor te zorgen dat geen enkel van die aspecten aan uw aandacht ontsnapt, ontwikkelden wij ons **Cybersecurity Accelerator Program (CSAP)**: een overkoepelend programma in vier stappen, dat u vanuit een holistische kijk op security een integraal aanbod aan diensten en oplossingen aanreikt. Zo helpt Inetum-Realdolmen u om snel en toch veilig de digitale transformatie van uw business te realiseren.

BENIEUWD NAAR DE VIER STAPPEN VAN ONS CYBERSECURITY ACCELERATOR PROGRAM?

Lees gauw door!



1. Identify & Inspire: een goede voorbereiding is het halve werk

Voor u ook maar een stap naar een betere beveiliging kan overwegen, moet u uiteraard eerst weten waar u op dit moment precies staat in uw verbeteringstraject. Daarom begint alles met meten en analyseren. En met experimenteren, maar dan wel om u te inspireren!

Om te vermijden dat u blind en zonder kompas vaart, brengen we eerst uw zwakke plekken of **cyberkwetsbaarheden** zorgvuldig in kaart en bepalen we uw **cybersecurity-maturiteit**. Dat doen we door middel van een **security audit en assessment**. Daarvoor kunnen we een beroep doen op onze eigen Cybersecurity Assessment Tool, maar ook op diverse audits die specifiek ontwerpen zijn op maat van een welbepaalde technologie (b.v. netwerken) of leverancier (b.v. Microsoft).

Indien nodig zetten we voor het opsporen en identificeren van uw kwetsbaarheden ook **ethische hackers** in. Daarvoor hanteren we verschillende technieken, van interne en externe **penetratietesten** tot het simuleren van een **ransomwareaanval**, en van **social engineering**, waarbij we menselijke zwaktes als nieuwsgierigheid of egoïsme proberen uit te buiten, tot het **beoordelen van code**.

Eenmaal de potentiële risico's geïdentificeerd, helpen we u ook om die te prioriteren, samen met alle acties die u kunt ondernemen om beter uitgerust te zijn tegen cyberaanvallen. De formele neerslag van die strategische analyseoefening is een cybersecurity **roadmap**. Met zijn concrete aanbevelingen, inclusief oplijsting van de nodige projecten en hiermee gepaard gaande budgetten, kan dit stappenplan bovendien als praktische handleiding dienen voor de komende jaren.

Twijfelt u of een voorgestelde beveiligings-oplossing wel geschikt is voor u? Geen nood: wij zetten graag een **proof of concept** voor u op om de mogelijkheden en toegevoegde waarde ervan te onderzoeken. Ter inspiratie organiseren wij ook **workshops** over allerlei innovaties in cybersecurity.

> "Cyberbeveiliging is geen conformiteitsverplichting, maar wel een essentieel aspect van de bescherming van uw onderneming."
>
> Pieter Byttebier, CCB

BENT U AL KLAAR VOOR NIS2?

Niet alleen de markt zelf, **ook de wetgever legt bedrijven steeds meer eisen op** inzake cybersecurity. Een treffend voorbeeld is NIS2, de **nieuwe Europese richtlijn die in 2024 in voege treedt** en beschouwd wordt als de GDPR op het vlak van cybersecurity. Het uiteindelijke doel ervan is om organisaties beter te beschermen, risico's beter te beheren en incidenten te voorkomen of de gevolgen ervan te beperken.

NIS2 heeft betrekking op **11 sectoren** meer dan NIS1. Volgens een eerste schatting van het Centrum voor Cybersecurity België (CCB) zouden er zo'n **2.400 Belgische ondernemingen** onder de nieuwe richtlijn vallen.

Bent u een van die ondernemingen? Dan raden wij aan om nu alvast werk te maken van een cybersecurity-maturiteitsanalyse en roadmap. Zo heeft u voldoende tijd om de noodzakelijke maatregelen te nemen om veilig te kunnen (blijven) opereren, in overeenstemming met de nieuwe NIS2-richtlijn. Bovendien laat dit u toe om de kosten te spreiden.

2. Protect & Integrate: zero trust security zorgt voor proactieve bescherming

Eenmaal het voorbereidende werk achter de rug, is het zaak om een solide en adequate beveiligingsinfrastructuur op maat van uw behoeften uit te bouwen. Belangrijk daarbij is dat u die infrastructuur naadloos weet te integreren in uw bestaande IT-omgeving. Maar nog belangrijker is dat die infrastructuur steunt op een innovatieve, toekomstgerichte beveiligingsarchitectuur: zero trust.

Onder die noemer gaat een nieuwe, **proactieve benadering** van security schuil. Centraal in die nieuwe aanpak staat een proces van **continue verificatie** op basis van het belangrijkste zero trust-principe: "Nooit vertrouwen, altijd verifiëren!"

Zero trust security laat u toe om sneller en efficiënter te reageren op bedreigingen en om aanvallen effectief af te slaan en zelfs te voorkomen. Daarvoor steunt het nieuwe beveiligingsconcept op een brede waaier aan **adaptieve controlemiddelen en -mechanismen**.

