OpStap naar weerbaarheid

Het vijfstappenplan voor cyberweerbare telecommunicatie

Eelco Vriezekolk
Agentschap Telecom

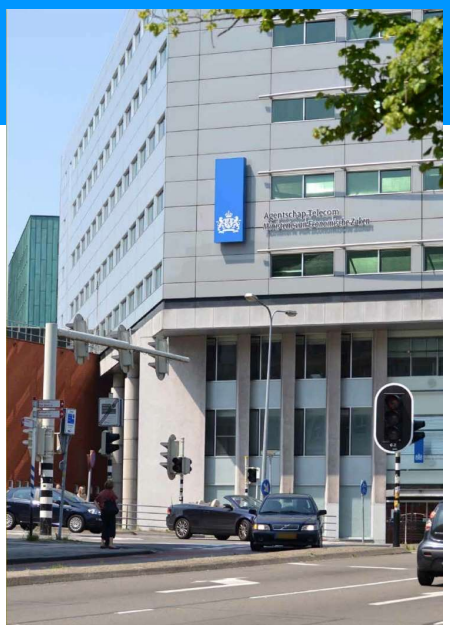
Zaalvoorzitter: Mirjam van Burgel, Agentschap Telecom

#OpStap2019

Agentschap Telecom

uitvoerder en toezichthouder
op digitale communicatie
in en voor Nederland

Voor een Veilig Verbonden Nederland



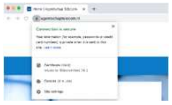
Agentschap Telecom is een onderdeel van het ministerie van Economische Zaken en Klimaat.

Telecommunicatie is onze specialiteit.

Digitale communicatie is breed.
Dus ons werkveld is ook enorm breed.
Dat gaat van internationale onderhandelingen over satelliet-posities tot toezicht op graafwerkzaamheden bij kabels en leidingen.

En voor sectoren waar telecommunicatie voor veilig van levensbelang is, zoals de maritieme sector, luchtvaart, en de zwaailichtsector.

Tot aan radio-omroep, radio-zendamateurs en (natuurlijk) onze mobieltjes.



Herkenning idensys

OpStap naar Weerbaarheid 2019 "Vijfstappenplan cyberweerbare telecommunicatie" 5

In al die sectoren zorgen we voor voldoende frequentieruimte,
voor storingsvrije apparatuur,
houden we continuïteit in de gaten,
en zorgen we voor digitaal vertrouwen.

Over Telekwetsbaarheid

Aanbieders
robuustheid technologie

- zorg- & meldplicht
- bereikbaarheid 1-1-2
- apparatuureisen
- vergunningverlening, … *etc*

Afnemers
weerbaarheid gebruikers

- bewustwording
- handelingsperspectief
- zelfredzaamheid

OpStap naar Weerbaarheid 2019 "Vijfstappenplan cyberweerbare telecommunicatie" 6

Het agentschap doet veel op aan de aanbod zijde van de markt.
Niet zonder succes, want we hebben in Nederland misschien wel de meest betrouwbare telecom ter wereld.
Maar de roep om robuustheid van die infrastructuur is groot, en wordt steeds groter.
100% betrouwbaarheid is niet mogelijk.
De enige zekerheid is *dat* het een keer zal uitvallen.
Dus gebruikers van telecommunicatie moeten zich daar op voorbereiden.
Wij noemen dat Telekwetsbaarheid.
Agentschap Telecom helpt met bewustwording, maar heeft ook een concrete oplossing.

https://www.agentschaptelecom.nl/onderwerpen/telekwetsbaarheid/documenten/videos/2019/februari/4/quickscan-uitval-telecom-lang

Voordat ik ik uitleg hoe wij dat doen, wil ik vragen: stel u voor dat u een nieuw product lanceert, een nieuwe dienst (Uber, AirBnB) of webshop of een intranet-toepassing. Dat is spannend, u hebt veel energie erin geïnvesteerd, en hoopt dat dat zich gaat terugverdienen.
En dan gebeurt er dit:

Heeft telecom aparte BCM-aandacht nodig?

