CYBERCRIME OP DE ZAAK

HOE BEREID JE JE VOOR OP EEN CYBERAANVAL?

INHOUDSOPGAVE

INTRODUCTIE

De wereld vindt steeds meer ‘online’ plaats. Dit zorgt ervoor dat jouw medewerkers overal kunnen werken, maar ook dat er nieuwe risico’s ontstaan. Vandaar dat T-Mobile Ondernemen het topic cybercrime op de zaak uitlicht.

Twee specialisten op het gebied van cybersecurity nemen ons mee in de wereld van cybercriminaliteit en delen hun kennis. Welke vormen van cybercrime bestaan er? Wat als jouw bedrijf wordt aangevallen en wat kun je doen om cybercrime te voorkomen? Het landschap van cybercriminaliteit wordt in kaart gebracht, zodat jouw organisatie voorbereid is op alle vormen van cybercrime en cybersecurity op de juiste manier kunt inzetten.

1 SPECIALISTEN AAN HET WOORD

Lodi Hensen en Bram Ketting, beiden professionals op het gebied van cybersecurity, gaan dieper in op cybercriminaliteit. Lodi Hensen is Cybersecurity Specialist bij Tesorion en vertelde tijdens deze TableTalk TV alles over de belangrijkste vormen van cybercrime en hoe jouw bedrijf hiermee om kan gaan. En als Risk- en Cybersecurity professional bij 3rd Risk deelt Bram Ketting hoe je als organisatie grip krijgt op de risico's die buiten de eigen organisatie liggen, waar je zelf verantwoordelijk voor bent.

1.1 OVER TESORION

Tesorion is een snelgroeiende, Nederlandse cybersecurity-specialist bestaande uit meer dan 160 experts, actief in heel Europa. Tesorion is in 2018 ontstaan uit de samensmelting van een aantal gerenommeerde ondernemingen met ieder hun eigen specialisatie op het gebied van cybersecurity.

1.2 OVER 3RDRISK.COM

3rdRisk.com is het eerste echt samen-werkingsplatform voor risicobeheer door derden. Met dit SaaS-platform kunnen organisaties hun derde partijen registreren, monitoren en actief beheren. Ze hebben ook de mogelijkheid om hun risicobeheeractiviteiten voor leveranciers (gedeeltelijk) uit te besteden aan 3rdRisk of een gespecialiseerde partner.

2 WAKE UP! CYBERCRIME IS HERE (TO STAY)

Hacking, malware, gijzelsoftware, phishing – het zijn termen die je vast weleens in de media voorbij hebt zien komen. Cybercriminaliteit komt steeds vaker voor en de impact ervan neemt daardoor ook toe. In 2019 werden in totaal 4.700 cybercrime-misdrijven geregistreerd. Dit komt neer op gemiddeld bijna 13 misdrijven per dag. Zo blijkt uit een analyse van Dutch Tech Magazine.

De toenemende digitalisering zorgt ervoor dat cyberdreigingen zich in een rap tempo ontwikkelen. Sinds half maart is heel Nederland een stuk digitaler geworden, en daarmee ook een stuk kwetsbaarder. Een perfect moment om zakelijk Nederland wakker te schudden op het gebied van cybercrime.

Lodi Hensen laat ons zien wat er dagelijks gebeurt op het gebied van cybercrime. Hensen is al 15 jaar actief in de cybersecuritywereld. Dagelijks geeft hij leiding aan een team dat als first responder optreedt, de digitale brandweer bij cybercrime-incidenten. En er zijn heel wat brandjes te blussen.

Nieuwsberichten over datalekken, cyberaanvallen en hackers vliegen ons dagelijks om de oren. Dat zorgt ervoor dat we al die berichten minder serieus nemen, omdat het toch dagelijks gebeurt. We worden blind voor alle berichtgeving. Maar op de achtergrond staat de wereld als het ware in brand, zonder dat we het doorhebben. De gedachte: ‘het overkomt mij toch niet’ is achterhaald. Er komt een dag dat je getroffen wordt door een aanval. Dan kun je maar beter goed voorbereid zijn.

Vaak zijn cybercrime-incidenten niet op het eerste gezicht zichtbaar. Om dit beter in kaart te brengen, schetst Hensen een voorbeeld waarbij het onzichtbare van de digitale wereld zich vertaalt naar de fysieke wereld. Want we zien namelijk steeds vaker dat de impact van een digitaal incident, ook impact kan hebben op de fysieke wereld. In de Van Dale wordt dit mooi omschreven als de Citrixfile.

