Veilig digitaal zaken doen

Uw bedrijfscontinuïteit bewaken in een digitale wereld

kpn

Inleiding

ICT-ontwikkelingen zetten het bedrijfsleven flink op zijn kop. Bedrijven grijpen gretig de vele kansen die de digitale revolutie biedt. Ze werken sneller, reageren sneller, zijn connected. Maar nieuwe kansen brengen onvermijdelijk nieuwe uitdagingen mee. Die maken de cruciale gegevens en primaire processen van uw bedrijf kwetsbaarder.

Niet alleen zijn digitale systemen gevoelig voor calamiteiten. Criminelen grijpen de nieuwe kansen ook met beide handen aan. Zo is de kans groot dat uw organisatie doelwit wordt van een DDoS-aanval. Dat is niet te voorkomen. Wél kunt u effectief de impact beperken en daarmee de bereikbaarheid van uw bedrijf en de continuïteit van de bedrijfsprocessen waarborgen.

Uw bedrijf werkt, communiceert en ádemt online. U moet dus beslist uw onlineomgeving beveiligen. Security is echter een kostenpost en goede keuzes zijn cruciaal. Optimale bescherming zonder afweging van de noodzaak kost geld. Bescherming die aansluit bij bedrijfsspecifieke risico's en keuzes levert juist geld op. Grijp die kans en kies in 4 stappen de online security die past bij uw bedrijf.

1. Baanbrekende kansen en nieuwe uitdagingen

De zakenwereld is het afgelopen decennium onherkenbaar veranderd. Zakelijke communicatie is volledig gedigitaliseerd. Internet en cloudtechnologie maken gegevens optimaal toegankelijk, werken kan altijd en overal. Klantgegevens worden doorlopend verzameld via websites en mailings. En het aantal webshops is explosief gegroeid. De digitale wereld biedt ongekende kansen voor bedrijven. Maar baanbrekende nieuwe kansen brengen nieuwe risico's mee.

Een nieuwe wereld

Internet is uit het bedrijfsleven niet meer weg te denken. We zijn volledig vergroeid met de digitale manier van werken en gegevens opslaan. Volgens het Cybersecuritybeeld Nederland 2015 van het Nationaal Cyber Security Centrum, hebben bedrijven steeds vaker geen analoge alternatieven meer voor ICT-systemen. Net als maatschappelijke processen zoals financieel verkeer, transport en energievoorziening maakt dit bedrijven afhankelijker van de beschikbaarheid van ICT-systemen en -netwerken. De primaire bedrijfsprocessen zijn kwetsbaar voor onder meer uitval van hardware en cybercrime. Dat brengt nieuwe uitdagingen mee. De digitale zakenwereld vraagt nadrukkelijk om een nieuwe analyse van reële bedreigingen én effectieve oplossingen. Want weet u bijvoorbeeld wat de gevolgen zijn als uw bedrijf langere tijd geen toegang heeft tot internet?

Fysieke en digitale risico's

Fysieke bedreigingen voor bedrijven zijn van alle tijden. In het digitale tijdperk zijn we afhankelijk van hardware. Calamiteiten zoals brand en elektriciteitsstoringen, maar ook problemen met de hardware zelf kunnen leiden tot dataverlies en uw website of webshop onbereikbaar maken. Digitale gegevensopslag en -uitwisseling kent echter ook nieuwe, digitale kwetsbaarheden. Zo kunnen gegevens onbedoeld in verkeerde handen vallen. Een USB-stick is in een oogwenk verloren. Een e-mail met attachments zó naar een verkeerd adres verstuurd. Dit heeft forse gevolgen, zoals verlies van gegevens en geschonden klantvertrouwen. Fysieke en digitale kwetsbaarheden vormen dus een reëel risico voor de bedrijfscontinuïteit. Bovendien kan uw bedrijf sinds 1 januari 2016 onder de Wet meldplicht datalekken te maken krijgen met boetes als u onzorgvuldig omgaat met digitale gegevens.

