VALID
STAY AHEAD

WHITEPAPER

# Houd jouw bedrijfsgeheimen veilig

## Vijf trends in cyberdreiging en vijf maatregelen om weerbaarheid te verhogen

# INHOUDSOPGAVE



# INFORMATIEBEVEILIGING: CRUCIAAL VOOR DE CONTINUÏTEIT VAN JOUW ONDERNEMING

**MediaMarkt, VDL, Mandemakers, de GGD... allemaal organisaties die zwaar werden geraakt door cybercrime. Ze vormen geen uitzondering want elke dag is er wel nieuws over hackers, gijzelsoftware en datalekken. Het aantal aanvallen neemt sterk toe en de hevigheid ook. Het is niet meer de vraag óf, maar wanneer je wordt getroffen. De impact is enorm, omdat we meer dan ooit afhankelijk zijn van digitale processen. Hoewel iedereen al veel doet aan informatiebeveiliging is er nog veel verbetering mogelijk.**

Informatiebeveiliging is niet alleen een kwestie van techniek, maar ook van bewustwording. Een hack begint vaak bij iemand die op een verkeerd linkje klikt of een zwak wachtwoord gebruikt. Als je wordt geraakt, kan je dat veel geld kosten. Je moet misschien losgeld betalen of krijgt te maken met productieverlies, schadeclaims en reputatieschade. Er zijn ook andere redenen om je securityniveau te willen verhogen. Zo komen er meer wettelijke regels voor de bescherming van data en worden hoge boetes uitgedeeld. Booking.com bijvoorbeeld, moest bijna een half miljoen euro betalen omdat het te laat melding maakte van een datalek. Daarnaast verlangen partners ook steeds vaker dat je security op orde is. Want als jouw systemen plat gaan, krijgen zij producten of diensten niet geleverd.

# WAT SPEELT ER OP DIT MOMENT?

## TREND 1: RANSOMWARE

Het fenomeen gijzelsoftware bestaat al langer, maar staat met stip op één. De reden: nu digitalisering sinds de pandemie bij veel organisaties een vlucht neemt, voeren cybercriminelen het aantal aanvallen op. Elke elf seconden wordt er één gelanceerd. Daarbij komt dat ze steeds agressiever en brutaler te werk gaan. Zo schromen ze niet om gevoelige data te publiceren en geven ze na betaling van losgeld lang niet altijd alle data terug. Gartner voorspelt dat er slachtoffers gaan vallen als criminelen kritieke infrastructuren lam leggen. Wat als de drinkwatervoorziening in gevaar komt?

Gartner denkt dat het einde van de 'ransomware-pandemie' nog lang niet in zicht is, omdat het een aantrekkelijk businessmodel is. Hoe vaak losgeld wordt betaald is niet precies bekend, maar er zijn wel aanwijzingen dat steeds vaker tot betalen wordt besloten. De overheid overweegt niet voor niets om een verbod op betalen in te stellen om criminelen niet te veel aan te moedigen. Inmiddels bestaat er al zoiets als ransomware as a service.  Dat heeft veel te maken met het bestaan van de bitcoin. Waar criminelen in het verleden veel moeite moesten doen om losgeld ongezien in ontvangst te nemen, kunnen ze nu eenvoudig op afstand miljoenen incasseren en wegsluizen. Ze lopen weinig risico om gepakt te worden.

**"Gartner voorspelt dat er slachtoffers gaan vallen als criminelen kritieke infrastructuren lam leggen"**

Daarnaast bedenken criminelen telkens weer nieuwe methodes waardoor virussen vaak lange tijd onontdekt blijven. Ook vallen ze back-upbestanden aan, waardoor het lastiger is om te herstellen van een geslaagde inbraak.

