Stay connected.
Stay safe.

Jaarverslag 2025 Skyleaf

CYBERWOLF
your digital bodyguard

spotit
YOUR SECURITY & NETWORK LAYER

Het jaar van blijvend vertrouwen en langetermijn-partnerschappen

2025 bevestigde opnieuw wat voor ons het belangrijkste is: vertrouwen. Meer dan ooit zien klanten spotit als hun voorkeurspartner voor cybersecurity en networking. Dat is het resultaat van sterke, duurzame relaties die we elke dag uitbouwen, gebaseerd op betrouwbaarheid, expertise en échte samenwerking.

Wat ons blijft onderscheiden, is onze geïntegreerde aanpak. Netwerk en security kan je niet los van elkaar bekijken. IT- en OT-omgevingen groeien steeds meer naar elkaar toe. Alleen door die samen te benaderen, kan een organisatie er zeker van zijn dat haar securityvisie klopt en toekomstbestendig is. Die holistische kijk blijft een fundament van onze strategie.

Dat velen ons daarin volgen, mag blijken uit onze resultaten. We realiseerden een solide groei, met een omzetstijging van 21%. Een belangrijke mijlpaal in 2025 was de hernieuwing van onze samenwerking met Fluvius, na een nieuwe openbare aanbesteding. Opnieuw geselecteerd worden, en dat voor een lange termijn en met een uitgebreidere scope, is een krachtig signaal van wederzijds vertrouwen. Maar groei op zich is nooit het einddoel. Wat echt telt, is wat achter die cijfers zit: de inzet van onze mensen, de kwaliteit van onze dienstverlening en de impact die we maken door organisaties te begeleiden in steeds complexere security- en connectiviteitsuitdagingen.

Een andere belangrijke vaststelling in 2025 is de groeiende waarde van onze 100% Belgische verankering. In de huidige geopolitieke context is digitale soevereiniteit belangrijker dan ooit. Vanaf dag één kozen we ervoor om uitsluitend met Belgische professionals te werken en onze kernactiviteiten binnen NOC en SOC volledig lokaal te organiseren. Dat garandeert beschikbaarheid, continuïteit en gemoedsrust, 24 uur per dag, 7 dagen op 7. Je kan spotit niet ‘uitzetten’.

In 2025 organiseerden we opnieuw een succesvolle editie van onze Academy, ons opleidingstraject voor startende medewerkers. Daarmee investeren we niet alleen in kennisdeling, maar ook in de versterking van onze lokale expertise. Zo garanderen we onze klanten de Belgische continuïteit en hands-on ondersteuning die ze verwachten.

Ook bij Cyberwolf zetten we in 2025 een volgende stap in onze internationale groei. We breidden onze samenwerkingen in de Verenigde Staten verder uit en werken vandaag samen met drie van de tien grootste banken in de VS om hun wealth-klanten te beschermen. Sinds de start kende Cyberwolf een groei van 300%. Het bewijst dat hooggespecialiseerde, in België ontwikkelde beschermingsdiensten ook internationaal erkenning krijgen op het hoogste niveau.

Dit Skyleaf Annual Report bundelt de hoogte-punten van 2025 en toont de gecombineerde expertise van spotit en Cyberwolf. Het geeft een helder beeld van hoe we denken, hoe we werken en hoe we onze klanten ondersteunen.

Dank voor het blijvende vertrouwen. We kijken ernaar uit om samen de volgende hoofdstukken te schrijven in een wereld waarin connectiviteit blijft toenemen en security alleen maar belangrijker wordt.

Steven Vynckier en Frederik Rasschaert, oprichters van spotit en Cyberwolf

Over Skyleaf

Ons bedrijf werkt met een holdingstructuur, wat betekent dat er een moedermaatschappij is die toezicht houdt op verschillende entiteiten. De holding heet Skyleaf, met spotit en Cyberwolf als entiteiten. De missie is duidelijk: de wereld een veilige online plek maken voor mensen, machines en bedrijven.

Wie is **Cyberwolf**?

Cyberwolf is een 24/7 digitale bodyguard voor het privéleven van executives, bestuurders, ondernemers, diplomaten en vermogende families wereldwijd. Waar spotit organisaties beschermt, beschermt Cyberwolf de mensen achter die organisaties. We beveiligen toestellen, e-mail, accounts en thuisnetwerken, monitoren dreigingen en dark web-activiteiten en grijpen in bij incidenten.

Ons doel is eenvoudig: mensen de vrijheid geven om zich met vertrouwen in de digitale wereld te bewegen. Cyberwolf brengt rust in een omgeving waar onzichtbare risico's vaak voor onzekerheid zorgen.

Wie is **spotit**?

Spotit creëert gemoedsrust voor alles wat te maken heeft met beveiliging en connectiviteit. Als strategische partner zetten we sterk in op visie, expertise en vertrouwen. We maken het verschil met een high-level security- en netwerkaanpak op lange termijn, waarbij we vertrekken van een actieplan met concrete doelstellingen.

Lokaal verankerd in België, ondersteunen meer dan 120 hoogopgeleide experts organisaties bij het veilig, performant en veerkrachtig maken van hun digitale infrastructuur. Dit voor zowel IT- als OT-omgevingen.

Wat zijn onze **waarden**?

Human to Human
Bij Skyleaf draait alles om échte connecties tussen mensen. We zetten collega's, klanten en partners centraal en geloven dat open communicatie en wederzijds respect de basis vormen voor sterke samenwerkingen.

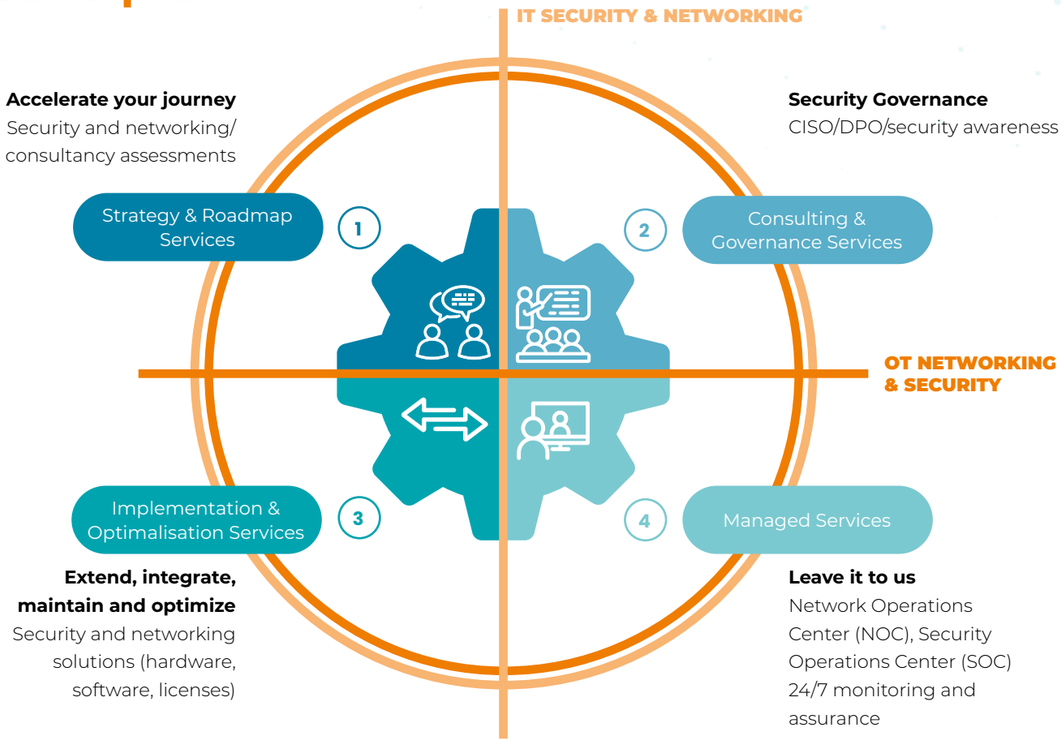
Excel
We streven naar uitmuntendheid en nemen geen genoegen met middelmatigheid. Excelleren zit in onze mindset: elkaar blijven uitdagen, continu verbeteren en elke dag beter willen doen voor onze klanten.

Entrepreneurship
Ondernemerschap zit in het DNA van ons team. We nemen verantwoordelijkheid, tonen initiatief en gaan samen 'the extra mile' om oplossingen te realiseren, ook buiten onze comfortzone.

Trust
Vertrouwen is cruciaal, zeker in cybersecurity. We gaan uiterst zorgvuldig om met gevoelige informatie en staan voor betrouwbaarheid, integriteit en het nakomen van onze beloftes.

Corporate Social Responsibility
Duurzaam ondernemen is voor ons een bewuste en geïntegreerde keuze. We verkleinen actief onze ecologische voetafdruk, gaan voor een transparant en integer bestuur met oog voor langetermijnwaardecreatie, en investeren in mensen door te focussen op welzijn, ontwikkeling en samenwerking met externe partners. Zo creëren we positieve impact, zowel binnen onze organisatie als daarbuiten, en nemen we verantwoordelijkheid voor vandaag én morgen.

Wat doet **spotit**?



Het 2025 van Skyleaf

We bundelden de krachten met SHIELD

Bekijk de getuigenis!

Ziekenhuizen en hogeronderwijsinstellingen dragen een grote maatschappelijke verantwoordelijkheid. Wanneer digitale systemen uitvallen, heeft dat directe impact op patiënten, studenten en medewerkers. Daarom bundelt spotit de krachten met SHIELD vzw en Cisco om de cyberweerbaarheid in deze sectoren structureel te versterken. Zo positioneren we ons als een gerichte partner voor zorg en onderwijs.