2.1 CYBERCRIME-INCIDENT CITRIXFILE

Wat gebeurde er precies? Vorig jaar rond de feestdagen werd een kwetsbaarheid gevonden in de serversoftware van Citrix dat thuiswerken faciliteert. Rijksoverheid haalde de servers offline, omdat de veiligheid niet gewaarborgd kon worden. Dat resulteerde in een overvloed aan mensen op de weg die niet meer thuis durfde te werken.

2.2 STIJGING IN CYBERAANVALLEN

De laatste tijd is er een enorme stijging van phishing attacks. Criminelen en andere partijen maken gretig gebruik van nieuws dat mensen triggert. Zij versturen een mail van je werkgever of zorgverzekeraar omdat men dan sneller geneigd is te klikken. Ook spelen ze in op trends. Door COVID-19 verwachten mensen een mail met een terugkomplan naar werk of informatie over hun contract. Partijen die de aanval inzetten op organisaties die bezig zijn met een vaccin, zijn nu ook een makkelijk doelwit.

3 WIE ZITTEN ERACHTER CYBERAANVALLEN?

Dat noemen we zogenoemde Threat Actors. Dit zijn kwaadwillende partijen of dreigingsactoren. Criminelen maar dan anders. Deze zijn onder te verdelen in subgroepen. Om je te wapenen tegen deze partijen wil je ze goed in kaart hebben voor jouw organisatie. Kies ervoor om je te weren tegen 1 groep. En wees je er bewust van dat er een kans bestaat dat op de een of andere manier deze groepen ooit bij je binnendringen, als dat de intentie is. Dit zijn ze:

3.1 STATELIJKE ACTOREN

Dit zijn grootschalige overheden die onbeperkte budgetten, onbeperkte middelen en onbeperkte mensen hebben die aanvallen kunnen plegen. Vaak zijn zij uit op informatie door middel van spionage, sabotage en beïnvloeding. Een statelijke digitale aanval verkrijgt toegang tot digitale systemen van een andere staat en is de grootste digitale dreiging voor onze veiligheid.

3.2 CRIMINELEN

Criminelen verplaatsen zich van het fysieke domein naar het digitale domein. Dat betekent dat zij vanaf hun zolderkamer een criminele organisatie kunnen runnen. De pakkans is vrijwel nihil en aantrekkelijk voor criminelen die zich bezighouden met ransomware (gijzelsoftware). Bestanden worden versleuteld, waardoor bedrijven losgeld moeten betalen. Belangrijke informatie bieden criminelen te koop aan bij organisaties die daar baat bij hebben.

3.3 ACTIVISTEN

Deze partij verplaatst zich ook van de fysieke wereld naar de digitale wereld. Zij gebruiken het internet om te protesteren, zoals bijvoorbeeld hackersgroep Anonymous. Websites worden ondergeklad of afgeperst, vaak met een sociaal,

ideologisch of politiek doel. Als je als organisatie al in het fysieke domein te maken hebt met activisme, moet je er rekening mee houden dat het ook gebeurt in het digitale domein.

3.4 SCRIPT KIDDIES

Dit zijn de zogenoemde cybervandalen. Jongeren die bij hun ouders thuis een heel netwerk hacken van een grootschalige organisatie. Gewoon, omdat het kan. Ze kijken hoever ze kunnen komen en doen het veelal voor de lol. Zij doen het niet voor financieel gewin, maar hebben vaak niet door wat de consequenties zijn. Het is een soort kwajongensgedrag waarin jongeren elkaar aansporen om hetzelfde te doen, met vaak grote gevolgen.

3.5 TERRORISTEN

Angst en terreur zaaien kan op verschillende manieren, ook in het digitale domein.

Deze groep kan informatie verzamelen die relevant is voor hun doelen. Dit zagen we een aantal jaar geleden in Amerika, waar een database met gegevens van militairen was gelekt. NAW-gegevens werden op een forum van IS gepubliceerd. Een DDoS aanval of een fysieke aanslag op een datacentrum ligt ook in het straatje van terroristen.

3.6 EMPLOYEES

Dit zijn je eigen medewerkers. De eerdergenoemde partijen vallen aan van buiten naar binnen - maar vergeet de insiders niet, je eigen werknemers.
Het zijn mensen die een geschil of conflict met je hebben en op deze manier aanvallen. Maar het kan ook zijn dat een werknemer een bepaald voordeel wil behalen bij een nieuwe werkgever met gevoelige informatie over jouw bedrijf. Zorg daarom voor een goede screening. En zorg voor goede technologische middelen die afwijkend gedrag kunnen scannen in het digitale domein van je organisatie.