## OOK IN NEDERLAND

RTL Nederland betaalde eind 2021 losgeld, mogelijk nadat het door ransomware was getroffen. Volgens de zender gaat het om 8.500 euro in bitcoin, wat volgens deskundigen een verrassend laag bedrag is. Meestal gaat het om tonnen of miljoenen euro's. Een mogelijke verklaring is dat aanvallers zagen dat back-ups niet waren aangetast. Het kan ook zijn dat ze proberen veel geïnfecteerde bedrijven een klein bedrag te laten betalen of gewoon niet zo ervaren zijn. RTL zegt te hebben betaald om opsporing mogelijk te maken. Het idee is dat het geld op een gegeven moment moet worden opgenomen en uitgegeven.
Volgens Forrester zijn de eisen voor losgeld afgelopen jaar met 300 procent opgevoerd. Dit zou kunnen leiden tot het omvallen van cyber verzekeraars in 2022. Hierdoor worden organisaties minder geneigd om een verzekering af te sluiten, maar schieten cybercriminelen daarmee in hun eigen voet, omdat de bereidheid tot betalen daardoor afneemt. Toen ROC Mondriaan werd getroffen, een onderwijsinstelling met 25.000 studenten, was de eis vier miljoen euro. Uit angst voor reputatieschade wordt meestal niet bekendgemaakt of er is betaald. Om dezelfde reden wordt ook lang niet altijd aangifte gedaan. Verzekeraar Hiscox neemt op basis van eigen onderzoek aan dat ongeveer 58 procent van de succesvol aangevallen bedrijven betaalt.

## TREND 2: SOCIAL ENGINEERING

Social engineering is het misbruik maken van vertrouwen. Door in te spelen op nieuwsgierigheid, hebzucht, angst of onwetendheid proberen criminelen vertrouwelijke gegevens los te krijgen. Door bijvoorbeeld beveiligingscodes te achterhalen, krijgen ze toegang tot een netwerk en installeren ze malware.

Phishing is een eenvoudige vorm van social engineering. Mensen worden via een mailtje verleid om op een linkje te klikken. Er zijn ook geraffineerdere methodes, bijvoorbeeld oplichting van mensen die iets te koop aanbieden op Marktplaats. De crimineel vraagt ter controle via WhatsApp of Messenger om een klein bedrag over te maken via een betaalverzoek. De link gaat alleen niet naar de echte iDEAL- of Tikkiesite maar naar een nep-site. De gegevens die iemand daar invult, gebruikt de oplichter om in te loggen op internetbankieren en geld naar zijn eigen rekening te sluizen.

**“Door bijvoorbeeld beveiligings-codes te achterhalen, krijgen ze toegang tot een netwerk en installeren ze malware”**

Ook via de telefoon, met babbeltrucs, wordt geprobeerd mensen om de tuin te leiden. Deepfake-technologie is al met succes ingezet om de stem van een algemeen directeur na te bootsen en een medewerker aan te zetten tot een betaalopdracht. Dit heet ook wel CEO-fraude.

### OOK IN NEDERLAND

Bol.com maakte in mei 2021 750.000 euro over op rekening van oplichters, terwijl de webwinkel dacht Brabantia te betalen. Bij die strop bleef het niet, want Bol.com moet van de rechter het bedrag alsnog aan de Brabantse prullenbakmaker betalen.

Bedriegers hackten het e-mailadres van een medewerkster van Brabantia en kregen zo toegang tot haar mailbox. Daardoor wisten ze dat Bol.com een betaling moest doen aan Brabantia. De criminelen stuurden vervolgens een e-mail, met daarin een brief. Daarin werd vermeld dat er sprake was van ‘wijziging van onze bankgegevens’. Betalingen moesten voortaan worden overgemaakt naar een ander nummer in Spanje. Hoewel de brief vol spelfouten zat, kwamen e-mailadres, lay-out en de handtekening van directieleden authentiek genoeg over om tot betalen over te gaan. Maar de rechter oordeelde dat er toch voldoende redenen waren om argwanend te zijn en was een telefoontje naar Brabantia ter controle op zijn plaats geweest.