We blijven groeien

In 2025 verwelkomde spotit 18 nieuwe collega's. Daarmee groeit het team verder, met talent van 24 tot 61 jaar. Het verloop bleef beperkt tot 14%, wat laag is voor de sector. Zo blijven we bouwen aan continuïteit, ervaring en frisse expertise, met één duidelijke focus: onze klanten elke dag beter ondersteunen.

Partnership met XONA

In het kader van NIS2 versterkten we ons aanbod rond secure remote access met een partnership met XONA, gespecialiseerd in OT- en ICS-omgevingen. Samen helpen we organisaties klassieke VPN-oplossingen te vervangen door zero-trust toegang, met rol- en tijdsgebonden rechten en volledige logging van alle sessies.

Cyberwolf kreeg tractie

In 2025 trad Cyberwolf bewust naar buiten. Via gerichte artikels en interviews maakten we duidelijk wat we doen: digitale bescherming bieden aan leidinggevenden en hun gezinnen. We positioneerden Cyberwolf ook expliciet als een bedrijfsvoordeel, zodat organisaties hun executives structureel kunnen ondersteunen op het vlak van persoonlijke cybersecurity. De Verenigde Staten werden een belangrijke groeimarkt. Onze aanpak kreeg er tractie, onder meer via samenwerkingen met drie van de tien grootste Amerikaanse banken. Met nieuwe investeringen, een versterkt team en een toenemende vraag sloten we het jaar af met een duidelijke basis voor verdere expansie in de VS. Daarnaast zetten we onze eerste stappen in sport en entertainment, met de onboarding van onze eerste bekende atleet.

3

Tijdens de Cisco Partner Summit 2025 werd spotit bekroond met drie awards: Security Partner of the Year – Belgium, Security Partner of the Year – North Theatre en Public Sector Partner of the Year – Belgium. De awards zijn het resultaat van een sterke en duurzame samenwerking met Cisco, die inmiddels meer dan tien jaar loopt en jaar na jaar wordt verdiept.

Whitepaper | IT Cybersecurity Maturity: Your Roadmap Towards Excellence

Veel organisaties overschatten hun cybersecurityniveau en ontdekken de kwetsbaarheden pas wanneer het fout loopt. Uit meer dan vijftig fundamental security assessments blijkt dat basismaatregelen vaak onvoldoende structureel zijn ingebed. We lanceerden eind 2025 een whitepaper die onze inzichten uit die assessments bundelt.

Lees hem hier

NPS-score van 53 toont vertrouwen van klanten in spotit

Al meer dan 5 jaar na elkaar laat spotit een uitgebreid Net Promoter Score (NPS) onderzoek uitvoeren door een externe partij. Het doel: dieper inzicht krijgen in wat klanten echt denken over onze dienstverlening en het identificeren van zaken vatbaar voor verbetering. Uit het onderzoek van 2025 bleek dat we een knappe score van 53 behalen.

Met de duurzame groeiambities van spotit scherp in het vizier, staat de tevredenheid van onze klanten centraal. Om die te meten bevragen we elk jaar een selectie van klanten. Via NPS-onderzoek krijgen we een holistisch beeld van hoe zij de samenwerking ervaren en wat hun verwachtingen voor de toekomst zijn. De Net Promoter Score (NPS), een heldere indicator van klantentevredenheid en klantloyaliteit, fungeert daarbij als kompas.

De NPS kan variëren van -100 tot 100. Elke score boven 0 wordt als positief beschouwd, omdat dat betekent dat er meer voorstanders zijn dan tegenstanders. Algemeen wordt aangenomen dat een score boven de 30 goed is en boven de 50 uitstekend is, terwijl een score boven 70 uitzonderlijk is. Dergelijke hoge scores zijn echter vrij zeldzaam. In veel sectoren is een NPS tussen 30 en 50 een realistisch doel en een indicatie van goede klanttevredenheid.

Met een knappe NPS-score van 53 mag spotit zich zeker en vast positioneren als een toonaangevende en sterke dienstverlener in de IT-sector. Klanten benadrukken dit jaar naast expertise en betrouwbaarheid ook partner in cybersecurity als kernsterktes. De feedback weerspiegelt een diep vertrouwen in spotits vermogen om als betrouwbare partner en expert te fungeren, met een menselijke aanpak als onderscheidende factor en steeds met heel veel kennis van zaken op het vlak van IT/OT cybersecurity en networking. Dat stemt ons uitermate tevreden. Want dit is 100% in lijn met hoe we in de markt willen staan: niet als een pure leverancier, wel als een betrouwbare partner.

DE VOLGENDE STAPPEN

Met enkel goed nieuws maken we uiteraard geen progressie. Aandachtig luisteren naar wat beter kan en kritisch zijn voor onszelf is en blijft de boodschap. Het onderzoek identificeerde dan ook enkele verbeterpunten. Meer proactieve communicatie (zoals de klant op de hoogte houden dat er wordt gewerkt aan het ticket) en ook meer inzetten op kennisdeling en -borging (tussen spotit en de klant) worden genoemd. We gaan hier uiteraard mee aan de slag en zien dit als mooie kansen om de algehele klanttevredenheid verder te verhogen.

ONDERZOEK CYBERWOLF

CEO's van BEL20-bedrijven zijn aantrekkelijk doelwit voor hackers

De grote meerderheid van de CEO's van de Bel20-bedrijven is kwetsbaar voor een cyberaanval via hun privétoestellen en -accounts. Dat blijkt uit een analyse gemaakt door Cyberwolf. Gedurende drie maanden hield Cyberwolf de digitale blootstelling van deze CEO's in de gaten. Daaruit blijkt dat 70% van hen makkelijk benaderbaar is via publiek zichtbare kwetsbaarheden in hun eigen organisatie of via andere mandaten die ze bekleden.

Hackers misbruiken vandaag gretig de hybride werkomgevingen van topmanagers. Een persoonlijke smartphone, email of thuisnetwerk bieden eenvoudig toegang tot waardevolle bedrijfsinformatie of -accounts. "Topmanagers zijn een strategisch en bewust doelwit voor zowel cybercrime als geavanceerde bedrijfsspionage door concurrenten of buitenlandse inlichtingendiensten. Maar het kan evengoed 'per ongeluk' – geautomatiseerde scans zoeken 24/7 naar elk mogelijk beveiligingslek, klaar om toe te slaan zodra ze een opening vinden", vertelt Daan Gheysens, CEO van Cyberwolf.

"De bestuurskamer hanteert geregeld dubbele standaarden: terwijl cybersecurity wordt bestempeld als topprioriteit, vragen bestuurders niet zelden om persoonlijke uitzonderingen op beveiligingsprotocollen."

Alarmerende cijfers

De ambitie om onze topmanagers beter te beschermen zou best hoger mogen liggen, want kwetsbaarheden zijn er overal. Onderzoek uitgevoerd door Cyberwolf op alle BEL20-topmanagers toont aan dat we ons geen illusies mogen maken over de huidige veiligheidscontext.

- 70% van alle BEL20-CEO's kan gemakkelijk worden getarget via publiek zichtbare kwetsbaarheden in hun eigen bedrijf of via mandaten die ze aanhouden in andere organisaties.
- Dat cijfer stijgt naar 95% wanneer kwetsbaarheden van gelieerde goede doelen of gespecialiseerde (sectorspecifieke) pers meetellen.
- Voor 80% van de BEL20-CEO's kan binnen vijf minuten een geloofwaardige deepfake van hun stem worden gemaakt.

Het onderzoek en bevindingen werden gedeeld met de geïmpacteerde organisaties en het CCB (Centrum voor Cybersecurity België). De resultaten werden ook opgepikt door de krant De Tijd.

“Dit is veel meer dan een klant-leverancierrelatie”

Fluvius beheert infrastructuur die essentieel is voor het dagelijkse leven in België. Het bedrijf zorgt voor de distributie van elektriciteit, aardgas, riolering en warmte. De maatschappelijke shift richting elektrificatie verhoogt de druk op die netwerken en maakt robuuste digitale infrastructuur belangrijker dan ooit. Al jaren rekent Fluvius daarvoor onder meer op spotit. Kurt Ceulemans, Afdelingshoofd Systemen en Operaties, en Wouter De Clercq, Diensthoofd Centrale Infrastructuur, gaan in gesprek met Steven Vynckier en Frederik Rasschaert, oprichters van spotit.

“Outsourcing is met de juiste partner geen verzwakking, maar een versterking.”

Wouter De Clercq
(Diensthoofd Centrale Infrastructuur bij Fluvius)

Fluvius is een grote organisatie die kritieke infrastructuur beheert. Dat brengt wellicht specifieke uitdagingen met zich mee op het vlak van netwerkbeheer?
Kurt Ceulemans: “Absoluut: het is duidelijk dat we middenin een maatschappelijke shift zitten. Elektrificatie is vandaag alomtegenwoordig. Daarin spelen wij een sleutelrol. Daarvoor volstaan de elektriciteitsnetten zoals we die kennen uit het verleden niet meer. Uiteraard worden ze uitgebreid en komen er extra kabels bij, maar dat alleen zal niet voldoende zijn. Daarom moeten we elektrificatie ook op een andere manier ondersteunen: door ons (IT-)netwerk slimmer te maken. We moeten grote hoeveelheden informatie uit het elektriciteitsnetwerk kunnen capteren, analyseren en er in realtime op reageren. De netwerken die die informatie en sturing transporteren, worden daardoor steeds belangrijker. Flexibiliteit is daarbij een sleutelbegrip.”
Wouter De Clercq: “Onze infrastructuur wordt almaar crucialer en ons IT-netwerk moet meegroeien met die evolutie. Zeker in een sterk geautomatiseerde omgeving is het essentieel dat we vandaag al klaarstaan voor morgen.”