Om zero trust te implementeren, volstaat het bijgevolg ook niet om één enkel product, dienst, oplossing of technologie in huis te halen. Net zo min als u er zich met één enkel project of implementatie eens en voor altijd van af kan maken. Zero trust vergt een **volgehouden inspanning** op lange termijn en een **voortdurende alertheid** voor nieuwe risico's en gevaren.

"Voor de aanschaf van beveiligings-producten geven de meeste bedrijven de voorkeur aan een lokale IT-partner."

Beltug, 'B2B Market Survey – ICT Trends 2022: Security'

EEN ZERO TRUST ARCHITECTUUR BERUST OP 5 ESSENTIËLE PIJLERS:

1. **Identiteiten:** verifieer grondig de identiteit en authenticeer steeds de gebruiker voor u hem of haar toegang verleent tot uw werkomgeving via multi-factor authentication, single sign-on, identity & access management, privileged identity management en risk-based authentication
2. **Toestellen:** verhinder dat een onveilig toestel toegang krijgt tot uw werkomgeving via mobile device management, device compliance en endpoint protection
3. **Netwerken en infrastructuur:** beveilig uw netwerken en infrastructuur dankzij segmentatie, threat protection en encryption
4. **Applicaties en API's:** krijg uw applicaties en API's onder controle via access authorization, accessibility, monitoring, patch management
5. **Data:** zorg ervoor dat uw data op elk moment veilig is dankzij classification, labelling, encryption, acces and data loss prevention, backup & recovery

Voor het beveiligen van elk van die pijlers heeft u de juiste **technologische oplossingen** en de juiste **technologische expertise nodig** om al die oplossingen ook correct geïmplementeerd en geïntegreerd te krijgen. Met ons **end-to-end-aanbod van diensten en oplossingen** zit u voor dat alles meteen goed. Daarbij komt dat wij u een **extra stevige onderbouw** voor de geschetste pijlers kunnen garanderen, met oplossingen voor zichtbaarheid en analyse, automatisering en orkestratie, en last but not least: governance.

BENIEUWD NAAR DE CONCRETE BEVEILIGINGSTECHNOLOGIEËN EN -OPLOSSINGEN DIE WIJ VOORSTELLEN VOOR DE IMPLEMENTATIE VAN ZERO TRUST SECURITY?

Lees meer in onze brochure: Zero Trust, de nieuwe norm in cybersecurityland uitgelegd.

3. Detect & Operate: alertheid blijft cruciaal

Staan uw beveiligingsarchitectuur en -infrastructuur helemaal op punt? Ook dan blijft waakzaamheid geboden!

De meerderheid van succesvolle cyberaanvallen is immers terug te voeren op een bekende kwetsbaarheid die niet tijdig werd ontdekt en aangepakt. Of erger nog: op een kwetsbaarheid die de organisatie helemaal niet kende en pas weken tot zelfs maanden na de feiten wordt opgepikt. Zo beweerden zes op de tien deelnemers (62%) aan een studie van het Amerikaanse onderzoekscentrum Ponemon Institute dat ze niet op de hoogte waren van kwetsbaarheden in hun organisatie voorafgaand aan een cyberaanval.

Dat toont meteen ook het belang aan van een volgehouden, procesmatig beheer van uw kwetsbaarheden. Bij dat proces van **'vulnerability management'** gaat u kwetsbaarheden in uw infrastructuur en applicaties definiëren, identificeren, classificeren en prioriteren. Door dat te doen op basis van een gedegen **risicoanalyse** helpen wij u de enorme hoeveelheid kwetsbaarheden te verwerken, waardoor u precies de focus krijgt die u nodig hebt om snel en effectief te handelen.

In een resolutievoorstel tegen internetfraude rapporteerde de Belgische Kamer van Volksvertegenwoordigers in totaal 37.982 incidenten van cybercriminaliteit voor het jaar 2021. Dat zijn **meer dan 100 cyberaanvallen per dag**, een stijging van 37% ten opzichte van 2019.

UW VEILIGHEID, MEER DAN OOIT ONZE ZORG

Een beveiligingsinfrastructuur implementeren is één ding. Maar daarna moet u die ook nog gaan **beheren** en **blijvend optimaliseren**. En wat zo mogelijk een nog grotere uitdaging vormt: u dient die ook **continu te monitoren** op potentiële bedreigingen en kwetsbaarheden.

Zo'n **24/7-operatie**, hoe geautomatiseerd ook, vergt doorgaans heel wat mankracht en expertise. Geen nood echter als u die niet zelf in huis heeft. Alles wat wij bij u implementeren, kunnen we ook voor u beheren, optimaliseren en controleren, ter plaatse en op afstand.

Alleen al in België kunnen we daarvoor buigen op bijna 100 securityspecialisten. Samen met de meer dan 85 nearshore-experts van **LiveSOC**, ons **Security Operations Center (SOC)** in Spanje, stellen zij ons in staat om u een brede waaier aan **managed security services** aan te bieden, van preventie tot herstel van schade. Zo kunnen wij u maximaal ontzorgen.