De schade door phishing loopt volgens de Nederlandse Vereniging van Banken op tot een ‘zorgwekkend hoog niveau’. Bankklanten gingen in 2020 voor 39,5 miljoen euro het schip in. In de eerste helft van 2021 ging het om 22,5 miljoen euro.

## TREND 3: FOCUS OP (I)OT

Het komt regelmatig voor dat hackers bedrijfsnetwerken binnenkomen via een met internet verbonden apparaat. Zo maakten beveiligingsonderzoekers eind 2021 bekend dat ze grote lekken hebben gevonden in ruim 150 typen printers van HP. Een kwaadwillende kan via zo'n lek ook gegevens van de printer zelf lezen.

**"Colonial betaalde zo'n vier miljoen euro om weer toegang te krijgen tot de eigen computersystemen"**

Overheden leggen inmiddels strenge eisen op aan fabrikanten van ICT-apparatuur. Behalve aan printers kun je hierbij ook denken aan routers, beveiligingscamera's of slimme deurbellen. In de EU gelden hiervoor vanaf 2024 minimumeisen. Zo mogen ze niet meer met zwakke, standaard wachtwoorden zijn uitgerust, moeten ze meer software-updates ondersteunen en getest zijn op veiligheidslekken.

Veel apparaten voldoen nu al aan deze eisen, vandaar dat criminelen hun aandacht verleggen naar OT, oftewel operational technology. Dat is hard- en software die industriële apparatuur en processen aanstuurt. Een bekend voorbeeld is de hack bij het Amerikaanse oliepijplijnbedrijf Colonial Pipeline. Dit incident staat te boek als de meest ontwrichtende digitale aanval ooit op de Amerikaanse energie-infrastructuur. Hoewel het de hackers niet lukte de pijpleiding over te nemen, viel wel de toevoer stil en ontstonden tekorten aan de pomp. Colonial betaalde zo'n vier miljoen euro om weer toegang te krijgen tot de eigen computersystemen.

## OOK IN NEDERLAND

Waterschappen zijn een voorbeeld van een doelwit waar cybercriminelen het vaak op gemunt hebben. Het aantal aanvallen kan jaarlijks makkelijk in de miljoenen lopen. Waterschap Aa en Maas bijvoorbeeld, maakt er ruim duizend per dag mee. In een interview met Binnenlands Bestuur zegt secretaris-directeur Piet Sennema dat 'goede beveiliging cruciaal is om bijvoorbeeld de aansturing van sluizen, en daarmee de veiligheid en volksgezondheid, te beschermen. Alle bedieningen gaan digitaal'.

Sennema ziet dagelijks duizenden pogingen om wachtwoorden te raden, alle waterschappen kampen hier volgens hem mee. Hij onderscheidt drie soorten aanvallers: "Je hebt landen die op zoek zijn naar kennis, mensen die hun best doen om de boel plat te leggen om geld te verdienen en je hebt kwajongens, die het gewoon leuk vinden om te proberen of het ze lukt om de bediening over te nemen." Aa en Maas kijkt daarom voortdurend of er gaten in de beveiliging zitten en welke lessen getrokken kunnen worden uit aanvallen op anderen.

## TREND 4: CLOUDCOMPUTING

Dat mensen afwisselend thuis en op kantoor werken is een onomkeerbare ontwikkeling. Volgens Gartner wil 75 procent van alle werknemers niet meer terug naar de oude situatie. Dankzij de cloud is het eenvoudig om overal en altijd toegang te hebben tot data en samen te werken.

Maar cloudcomputing brengt ook risico's met zich mee. Gartner ziet dat aanvallers vaker hun pijlen op thuiswerkers richten in de hoop wachtwoorden en toegangscodes buit te maken om zo een bedrijfsnetwerk binnen te komen.