Wat maakt jullie IT- en OT-omgeving fundamenteel anders dan die van een klassieke organisatie?
Wouter De Clercq: “Dan denk ik vooral aan het belang van continuïteit: de beschikbaarheid van elektriciteit en gas is voor de maatschappij cruciaal. Precies daarom is het zo belangrijk dat we digitale componenten onder controle hebben en actief kunnen aansturen. Het is een fundamentele evolutie die we vandaag doormaken en waarvan het belang alleen maar zal toenemen.”
Kurt Ceulemans: “Die beschikbaarheid en continuïteit hangen vandaag nauw samen met convergentie. Waar je vroeger duidelijke muren kon optrekken tussen IT- en OT-systemen, moeten die grenzen nu bewust worden afgebouwd. Die evolutie is nodig om flexibiliteit mogelijk te maken en ook te vermarkten. Denk maar aan batterijparken of bedrijven die bereid zijn hun productie tijdelijk te verlagen: daarvoor is de link tussen IT en OT cruciaal. Informatie moet veilig, betrouwbaar en snel van het ene domein naar het andere kunnen stromen, zodat er ook onmiddellijk op kan worden geageerd. Alleen zo kunnen we het elektriciteitsnetwerk continu in evenwicht houden. Een tijdelijke uitval van ons IT-netwerk was vroeger wel vervelend maar de impact bleef beperkt, terwijl een storing vandaag rechtstreekse gevolgen kan hebben voor het elektriciteitsnet en eindgebruikers.”
Frederik Rasschaert: “Een bijkomende uitdaging is dat je steeds meer beschikbaarheid nodig hebt, terwijl je tegelijk ook meer security moet toevoegen. Dat betekent dat je het netwerk continu moet onderhouden. En om te vermijden dat je het moet stilleggen, moet je het netwerk steeds redundanter maken.”
Kurt Ceulemans: “Redundanter én intelligenter. Waar je vroeger gewoon een extra component toevoegde aan je netwerk en het probleem opgelost was, volstaat dat vandaag niet meer. Nu moet je heel bewust nadenken over de juiste architectuur. Net daar ligt de grote uitdaging. Om ons daarin te ondersteunen, hebben we sterke partners nodig, waaronder spotit.”

Het ideale moment om even terug te blikken naar het begin van jullie samenwerking, in 2017. Waarom besliste Fluvius toen om samen te werken met spotit?
Kurt Ceulemans: “Daarvoor ga ik nog verder terug in de tijd, naar de vrijmaking van de energiesector, een 20 jaar geleden. Toen werden productie en distributie van elektriciteit en gas geleidelijk aan van elkaar gesplitst en ontstonden verschillende organisaties, waardoor ook de IT-diensten moesten worden opgesplitst. Er is toen beslist om een aantal IT-elementen uit te besteden, waaronder delen van het serverbeheer en delen van het beheer van het digitale netwerk. Bij een iteratie van de aanbesteding in 2017 heeft spotit zich kandidaat gesteld voor dit laatste lot.”
Wouter De Clercq: “We waren op zoek naar diepe technische expertise en operationele maturiteit. Betrouwbaarheid binnen die specifieke domeinen was cruciaal. Spotit was toen nog een relatief klein bedrijf. Dat hield voor ons een zeker risico in, maar we zagen dat ze over de juiste expertise en een sterk operationeel model beschikten. We hebben toen heel bewust die sprong gewaagd om voor hen te kiezen.”

Kurt Ceulemans: “Ook al was spotit toen nog relatief jong, het heeft de uitdaging ten volle opgenomen en is zijn samen met ons meegegroeid. In die acht jaar werd een sterk trackrecord opgebouwd en de samenwerking zat goed.”

Vorig jaar werd na een nieuwe aanbesteding het partnership vernieuwd. Waarom?
Kurt Ceulemans: “Spotit kwam als beste kandidaat uit de aanbesteding. Los daarvan is voor mij vertrouwen een sleutelelement. Weten dat we echt op elkaar kunnen rekenen.”
Steven Vynckier: “We kunnen hier echt van een partnership spreken, in goede dagen maar ook in kwade. In IT doen zich af en toe problemen voor. Het is de manier waarop je daarmee omgaat die het verschil maakt. Door issues snel en met zo weinig mogelijk impact op te lossen, toon je echte samenwerking, ook in moeilijke periodes.”

Kun je de samenwerking met spotit echt als een partnerschap beschouwen?
Kurt Ceulemans: “Absoluut. Onlangs zaten we bijvoorbeeld met een organisatorische uitdaging en hebben we spotit gevraagd hoe zij ons daarbij konden ondersteunen. Die openheid en bereidheid om mee te denken appreciëren we enorm. Dat is die extra stap die maakt dat één plus één drie wordt.”
Wouter De Clercq: “We werken dagelijks samen als één geïntegreerd team en communiceren open. Wij nemen natuurlijk wel de eindbeslissingen, maar spotit denkt actief mee, zoekt samen met ons naar oplossingen en opportuniteiten. Dat is dus veel meer dan een gewone klant-leverancierrelatie.”

Hoe bereiden jullie je vandaag voor op de toekomst? Welke projecten staan op de roadmap?
Wouter De Clercq: “Er lopen heel wat projecten. We zetten sterk in op verdere automatisatie van netwerkbeheer en op een continue lifecyclevernieuwing binnen data- en telecomcommunicatie. Die connectiviteit met nieuwe systemen en toestellen is essentieel om alles online en operationeel te houden. De uitdagingen stoppen niet, dus moeten we blijven investeren in digitalisering en de maturiteit van onze organisatie.”
Kurt Ceulemans: “Alleen al in het elektriciteitsnet investeren we de komende tien jaar meer dan tien miljard euro. Dat is een gigantische operatie. Onze schakelposten worden digitaal, net als andere onderdelen van het netwerk. Veel mensen weten niet dat we ook een groot deel van het rioleringsnetwerk beheren. Ook daar zetten we volop in op digitalisering, met meetpunten in de rioleringen en digitale monitoring van buffers en bekkens. Hetzelfde geldt voor warmte, bijvoorbeeld bij de distributie van restwarmte uit verbrandingsovens. Overal zetten we stappen richting een datagedreven organisatie. Ons IT/OT-netwerk is daarvoor de basis.”

Mooi om daar als IT’er aan mee te werken, toch?
Wouter De Clercq: “Absoluut. Fluvius is een grote organisatie met heel veel IT. Dat geeft veel voldoening, omdat je zowel in de breedte als in de diepte kan werken. De nieuwe evoluties zijn een extra uitdaging die natuurlijk ook druk met zich meebrengt. Dat vraagt om sterke partners om de juiste beslissingen te nemen en verder te groeien in maturiteit.”
Steven Vynckier: “De mensen die bij ons werken, willen zichzelf blijven uitdagen. En Fluvius biedt die uitdagende omgeving waar zij zich technisch en technologisch kunnen blijven ontplooien. Ze bouwen bovendien mee aan verschillende nutsvoorzieningen. Daarnaast is er het one-teamgevoel, met een symbiose tussen twee teams, en het partnership waarbij effectief geluisterd wordt naar elkaar.”
Frederik Rasschaert: “Een van de sterke punten in onze relatie is dat Fluvius veel uitdagingen heeft binnen ons expertisegebied. Dat is exact waar wij dagelijks mee bezig zijn. Daardoor is er een grote betrokkenheid binnen onze organisatie, van het hoger management tot de mensen op de werkvloer. Dat engagement is wat ons partnership mee definieert.”

“We moeten grote hoeveelheden informatie uit het elektriciteitsnetwerk kunnen capteren, analyseren en er in realtime op reageren. De netwerken die die informatie transporteren, worden daardoor steeds belangrijker.”

Kurt Ceulemans (Afdelingshoofd Systemen en Operaties bij Fluvius)

Wat mogen lezers hier vooral van onthouden?
Wouter De Clercq: “Voor bedrijven die ook overwegen om IT te outsourcen wil ik benadrukken dat outsourcing met de juiste partner geen verzwakking is, maar een versterking. Je haalt iemand binnen die meedenkt, mee investeert en verantwoordelijkheid opneemt.”
Kurt Ceulemans: “Bij de keuze van de juiste partner is vertrouwen essentieel, en de zekerheid dat je bij een probleem of opportuniteit kan terugvallen op die partner. Dat je de telefoon kan nemen, elkaar kan bellen en samen rond de tafel kan zitten, met de nodige ernst en betrokkenheid. Dat is key. Uiteindelijk wil je dat het netwerk blijft functioneren en ook klaar is voor de toekomst. En daarin hebben we vandaag een sterke partner gevonden.”
Steven Vynckier: “We zijn Fluvius in elk geval dankbaar voor het vertrouwen. Het was destijds een moedige keuze om met een kleinere partij samen te werken. Dankzij dat vertrouwen hebben wij kunnen groeien. Dat is een echte win-winsituatie.”
Kurt Ceulemans: “Wij zijn er van onze kant ook fier op dat we hebben bijgedragen aan de groei van een sterk Belgisch bedrijf. Dat mogen we zeker benoemen.”

En hoe kijken jullie vooruit?
Kurt Ceulemans: “De verwachtingen blijven hoog. De uitdagingen blijven evolueren; ons netwerk zal nooit ‘af’ zijn. Het is een constante samenwerking waarin we samen de volgende stappen zetten. En daarin blijven we rekenen op spotit.”
Wouter De Clercq: “Spotit heeft zich intussen duidelijk gepositioneerd als expert en als drijvende kracht achter innovatie. We rekenen erop dat ze ook in de toekomst voorop blijven lopen binnen hun domeinen en die expertise verder blijven verdiepen.”
Steven Vynckier en Frederik Rasschaert: “Challenge accepted!”

Wie is Fluvius?