OpStap naar Weerbaarheid 2019 "Vijfstappenplan cyberweerbare telecommunicatie" 8

Mike heeft het zo slecht nog niet gedaan.

Hij heeft aandacht voor uitval van elektriciteit. Er is noodstroom aangelegd. En het werkt.
Hij heeft aandacht voor fysieke toegangsbeveiliging, en camerabeveiliging.
Hij heeft aandacht voor cyberbeveiliging. Antivirus-software, updates, firewalls etc.
Maar hij heeft niet stilgestaan bij de uitval van telecom, en de gevolgen daarvan.

Waarom speciale aandacht voor telecom?
Dat is toch gewoon een bron van verstoring, net als uitval van ander infra?
Kunnen we dat behandelen net als fysieke inbraakbeveiliging?
En waarom zou het anders zijn dan andere soorten cyberincidenten?

Heeft telecom aparte BCM-aandacht nodig?

OpStap naar Weerbaarheid 2019 "Vijfstappenplan cyberweerbare telecommunicatie" 9

Uiteraard niet verkeerd om ook naar telecom te kijken.

Maar je moet al zo veel. En alles kost aandacht en tijd, energie en geld.
Die zijn schaars, dus die wil je graag optimaal inzetten.

En dan is telecom één van de vele oorzaken van BC-verstoringen.
Maar er is iets speciaals aan de hand: 3 zaken die anders zijn.
Drie zaken die maken dat telecom heeft wel degelijk eigen aandacht nodig heeft.

Telecom is onzichtbaar

Bron: Eindhovens Dagblad

Bus:

1. GPS-ontvanger in de bus,
2. locatie doorgegeven aan verkeerscentrale,
3. spraakverbinding tussen chauffeur en centrale,
4. data-verbinding voor de OV-chip,
5. misschien een camera-verbinding.
6. Maar ook: KAR-systeem waarmee de bussen voorrang kunnen aanvragen bij verkeerslichten.

Dat zie je niet, maar is er wel!

En het grootste deel van de tijd werkt het uitstekend. Alleen bij een storing merk je dat het er was.
En hoe afhankelijk je bent. Want valt een van deze systemen uit, dan zal de bus niet rijden (of iig de dienstregeling flink verstoord raken). Ook al is er diesel, een chauffeur en is de weg vrij!

Telecom is vervlochten

Die afhankelijkheid zien we niet alleen bij Openbaar Vervoer, maar op allerlei plaatsen in de maatschappij.
Telecom is niet meer een losstaand iets, dat ondersteunend is.
Het is onlosmakelijke kluwen van telecom, primaire processen, en ondersteunende processen.

Omdat het betrouwbaar is, efficiëntie verhoogt, kosten verlaagt omarmen we het snel. Vooral in NL zijn we gebrand op gebruik van nieuwe technologie. Digitalisering is een keuze, geen natuurverschijnsel.

Gebruik van telecom explodeert

Gebruik is in een stroomversnelling geraakt. De ontwikkelingen gaan steeds sneller.
2G / GSM -> 3G / UMTS -> 4G / LTE: intervallen steeds korter
VHS banden -> DVD -> streaming: intervallen steeds korter

Bankfilialen → thuisbankieren
Reisbureaus → booking.com, airbnb
Taxi → Uber
Postkantoor → nu een fitness- of horecabestemming

