DIGITALE TRANSFORMATIE KAN NIET ZONDER SECURITY

In 5 stappen naar een veilige digital workspace

kpn

Inleiding

Het is momenteel een kenmerk van de Nederlandse economie: grote bedrijven die vasthouden aan de oude wereld vechten om te overleven terwijl kleinere, slagvaardige bedrijven met innovaties stappen maken naar de nieuwe digitale wereld.

Nederlandse bedrijven zijn voor hun voortbestaan steeds vaker afhankelijk van een digitale transformatie. Digitalisering biedt enorme kansen en mogelijkheden, nieuwe samenwerkingsverbanden en nieuwe afzetgebieden. Daarbij is het belangrijk dat de bedrijfsprocessen optimaal aansluiten bij de wensen en de mogelijkheden die werknemers en consumenten hebben om met uw digitale 'winkel' te werken. Werknemers en klanten moeten de mogelijkheid hebben om altijd en overal en op elk gewenst apparaat te werken.

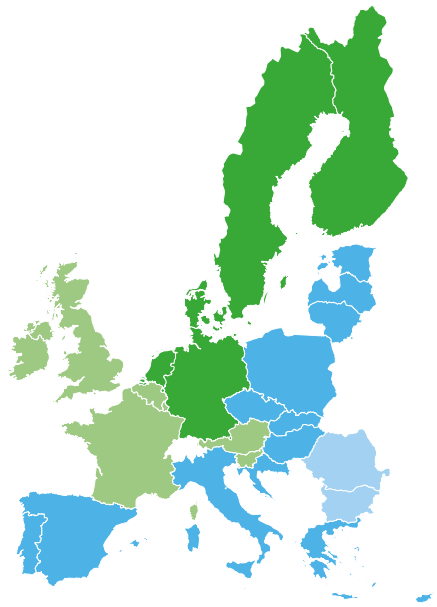
Tegelijkertijd introduceert digitalisering ook een nieuw fenomeen waar u rekening mee moet houden: cybercrime. Internetcriminelen staan een succesvolle digitalisering steeds vaker in de weg. Een groot deel van de Europese CIO's vreest zelfs dat cyberdreigingen innovatie en digitale transformatie afremmen. Digitale transformatie is dan ook onmogelijk zonder een goede beveiliging. In deze whitepaper zetten we vijf stappen uiteen die bijdragen aan veilig en betrouwbaar werken in een nieuw digitaal tijdperk.

Nederland innovatiekoploper

Nederland behoort op het gebied van digitale transformatie en innovatie tot de wereldtop. Meerdere instanties bevestigen dit:

- Het World Economic Forum roemt de Nederlandse economie in een rapport als 'een van de meest geavanceerde en innovatieve ter wereld'.
- In de Global Innovation Index 2015 (GII) staat Nederland als vierde genoteerd als het gaat om de meest innovatieve landen ter wereld.
- Volgens het gezaghebbende European Innovation Scoreboard 2016 is Nederland een van de vijf 'innovatieleiders'.

Deze koppositie is belangrijk voor de Nederlandse economie en welvaart. Digitale transformatie levert bedrijven concurrentievoordeel, nieuwe afzetmarkten en forse kostenbesparingen op en is de motor voor innovatie. Ook biedt digitale transformatie oplossingen voor maatschappelijke problemen zoals klimaatverandering en vergrijzing. Door bijvoorbeeld zorgprofessionals een 'digital workspace' te bieden, wordt zorg efficiënter en kan een vergrijzende bevolkingsgroep een betere zorg worden verleend.



Bron: European Commission

Succesvolle digitale transformatie

De meeste bedrijven staan nog aan het begin van hun 'digitale transformatie'. Toch zijn er ook al successen te melden:

- **KLM** creëerde een concurrentievoordeel met de belofte vragen van passagiers via Twitter, Facebook en LinkedIn binnen één uur te beantwoorden. Bij het boeken van een ticket kunnen klanten bovendien kiezen voor de optie 'ask a local'. KLM brengt de klant dan in contact met een 'local' die via WhatsApp allerlei informatie doorgeeft over de eindbestemming.

- **Schiphol** wil de beste digitale luchthaven ter wereld te worden. Internet of Things-toepassingen op basis van het LoRa (Long Range Low Power)-netwerk staan daarbij hoog op de agenda. Een voorbeeld is het op afstand monitoren van de volheid van prullenbakken. Ook het op afstand monitoren van de lampen die worden gebruikt om werkzaamheden op het landingsterrein af te bakenen, behoort tot de mogelijkheden. Door grote hoeveelheden data te combineren en via slimme software te analyseren, kan Schiphol continu realtime scenario's draaien, de klanttevredenheid voorspellen en daarop anticiperen.