Fluvius is het netbedrijf dat verantwoordelijk is voor het aanleggen, beheren en onderhouden van distributienetten voor elektriciteit, aardgas, riolering en warmte. Fluvius beheert ook het gemeentelijke openbare verlichtingspark. In totaal beheert het bedrijf 230.000 kilometer aan nutsleidingen en 7 miljoen aansluitingen. Fluvius is in alle Vlaamse steden en gemeenten actief.

FACTS &STATS

€32.000.000
Omzet spotit

5 SECTOREN WAAR WE HET MEEST ACTIEF ZIJN

1. Nutsbedrijven & energiesector
2. Productie- & procesindustrie
3. Logistiek & haven
4. Farmatech & lifesciences
5. Gezondheidszorg & onderwijs

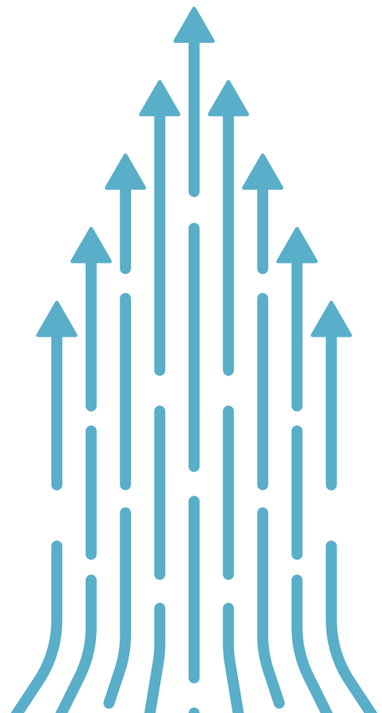
MEEST POPULAIRE ASSESSMENTS IN 2025

- Pentest
- Fundamental security assessment
- NIS2 assessment

+21%
groei

X3
groei Cyberwolf

+19%
groei managed services



230
actieve klanten (in portefeuille)

CASE

Fednot ondersteunt notarissen veilig en vlot digitaal

Fednot, de federatie van het notariaat in België, speelt een cruciale rol in de ondersteuning van notariskantoren op juridisch, administratief en technologisch vlak. Met meer dan 1.100 kantoren, 1.754 notarissen en bijna 10.000 medewerkers is **digitalisering onmisbaar om efficiëntie te bevorderen en dienstverlening te optimaliseren**. IT vormt het fundament.

Standaardisatie is een van de kernpijlers in Fednots IT-strategie. “Concreet betekent dit dat we minder IT-tools gebruiken, maar de tools die we wél inzetten optimaal benutten. Op termijn willen we het aantal applicaties verminderen en beter integreren. Minder tools, maar meer samenhang”, zegt Program Manager Vincent Arijs.

Die aanpak geldt ook voor samenwerkingen met partners. “We hebben bewust gekozen voor minder leveranciers, maar wel voor partners die onze organisatie door en door begrijpen en ons effectief vooruithelpen. Met spotit hebben we zo’n relatie. We kunnen diepgaande technologische gesprekken voeren en krijgen precies de ondersteuning die we nodig hebben”, benadrukt Arijs. **Ook automatisatie is een sleutelelement in de modernisering** van IT-processen, net als een robuuste beveiliging.

Een van de grootste recente uitdagingen was de netwerkvernieuwing van het SDN-datacenter, een cruciaal onderdeel van Fednots IT-infrastructuur. Aangezien Fednot **de kritische applicaties voor alle notarissen in België** beheert, was het essentieel om een sluitend migratieplan op te stellen dat de downtime tot een absoluut minimum beperkte.

De volledige migratie verliep uiterst vlot, tot grote tevredenheid van Arijs: “De migratie van het datacenternetwerk was geen eenvoudige opdracht: het project was technisch complex en moest worden afgestemd op tal van andere lopende interventies. Bovendien moest de uitrol grotendeels buiten de werkuren plaatsvinden om de operationele continuïteit te garanderen. Ik wil hierbij graag de enorme flexibiliteit van het spotit-team benadrukken.”

“Het team van spotit bracht niet alleen sterke technische expertise mee, maar ook een uitzonderlijke flexibiliteit. Ze stemden zich moeiteloos af op onze planning en zorgden ervoor dat de impact op onze werking tot een minimum werd beperkt.”

Vincent Arijs (Program Manager bij Fednot)

BELANGRIJKE VASTSTELLINGEN IN 2025 (BRON: CCB)

- TOENAME VAN NIET-GEPATCHTE KWETSBAARHEDEN
- TOENAME VAN MALVERTISING EN VALSE SOFTWARE
- TOENAME VAN CEO-FRAUDE

DE GROOTSTE CYBERBEDREIGINGEN IN BELGIË (BRON: CCB)

- OPERATIONELE DISRUPTIE
- DIEFSTAL VAN DATA

TOP 3 VAN AANVALLEN VOLGENS VOLUME IN HET SPOTIT SOC

- PHISHING
- MALICIOUS CODE
- INTRUSION (ATTEMPTS)

Inzichten in cyberdreigingen in 2025

HOE GERAKEN ZE BINNEN? DE MEEST GEBRUIKTE MANIEREN (BRON: SPOTIT CSIRT)

- EXPLOIT
- EXPOSED SECURITY INFRA
- ACCOUNT COMPROMISE

TOP 4 VAN AANVALLEN IN BELGIË (BRON: CCB)

- ACCOUNTCOMPROMITTERING
- RANSOMWARE
- DDOS-AANVAL
- PHISHING

MEEST GEBRUIKTE AANVAL GELINKT AAN MOTIEF IN EUROPA (BRON: ENISA)

- RANSOMWARE – FINANCIEEL GEWIN
- DDOS – IDEOLOGIE
- EXPLOITS EN ADVANCED PERSISTENT THREATS – SPIONAGE

Naast cijfers van het Centre for Cybersecurity Belgium zijn ook volgende rapporten interessante bronnen om te raadplegen.
Unit 42 Incident Response Report 2025 / Threat exposure Brucon 2025 / ENISA Threat Landscape 2025 / 2025 Report on the State of the Cybersecurity in the Union / Internet Organised Crime Threat Assessment IOCTA 2025 / Unit42 Attack Surface Threat Report / Verizon data breach report 2025

NIS2 ÉÉN JAAR LATER

“Belangrijke stap voor cyberweerbaarheid van bedrijven”

2025 was het eerste volledige jaar waarin de NIS2-richtlijn effectief van kracht was. De Europese wetgeving, die in België al in oktober 2024 werd omgezet naar nationale wetgeving, heeft een grote impact op duizenden ondernemingen. Dries Wouters, Strategic Architect bij spotit, blikt terug op het eerste jaar NIS2 en schetst waar bedrijven vandaag staan.

“Veel organisaties hebben al geïnvesteerd in essentiële securitymaatregelen en basisbescherming. Waar het vaak misloopt, is op het vlak van documentatie en beleid.”

Dries Wouters (Strategic Architect bij spotit)

Wat is NIS2 precies?

“NIS2 staat voor Network and Information Security Directive 2, een EU-richtlijn die de cyberbeveiliging versterkt voor essentiële en belangrijke organisaties in Europa. In België gaat het vandaag om zo’n 3.500 bedrijven die zich geregistreerd hebben als NIS2-plichtig, waarvan ongeveer 1.500 als essentieel en 2.000 als belangrijk zijn geclassificeerd. Het gaat om bedrijven in sectoren die een cruciale rol spelen voor onze maatschappij en economie, zoals energie, transport, gezondheidszorg, water, digitale infrastructuur, overheid en maakindustrie. In die sectoren mag er op het vlak van cybersecurity weinig of niets fout lopen, omdat incidenten meteen een grote impact kunnen hebben op de economie en de continuïteit van essentiële diensten. Met NIS2 verplicht Europa bedrijven daarom om hun cyberweerbaarheid structureel te verhogen: niet alleen om aanvallen te voorkomen, maar vooral om beter voorbereid te zijn wanneer het toch misloopt en de impact zo beperkt mogelijk te houden. De wetgeving houdt wel rekening met de omvang van organisaties: bedrijven met minstens 50 medewerkers of een jaaromzet van 10 miljoen euro of meer vallen onder het toepassingsgebied, terwijl kleinere kmo’s buiten de scope blijven. Met andere woorden: hoe groter en kritischer de organisatie, hoe zwaarder de verplichtingen en verwachtingen op het vlak van cybersecurity en governance.”

België wordt vaak als voorbeeld genoemd. Waarom?

“België is het enige land dat de NIS2-richtlijn tijdig én vrij volledig heeft omgezet in nationale wetgeving. Daarnaast werd met het CyberFundamentals-framework (CyFun) een concreet en bruikbaar kader uitgewerkt om bedrijven te helpen met de implementatie. In veel andere Europese landen ontbreekt dat nog, wat maakt dat NIS2 daar minder leeft. Dat is opvallend, want de ambitie van Europa is net om de cyberweerbaarheid van de volledige economie op te krikken.”

Wat moesten Belgische bedrijven concreet doen in het afgelopen jaar?

“De eerste stap was registreren bij het Centrum voor Cybersecurity, zodat de overheid weet welke organisaties onder NIS2 vallen. Daarna moeten bedrijven maatregelen nemen om hun risico’s te beperken en ernstige incidenten binnen de 24 uur melden. Er ligt ook een sterke focus op supply chain-risico’s en op de verantwoordelijkheid van het management. Bestuurders zijn persoonlijk verantwoordelijk voor de naleving en moeten zelfs een verplichte opleiding volgen.”

Waar staan we vandaag in het hele traject?

“We zitten nog volop in de overgangsperiode. Tegen april 2026 moet de meest kritische groep aantonen dat ze actief bezig is met verbeteringen, en tegen april 2027 moeten organisaties het vereiste maturiteitsniveau behalen. Na de grote informatie- en registratiedruk van begin 2025 zitten de meeste bedrijven vandaag in de implementatiefase.”