Dus ja, telecom heeft aparte BCM-aandacht nodig

Onzichtbaar

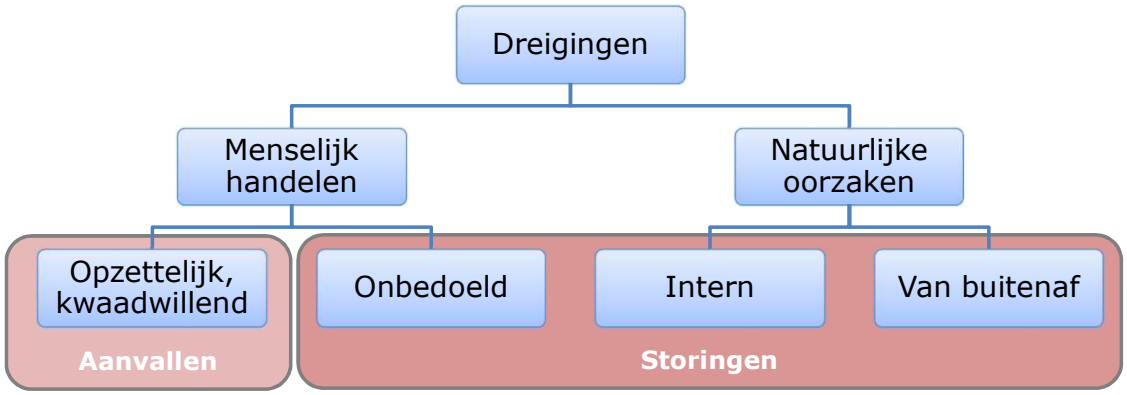
(behalve bij incidenten)

Vervlochten met bedrijfsprocessen

Gebruik van telecom **neemt explosief toe**

Dus, ja, we ontkomen er niet aan om specifiek aandacht te besteden aan afhankelijkheid en continuïteit van telecommunicatie, in al zijn verschijningsvormen.

Bronnen van verstoring en uitval



In eerste instantie richtten we ons op niet-opzettelijke aanleidingen.
Daar was een duidelijke reden voor: wij merkten vanuit onze praktijk dat daar weinig aandacht voor was. Té weinig.
Nu we een duidelijke aanpak hebben, nemen we ook opzettelijke verstoringen mee.

Telecom kan stuk door:
- schade van buitenaf (Stroomstoring Amsterdam)
- spontane defecten, slijtage
- onbedoeld menselijk handelen (kabelschade Deventer, feb 2017)
- de spreekwoordelijke hacker.

Let wel: het gaat ons om *storing* van telecommunicatie of *misbruik* van telecommunicatie.
Ik ga onze aanpak toelichten, en daarbij aangeven hoe we die uitbreiding naar cyberweerbare telecom vormgeven.

Vijfstappenplan

1. Bewustwording

2. Afhankelijkheden

3. Risico's

4. Maatregelen

5. Blijf fit

OpStap naar Weerbaarheid 2019 "Vijfstappenplan cyberweerbare telecommunicatie" 15

Je moet dus aandacht besteden aan de gevolgen van uitval van telecom.
Maar hoe doe je dat dan?

Daarvoor hebben we een vijfstappenplan ontwikkeld, op basis van ervaringen in diverse sectoren. Variërend van een gemeente tot aan een transport-knooppunt, en van een chemische fabriek tot aan een instelling voor ouderenzorg.