Vooral de zogeheten 'statelijke actoren' zijn succesvol in het achterhalen van persoonsgegevens. Het onderzoeksbureau draagt multifactor authenticatie aan als mogelijke oplossing. Meestal is dan een pincode nodig en een app voor toegang door gezichtsherkenning of een vingerafdruk.

### OOK IN NEDERLAND

De gemeente Ede waarschuwde eind 2021 dat hackers de inloggegevens van een medewerker hebben weten te bemachtigen. Dat lukte door een phishingmail te sturen. Vanuit het mailadres van de medewerker zijn vervolgens grote hoeveelheden nieuwe phishingmails verstuurd naar willekeurige e-mailadressen, 'zowel binnen als buiten de gemeente'. Omdat die mails allemaal op @ede.nl eindigen zien ze er bedrieglijk echt uit. In de mail staat dat de outlook-mailbox vol zit en moet worden bijgewerkt. Als afzender wordt 'IT Services Helpdesk' vermeldt. Wie op de link in de mail klikt, komt op een nepwebsite terecht. Daar ingevulde gegevens zijn bruikbaar voor kwaadwillenden om in een organisatie te infiltreren.

## TREND 5: BEDRIJFSSPIONAGE

Spionage is van alle tijden, maar vormt momenteel volgens het Cyber Security Beeld Nederland (CSBN) een verhoogd risico doordat hackers vaker worden ingehuurd door staten. Daar komt bij dat organisaties vaak meer tijd nodig hebben om beveiligingsupdates op de juiste manier door te voeren. Tot die tijd zijn ze dus kwetsbaar voor nieuwe aanvalsmethodes.

Volgens CSBN is gebleken dat er aan het begin van de COVID-crisis door staten is gespioneerd om medische kennis buit te maken. Het zou daarbij onder meer gaan om testresultaten en gegevens over vaccins. Wereldwijd zouden farmaceutische en medische industrie en onderzoekscentra vaker worden aangevallen. Zo opgedane kennis wordt vervolgens doorgespeeld aan eigen instanties die zich met research en development bezig houden. Ook na de pandemie valt voordeel te halen met gestolen data. CSBN noemt China als voorbeeld van een land dat zich schuldig maakt aan bedrijfsspionage voor de ontwikkeling van nieuwe technologie.


## OOK IN NEDERLAND

Nederland is volgens de AIVD steeds vaker doelwit van digitale spionage. Rusland, China en Noord-Korea proberen op grote schaal in te breken bij bedrijven en overheidsorganisaties om kennis en technologie te stelen. Ons land is aantrekkelijk omdat het een belangrijke speler is op gebied van economie, wetenschap en techniek.

Hackers proberen binnen te komen via thuiswerkers maar ook via toeleveranciers van potentiële doelwitten. Statelijke actoren opereren overigens niet alleen op afstand volgens de AIVD, maar infiltreren ook fysiek. Russische spionnen werkten onder valse voorwendselen voor Nederlandse hightech bedrijven en verkregen zo belangrijke informatie over onder meer kunstmatige intelligentie.

# INFORMATIEBEVEILIGING VERBETEREN: GA GOED VOORBEREID OP WEG

CSBN stelt dat ons land zó afhankelijk is van digitale diensten dat een cyberincident ‘ons land in het hart kan raken en verlammen’. De dreiging is permanent en vraagt om verhoging van de digitale weerbaarheid om risico’s te beheersen, waarbij je in het achterhoofd moet houden dat je ook in de problemen kunt komen door cyberincidenten bij anderen. Wil je altijd op alles voorbereid zijn, dan moet je dus een meerjarige roadmap ontwikkelen, in lijn met de visie en de ambitie van je organisatie.