Hoe moeten ze dat aanpakken? En hoe helpt spotit hen daarbij?

“We werken voor hen een NIS2-roadmap uit. Een drieledig assessment vormt het startpunt. Eerst organiseren we een risicoworkshop met verschillende profielen binnen de organisatie, van IT en security tot directie, finance en marketing. Zo brengen we risico’s in kaart vanuit meerdere perspectieven. Daarna volgt

een self-assessment op basis van concrete thema's, wat resulteert in een maturiteitsscore per domein. Op basis daarvan vertalen we alles naar een concreet actieplan en een haalbare cybersecurityroadmap, meestal over een periode van één tot anderhalf jaar."

Wat zijn daarbij de grootste uitdagingen?
"Veel organisaties hebben al geïnvesteerd in essentiële securitymaatregelen en basisbescherming. Waar het echter vaak misloopt, is op het vlak van documentatie en beleid. Bij een NIS2-assessment kijken we daarom altijd naar twee aspecten. Enerzijds is er de beleidskant: bestaat er een formeel en gedocumenteerd kader dat beschrijft wat moet gebeuren, wanneer en waarom? Anderzijds bekijken we de implementatie: hoe goed zijn die maatregelen in de praktijk opgezet, zijn ze volledig, en zitten er geen hiaten in? Zeker bij organisaties met een lagere maturiteit zien we dat de technische implementatie vaak redelijk oké is, terwijl de documentatie achterblijft. Back-up en recovery zijn daar een typisch voorbeeld van. Veel bedrijven maken elke nacht een back-up, maar hebben nooit expliciet bepaald welke data voor hen het meest kritisch zijn en hoe snel ze opnieuw operationeel moeten zijn. Als je je geen volledige dag dataverlies kan permitteren, volstaat een nachtelijke back-up niet. Dan moet je ook nadenken over frequentie, herstelprocedures en beschikbare reservecapaciteit. Back-ups maken is uiteraard noodzakelijk, maar zonder een doordachte strategie rond herstel en continuïteit is dat onvoldoende."

Is NIS2 het eindpunt?
"Absoluut niet. NIS2 past in een bredere Europese beweging; er komen onder meer ook nog de Cyber Resilience Act en de AI Act aan. Cybersecurity wordt steeds meer een vast onderdeel van wetgeving. De mindset verschuift daarbij van louter beschermen en vermijden naar voorbereid zijn op incidenten en snel kunnen herstellen. Dat is waar cyber resilience écht om draait. Om organisaties daarin te ondersteunen, bieden we met spotit verschillende vormen van dienstverlening aan. We helpen bedrijven strategisch met consultants die samen met hen beleid uitwerken rond information security, netwerkbeveiliging en business continuity. Daarnaast nemen onze managed services een deel van de operationele zorgen over. Als een firewall bijvoorbeeld iets detecteert, volgen wij dat 24/7 op voor de klant. Dat kan aangevuld worden met technologische ondersteuning en met implementatiediensten waarbij onze engineers systemen correct opzetten of finetunen. Door die combinatie groeien organisaties stap voor stap naar een hoger niveau van cyberweerbaarheid."

"Cybersecurity wordt steeds meer een vast onderdeel van wetgeving. De mindset verschuift daarbij van louter beschermen en vermijden naar voorbereid zijn op incidenten en snel kunnen herstellen. Dat is waar cyber resilience écht om draait."

Dries Wouters (Strategic Architect bij spotit)

ZUIDNATIE WERKTE MET SPOTIT AAN EEN HAALBARE NIS2-ROADMAP

"Van assessment naar concrete roadmap"

Logistiek dienstverlener Zuidnatie zet al jaren heel actief in op cybersecurity. Het bedrijf werkt daarvoor al geruime tijd samen met spotit, zowel op het vlak van security als netwerking. Toen NIS2 op de agenda kwam, was het dan ook logisch om diezelfde partner te betrekken. "Het hele NIS2-verhaal overviel ons eerlijk gezegd wat, met meer dan honderd vereisten waaraan je als organisatie moet voldoen. Dat kan je onmogelijk van vandaag op morgen realiseren", vertelt Floris Verswijvel, IT-manager bij Zuidnatie. "Ik merkte bovendien dat veel collega IT-managers, ook buiten onze sector, met dezelfde vragen worstelden. De technologie is vaak wel aanwezig bij organisaties, maar de formele documentatie van alle policies en procedures is dat veel minder."

Spotit startte het traject met een grondig NIS2-assessment. De resultaten daarvan werden vertaald naar een roadmap die met de directie werd besproken. "Dat maakte in één keer helder welke richting we uit moesten om de NIS2-doelstellingen te behalen. Wat zijn de prioriteiten? Hoe kunnen we het traject opsplitsen in behapbare fases? Wat zijn quick wins en wat zijn eerder nice to haves? Die aanpak zorgde ervoor dat we met een realistische inspanning toch snel waarde konden creëren."

Wat Zuidnatie vooral waardeert, is de pragmatische manier waarop spotit daarbij te werk gaat. "Ze hebben niet alleen de expertise om richting te geven, maar houden ook rekening met wie we zijn als organisatie. Ze kijken naar wat er al aanwezig is in onze IT-omgeving en hoe bestaande oplossingen kunnen worden meegenomen in het traject", aldus Verswijvel.

Vandaag werkt Zuidnatie actief aan een vijftigtal actiepunten binnen het NIS2-kader. Het doel is om eerst te voldoen aan het 'important' level en vervolgens verder door te groeien richting 'essential' waartoe we wettelijk verplicht worden. "Het eindresultaat is niet zomaar een oefening op papier. Het is een aanpak die ons niet alleen helpt om compliant te worden, maar die ook echt bijdraagt aan onze dagelijkse werking", vindt hij.

CASE

Bij Roger & Roger kraken alleen de chips, niet de beveiliging

Roger & Roger is een dynamisch Belgisch bedrijf dat vooral bekend staat om Croky, maar hun activiteiten reiken veel verder dan chips alleen. Vandaag combineert de groep twee belangrijke pijlers: chips en snacks, en diepvriesgroenten. **Met vijf fabrieken die 24/7 draaien, is IT van levensbelang.**

De pittige groei van Roger & Roger bracht ook nieuwe uitdagingen met zich mee. Hun bestaande infrastructuur, opgebouwd rond een MPLS-netwerk en één centrale firewall, was niet langer voldoende. **De uitdagingen waren veelzijdig.** Het bedrijf moest een balans vinden tussen synergie en risico en moest keuzes maken over de focus van het interne IT-team. Daarbovenop speelde het verschil tussen de kantooromgeving en de fabriek.

In maart 2022 begon de samenwerking met spotit met een whiteboardsessie waarin de segmentatie van het netwerk werd uitgetekend. Uit die sessie groeide een roadmap, opgedeeld in hapklare werkpakketten. Zo werd de migratie beheersbaar en bleven de kosten voorspelbaar. **De aanpak ging verder dan alleen firewalls:** er kwamen dedicated management zones, vendor- en supplier access, herziening van URL filtering en nieuwe policies om IT en OT duidelijk te scheiden.

In 2023 werden alle sites aangesloten op het spotit Network Operations Center (NOC) en Security Operations Center (SOC), wat 24/7 monitoring en operationele ondersteuning bracht. **De migraties verliepen in een productiecontext waar elke minuut telt.** Tijdens de firewallmigratie in Moeskroen kreeg spotit exact tien minuten downtime toegewezen. Uiteindelijk slaagde het team erin de ingreep onopgemerkt uit te voeren. “Vertrouwen is erg belangrijk”, vertelt Group IT Director Koen Van Ceulebroeck. “We testten spotit en ze bewezen hun waarde. Dat vertrouwen is de basis van onze samenwerking”

De komende jaren ligt de focus op **het verder versterken en uniformeren van de digitale fundamenten** binnen de groep, zodat alle sites volgens dezelfde best practices werken. Tegelijk bouwt het bedrijf verder om IT- & OT-zichtbaarheid naar een nog hoger niveau te tillen en zo risico’s nog sneller te detecteren.

“We moesten factory resets doen, certificaten vervangen en tunnels opnieuw opbouwen. Dat zijn zaken waar je als IT-directeur van wakker ligt. Maar dankzij de samenwerking met spotit konden we alles uitvoeren zonder impact op de productie.”

Koen Van Ceulebroeck (Group IT Director bij Roger & Roger)

MEDEWERKER AAN HET WOORD

ONZE SPECIALISTEN TESTEN HET UIT

Kan jouw bedrijf een cyberaanval doorstaan?

Ethisch hacken, pentesting, penetratietesten: het zijn termen die je steeds vaker hoort in de wereld van cybersecurity. In essentie draait het allemaal om één zaak: proactief testen hoe sterk je digitale verdediging écht is. Ethical hackers simuleren realistische aanvallen, brengen kwetsbaarheden aan het licht en helpen organisaties hun beveiliging tijdig bij te sturen. Hoe dat in de praktijk verloopt? Keanu Nys, Ethical Hacker en Offensive Security Lead bij spotit, licht toe.

Lees hier de frequently asked questions over pentesten

“Zo’n penetratietest is eigenlijk een gecontroleerde, realistische cyberaanval waarbij ethische hackers op zoek gaan naar zwakke plekken binnen een vooraf bepaalde scope. We bootsen na wat echte aanvallers proberen, maar dan veilig, gecontroleerd en met één doel: je beveiliging sterker maken. Alle bevindingen en aanbevelingen komen terecht in een helder pentestrapport waarmee organisaties gericht kunnen verbeteren.”