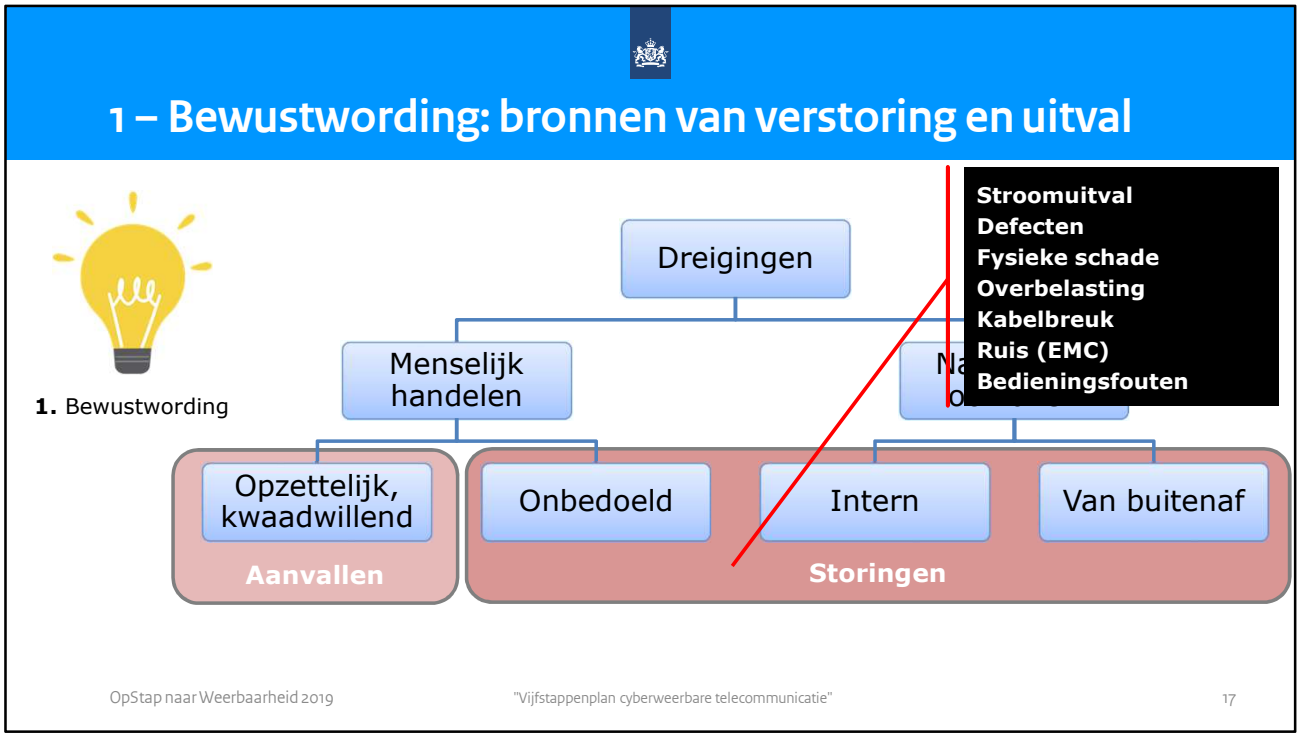
Bij elke stap hebben we hulpmiddelen. Dus: vijfstappenplan + toolkit.
Beproefd in de praktijk: cases bij publieke partijen, for-profit, semi-profit.

1 – Bewustwording

1. Bewustwording

- Twee video's
- Incidentenmonitor
- Serious game
- Kenniscafé

Bewustwording is de eerste stap. Belangrijk.
In onze ervaring vergt dit echt toelichting, vanwege de onzichtbaarheid van telecom die ik net toegelicht heb.
Maar veel organisaties pikken het dan snel op.
Vooral organisaties waar veiligheidsdenken onderdeel is van de cultuur (denk aan de Zorg).
(Vreemd genoeg is een globale relatie: hoe technischer de aard van het werk, hoe minder urgentie gevoeld wordt.)



Voor storingen zijn er eigenlijk maar zeven algemene kwetsbaarheden.

1 – Bewustwording: aanvallers en hun motieven

1. Bewustwording

	Diefstal van informatie	Schade toebrengen	Financieel gewin	Springplank
Klanten, (ex-) medewerkers		wraak		toegang
Activisten		media-aandacht		toegang
Criminelen			afpersing	botnet
Concurrenten	bedrijfsgeheimen			toegang
Buitenlandse mogendheden	bedrijfsgeheimen			toegang

Maar voor aanvallen ligt dat anders. Er zijn verschillende groepen aanvallers, ieder met hun eigen motieven.