4 CYBERSECURITY: HOE HOOG WIL JE DE LAT LEGGEN

Je bedrijf beschermen tegen cybercriminaliteit kun je zien als een kogelvrijvest. Het doel is kogels tegenhouden. Maar naarmate je meer bescherming in dat vest stopt, wordt het vest zwaarder en dus ook moeilijker om ermee rond te lopen. Hoe ver wil je gaan? Je wilt je personeel niet eindeloos belasten met continue wachtwoorden veranderen en van systemen switchen. Kies een manier die werkbaar blijft. Je kunt je beschermen, maar niet tegen elk kaliber. Wees je bewust hoe je bedrijf er van de buitenkant uitziet. Een open deur is een gemakkelijk doelwit om open te breken. Breng daarom alle partijen in kaart, met alle bijbehorende aanvalstechnieken. En bedenk dan: Wat heb ik? Waar kan ik mij tegen wapenen? Waar komen de schutters vandaan? En wat zijn trends in mijn sector?

4.1 CYBER KILL CHAIN

Vliegtuigbouwbedrijf Lockheed Martin was in het verleden slachtoffer van een cyberaanval. Zij hebben een model ontwikkeld die in kaart brengt welke stappen een cybercrimineel zet om een aanval te plegen. De Cyber Kill Chain. Dit zijn de stappen:

FASE 1 RECONNAISSANCE

Dit is de voorverkenningsfase waarin cybercriminelen de organisatie bestuderen. Met een verrekijker analyseren zij als het ware de situatie. Waar zitten die open deuren? En waar zit de zwakke plek van de organisatie?

FASE 2 WEAPONIZATION

Hier gaat de cybercrimineel bepalen welke middelen hij gaat inzetten. Werkt jouw bedrijf bijvoorbeeld met Mac-computers? Dan weten zij dat ze geen Windows-software kunnen verzenden om in te breken of schade aan te richten.

FASE 3 DELIVERY

Op basis van de verzamelde informatie selecteren zij een specifiek medium voor hun aanval. Ze kijken in deze fase hoe ze de software bij de organisatie naar binnen krijgen.

FASE 4 EXPLOITATION

Vervolgens gaan ze dat uitbuiten. Bijvoorbeeld als een systeem niet up-to-date is of een bepaalde medewerker niet helemaal security-aware is. Zijn er geen open deuren? Dan proberen de aanvallers met phishing mails binnen te komen.

FASE 5 INSTALLATION

Hier wordt het kwaadaardige programma via de achterdeur geïmplementeerd. Het systeem wordt geïnfiltreerd met bijvoorbeeld een Trojaans paard, zonder dat het doelwit dit doorheeft.

FASE 6 COMMAND AND CONTROL

In deze fase krijgt de aanvaller als het ware de touwtjes in handen. De hacker heeft een ingang gevonden en dringt steeds dieper in het systeem om data te exfiltreren.

FASE 7 ACTIONS ON OBJECTIVE

Eenmaal toegang tot het systeem kan de cybercrimineel gerichter zijn acties uitvoeren. Zijn stappen worden concreter om uiteindelijk zijn doel te bereiken.

4.2 EEN DIGITALE WAAKHOND

Nu je weet welke stappen doorlopen worden, kun je bepalen hoe je je security wil inregelen, en op welke vlakken dat moet. Denk aan een digitale waakhond in de vorm van netwerk-sensoren of endpoint-sensoren. Dit is de vervanger van de traditionele antivirus en kijkt en luistert continu mee wat er gebeurt op de computer en het netwerk. Ze slaan direct alarm als ze iets verdachts zien.

4.3 TIPS & TRICKS

1. VERBETER JE ZICHTBAARHEID

Zorg dat je de zichtbaarheid van jouw infrastructuur en jouw netwerk goed in kaart hebt. Dit moet in de breedste zin van het woord in orde zijn. Weet welke middelen je hebt en welke afwijkingen er zijn. Ga ermee aan de slag en maak er een continu proces van om dit te waarborgen.

2. BEN ALTIJD UP-TO-DATE

Zorg dat je je updates op orde hebt. Zo ben je minder kwetsbaar en een minder makkelijk doelwit.