Cybercriminelen en cybersecurity

Niet alleen het bedrijfsleven, ook criminelen profiteren van de digitale revolutie. Bewuste aanvallen op kritische bedrijfsprocessen en digitale datadiefstal groeien al jaren explosief. DDoS-aanvallen, malware, phishing: het zijn inmiddels bekende termen. De gevolgen kunnen uiteenlopen. Eén gevaar is het weglekken of diefstal van data, bijvoorbeeld door middel van phishing en spyware. Hackers kunnen ongemerkt toegang krijgen tot uw netwerk en op hun gemak uw organisatie en gegevens bestuderen, voordat ze aanvallen. Zeker als ze gevoelige bedrijfsinformatie of klantgegevens buitmaken, staat de integriteit van uw bedrijf op het spel.

Cybercrime bedreigt ook de continuïteit van uw bedrijf, door data onbereikbaar te maken voor klanten of medewerkers. Criminelen kunnen hiervoor ransomware inzetten, zoals het in 2014 heel actieve Cryptolocker en het begin 2016 opgedoken Locky. Deze gijzelsoftware versleutelt uw gegevens en u krijgt de sleutel pas na betaling van losgeld. Nog eenvoudiger werkt distributed denial of service: een DDoS-aanval. Zo'n aanval is al voor enkele euro's te koop. Bij DDoS wordt een groot aantal gehackte computers – een botnet – ingezet om aanvragen naar één DNS-server te versturen. Deze raakt overbelast en bijvoorbeeld uw website, e-mail, VPN en CRM-applicaties worden onbereikbaar. Klanten komen niet meer op de website en medewerkers niet op het bedrijfsnetwerk. Aan deze verstoring van interne bedrijfsprocessen en bereikbaarheid hangt een prijskaartje. Het is zaak om te weten wat het uw organisatie kost om een dag lang niet productief te zijn.

2. Focus op business continuity

Kleine verstoringen van ICT-toepassingen zijn meestal niet onoverkomelijk. De kernactiviteiten van uw bedrijf moeten echter doorgaan. Raakt de business continuity verstoord, heeft dat immers financiële gevolgen. Een continuïteitsbreuk kan ontstaan door dataverlies of systeemuitval als gevolg van calamiteiten. Ook kwade opzet kan kernactiviteiten stilleggen en data onbereikbaar maken. Het digitale tijdperk vraagt daarom nadrukkelijk om een hernieuwde focus op bedrijfscontinuïteit.

DDoS: een groeiend probleem

DDoS-aanvallen zijn een belangrijk voorbeeld van bedreigingen voor de digitale continuïteit. De lijst met slachtoffers van DDoS-aanvallen is indrukwekkend: van de overheid tot de retail en van het mkb tot grote corporates. En de frequentie van aanvallen groeit. Zo maakte Verisign bekend in kwartaal 4 van 2015 maar liefst 85% meer aanvallen afgeslagen te hebben dan in hetzelfde kwartaal in 2014. Bovendien is de trend om meerdere aanvallen uit te voeren op één DNS-server. Belangrijke reden voor de toename: DDoS-aanvallen zijn eenvoudiger te organiseren dan ooit. Iedereen kan nu voor een schijntje op internet een DDoS-aanval inkopen.

Van kwade klanten tot beroepscriminelen

DDoS-aanvallen worden om diverse redenen gepleegd. Bedrijven willen bijvoorbeeld imagoschade toebrengen aan de concurrent, of ontevreden klanten zinnen op wraak. Deze partijen missen de technologische kennis om een DDoS-aanval uit te voeren, maar kunnen zo'n aanval wél eenvoudig online bestellen. Er zijn zelfs 'fun hackers' die uit baldadigheid aanvallen plegen. Beroepscriminelen kunnen DDoS gebruiken als afleidingsmanoeuvre in complexe, gelaagde aanvallen. Terwijl de organisatie focust op herstel van de bereikbaarheid, wordt aan de achterkant bijvoorbeeld dataroof gepleegd. Deze trend blijkt uit het rapport *Denial of Service: how businesses evaluate the threat of DDoS-attacks* van Kaspersky Labs uit 2015. Bij zo'n aanval krijgt u tegelijk te maken met dataverlies, inbreuk op de data-integriteit en eventueel een boete in het kader van de meldplicht datalekken.