- **Havenbedrijf Rotterdam** zet met partners sterk in op innovatie. Zo verbindt de haven sensoren aan het LoRa-netwerk. Vervolgens analyseren ze de resultaten realtime. Zo is het havenbedrijf in staat om zeer nauwkeurige voorspellingen te doen over de waterstand. Dankzij deze informatie kunnen zij reders weken op voorhand informeren over de maximale beladingen. Maar bijvoorbeeld ook afvalinzameling wordt een stuk slimmer.

Cybercrime bedreigt digitale transformatie

Cybercriminelen vormen echter een steeds grotere bedreiging voor onze digitale vooruitgang. Bijvoorbeeld door de netwerken en verbindingen te verstoren die zo belangrijk zijn voor de digitale transformatie.

Onderzoek van Vanson Bourne toont aan dat bijna negen op de tien ondervraagde Europese CIO's al eens slachtoffer is geweest van een cyberaanval, of op korte termijn een aanval verwacht. 73 procent van de ondervraagden vreest dat deze cyberdreiging de ontwikkelingen op het gebied van IT en innovatie afremt.

Met name de Nederlandse ICT-infrastructuur ligt onder vuur. Cybercriminelen gebruiken steeds vaker en frequenter de Nederlandse netwerken om cyberaanvallen uit te voeren. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) vermeldde in zijn jaarverslag over 2015 bovendien 'een recordaantal digitale-spionageaanvallen op Nederlandse overheidsinstellingen en organisaties'. Aanvallers zoeken daarbij naar zeer specialistische en soms zelfs experimentele technologie die haar marktwaarde nog moet bewijzen. Minister-president Mark Rutte noemde cybercrime 'big business' voor Nederland.

Voor de 'populariteit' van Nederland onder cybercriminelen zijn meerdere oorzaken aan te wijzen:

- De verbindingen in Nederland zijn snel en betrouwbaar, en daardoor uitermate geschikt voor het uitvoeren van cyberaanvallen.
- In Nederland zijn veel mensen online die allemaal een potentieel doelwit vormen.
- Amsterdam heeft met de AMS-IX een van de grootste internetknooppunten ter wereld. Dit maakt van Nederland een aantrekkelijke 'hub' om aanvallen uit te voeren op andere landen.
- De pakkans is relatief laag. De oorzaken daarvan zijn divers. Zo zijn de beschikbare middelen voor actieve opsporing en vervolging beperkt, gebruiken cybercriminelen geavanceerde aanvalsmethoden en zijn sommige opsporingsmethoden door de privacywetgeving niet meer uitvoerbaar.

Schade cybercrime neemt toe

Cyberaanvallen kosten Nederlandse bedrijven en overheden veel geld, in 2015 zelfs tien miljard euro. Een jaar eerder lag dit bedrag op 6,75 miljard euro.

Dat cybercriminaliteit een groot probleem is voor het Nederlandse bedrijfsleven blijkt ook uit de Global Data Protection Index 2016 van EMC. Zeker 46 procent van de onderzochte bedrijven had in het jaar dat voorafging aan het onderzoek dat plaatsvond in maart en april 2016 te maken met ongeplande systeemuitval. 20 procent verloor daarbij data. De kosten die daarmee gemoeid waren, bedroegen in Nederland gemiddeld 517.000 euro per incident. Een dergelijke schadepost gaat zeker ten koste van innovatie en de initiatieven om te komen tot een 'digital workspace'.

Er zijn meerdere aspecten aan te wijzen die bijdragen aan deze kostenpost, zoals:

- De herstelkosten om de ICT-voorzieningen weer operationeel te krijgen.
- Gemiste inkomsten door een verstoring van de dienstverlening gedurende een korte of lange periode.
- Het verlies van het vertrouwen van klanten die in een 24-uurseconomie een ononderbroken dienstverlening verwachten.
- Imagoschade bij het grote publiek. Zeker bij veel media-aandacht is dat een risico.
- Hoge boetes. Bij het niet melden van dataverlies loopt het slachtoffer bijvoorbeeld het risico dat de Autoriteit Persoonsgegevens een boete oplegt tot maximaal 820.000 euro.