De voordelen zijn duidelijk: een pentest verhoogt je security maturity, geeft inzicht in je weerbaarheid en toont welke kwetsbaarheden een aanvaller zou kunnen misbruiken. Door proactief te testen, bijvoorbeeld vóór een nieuwe toepassing live gaat, voorkom je verrassingen en hou je je beveiliging structureel op niveau.

Verschillende soorten tests

Spotit biedt een breed gamma aan penetratietesten, telkens afgestemd op de specifieke noden van een organisatie.

1. Voor een **externe infrastructuurtest** brengen onze specialisten het publieke aanvalsoppervlak in kaart en onderzoeken ze of iemand vanop het internet toegang kan krijgen tot systemen of gegevens.
2. Bij een **interne infrastructuurtest** bekijken we wat er mogelijk is wanneer een aanvaller al binnen geraakt: van laterale bewegingen tot privilege-escalaties. Wat kan iemand met een verloren laptop? Hoe ver geraakt een medewerker met beperkte rechten? En hoe veilig zijn de ‘crown jewels’ bij een interne aanval?
3. Bij een **fysieke penetratietest** onderzoeken we of een onbevoegde fysieke toegang kan krijgen tot beveiligde ruimtes, van kantoorgebouwen tot server- of productiesites. Afhankelijk van de scope simuleren we technieken zoals tailgating, impersonatie, badgeklonen of lockpicking om te evalueren hoe ver een aanvaller zou raken.
4. Daarnaast voeren we **webapplicatiepentesten** uit op onder andere klantportalen, e-commerceplatformen, API’s en SaaS-oplossingen.
5. Bij cloudmigraties tot slot is het cruciaal om te controleren of de omgeving correct en veilig geconfigureerd is. **Spotit analyseert Azure- en Entra ID-omgevingen** op kwetsbaarheden zoals onbeschermde opslag, blootgestelde services en te ruime toegangsrechten.

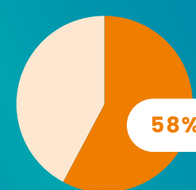
Wat veel mensen niet weten, is dat ook operationele technologie (OT) in aanmerking kan komen voor penetration testing. “In industriële omgevingen waar IT en OT samenkomen, blijven verouderde systemen vaak kwetsbaar. We testen segmentatie, industriële netwerken, draadloze systemen en zelfs fysieke toegangsbeveiliging om risico’s vroegtijdig bloot te leggen”, besluit Nys.

ONDERZOEK

6 op de 10 bedrijfswachtwoorden binnen uur te kraken

6 op de 10 Belgische werknemers (58%) hebben een paswoord dat cybercriminelen binnen het uur kunnen hacken. Dat blijkt uit een onderzoek van ons team van hacking-experten. Zij voerden het paswoordsterkte-onderzoek uit bij 67.557 medewerkers van verschillende kleine en middelgrote bedrijven en multinationals. Vooral erg korte wachtwoorden, waarbij de bedrijfsnaam met een jaartal gecombineerd wordt, zijn erg populair.

“Mensen gebruiken een wachtwoord dat erg gemakkelijk te onthouden is, maar dat houdt heel wat risico’s in”, zegt Keanu Nys. “Ze rekenen vaak op voorspelbare patronen, zeker in een werkcontext, waardoor het voor aanvallers erg gemakkelijk is om een paswoord te raden. De combinatie van de naam van het bedrijf en een jaartal of seizoensgebonden combinaties worden dan ook veelvuldig gebruikt. Dat laatste zien we vooral wanneer wachtwoorden om de drie maanden verplicht moeten worden aangepast. We raden het ook af om een korte vervaldatum in te stellen voor wachtwoorden. Kies eerder voor een sterk en lang wachtwoord dat veel langer goed is, om te voorkomen dat gebruikers terugvallen op een simpele variant die ze makkelijk kunnen onthouden.”



MAAR LIEFST 58% HEEFT EEN PASWOORD DAT CYBERCRIMINELEN IN EEN VINGERKNIP KUNNEN HACKEN.

ENKELE KLANTEN AAN HET WOORD

“De pentester kwam zeer deskundig over en lichtte de verschillende cases op een duidelijke en overzichtelijke manier toe. Alles werd ook onderbouwd met heldere screenshots.”

Steve Detremmerie (Technical IT Manager bij Grandeco Wallfashion Group)

“De resultaten van de pentest waren bijzonder waardevol: enkele kritieke kwetsbaarheden werden blootgelegd en hun rapport bevatte duidelijk advies over hoe deze geremedieerd konden worden. Wij raden spotit dan ook van harte aan voor het testen van je IT-infrastructuur.”

Sam Vandevelde (Afdelingshoofd IT bij Verhelst Group)

“People management en coaching zijn hier geen bijzaak”

People management krijgt bij spotit een prominente plaats. Niet als ondersteunend proces op de achtergrond, maar als een essentieel onderdeel van hoe mensen samenwerken, groeien en zich goed voelen in hun job. Sanne Vinck, Head of HR, geeft tekst en uitleg.

Wat typeert volgens jou de cultuur bij spotit?
“Voor mij is dat vooral de balans tussen duidelijkheid en zorg. Verwachtingen zijn helder, feedback is geen momentopname maar een continu gesprek, en er is altijd ondersteuning dichtbij. Dat creëert een veilige werkomgeving waarin mensen zich durven uitspreken, verantwoordelijkheid opnemen en zelf hun ontwikkeling mee vormgeven. En het zorgt er ook voor dat iedereen zich correct en gelijk behandeld voelt.”

Hoe kijk je naar groei, zowel voor mensen als voor de organisatie?
“Groei is voor ons geen checklist of trend. Het gaat over duurzame relaties, over samen vooruitgaan op een manier die haalbaar blijft. Loopbanen verlopen zelden rechtlijnig en dat hoeft ook niet. Het is een traject met verschillende fases. Bij spotit proberen we dat traject samen af te leggen, met aandacht voor het werk, maar ook voor de mens achter de rol.”

People management is daarin voor jullie geen bijzaak. Waarom is individuele coaching zo belangrijk voor jullie?
“Omdat goed werk begint bij mensen die zich ondersteund en begrepen voelen. People management gebeurt bij ons niet los van de dagelijkse realiteit. Het zit vervat in hoe we samenwerken, hoe we verwachtingen benoemen en hoe we met elkaar in gesprek gaan. Als mensen weten waar ze staan en voelen dat er ruimte is om te groeien, komt dat vanzelf ook het werk ten goede.”

Hoe geven jullie dat concreet vorm?
“We proberen een omgeving te creëren waarin verwachtingen duidelijk zijn en gesprekken open kunnen verlopen. Dat vraagt structuur, maar ook nabijheid. Mensen moeten weten wat er van hen verwacht wordt, maar evengoed voelen dat ze ondersteund worden onderweg. Die combinatie maakt het verschil. Daarom hebben we het afgelopen jaar sterk ingezet op de rol van het middle management. Vanuit hr hebben we samen met hen een duidelijke aanpak uitgewerkt waarbij zij hun mensen actief en proactief opvolgen, minstens per kwartaal. Het gaat dan niet alleen over prestaties, maar ook over hoe iemand zich voelt, welke doelen iemand wil stellen en waar iemand naartoe wil groeien. Wij ondersteunen dat proces en hebben het gestroomlijnd, zodat iedereen binnen de organisatie volgens dezelfde principes werkt. Zo creëren we consistentie, zonder het persoonlijke aspect te verliezen.”

Jullie hanteren één aanpak, maar met ruimte voor individuele trajecten. Hoe verzoen je die twee?
“Geen twee loopbanen zijn hetzelfde, en dat hoeft ook niet. We werken met een gedeeld kader dat zorgt voor duidelijkheid en gelijkheid binnen de organisatie. Tegelijk laten we ruimte voor persoonlijke ambities, teamdynamieken en individuele noden. Het is geen strak keurslijf. We willen richting geven zonder te beperken, ondersteunen zonder te controleren. Zelf neem ik daarin een rol op als vertrouwenspersoon, onder meer rond psychosociale vraagstukken. Mensen moeten weten dat ze ergens terechtkunnen, ook wanneer het moeilijker gaat. Dat maakt deel uit van dezelfde visie: zorg dragen voor mensen, in alle facetten van hun werk.”

MEDEWERKER AAN HET WOORD

OT-SECURITY VRAAGT EEN EIGEN AANPAK

Eén jaar spotit OT in de praktijk

Begin 2025 versterkte spotit zijn activiteiten in Operational Technology (OT) met een gespecialiseerd team. “Natuurlijk waren we voordien met spotit ook al bezig met connectiviteit en beveiliging van industriële omgevingen. Maar 2025 was het jaar waarin we daarvoor een aparte businessunit opstartten”, zegt Erik De Nert, Head of Operational Technology bij spotit. Een terugblik op het eerste jaar.

“Veel bedrijven beseffen niet hoeveel OT er eigenlijk aanwezig is in hun organisatie”, zegt De Nert. “Machines, PLC’s, sensoren, maar ook draadloze netwerken, HVAC-installaties, magazijnen en logistieke systemen: alles is vandaag geconnecteerd, vaak historisch gegroeid en niet altijd goed beveiligd. En dat terwijl het aantal cyberaanvallen op industriële omgevingen blijft stijgen.”

Cybersecurity in OT draait bovendien om veel meer dan data. “Als er iets foutloopt in IT, ligt misschien een server plat of kan niemand e-mails versturen. In OT zijn de gevolgen veel groter: productie die stilvalt, impact op de productkwaliteit en risico’s voor de veiligheid van mensen of voor het milieu, bijvoorbeeld in sectoren als scheepvaart, energie of kernenergie.”