2 – Afhankelijkheden

2. Afhankelijkheden

- Checklist, brainstorm
- Telecom-matrix

Vanwege die verwevenheid en onzichtbaarheid van telecom, is het vaak nodig om expliciet even de relatie tussen bedrijfsprocessen en telecomdiensten in kaart te brengen.

Twee instrumenten voor. Dat zien we vaker in onze toolkit: we hebben twee hoofdsporen: Snel & Grondig. Je kan kiezen naar behoefte. Grondige tools leveren het beste resultaat, maar als je weinig capaciteit hebt kan je starten met de eenvoudige tools.

Checklist in dit geval is een lijst met veelgebruikte telecomdiensten, aan de hand waarvan je alleen of met een collega brainstormt over het belang daarvoor voor jouw organisatie.

Telecom-matrix

2. Afhankelijkheden

Betrek medewerkers uit *gehele organisatie*

Processen:
- primaire processen
- ondersteunende processen
- gebouwprocessen

"Leidt verstoring langer dan XX uur tot onacceptabele gevolgen?"

of

"Worden via deze telecomdienst vertrouwelijke gegevens verstuurd?"

Interviews → Processen → Beoordeling → Matrix + Essentiële gegevens

OpStap naar Weerbaarheid 2019 "Vijfstappenplan cyberweerbare telecommunicatie" 20

- Met wie communiceert u? En hoe?
- Welke gegevens heeft u nodig bij uw werkzaamheden? Hoe bereiken die gegevens u?
- Wat zijn de gevolgen als uw werkzaamheden tijdelijk niet meer uitgevoerd kunnen worden?
- Welke processen moeten ook doorgang hebben bij verstoringen?

Drempel: "uitval van telecom van langer dan XX uur leidt tot onacceptabele problemen."
Vliegveld: 30 minuten
Gemeente: 48 uur

Telecom-matrix

2. Afhankelijkheden

Beoordelingsformulier 'Belangrijkheid van een bedrijfsproces'

	Bedrijfsproces	hoog	midden	laag
1	Meldingen versturen/ontvangen van persoonsalarmeringen bewoners (bewoners = intramuraal)	H		
2	Cameratoezicht op bewoners in de nacht		M	
3	Toegang tot Elektronisch Cliënten Dossier (ECD) voor medische gegevens	H		
4	Voorschrijven of aanpassen van medicatie in het medicatiesysteem		M	
5	Bereikbaarheid dienstdoende verpleeghuisarts	H		
6	Thuiszorg-medewerker: ontvangen van persoonsalarmeringen cliënten	H		
7	Thuiszorg: toegang tot het Elektronisch Cliënten Dossier (ECD)		M	
8	Thuiszorg: op afstand meekijken met wondverzorging			L
9	Contactgegevens vinden van andere medewerkers via intranet Vita			L
10 :	Brandmeldsysteem: doorzetten van brandmeldingen naar brandweer :	H		

Telecom-matrix

2. Afhar

Bedrijfsproces	vitaliteit	Telecom-techniek: kantoor LAN	interne telefonie	vaste telefonie	mobiele telefonie & data	verbinding OMS	e-mail	VPN naar IT dienstverlener	IT dienstverlener data center	internet toegang Vita	internettoegang cliënten thuiszorg
1 Meldingen versturen/ontvangen van	H		X		(X)				X	X	
2 Cameratoezicht op bewoners in de nacht	M	X									
3 Toegang tot Elektronisch Cliënten Dossier (ECD) voor medische gegevens	H	X									
4 Voorschrijven of aanpassen van medicatie in het medicatiesysteem	M	X						X			
5 Bereikbaarheid dienstdoende verpleeghuisarts	H		X		X						
6 Thuiszorg: ontvangen van persoonsalarmeringen cliënten	H			(X)	X						
7 Thuiszorg: toegang tot het Elektronisch Cliënten Dossier (ECD)	M	X			X				X		(X)
8 Thuiszorg … dverzorging	L	X			X						X
9 Contactg … lewerkers via intranet Vita	L	X						X	X		
10 Brandmeldsysteem: doorzetten van brandmeldingen naar brandweer	H					X					
Belang telecom-techniek:		H	H	M	H	H	L	H	H	H	L