Continuity is key

Continuïteit van de belangrijkste bedrijfsprocessen is van levensbelang voor bedrijven. Als een omvangrijke DDoS-aanval uw bedrijfswebsite platlegt of brand uw servers uitschakelt, kan dit direct leiden tot omzetverlies en imagoschade. Zeker bij bekende bedrijven en overheden is het uitvallen van de diensten nieuwswaardig én snel gedeeld via sociale media. En dat zijn alleen nog de gevolgen van de continuïteitsbreuk. Als hackers ondertussen gevoelige data buitmaken of data wegLekken door een menselijke fout, krijgt u te maken met de meldplicht datalekken. Bovendien kan het vertrouwen van klanten en relaties hierdoor nog een extra klap krijgen.

Rijksoverheid als doelwit

Dat geen enkel netwerk immuun is voor DDoS-aanvallen, blijkt wel uit de slachtoffers. Zo werd op 10 februari 2015 de server van diverse overheidwebsites platgelegd. Onder meer Rijksoverheid.nl en Defensie.nl waren het grootste deel van de dag onbereikbaar. Niet alleen burgers hadden hier last van, ook publieksvoorlichters konden niet meer bij de informatie die ze nodig hadden. Naast de overheidswebsites waren ook andere websites, zoals Geenstijl.nl, slachtoffer van de aanval. Dit bleek *collateral damage* te zijn. Pas na 10 uur werd de aanval afgeslagen. Uit de antwoorden op Kamervragen in maart 2015 bleek dat er wel degelijk back-ups bestonden van de getroffen websites. Deze waren echter door dezelfde aanval uitgeschakeld. Een duidelijke les voor het veiligstellen van bedrijfsgegevens: bewaar uw back-ups altijd op een andere fysieke of digitale locatie.

Goed nieuws

Het slechte nieuws is dat calamiteiten nooit volledig uit te sluiten zijn. Ook criminele bedreigingen zijn niet helemaal weg te nemen. DDoS-aanvallen kunt u bijvoorbeeld simpelweg niet voorkomen. Zolang hackers een botnet kunnen creëren, kunnen ze een aanval uitvoeren op uw bedrijf. De dreiging van DDoS-aanvallen blijft bovendien groeien. Iedere organisatie kan – en hoogstwaarschijnlijk zál – ermee te maken krijgen. Het goede nieuws is dat u met de juiste maatregelen wel degelijk de continuïteit kunt waarborgen.

3. Continuïteit beschermen in 4 stappen

De vraag is niet óf uw bedrijf te maken krijgt met een DDoS-aanval. De vraag is hoe, wanneer en hoe vaak. Toch staat u zeker niet machteloos. U kunt namelijk wel de impact van DDoS-aanvallen beperken. Hetzelfde geldt voor problemen met hardware en software. Het kan altijd fout gaan. Maar online security en goede back-up-faciliteiten zorgen ervoor dat de belangrijkste bedrijfs-processen doorgaan. Zo blijft het voor stakeholders *business as usual*. Maar hoe beschermt u de continuïteit effectief en betaalbaar?

Kroonjuwelen bewaken

Wilt u passende securitymaatregelen nemen, dan moet u inzicht hebben in de impact van de risico's. Wat zijn de gevolgen van een DDoS-aanval of uitval van cruciale ICT-systemen door een calamiteit? Ondervindt uw organisatie weinig schade als de website korte tijd niet bereikbaar is of de interne communicatie even wegvalt? Of leidt dit tot forse gemiste omzet – direct door de continuïteitsbreuk of indirect door imagoschade?
Dit hangt sterk af van de primaire bedrijfsprocessen.
U moet bepalen wat de kroonjuwelen van het bedrijf zijn, die optimale bescherming verdienen. Een *business impact analyse* helpt hierbij. Zo stelt u in 4 stappen vast wat de kritische bedrijfsprocessen zijn en welke bescherming zij verdienen.