Cyberdreiging gaat niet weg

Door de hoge kosten die ermee gemoeid zijn, vormen digitale bedrijfsspionage, diefstal van gegevens en cyberaanvallen een directe bedreiging voor onze concurrentiepositie en economische groei. Cyberaanvallen verstoren bovendien de ICT-infrastructuren die voor een digitale transformatie zo hard nodig zijn.

Helaas duidt alles erop dat de cyberdreiging voorlopig blijft toenemen. Die toename heeft meerdere oorzaken:

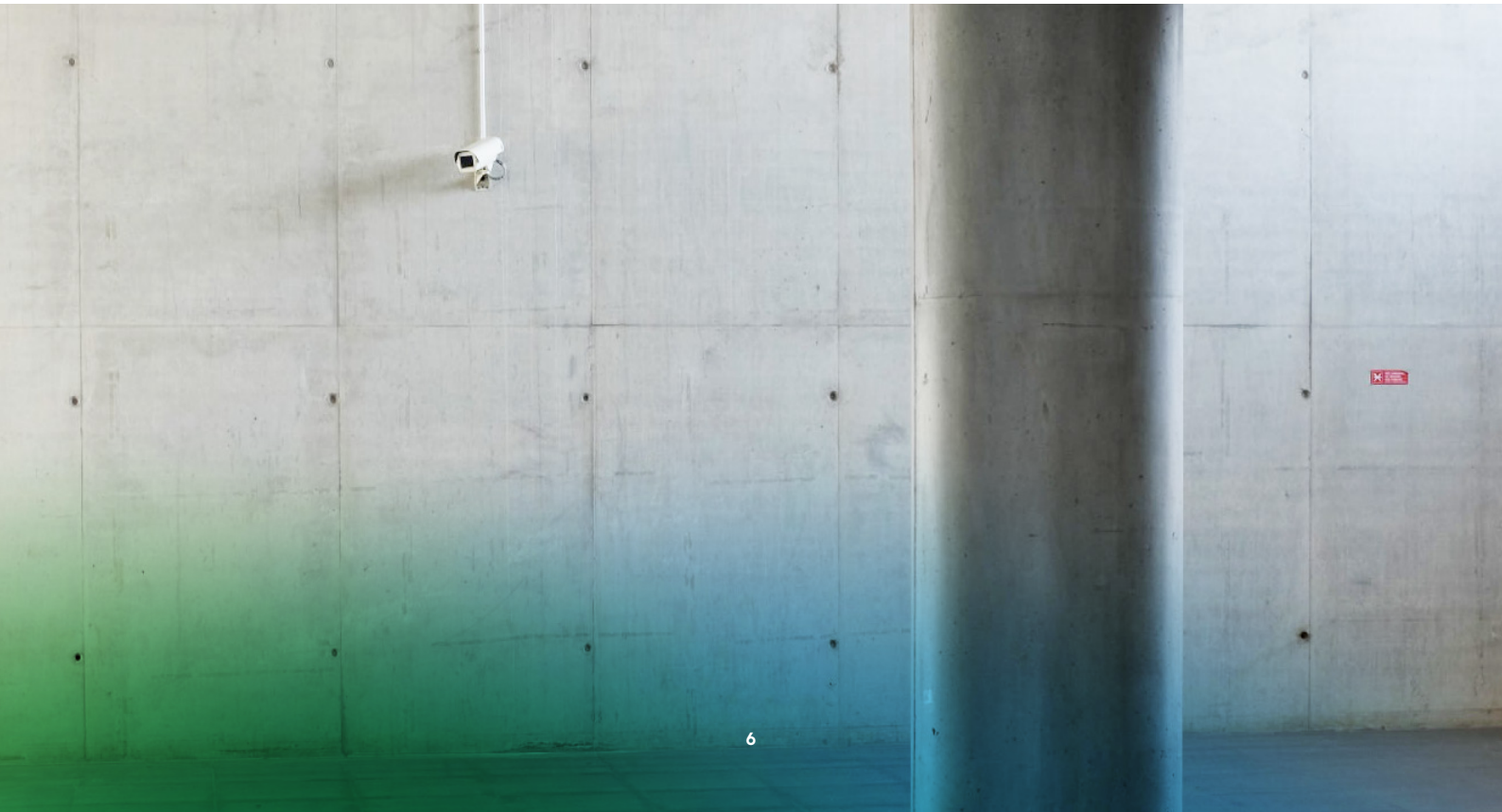
- Cybercriminaliteit loont, meer dan bijvoorbeeld handel in harddrugs. Naar verwachting bestaat misdaad in Nederland over vijf jaar voor 50 procent uit cybercriminaliteit.
- De technieken om systemen of netwerken mee aan te vallen, zijn steeds eenvoudiger verkrijgbaar. Ze zijn voor een luttel bedrag via internet te huur en door iedereen te gebruiken.
- Door de digitalisering zijn er voor cybercriminelen meer mogelijkheden om bedrijven aan te vallen.
- De pakkans is zoals eerder al aangehaald relatief laag.