Medicatie-dossier

Elektronisch Cliëntendossier

OpStap naar Weerbaarheid 2019 "Vijfstappenplan cyberweerbare telecommunicatie" 22

Belang is Hoog als die telecom-techniek voor minstens één bedrijfsproces met Hoog belang wordt gebruikt.
Op basis van de interviews: twee essentiële gegevensverzamelingen.
Je ziet dat door het Medicatiedossier het kantoor LAN en de VPN verbinding extra belangrijk worden.

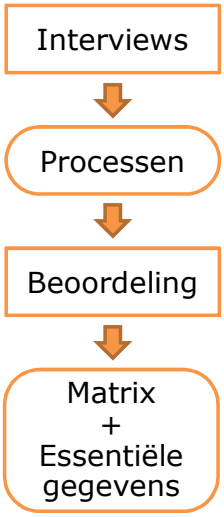
Als je de Snelle route gebruikt, dan doe je in feite hetzelfde, maar iets minder gestructureerd. Dat bedoelen we met de 2 routes Snel & Grondig.
Dit zou een leuke opdracht kunnen zijn voor een stagiair of afstudeerder.

Telecom-matrix: wat levert het op

2. Afhankelijkheden

Belangrijke bedrijfsprocessen, met:

- telecom die daarvoor nodig is
- belangrijke gegevensverzamelingen.



Levert een goed overzicht, maar vooral ook gezamenlijk inzicht.

3 – Risico's

3. Risico's

- Checklist, brainstorm
- Raster-methode

Weer een grondige en een snelle methode.

Raster-methode

3. Risico's

a) Teken de fysieke onderdelen van telecomdienst

b) Beoordeel enkele fouten en gedeelde fouten

c) Longlist

d) Beoordeel maatschappelijke risicofactoren

e) Shortlist

Diagrammen

↓

Beoordeling

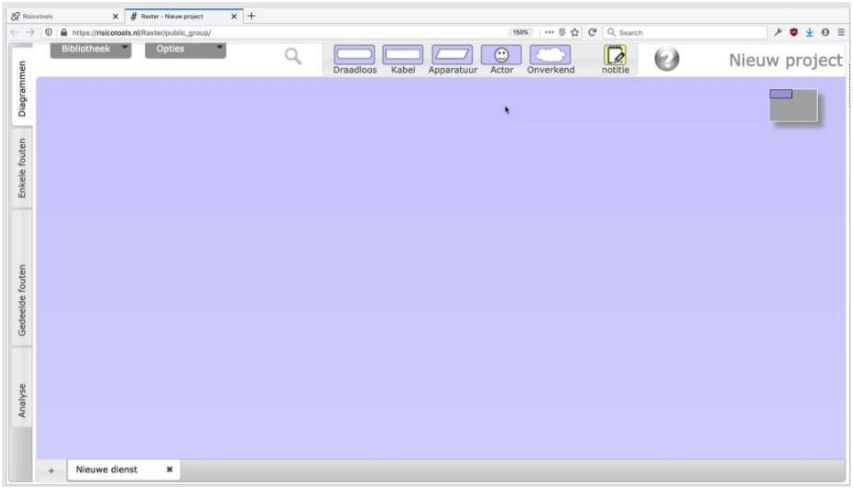
↓

"Top 10"

Om risico's in kaart te brengen, moet je weten welke spullenboel je hebt.

Apparatuur? Dan gevoelig voor stroomuitval. Waar staat de apparatuur, en wat is het effect?
Twee kabels in dezelfde ondergrondse goot: bij een graafincident kunnen beide tegelijkertijd doorgesneden raken. Ben je dan je redundantie kwijt?