Een hulpmiddel om op een gestructureerde manier stapsgewijs te verbeteren is het Cybersecurity Framework. Dat is bedacht door het Amerikaanse National Institute of Standards and Technology (NIST). Valid heeft dit framework geadopteerd om haar klanten optimaal te ondersteunen. Het framework bestaat uit vijf pijlers:

1. **Identify:** inventariseer welke systemen, applicaties en data je in huis hebt. Welke zijn belangrijk? Bepaal welke risico’s je loopt op het gebied van beschikbaarheid, vertrouwelijkheid en integriteit (dit laatste is het onbedoeld wijzigen van bestanden) en een beleid hoe hiermee om te gaan.
2. **Protect:** voorkom incidenten door techniek, procedures en aandacht voor de mens (“security awareness”).
3. **Detect:** monitor netwerken en systemen proactief en onderschep dreigingen vroegtijdig.
4. **Response:** als er een incident is, moet je reageren met passende acties.
5. **Recover:** als je toch getroffen wordt, moet je organisatie snel weer in de lucht komen.

# WELKE MAATREGELEN PASSEN HIERBIJ?

1. **Breng je IT-landschap in kaart en los kwetsbaarheden direct op.** Bijvoorbeeld door het installeren van een *vulnerability management* oplossing, antimalware of software voor Role-Based Access Controls. Bepaal wat je belangrijkste gegevens zijn, je kroonjuwelen. Die verdienen extra bescherming. Breng op basis van je risico-inschatting prioriteiten aan en weeg kosten af tegen de baten. Met andere woorden: definieer een strategie en ontwikkel een roadmap om je doelen te bereiken.
2. **Verhoog het bewustzijn van je medewerkers om incidenten te voorkomen.** Veel hacks beginnen bij mensen die op een verkeerd linkje klikken of door gebruik van eenvoudige wachtwoorden. Implementeer maatregelen om menselijke risico's te beheersen zoals een security awareness-programma. Daar horen trainingen bij maar ook het regelmatig aanbieden van nieuwsbrieven en video's over de laatste dreigingen. Je kunt ook denken aan technische oplossingen, zoals het weigeren van al te voor de hand liggende passwords en aan Multi Factor Authentication zodat je wachtwoorden beveiligd tegen diefstal of hacks.
3. **Implementeer de juiste tooling om te kunnen monitoren** (bijvoorbeeld endpoint detection and response). Je moet – liefst in real-time – weten wat er speelt bij gebruikers en in netwerken. Ook hier gaat het weer om het vinden van de juiste balans tussen kosten en baten. Zorg ook dat je op de hoogte bent van de laatste security-ontwikkelingen. Volg bijvoorbeeld de berichtgeving van het NCSC (Nationaal Cyber Security Centrum) of van Talos, het grootste commerciële cyberresearch centrum ter wereld.
4. **Maak een draaiboek waarin je rollen, taken en verantwoordelijkheden vastlegt.** Zo kun je risico's op de juiste manier inschatten en weet iedereen wat hem of haar te doen staat bij een incident. Dicht eventuele gaten in je beveiliging met updates en patches.
5. **Als je wordt getroffen,** wil je als gezegd zo snel mogelijk weer operationeel zijn, liefst ook met zo min mogelijk dataverlies. Een manier om altijd over een recente kopie van gegevens te beschikken, is back-ups bewaren met air gap of immutable back-ups maken.

**"Je moet – liefst in real-time – weten wat er speelt bij gebruikers en in netwerken"**

Wat het herstel betreft: omdat aan herstel een prijskaartje hangt, is het goed om vooraf vast te stellen welk tijdsverlies je acceptabel vindt en of je echt alles wilt back-uppen. Dit leg je vast in een Business Continuity Plan. Je hoeft het back-uppen niet per se zelf uit te voeren, je kunt ook de hulp van een partner inroepen, met Disaster Recovery as a Service.

# ZELF DOEN
# OF UITBESTEDEN?

Dat het belangrijk is om informatiebeveiliging op orde te hebben en voortdurend te werken aan verhogen van de weerbaarheid, is duidelijk. De meeste organisaties ontbreekt het echter aan de mensen en middelen om alle dreigingen bij te houden en om steeds updates en upgrades door te voeren. Daarom kiezen steeds meer organisaties ervoor om security deels of geheel uit te besteden. Eigen experts kunnen zich dan richten op waar ze het best in zijn, zoals het vertalen van businesswensen naar IT-oplossingen.