Stap 1: kritische processen identificeren

Stap 1 is bepalen wat de bedrijfskritische processen zijn. Oftewel: welke processen moeten altijd doorgang vinden? Een bedrijfsscan maakt dit inzichtelijk. Hiermee worden alle bedrijfsprocessen doorgelicht en wordt vastgesteld wat de gevolgen zijn als de processen voor kortere of langere tijd uitvallen. Voor ieder proces en de bijbehorende gegevens stelt u vast wat altijd bereikbaar moet zijn en voor wie, willen de kernactiviteiten niet verstoord worden.

Stap 2: aannemelijke risico's en mogelijke maatregelen vaststellen

Of voor een risico een vergaande oplossing nodig is, hangt af van de risicobereidheid: in hoeverre risico's acceptabel zijn. Een scenario dat het ene bedrijf volledig ontregelt, heeft op een andere organisatie slechts beperkte impact. Daarom moet u per scenario bekijken of bescherming nodig is. Vervolgens is het zaak om vast te stellen welk verlies uw bedrijf kan lijden. Is het een probleem als data verzameld of aangemaakt in de afgelopen 2 uur verloren gaan? Kunt u meer of juist minder gegevens missen? Ook de duur van een storing is van belang. Hoe lang mag een dienst maximaal uitvallen? Dit wordt wel de maximale downtime genoemd.
Het maximale verlies en de maximale downtime moeten per scenario worden bepaald om te komen tot de juiste securityoplossingen.

Stap 3: passende maatregelen kiezen en uitvoeren

Optimale online bescherming klinkt altijd goed, maar er hangt wel een prijskaartje aan. Dit hoeft echter geen struikelblok te vormen: optimale bescherming is lang niet altijd nodig. De passende mate van security hangt af van de afweging tussen noodzaak en kosten. Beveiliging moet natuurlijk niet meer kosten dan het negatiefste scenario. De juiste mate van security levert geld op: het voorkomt risico's die kostbaarder zijn dan de gekozen beveiliging. Het is dus zaak dat u de security afstemt op de risicobereidheid. Bijvoorbeeld door optimale bescherming in te kopen voor de kroonjuwelen, maar genoegen te nemen met beperktere bescherming voor minder cruciale processen.

Stap 4: blijven testen en evalueren

Veel bedrijven denken dat ze alle gegevens en systemen veiliggesteld hebben. Helaas blijkt de praktijk vaak weerbarstig. Testen en evalueren van de maatregelen maakt het verschil tussen schijnveiligheid en echte veiligheid. Grondige tests leveren vaak waardevolle inzichten op, waarmee u de beveiliging kunt aanscherpen en schade voorkomt. Dit is geen eenmalige actie:
u moet maatregelen blijven testen en evalueren. Een business impact analyse is altijd een momentopname en maatregelen die u neemt, kunnen verouderen.
Hoe vaak u tests moet draaien hangt af van uw keuzes, en van kwetsbaarheden en veranderingen in uw organisatie. Serieuze digitale ambities op bedrijfsniveau vragen zeker om jaarlijkse analyse en tests van de securityoplossingen.

4. Passende oplossingen voor digitale uitdagingen

Oplossingen kiezen die aansluiten bij de eisen en wensen van uw bedrijf, vraagt om een brede blik. Niet alleen zijn diverse oplossingen mogelijk, u kunt ze ook op verschillende manieren inzetten. Voor het beschermen van de continuïteit zijn er in ieder geval 3 belangrijke oplossingsrichtingen.

Door de wasstraat

DDoS-aanvallen vormen een lastig probleem. Kwaadaardig verkeer komt immers via dezelfde route bij de server als legitieme bezoekers. Toch is er een effectieve oplossing: het verkeer 'wassen'. Deze mitigerende maatregel houdt in dat het verkeer naar de server wordt omgeleid via een service provider. De provider maakt in een wasstraat onderscheid tussen legitiem en kwaadaardig verkeer. Klanten krijgen via de wasstraat gewoon toegang tot bijvoorbeeld de website, zonder dat ze verschil merken. Aanvallers wordt de toegang ontzegd. Het is wel goed om te controleren waar de data worden gewassen. Gebeurt dit in het buitenland, dan kan namelijk andere privacywetgeving van toepassing zijn op de omgeleide gegevens.