3. BEREID JE VOOR OP ELK INCIDENT

Net als de jaarlijkse BHV-cursus, waarbij je je voorbereid op ongelukken, moet je dat ook voor de digitale veiligheid doen. Kijk waar mensen zich digitaal bevinden, wat zij doen en wat hun strategie is.

4. INVESTEER IN EEN (GEAUTOMATISEERD) DETECTIE- EN RESPONSE SYSTEEM

En het liefst een systeem dat 24 uur per dag automatisch aan het werk is om te reageren op binnendringers. Doet een werkstation iets geks? Isoleer de boel direct. Zo kan je meteen ingrijpen en de volgende dag kijken wat de vervolgstappen zijn.

“Met Covid-19 komen we erachter dat er bepaalde risico’s spelen in de supply chain die we van tevoren niet in kaart hadden. Zoals afhankelijk zijn van subleveranciers in China.”

5 GRIP KRIJGEN OP RISICO'S DIE BUITEN JE ORGANISATIE LIGGEN

Bram Ketting is al 12 jaar werkzaam in cybersecurity en gespecialiseerd in third-party management. Dit is het proces waarbij derde (externe) partijen onder de loep worden genomen om te zien welke risico's er in het ecosysteem van de organisatie spelen. Het landschap wordt in kaart gebracht, zodat duidelijk wordt met welke externe partijen de organisatie een contractuele verplichting heeft.

5.1 WIE ZIJN DIE DERDE PARTIJEN?

Een derde partij is elke entiteit waar een bedrijf mee samenwerkt. Denk aan leveranciers, distributeurs of fabrikanten. Het zijn partijen die bijvoorbeeld payrolldiensten verzorgen of de catering in je kantine. De reden waarom organisaties met derde partijen werken is makkelijk te verantwoorden. Als bedrijf is het lastig om bepaalde kennis en recources uit de markt te krijgen, omdat deze simpelweg te schaars of te duur zijn. Dan is het handiger en goedkoper om dit in te huren. Veel bedrijven outsourcen naar India, om kosten te besparen. Zij hebben gespecialiseerde kennis op IT-gebied en zijn een stuk goedkoper.

Een andere reden om zaken uit te besteden is omdat er lokaal steeds meer wetten en regelgeving gehanteerd worden. De lasten worden zo hoog, waardoor het beter is om het uit te besteden. Een mooi voorbeeld waarbij de inzet van derde partijen goed tot uiting komt, zijn de Werelddeal Weken van KLM. De aanbiedingen worden online aangeboden, waardoor er enorme druk ligt op de customer support. Op dat moment is het makkelijk als je kan opschalen naar een derde partij, zonder dat je extra mensen in dienst hoeft te nemen.

5.2 VERSCHUIVING NAAR KERNACTIVITEITEN

Een belangrijke verschuiving vindt plaats als organisaties hun ecosystemen van derden uitbreiden om kernactiviteiten uit te voeren. Er is namelijk een enorme groei aan derde partijen. Dit verhoogt de complexiteit van de beveiliging van de organisatie. We zien steeds vaker dat organisaties hun volledige core business aan derde partijen overlaten, waardoor zij volledig afhankelijk zijn.
De potentiële impact als je aangevallen wordt door cybercriminelen is dan vele malen groter.

60% van alle datalekken gebeuren extern, omdat een derde partij zijn zaken niet goed heeft beveiligd. Als organisatie sta je met de rug tegen de muur.

Vanuit de reputatiekant is het belangrijk om hier aandacht aan te besteden. Want niet de derde partij komt bij een datalek in het nieuws, maar de overkoepelende organisatie. Terwijl bij de derde partij vaak de oorzaak ligt.

Door COVID-19 zijn er meer risico's doordat de hele workforce in een lockdown kwam. Thuis aan de keukentafel ben je een stuk minder scherp om hier toezicht op te houden. Aangezien veel derde partijen ook afhankelijk zijn van een nieuw, afgelegen personeelsbestand, maken de meeste compliance-leiders zich zorgen over het risico van cybersecurity als gevolg van praktijken zoals het gebruik van onveilige netwerken. Zorg er dus voor dat de derde partij waarmee je samenwerkt, dit in kaart heeft.

6 DE CIJFERS

De risico's van derden in kaart brengen is complex. Deze zijn vaak multi-dimensionaal, omdat ze zich kunnen verspreiden over derde partijen en vervolgens een impact hebben op verschillende niveaus van de organisatie. Vaak ziet een bedrijf dit niet aankomen, maar zijn wel volledig aansprakelijk. Kijk goed wat zich tijdens de contract-lifecycle afspeelt en hoe het ecosysteem van een derde partij in elkaar zit. Een datalek kan zich namelijk gemakkelijk vertalen naar een financieel-, security- of reputatierisico. Met de meest kritische partijen moet je dit waarborgen.