Een ander groot voordeel is dat je voor een vast bedrag zowel hard- en software als diensten afneemt. Advies, training, back-up en Disaster Recovery neem je af tegen voorspelbare kosten.

# DE MEERWAARDE VAN VALID MANAGED SECURITY SERVICES

De kracht van Managed Security Services met Valid is dat wij nooit een standaardpakket bieden, maar altijd zoeken naar een oplossing die past bij de schaal en behoeften van jouw organisatie.

Valid bestaat inmiddels meer dan twintig jaar. We hebben veel kennis en ervaring op het gebied van security. Daardoor weten we precies wat er nodig is om data optimaal te beschermen. Kenmerkend voor ons is dat we dicht bij onze klanten staan, betrokken zijn en snel en pragmatisch handelen. Zo helpen we grote en kleine organisaties in diverse branches om voorop te lopen.

In onze aanpak doorlopen we vier stappen:

1. **Evalueren:** hoe goed is het gesteld met je IT- en Security-landschap? Met Security Scans brengen we de situatie nauwgezet in beeld. Welke ambitie heb je en welke risico's loop je? Een uitgebreide phishing security test als nulmeting helpt bijvoorbeeld heel goed om de huidige vatbaarheid voor phishing in kaart te brengen.
2. **Richten:** we stellen een roadmap en een verbeter- en beheersplan op. Je krijgt een dashboard dat helder inzicht geeft in meetgegevens. Dat helpt om het securityniveau op het gewenste niveau te brengen en te houden.
3. **Aanpakken:** we leggen vast wie wat doet, zodat je snel meters kunt maken. Wij kunnen jou bijstaan met onder meer programma-, project- en interim-management.
4. **Oplossen:** wat doe je als het toch fout gaat en elke minuut telt? Ook dan kun je op onze hulp rekenen. Onze experts helpen je om de impact in te perken.

Als partner van partijen die voorop lopen in security (Cisco, Kaspersky, Microsoft, Palo Alto Networks, Rapid7, Veeam, etc.) vinden we altijd een passende oplossing, voor elk vraagstuk.

# WAT KLANTEN VINDEN VAN ONZE AANPAK

**“Ik waardeer de open en proactieve security-houding van Valid. Het geeft me het vertrouwen dat we adequaat kunnen handelen in geval van cyberaanvallen.”**

- Christiaan de Geest, ICT Security & Compliancy Officer – CSU

**“De Security Volwassenheidsscan van Valid heeft ons waardevolle inzichten gegeven in ons security-volwassenheidsniveau. Na de scan ondersteunde Valid ons tevens bij het bereiken van het gewenste volwassenheidsniveau.”**

- Jan Ris, Manager Digital & Innovation – Vesteda

**“Valid wees ons op de beleids-regels voor back-up en retentie in Office 365.**
**Met hun Office 365 back-upoplossing zijn we in control, als het aankomt op onze Office-data. Deze oplossing is een mooie aanvulling op de rest van hun dienstverlening, het geeft ons veel rust.”**

- Jelle van der Werff, Teamleider Informatisering & Automatisering – VNG

**“Woonpunt blijft vooroplopen met de Disaster Recovery-oplossing van Valid. Door de juiste combinatie van back-up en replicatie kunnen wij onze bedrijfscontinuïteit garanderen.”**

- Baktash Olomi, Teamleider informatievoorziening – Woonpunt

## Meer weten?

Onze experts vertellen je graag hoe Valid kan helpen om de data van jouw organisatie te beveiligen. Is je interesse gewekt en wil je een vrijblijvend gesprek?

Neem contact op via 088 900 95 00 of vul het contactformulier in op www.valid.nl/security.

**Valid – Stay Ahead.**