Die risico’s worden nog versterkt door de aard van OT-systemen. “We werken vaak met omgevingen die tientallen jaren oud zijn, met protocollen die nooit ontworpen zijn om met IT of de cloud te communiceren. Tegelijk zien we een sterke digitaliseringsdrang: bedrijven verzamelen meer data, gebruiken AI en koppelen systemen. Dat legt kwetsbaarheden bloot, terwijl je die systemen niet zomaar kan patchen of stilleggen voor updates.”

Een klassieke IT-aanpak volstaat dan ook niet voor productieomgevingen; die vragen een andere mindset en andere technologie. Met spotit werken we rond drie pijlers: we zetten in op cyberveilige, beheersbare en compliant productieomgevingen.

Bewustwording als eerste stap

“We merken dat onze OT-focus aanspreekt bij klanten met productieomgevingen”, blikt hij terug op het eerste jaar. “We kregen enerzijds vragen van bedrijven die nog helemaal aan het begin staan en zich afvragen hoe ze aan zo’n OT-project moeten beginnen, en anderzijds ook van ondernemingen die al verder staan en naar ons komen voor een OT SOC. Daardoor werken we vandaag aan OT-projecten doorheen onze volledige portfolio. De klantenbasis is bijzonder breed, van voeding en farma tot energie, havens en logistiek.”

Hét startpunt van een OT-traject? Bewustwording. “Dat werkt in twee richtingen: IT-teams moeten begrijpen wat er leeft in productieomgevingen, en anderzijds moeten mensen in productie zich bewust zijn van potentiële risico’s. Daarna brengen we alle systemen in kaart. Welke zijn waarmee geconnecteerd? Welke kwetsbaarheden zijn er? En hoe communiceren netwerken onderling, richting IT en naar de buitenwereld? Naast dat technische aspect komt ook het organisatorische aan bod, want externe leveranciers spelen ook een belangrijke rol. We brengen via een scan de systemen van de productieomgeving in kaart, stellen een rapport op en werken op basis daarvan een concreet actieplan en roadmap uit. De volgende cruciale stap is meestal het scheiden van IT- en OT-netwerken via firewalls. Door die omgevingen correct te segmenteren, dek je al een groot deel van de risico’s af.”

2026: remote access en OT-monitoring

Remote access is bij veel bedrijven een hot topic, merken ze bij spotit. “In bijna elk gesprek komt dat

Mathieu Millecam (Head of OT Architecture) en Erik De Nert (Head of OT)

naar voren. Remote access is een van de belangrijkste manieren waarop aanvallers binnendringen. Ongeveer 50 procent van de cybersecurity-incidenten gebeurt via een of andere vorm van ongecontroleerde externe toegang, vaak zonder multifactor-authenticatie. Bovendien werken productieomgevingen met veel verschillende leveranciers die toegang nodig hebben. Die toegang moet gecontroleerd zijn, maar mag ook niet zo complex worden dat mensen ze beginnen te omzeilen. Klassieke IT-oplossingen schieten daarin vaak tekort. Daarom werken we bij spotit met OT-specifieke remote-access oplossingen van Xona en Cisco. We zetten hun oplossing in voor third-party- en remote access, specifiek afgestemd op OT- en cyberfysieke omgevingen.”

“Daarnaast stijgt ook de vraag naar actieve monitoring van industriële netwerken en het vroegtijdig detecteren van kwetsbaarheden, bedreigingen en afwijkend gedrag. In een omgeving waar continuïteit en betrouwbaarheid cruciaal zijn, wordt continue zichtbaarheid in het OT-netwerk steeds belangrijker. Met onze gekende partners Palo Alto, Cisco en Nozomi Network werken we de best passende oplossing uit die zowel zichtbaarheid als controle biedt”, besluit hij.

Zo doe je het in de praktijk

“Begin met awareness: heb je voldoende kennis van je productieomgeving en zitten de juiste mensen rond de tafel? Breng daarna je assets, leveranciers en kwetsbaarheden in kaart. En start bij segmentatie van boven naar beneden: scheid eerst IT van OT en zorg voor veilige en gecontroleerde OT remote toegang. Daarmee dek je meteen een groot deel van de risico’s af.” Een solide netwerkbasis is daarbij onmisbaar. “Security en netwerk gaan hand in hand. Als de basis goed zit, kan je verder werken aan detectie van anomalieën en gerichte monitoring. Logisch dus dat bedrijven waar we gestart zijn met de juiste stappen, vandaag al doorgroeien richting permanente monitoring via NOC en SOC.”

CASE

Pemco International versterkt zijn cyberweerbaarheid

Voor Pemco International, producent van industriële coatings en geëmailleerd glas, werd **cybersecurity een strategische prioriteit**. Omwille van strengere regelgeving en een toenemende dreiging, schakelde het bedrijf spotit in om zijn beveiliging te versterken. Met de Cortex XDR-oplossing van Palo Alto Networks en het 24/7 SOC van spotit bouwde Pemco aan meer gemoedsrust en cyberweerbaarheid.

“Onze ovens draaien 24 uur op 7. Als een cruciale IT-component uitvalt, kunnen we de productie niet zomaar stilleggen of opnieuw opstarten”, vertelt Voicu Potrovita, Global IT Manager bij Pemco International. **“IT ondersteunt niet alleen onze administratie, maar ook rechtstreeks de productieprocessen.”**

Als chemisch productiebedrijf valt Pemco onder de Europese NIS2-wetgeving, die bedrijven in kritieke sectoren verplicht om hun cybersecurity op te schroeven. Bovendien sloot de Amerikaanse investeringsmaatschappij achter Pemco een cyberverzekering af waaraan een aantal voorwaarden verbonden waren. “Het was geen plotse crisis, maar eerder de volgende logische stap in onze evolutie. We wisten dat we professionele ondersteuning nodig hadden”, zegt Potrovita.

Hij kende spotit al uit een eerdere samenwerking bij een vroegere werkgever. Toen Pemco op zoek ging naar een betrouwbare securitypartner, was de keuze snel gemaakt. “We hebben wel enkele leveranciers vergeleken, maar **spotit bood duidelijk de juiste expertise én de nabijheid die we zochten**. Ze zijn Belgisch, verstaan onze context en hebben een uitstekende reputatie in cybersecurity.” Spotit stelde voor om niet enkel de basisbeveiliging te versterken, maar het IT-netwerk van Pemco ook te laten monitoren door het spotit Security Operations Center (SOC).

Sinds de ingebruikname van Cortex XDR en de aansluiting op het SOC heeft Pemco meer zicht gekregen op wat er zich in de IT-omgeving afspeelt. Er worden meldingen gegenereerd bij verdachte bestanden of ongewone datastromen, wat het bedrijf toelaat om sneller te reageren. Belangrijker nog: **de IT-afdeling kan met een gerust hart functioneren**.

“Cybersecurity is een continu spel van kat en muis. Vandaag zijn we beter beschermd dan gisteren, en morgen zullen we nog sterker staan. Met spotit weten we dat we in die evolutie niet alleen staan.”

Voicu Potrovita (Global IT Manager bij Pemco International)

“Cijfers zijn belangrijk voor vertrouwen”

Ze werken vooral achter de schermen, maar het financeteam speelt een cruciale rol om alles vlot te laten verlopen. Het team van zes mensen staat in voor alles wat met orders en finance te maken heeft. “Zo vormen we een belangrijke schakel in het traject naar een sterke customer experience”, vertelt Martine Theunis, Head of Finance.

Een groot deel van ons werk draait rond orders. Alles wat sales bij een klant verkoopt, zetten wij correct om in een order. We maken de bestelbon op, volgen de levering op en zorgen dat het nodige materiaal tijdig beschikbaar is. Ook het verlengen van licenties nemen we voor onze rekening.

Daarnaast ligt ook het financeluik bij ons. Aankoopfacturen komen binnen via Peppol, worden door ons nagekeken en in een goedkeuringsflow geplaatst. Elke donderdag voeren we de betalingen uit, zodat leveranciers tijdig worden betaald. We maken de verkoopfacturen op, beantwoorden vragen van klanten daarover en volgen de betalingen op. Daarnaast nemen we uiteraard ook alle wettelijke taken op ons, zoals de btw-aangifte, vennootschapsbelasting en andere administratieve verplichtingen.

Om alles vlot te laten verlopen, werken we regelmatig samen met andere teams binnen spotit. Bij vragen over een factuur overleggen we bijvoorbeeld met sales of met de service managers. Over geregistreerde en gefactureerde uren hebben we dan weer contact met de mensen van planning en operations. Daarnaast maak ik elke maand een rapportering voor het directiecomité, zodat zij de juiste beslissingen kunnen nemen en indien nodig kunnen bijsturen.

Een van de grootste uitdagingen is elke maand zo snel mogelijk de juiste cijfers op tafel te leggen. Dat begint al bij de verkoopfacturen, die correct en tijdig moeten worden uitgestuurd zodra we de maand hebben afgesloten. Naarmate het bedrijf groeit, neemt ook het aantal aankoopfacturen toe en moeten die snel verwerkt worden zodat onze analyses accuraat blijven.

Het begin van het jaar is altijd bijzonder intens. In januari sluiten we het boekjaar af en in de laatste week van die maand komt de auditor al langs. Dan moeten alle cijfers en details beschikbaar zijn en moet alles gereconcilieerd zijn. Er wordt gecontroleerd of alles correct geboekt is en ook de omzet wordt nagegaan aan de hand van de uren die door medewerkers geregistreerd zijn. In februari starten we met een nieuw boekjaar.

Een belangrijke mijlpaal is elk jaar opnieuw de jaarrekening tijdig neerleggen. Op tijd correcte cijfers rapporteren blijft essentieel, zodat klanten zien dat we het goed doen en het vertrouwen in ons bedrijf blijft groeien.