35%

van de organisaties heeft goed in kaart met welke derde partijen zij zakendoen

41%

heeft genoeg ervaring om kritische leveranciers te managen

83%

heeft in de afgelopen 3 jaar een incident met een derde partij meegemaakt

28%

werd geconfronteerd met een grote verstoring van alle bedrijfsfuncties

7 DE OPLOSSING

De sleutel tot grip en controle krijgen op de risico's is samenwerking, automatisering en standaardisatie. Het is aannemelijk dat in de toekomst het grootste gedeelte van een organisatie gaat bestaan uit derde partijen. Er moet meer expertise komen in dit vakgebied, waarbij je kijkt naar tools en instrumenten om controle te krijgen binnen de omgeving. We zijn allemaal onderdeel geworden van het ecosysteem. Ook jij bent een derde partij voor een andere organisatie. We moeten dit samen aanpakken.

7.1 ER ZIJN 3 OPLOSSINGEN OM GRIP TE KRIJGEN:

1. ZOEK DE SAMENWERKING OP

Bedrijven voeren bepaalde veranderingen door, waardoor de vraag ontstaat: hoe zijn we in deze situatie terecht gekomen? We zitten in een ecosysteem waarin we moeten samenwerken om het op te lossen.

2. AUTOMATISEER MEER

Processen moeten geautomatiseerd worden. Hiermee elimineer je de kans op menselijke fouten. Wees transparant naar elkaar zodat er een duidelijk beeld van de situatie ontstaat.

3. CREËER OVERZICHT DOOR TE STANDAARDISEREN

Iedereen heeft vragen en heeft de neiging om deze op elkaar af te vuren. Hierdoor ontstaat chaos. Dit is te voorkomen door onderling met elkaar af te stemmen welke processen gehanteerd moeten worden. Zo is het voor iedereen duidelijk.

Belangrijke vragen voor de Raad van bestuur met betrekking tot de huidige interne uitvoering van het risico voor derden.

4 VRAGEN OM OVER NA TE DENKEN:

1. Hebben we een volledig overzicht van de populatie van derden?
2. Hoe detecteren en monitoren we risico's van derden?
3. Waar zijn de hoogste risicoconcentraties?
4. Wat doen we met deze risico's?

HEB JE DE ACTIEPUNTEN IN KAART?

De volgende zes stappen helpen je om de risico's van derden in kaart te brengen.

1. CAPACITEITSOPBOUW

Kom met verschillende teams bij elkaar (zoals het privacyteam, securityteam, sustainabilyteam etc.) en zet met elkaar een Supply chain Third-risk party Competencies op. Hier breng je de risico's in kaart.

2. EISEN- EN BEHOEFTENOVERZICHT

Zet op een rij: welke eisen krijgen we opgelegd van onze klanten? Waar moeten we aan voldoen en is er een specifieke wet- en regelgeving?

3. MAAK EEN DERDE PARTIJ CATALOGUS

Breng inzichtelijk wie deze derde partijen zijn.

4. SEGMENTEER DE VERSCHILLENDE PARTIJEN

Rangschik de partijen onder in verschillende segementen om een duidelijk overzicht te hebben van de verschillende partijen.

5. DUE DILIGENCE-EVALUATIES

Benader deze partijen en stel ze vragen om een feeling te krijgen bij hun werkwijze. Vraag bijvoorbeeld rapporten op.

6. RISICOBEWAKING & -UITTREDING

Ga actief monitoren. Wat gebeurt er tijdens de lifecycle en de contractsduur? Maak duidelijk dat zij kritieke data verwerken, en dat jullie graag willen meekijken. Richt vervolgens het proces op een structuele wijze in.

7.2 DE VEILIGHEIDSRISICO'S INSCHATTEN

Hoe kun je dan een goede inschatting maken van de veiligheidsrisico's bij een leverancier, vraag je je misschien af? Kijk goed welke type business je met de derde partijen draait. Wat zijn de core-processen die jullie hebben uitbesteed? Kijk dan welke type data zij precies verwerken. Hebben ze toegang tot alle gegevens? Gaat het om gevoelige persoonsgegevens of innovatietrajecten? En hoe kritisch zijn ze?