Met **SIEM & SOC as a Service** bieden wij een 24/7 managed service die big security data analyseert en correleert door middel van SIEM-technologie (Security Information & Event Management) en het resultaat vervolgens onder het wakend oog brengt van de security-experten in ons SOC. Wilt u kleinschaliger starten, dan bieden we ook onze MicroSOC. Hiermee zorgen we ervoor dat de belangrijkste onderdelen van uw omgeving worden gemonitord en u op de hoogte wordt gebracht in geval van calamiteiten zonder nood aan een volledig uitgebouwde SIEM-/SOC-oplossing.

4. Respond & Optimize: het werk is nooit af

Heeft u een plan klaarliggen voor als het toch eens fout gaat? Snel en gepast reageren op een beveiligingsincident kan de toegebrachte schade niet alleen beperken, maar ook erger helpen voorkomen en het benodigde herstel bespoedigen.

Amper de helft van de bedrijven in België beschikt vandaag al over een securityplan, zo blijkt uit de jongste gebruikersenquête van Beltug. Al scoren grote (74%) en middelgrote (61%) bedrijven op dat gebied wel een stuk beter.

Nochtans vallen **ook kleinere bedrijven** steeds vaker ten prooi aan cybercriminelen. In 2020 kregen niet minder dan vier op de tien kmo's (42%) in België en Nederland af te rekenen met cyberincidenten. In vier op de tien getroffen bedrijven (38%) leidde zo'n incident zelfs tot een regelrechte bedrijfsstilstand.

Bent u effectief het slachtoffer geworden van een cyberaanval? Ook dan laten wij u uiteraard niet in de steek. Naast advies en ondersteuning bij het opstellen van een recovery-plan, kan u bij ons steeds terecht voor de eigenlijke **afhandeling van incidenten**, het zogenaamde 'Incident Response'-luik. Met onze gespecialiseerde **incidentrespons-teams** helpen we u snel opnieuw operationeel.

"48% weet niet wat te doen of hoe gepast te reageren bij een cyberaanval."

Agoria, Cybersecurity in de maakindustrie - 2021

Een **Chief Information Security Officer (CISO)** kan om meerdere redenen een toegevoegde waarde betekenen voor uw bedrijf - als u al niet wettelijk verplicht bent om zo'n profiel aan te stellen. Is een voltijdse CISO voor u nog te hoog gegrepen? Dan stellen wij graag onze **CISO as a Service** aan u voor: een security-expert die deeltijds de rol van CISO bij u komt opnemen.

VOOR U HET VERGEET: VERLIES ZEKER OOK DE GOVERNANCE NIET UIT HET OOG

IT-beveiliging gaat om **meer dan technologie alleen**. Governance is een minstens zo belangrijk aspect van cybersecurity. Die governance laat zich concreet vertalen in het **veiligheidsbeleid** dat u voert, de **veiligheidsprocedures** die u hanteert en de **veiligheidscultuur** die u installeert. Zo is het bijvoorbeeld essentieel dat u ervoor zorgt dat uw medewerkers op de hoogte zijn van de beveiligingsrisico's en hun rol in het beschermen van de organisatie.

Daarbij is het belangrijk dat u zich realiseert dat cybersecurity geen statisch gegeven is, maar een **cyclisch proces**. Noem het gerust een eeuwig work-in-progress. Anders gezegd: als verantwoordelijke voor cybersecurity is uw werk nooit écht af. Daarom omvat effectieve cybersecurity-governance bijvoorbeeld ook het continu verbeteren van de beveiligingsattitude door middel van **regelmatige training, bewustmaking** en incidentrespons-planning.

Door uw **cybersecurity-doelen** af te stemmen op uw algemene bedrijfsdoelstellingen en strategieën voor risicobeheer, raakt cybersecurity ten slotte helemaal geïntegreerd in de cultuur en operaties van uw organisatie. Zo geldt cybersecurity ook niet langer als een kostenpost of een verplichte last, maar als een **rendabele strategische investering**.

SAMEN MAKEN WIJ ER WERK VAN!

Hoe veilig is uw IT-omgeving? Heeft u al een 'foto' genomen? Hoe zorgen voor een zero trust-architectuur en die ook up-to-date houden? Misschien heeft u zelf al stappen gezet in dit **Cybersecurity Accelerator Program**, maar wenst u bepaalde onderdelen verder uit te werken. In alle gevallen kan u bij ons aankloppen. Voor alle services en technologische pijlers die in dit document aan bod komen, hebben wij de nodige expertise in huis. Samen maken wij zo werk van een veiligere werkomgeving!

NEEM CONTACT OP

Powered by our Cybersecurity Partners

Microsoft · paloalto NETWORKS · FORTINET · CHECK POINT · vmware · TREND MICRO

HPE aruba networking · HOXHUNT · citrix · CROWDSTRIKE · AvePoint · CISCO

tenable · kaspersky · VEEAM · COMMVAULT · Secutec · THALES

splunk> · zscaler · netskope · MICRO FOCUS · Forcepoint

Inetum-Realdolmen
A. Vaucampslaan 42
1654 Huizingen, Belgium
+32 2 801 55 55
www.inetum-realdolmen.world
info@inetum-realdolmen.world

inetum realdolmen
Positive digital flow