De risico's zitten in de details. Raster helpt je om dat op een gestructureerde manier stapsgewijs boven tafel te krijgen.

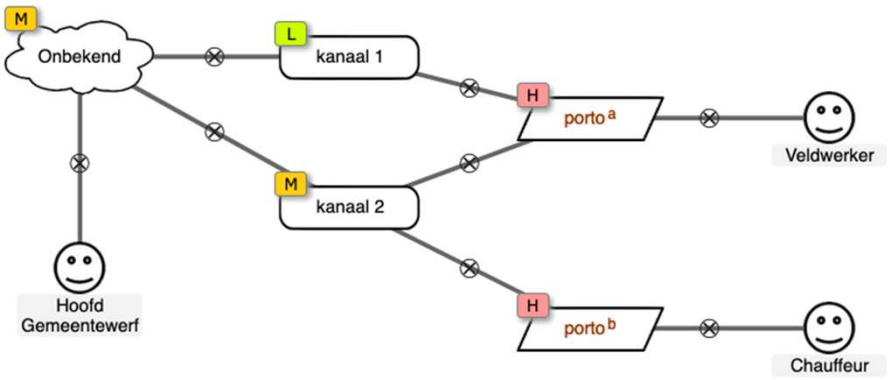


Raster wordt ondersteund door software.
Die helpt je om de diagrammen te tekenen, en om de beoordelingen te maken.

(Video van de tool in actie).

Raster-methode

3. Risico's



OpStap naar Weerbaarheid 2019 "Vijfstappenplan cyberweerbare telecommunicatie" 27

Diagram van een portofoon-systeem van een gemeente.

Wiebertje: apparatuur
Ronde rechthoekjes: draadloze verbindingen
Gewone rechthoekjes: kabels (staan niet in dit voorbeeld).

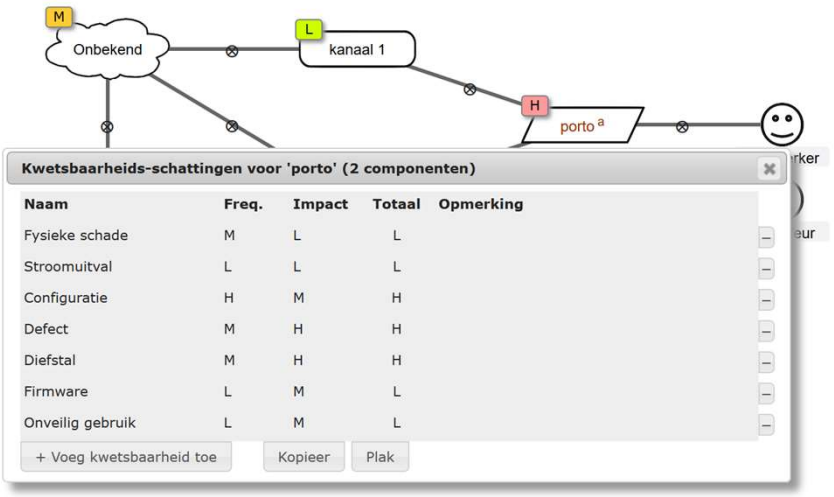
Chauffeur van vrachtwagen heeft eenkanaals porto.
Veldwerker kan twee kanalen gebruiken.
Hoofd van de Gemeentewerf is bereikbaar, maar we weten (nog) niet hoe. Vandaar het wolkje.

Raster staat dus toe dat delen van het netwerk onbekend blijven.

Kleurtjes geven risico-niveau aan. Volgende sheet laat zien hoe dat tot stand komt.