Traditionele beveiliging schiet tekort

Voorheen volstond het om gegevens en IT-netwerken te beschermen door het toevoegen van steeds meer IT-beveiligingsoplossingen, zoals firewalls, inbraakdetectie- en inbraakpreventiesystemen en antimalware. Deze aanpak voldoet niet meer.

De traditionele beveiligingsaanpak schiet om meerdere redenen tekort:

- Digitale inbrekers gaan steeds ingenieuzer te werk. Inbraken zijn achteraf vaak niet te traceren.
- Data bevindt zich al lang niet meer alleen binnen het bedrijfsnetwerk maar – zeker als fysieke werkplekken zijn vervangen door digital workspaces – ook op mobiele apparaten en in de cloud. Dit maakt de beveiliging van gegevens complexer.
- De inzet van steeds weer nieuwe security-oplossingen vergroot de kans dat hackers kwetsbaarheden ontdekken. Ook worden het beheer en onderhoud van de security-omgeving steeds ingewikkelder.
- Het tekort aan securitytalenten wordt een steeds groter probleem. IT-teams beschikken vaak niet over de vaardigheden, kennis en juiste middelen om een ‘versnipperde’ security-omgeving in de lucht te houden en te reageren op actuele dreigingen.



5 stappen voor verbetering

Gezien de grote uitdagingen waar securityteams voor staan, is het niet vreemd dat veel organisatie informatiebeveiliging als een last zien. Uit de Nationale IT Security Monitor 2015 blijkt zelfs dat 60 procent van de bedrijven investeren in security als een noodzakelijk kwaad ziet.

De voor Nederlandse bedrijven en overheden noodzakelijk digitale transformatie is echter onmogelijk zonder een goede beveiliging. Digitalisering en beveiliging zijn onlosmakelijk met elkaar verbonden en bieden organisaties de mogelijkheid om een voorsprong te nemen op de concurrentie.

Om bedrijven te helpen bij het verbeteren van de beveiliging heeft KPN vijf stappen gedefinieerd die er ook nog eens voor zorgen dat u compliant bent en blijft:

Stap 1: **Identificeer de belangrijkste assets**
Deze stap draait om het in kaart brengen van de kroonjuwelen in uw IT-infrastructuur en de belangrijkste data. Waar bevinden bijvoorbeeld alle apparaten zich die zijn verbonden met het netwerk? Is dat in een eigen computerruimte, in een extern datacenter of in de cloud? En bezit u bijvoorbeeld persoonsgegevens die u zeker niet mag kwijtraken, of data die u onderscheidt van de concurrentie? Waar zijn die gegevens opgeslagen, en wat zijn de mogelijkheden voor cybercriminelen om die data te stelen? De risico's die u loopt, moeten continu inzichtelijk zijn.

Stap 2: **Bescherm tegen bedreigingen**
Welke beschermende maatregelen heeft u nodig om voorbereid te zijn op een security-incident? Hier draait het niet alleen om technische oplossingen zoals encryptie, back-up en het verlenen van toegang tot data. Maar bijvoorbeeld ook om het trainen van uw medewerkers, zodat zij zich bewust zijn van de risico's en weten hoe ze moeten handelen in het geval van een incident. Bijvoorbeeld calamiteitenoefeningen kunnen hiervoor een geschikt middel zijn.

Stap 3: **Spoor bedreigingen actief op**
Cybercriminelen doen er alles aan om traditionele securitymaatregelen te omzeilen, zodat zij zo geruisloos mogelijk een netwerk binnen kunnen dringen. Een goede verdediging vraagt dan ook om een continue monitoring van bijvoorbeeld e-mail, netwerk en apparaten. Er is kortom een proactieve benadering nodig om onregelmatigheden 24/7 op te sporen, te onderzoeken en op te lossen. Ook is het belangrijk om regelmatig te controleren of de getroffen beveiligingsmaatregelen nog steeds werken zoals gedacht.