Je moet er altijd vanuit gaan en beoordelen op basis van het scenario: wat als het misgaat? Wat zijn de kosten en hoe afhankelijk ben je van deze partij? Bekijk dit dan vanuit data en continuïteit.

8 EEN VEILIG BEDRIJFSNETWERK

Naast bovengenoemde tips en adviezen kun je meer doen om je organisatie te voorzien van een veilig bedrijfsnetwerk. Met een besloten IP-VPN of Ethernet netwerk werken al je bedrijfslocaties veilig, razendsnel en kostenefficiënt samen. Met Cloud Connect hebben je medewerkers veilige en gegarandeerde verbinding met de meestgebruikte cloud providers.

8.1 IP-VPN

IP-VPN (Virtual Private Network via IP-protocol) is een besloten netwerk voor de datacommunicatie binnen jouw organisatie. Met IP-VPN hebben medewerkers veilig, snel en makkelijk remote access tot alle beschikbare toepassingen en gegevens binnen het bedrijfsnetwerk. Denk aan: Office-applicaties, fileservers, bedrijfsspecifieke ERP- en CRM-applicaties en supply chain management toepassingen.

ALLES WORDT VOOR JE GEREGELD

T-Mobile legt de verbindingen, installeert de hardware en zorgt voor het beheer en het onderhoud van je bedrijfsnetwerk. Of het nu via koper, glasvezel of radioverbinding verloopt. Eventuele onderhoudscontracten zijn onderdeel van deze dienst. Bovendien heb je altijd een vast aanspreekpunt bij wie je terecht kunt met vragen en verzoeken.

8.2 ETHERNET CONNECT

Met Ethernet Connect ben je verzekerd van een betrouwbaar, besloten netwerk tussen locaties. Daarbij zijn schaalbare, hoge bandbreedtes mogelijk tot wel 1Gbit/s.

BESTAAND NETWERK VERVANGEN?

Ben je op zoek naar vervanging voor je huidige vaste verbindingen, Frame Relay, ATM of LAN Interconnect? Ook dan is zakelijk ethernet een uitstekend alternatief. Je krijgt een point-to-point (E-Line) verbinding met zeer hoge bandbreedtes die je makkelijk kunt opschalen.

VAN VERBINDING TOT BEHEER

T-Mobile legt de verbindingen, installeert de hardware en zorgt voor de bewaking én het beheer van uw Ethernet VPN. Zo kunnen de Local Area Netwerken (LAN's) op al jouw vestigingen veilig met elkaar communiceren als één gesloten netwerk. We bieden een uitgebreide Service Level Agreement (SLA), met de keuze uit diverse service-gradaties en aansluitopties.

8.3 CLOUD CONNECT

Voorkom dat je met reguliere cloud access afhankelijk wordt van het publieke internet om je cloud-omgeving te bereiken. Met Cloud Connect heb je geen last meer van onvoorspelbare bandbreedte of latency. Dus ook geen onvoorziene kosten en veiligheidsrisico's, maar gegarandeerd veilig transport van verkeer.

GESCHIKT VOOR DE MEESTE CLOUD PROVIDERS

Cloud Connect van T-Mobile is compatibel met de meest gangbare Cloud Service Providers (CSP's):

- Azure | Microsoft Azure ExpressRoute
- Microsoft 365 | Microsoft Azure ExpressRoute – O365
- AWS | Amazon Web Services (AWS) Direct Connect
- Google | Google Carrier Peering Layer3
- Salesforce | Salesforce Express Connect
- IBM | IBM Cloud Direct Link

AANVULLEND OP IP-VPN

Cloud Connect van T-Mobile voegt gateway-functionaliteit toe aan je IP VPN-verbinding. Je kunt rekenen op 1:1 bandbreedte van 50Mbit/s tot 1Gbit/s, afhankelijk van de cloud provider die je gebruikt.

TIP: VOOR HET GEBRUIK VAN WACHTWOORDEN

Hergebruik geen wachtwoorden en investeer in een wachtwoordmanager die ervoor zorgt dat je altijd unieke wachtwoorden hebt. Maar ook makkelijk te onthouden zijn. Je logt direct in, omdat ze al in het systeem zitten. Als het kan, maak dan gebruik van een tweestapsverificatie, zodat je altijd een fysiek apparaat nodig hebt om toegang te krijgen tot je account.

CONTACT

Wil je erachter komen wat de beste security-oplossingen zijn voor jouw bedrijf? Kijk dan op T-Mobile.nl/Ondernemen of neem contact op met ons Ondernemen Team via 0800 0200 740