De kosten van deze DDoS-oplossing hangen onder meer af van de gewenste reactiesnelheid. Hoe korter de maximale downtime, hoe sneller op een aanval gereageerd moet worden. Sommige service providers monitoren het netwerkverkeer voortdurend en bieden realtime inzicht in aanvallen. Dit maakt het eenvoudiger om snel te reageren en de continuïteit beter te bewaken. Om het effect van de beveiligingsmaatregel te controleren, kunt u een DDoS-aanval laten simuleren. Zo'n stresstest toont aan of de maatregel voldoende bescherming oplevert.

Cruciale data altijd veilig

Iedereen begrijpt het nut van back-ups. Toch regelen in de praktijk lang niet alle bedrijven dit goed. Een back-up die op dezelfde fysieke of digitale locatie wordt bewaard, garandeert niet dat de gegevens echt veilig zijn. Het is zaak om data die van belang zijn voor de primaire bedrijfsprocessen extern op te slaan, op meerdere locaties. Laat de back-ups automatisch maken op vaste tijden. Voor echte veiligheid is ook geregeld testen van de back-upfaciliteit cruciaal. Deze taken uitbesteden kan voorkomen dat ze op het tweede plan komen doordat actuele zaken uw aandacht opeisen. Deskundige dienstverleners kunnen zekerheid bieden door zowel de back-ups als intensieve tests professioneel uit te voeren. Zo voorkomt u dataverlies bij calamiteiten en wordt uw bedrijf minder gevoelig voor bijvoorbeeld ransomware, omdat u altijd back-ups heeft van versleutelde gegevens.

Snel back in business

Om de bedrijfscontinuïteit te beschermen is het belangrijk dat cruciale data en systemen binnen enkele minuten weer beschikbaar zijn. Ongeacht de oorzaak van de onbereikbaarheid. Met een traditionele back-up loopt u meestal risico op maximaal 24 uur dataverlies. Met *disaster recovery as a service* (DRAAS) kunt u het dataverlies beperken tot enkele minuten. De dienstverlener zorgt voor tijdelijke uitwijkmogelijkheden voor de werkzaamheden, terwijl uw ICT-voorzieningen weer worden opgebouwd. En in geval van een calamiteit of aanval zijn (back-ups van) uw virtuele machines gauw weer operationeel. Zo is uw bedrijf snel *back in business*.

Digitale risico's? Digitale oplossingen!

ICT verandert de zakelijke wereld in een ongekend tempo. Bedrijven profiteren volop van alle nieuwe kansen. De keerzijde is dat digitalisering nieuwe kwetsbaarheden meebrengt. Calamiteiten en aanvallen kunnen de bedrijfscontinuïteit ernstig ondermijnen. De digitale ontwikkelingen creëren echter niet alleen een probleem. Ze helpen ook de gevolgen effectief te beperken. Voor digitale risico's zijn passende digitale oplossingen – voor ieder bedrijf.

5. KPN Security Services

KPN gelooft in een wereld waarin iedereen beschermd is. Thuis, onderweg en op het werk. Onze missie: veilige, betrouwbare en toekomstbestendige netwerken en diensten leveren. We voegen waarde toe aan uw ICT-infrastructuur. Zo helpen we uw bedrijf veilig de stap naar groei te maken.

KPN Security Services biedt een uitgebreid pakket diensten. Een kleine greep uit ons aanbod geeft u een idee van de mogelijkheden. Zo beschermt AntiDDoS van KPN uw netwerk tegen DDoS-aanvallen en monitort doorlopend het netwerkverkeer. Daarbij houden we uw bedrijfsdata veilig binnen ons KPN-netwerk. Onze Back-up Online XL biedt extra veiligheid voor uw bedrijfsgegevens, door ze op 2 externe locaties op te slaan.

En met KPN Disaster Recovery Services zijn uw systemen in geval van calamiteiten binnen de afgesproken tijd weer operationeel. KPN Security Services ontzorgt. Zo kunt u zich veilig richten op de kernactiviteiten van uw bedrijf.

Meer weten over onze missie en diensten?
Kijk op kpn.com/security.

Contactgegevens
managedsecurityservices@kpn.com
www.kpn.com/security

kpn.com/security