Stap 4: **Reageer op incidenten en aanvallen**
Nadat opvallende incidenten zijn gedetecteerd, is het zaak om erger, zoals diefstal van data, te voorkomen. Een adequate voorbereiding op cyberincidenten helpt daarbij. Het is verstandig in een 'incident response plan' zo goed als mogelijk vast te leggen wie waarvoor verantwoordelijk is en welke acties worden ondernomen. Securitypartners kunnen hierbij van grote waarde zijn. Immers is het mitigeren van een cyberaanval voor het gros van de organisaties geen core business. Ervaren experts kunnen u ondersteunen bij het plannen en uitvoeren van de juiste maatregelen en zo helpen met het afslaan van een aanval en het beperken van de schade.

Stap 5: **Lessons learned**
Na een aanval of incident is het goed om te leren van de aspecten die wel en niet goed zijn gegaan tijdens de aanval en het herstelproces. Op basis van deze kennis kunt u bijvoorbeeld uw disaster-recoveryplannen aanpassen. In deze fase dient niet alleen het responseteam op de hoogte te zijn van de lessons learned, maar alle relevante medewerkers binnen de organisatie. Security is namelijk niet alleen een taak van IT.

Welke stappen passen bij u?

1 2 3

Welke stappen daadwerkelijk toepasbaar zijn, hangt ook af van het securityniveau binnen de organisatie. Uiteraard zijn hierin vele tinten grijs te onderscheiden, maar grofweg valt de security van een organisatie binnen een van deze drie niveaus:

Securityniveau 1: **Basic**
De organisatie is onder meer beschermd tegen zaken als spam, identiteitsdiefstal en bedreigingen in e-mail. Medewerkers kunnen veilig vanuit huis werken of veilig gebruikmaken van openbare wifiverbindingen. Ook maakt de organisatie regelmatig back-ups van belangrijke gegevens. Op dit niveau is de organisatie klaar voor de securitystappen 1 en 2, het identificeren van de belangrijkste assets en het beschermen tegen cyberdreigingen. Van een optimale beveiliging is nog geen sprake. De organisatie vangt bijvoorbeeld geavanceerde malware en spyware nog niet af.

Securityniveau 2: **Modern**
Op dit niveau is er sprake van een 'volwassen aanpak' gebaseerd op de risico's. Het securityteam staat los van IT en is klaar voor securitystap 3: het actief opsporen van dreigingen. De kans dat een organisatie na een incident niet meer kan functioneren, is heel klein maar niet volledig uit te sluiten.

Securityniveau 3: **Geavanceerd**
De organisatie is in hoge mate beschermd. Voor de bescherming van businessprocessen wordt gebruik gemaakt van geautomatiseerde processen en analisten die afwijkende patronen detecteren. Medewerkers kunnen hun applicaties en gegevens veilig gebruiken. Organisaties met een geavanceerd securityniveau doorlopen ook de securitystappen 4 en 5. Daardoor zijn de incident-responseprocessen op orde en worden 'lessons learned' besproken. Om niet terug te vallen naar een lager niveau, is uiteraard continue aandacht nodig van zowel IT als het management.

Een redelijke beheersing van securityrisico's is voor iedere organisatie wenselijk. Denk daarbij allereerst aan inzicht in de risico's waaraan uw organisatie blootgesteld is, hoe u deze risico's verkleint en hoe u bij een incident kunt reageren. Welk securityniveau daarbij past, is afhankelijk van tal van factoren. Niveau 3 lijkt op het eerste oog het beste uitgangspunt, maar past in de praktijk lang niet altijd bij een organisatie. Daarom is het van belang om samen met u het gewenste niveau in kaart te brengen en vervolgens de transitie in gang te zetten. De manier waarop KPN Security Services dat doet, is volledig afhankelijk van uw situatie. Op basis van uw wensen bepaalt KPN Security Services samen met u een goede strategie en wordt in samenspraak een stappenplan opgesteld.

CONCLUSIE

Security is een enabler voor de digitale transformatie die voor bedrijven zo noodzakelijk is om te overleven; het succes van vernieuwende projecten valt of staat met een goede beveiliging. Door te voorkomen in plaats van te genezen, kunt u daadwerkelijk de digitale transformatie realiseren. U kunt 'disruptieve' ontwikkelingen blijven volgen en de concurrentie de baas blijven.