Straffe prestaties dankzij een sterk team

Elke dag bouwen onze medewerkers mee aan de toekomst van onze organisatie én onze klanten. Maak kennis met onze verschillende teams:

MANAGED SERVICES

- **SOC-team:** ons Security Operations Center bewaakt en beschermt 24/7 de IT-omgevingen van klanten tegen bedreigingen, met realtime detectie en respons.
- **CSIRT:** apart team dat snel en deskundig reageert op beveiligingsincidenten om schade te minimaliseren.
- **NOC-team:** beheert en optimaliseert netwerkprestaties en uptime, met een proactieve en probleemoplossende aanpak.

DOMAIN EXPERTS

- **OT-team:** richt zich op de beveiliging en connectiviteit van industriële systemen, met expertise in unieke OT-uitdagingen.
- **Offensive-team:** voert ethische hacktests en kwetsbaarheidsanalyses uit om systemen te versterken tegen mogelijke aanvallen.
- **Consulting-team:** helpt organisaties risico's te beheren, compliance te waarborgen en een sterke beveiligingsstrategie te ontwikkelen.

TECHNOLOGY

- **Internal IT Operations-team:** zorgt dat onze medewerkers over toptools beschikken om productief en kwaliteitsvol werk af te leveren.
- **Service Excellence-team:** combineert ontwikkeling en operationele expertise om snelle, betrouwbare en schaalbare oplossingen te leveren. Het team bestaat uit **DevOps** (automatiseren repetitieve processen en taken ten voordele van de klant of spotitcollega), **Data Science** (doen analyse van bestaande data (klanten of spotit) en verwerken deze tot nuttige rapportering) en **Platformation** (richten het IT-ticketingsysteem in en kijken voor continue verbetering bij de afhandeling van tickets).

OPERATIONS

- **Architecten-team:** vertaalt de Netwerk- en security-uitdagingen naar technologische oplossingen op maat
- **Projects & Service Management-team:** implementeert maatwerkoplossingen voor complexe IT-projecten, van start tot finish met een focus op kwaliteit.

SALES & MARKETING

- **Presales, Sales & Marketing, Service Development-team:** verbindt klantbehoeften met spotit oplossingen, met een klantgerichte aanpak en overtuigende communicatie.

STAFF

- **HR-team:** zet zich in om talent aan te trekken, te ontwikkelen en te ondersteunen, met een focus op een stimulerende en positieve werkcultuur.
- **Finance & Orders-team:** waarborgt financiële stabiliteit en groei met nauwkeurige planning, analyses en strategisch beheer.
- **Legal:** goede afspraken (op papier) maken goede vrienden.
- **Facilities & Reception:** zorgt voor een piekfijne kantoorruimte en steeds een warm ontvangst.

Goesting om ons team te vervoegen?
jobs.spotit.be

Ons partner ecosysteem

Onze strategische technologiepartners

Wij geloven in de kracht van samenwerking. Daarom kiezen we bewust voor technologiepartners die tot de top van hun sector behoren. Stuk voor stuk merken die innovatie en kwaliteit combineren en die, net als wij, gaan voor duurzame oplossingen. Met deze strategische allianties bouwen we aan langetermijnrelaties die onze klanten ten goede komen – vandaag en morgen.

Onze academische partners, sectorfederaties en netwerkorganisaties

Als specialist in cybersecurity en netwerking nemen we onze rol in het bredere ecosysteem ernstig. Via ons lidmaatschap van organisaties blijven we niet alleen op de hoogte van technologische en beleidsmatige evoluties, maar leveren we ook actief onze bijdrage aan de toekomst van de sector. Zo bouwen we mee aan een sterk, innovatief en veerkrachtig ondernemingsklimaat.

Onze fijne klanten

Heel wat ondernemingen in België doen een beroep op ons. En daar zijn we trots op! Hieronder een selectie:

Bekijk onze andere referenties op onze website:

Speerpunten voor de toekomst

Sterkere focus op governance, risk & compliance
Governance, risk management en compliance (GRC) zijn al jaren een vaste waarde binnen onze dienstverlening. Met een **ervaren team van specialisten** ondersteunen we klanten in uiteenlopende sectoren. Vandaag wint GRC snel aan belang, zeker met de komst van NIS2 en steeds strengere regelgeving. Daarom investeren we gericht in de verdere uitbouw van onze GRC-activiteiten. Zo blijven we een betrouwbare partner voor bedrijven die hun risico's willen beheersen, hun compliance willen versterken en klaar willen zijn voor de toekomst.

Gemoedsrust dankzij ons 100% Belgische SOC én NOC
Al tien jaar onderscheiden we ons met een **unieke combinatie van SOC (Security Operations Center) en NOC (Network Operations Center)**. Waar veel partijen zich enkel op cybersecurity focussen, bieden wij ook de **onderliggende netwerkexpertise** die cruciaal is voor een sterke beveiligingsaanpak. Want echte veiligheid begint bij een stabiel, performant netwerk. Bovendien zijn al onze diensten **100% Belgisch**. In tijden van geopolitieke onzekerheid is dat voor veel klanten een geruststellende factor én een bewuste keuze.

Versnelling hoger voor OT Security & Networking
Operational technology is het kloppend hart van sectoren zoals logistiek, industrie, nutsvoorzieningen en farma/life sciences. Toch krijgen OT-netwerken vaak niet de aandacht die ze verdienen. Om daar verandering in te brengen, **zetten we volop in op OT Security & Networking** met een aparte businessunit. Zo bieden we onze klanten de gespecialiseerde kennis, aanpak en technologie die nodig zijn om hun operationele systemen toekomstbestendig én cyberveilig te maken.

Sterke groei in de publieke sector
Tot voor kort waren we minder zichtbaar in de publieke sector, maar daar komt snel verandering in. We zetten volop in op **samenwerking met overheden en organisaties in de zorg- en onderwijswereld**. Een belangrijke mijlpaal daarin is ons partnership met Shield vzw, een samenwerkingsverband dat instellingen in de gezondheidszorg en het hoger onderwijs ondersteunt bij het opzetten en beheren van een performante en veilige cybersecurity-architectuur. Met onze oplossingen en expertise bouwen we actief mee aan een digitale en weerbare publieke sector.

Snelle en doeltreffende ondersteuning bij cybercrisissen
Met ons CSIRT-team (Cyber Security Incident Response Team) staan we paraat om bedrijven te ondersteunen bij digitale incidenten en crisissituaties. Maar we gaan nog een stap verder. **We breiden ons aanbod uit met offensive security**, waarbij we – steeds in overleg met de klant – doelgerichte aanvallen simuleren. Zo brengen we kwetsbaarheden aan het licht vóór echte hackers dat doen. Voor deze nieuwe businessunit hebben we een ervaren expert aangesteld, zodat we onze klanten ook proactief kunnen wapenen tegen cyberdreigingen.

Cyberwolf versnelt internationaal
Cyberwolf bouwde de voorbije jaren een sterke klantenportefeuille uit in zowel Noord-Amerika als Europa. Die **internationale groei** willen we nu verder versnellen. Tot nu toe werkten we bewust onder de radar. Maar de volgende stap is duidelijk: onze zichtbaarheid vergroten, zonder onze kenmerkende discretie te verliezen. Cyberwolf blijft een stille kracht – maar wel één die steeds meer impact maakt.

10 TIPS

voor meer gemoedsrust in cybersecurity & networking

Breng je IT-landschap helder in kaart
Start met een volledig en actueel overzicht van je assets: toestellen, applicaties, data en gebruikers. Identificeer waar de grootste risico's zitten en pak die eerst aan.

01

Leg een sterke beveiligingsbasis
Voer een grondige security-audit uit en los kritieke kwetsbaarheden meteen op. Een solide fundament voorkomt dat kleine problemen grote incidenten worden.

02

Beperk toegang volgens het zero trust-principe
Vertrouw niemand automatisch, ook niet binnen je eigen netwerk. Geef enkel toegang op basis van noodzaak, rol en context.

03

Implementeer multi-factor authenticatie (MFA)
Bescherm alle kritieke accounts en extern toegankelijke systemen met MFA. Het is een eenvoudige maatregel met een grote impact op je veiligheid.

04

Segmenteer je netwerk en bescherm zones actief
Zorg voor een duidelijke scheiding tussen IT- en OT-omgevingen en inspecteer verkeer tussen zones met next-generation firewalls.

05

Hou systemen up-to-date met patch management
Inventariseer kwetsbaarheden, automatiseer updates en zorg voor een gestructureerd patch managementproces om gaten in je beveiliging snel te dichten.

06

Bescherm data met sterke encryptie en back-ups
Versleutel gevoelige gegevens, zowel in transit als in rust. Combineer dit met een doordachte back-upstrategie en een getest recoveryplan.

07

Investeer in monitoring en detectie
Bouw een operationele capaciteit uit om je omgeving continu te monitoren. Met 24/7 toezicht via SOC of geautomatiseerde tools detecteer je incidenten sneller en beperk je de impact.

08

Maak mensen mee verantwoordelijk
Sensibiliseer en train medewerkers rond phishing, social engineering en veilig online gedrag. Menselijk bewustzijn blijft een cruciale verdedigingslaag.

09

Veranker cybersecurity in je werking
Werk aan duidelijke security governance, incident response procedures en continue opvolging. Integreer risicobeheer in je dagelijkse werking en verbeter stap voor stap.

10

Meer info? Contacteer ons!

Klaar om uw netwerk- en beveiligingsbehoeften te bespreken?

Wij zijn steeds beschikbaar. Aarzel niet om ons te contacteren voor een vrijblijvend gesprek en een lekkere koffie. Bezoek ons in een van onze kantoren, of plan een gesprek met een expert.

www.spotit.be
+32 (0)9 322 04 44
info@spotit.be


spotit
YOUR SECURITY & NETWORK LAYER