Raster-methode

3. Risico's



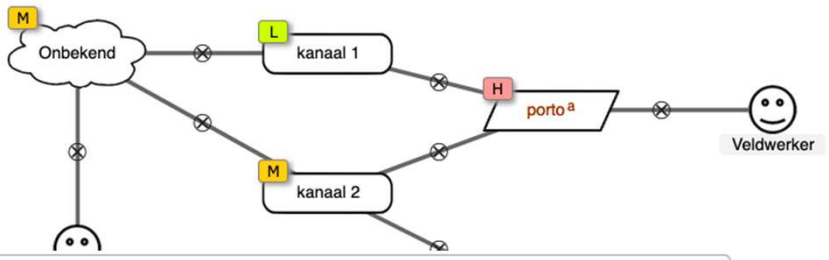
OpStap naar Weerbaarheid 2019 "Vijfstappenplan cyberweerbare telecommunicatie" 28

Neem bijvoorbeeld een portofoon.
Er is een standaardlijst van kwetsbaarheden voor apparatuur (kan je aan toevoegen, weghalen)

Van elk bepaal je gezamenlijk de frequentie (hoe vaak komt het voor), en de impact. Hiervoor bestaan richtwaarden! Zo objectief mogelijk; mijn Matig is jouw Hoog. Bijvoorbeeld: Matige frequentie betekent "Eens per 50 jaar".

Voor bewuste verstoring (de onderste drie) is Frequentie een combinatie van het type aanvaller en de moeilijkheid van de aanval.

Raster-methode



3

▾ Gedeelde foutoorzaken voor "Jammen" (draadloos) V

Naam	Freq.	Impact	Totaal	Opmerking
Jammen	L	H	M	
└ Portofoonkanalen	L	V	V	

:hauffeur

Gedeelde foutoorzaken: één incident waardoor meerdere onderdelen uitvallen.
Bijvoorbeeld graafschade waarbij twee kabels in dezelfde buis worden kapotgetrokken.
Bijvoorbeeld stroomstoring waarbij alle apparatuur in een serverruimte uitvalt.

In ons portofoon-voorbeeld van de gemeentewerf: als beide kanalen verstoord raken is geen communicatie meer mogelijk.
Dat is uitzonderlijk (Frequentie is Laag) maar de gevolgen zijn groot (Impact is Very high, vuurrood).

Het gaat te ver voor nu om uit te leggen hoe dat precies werkt, maar alle documentatie staat online.

Raster-methode

3. Risico's

a) Teken de fysieke onderdelen van telecomdienst

b) Beoordeel enkele fouten en gedeelde fouten

c) Longlist

d) Beoordeel maatschappelijke risicofactoren

e) Shortlist

Diagrammen

Beoordeling

"Top 10"

Als alle kwetsbaarheden zijn beoordeeld op frequentie en impact kan je de grootste risico's bepalen.
Dat is in eerste instantie iets dat vanzelf uit de beoordeling rolt: de Top-zoveel van alle kwetsbaarheden.

Maar risico's spelen zich af in een maatschappelijke context.

Raster-methode

3. Risico's

Factor	*Omschrijving*
Angst	De mate van bezorgdheid en verontrusting.
Bekendheid	De mate waarin het risico als veelvoorkomend en bekend gezien wordt.
Betrokkenheid kinderen	De mate waarin kinderen aan het risico worden blootgesteld.
Institutioneel toezicht	Nauw en effectief toezicht op risico's door autoriteiten, die de mogelijkheid hebben om in te grijpen waar nodig.
Kunstmatigheid	'Onnatuurlijkheid' van de oorsprong van risico's.
Media aandacht	Hoeveelheid aandacht in de (sociale) media.
Mobilisatie	Vermogen om protest en tegenwerking op te roepen.
Mogelijk catastrofaal	Angst voor plotselinge, ontwrichtende en grote effecten.
Oneerlijkheid	Ongelijkheid tussen degenen die de voordelen genieten en degenen die de risico's dragen.
Persoonlijke invloed	Mate van invloed die een individuele belanghebbende

OpStap naar Weerbaarheid 2019 "Vijfstappenplan cyberweerbare telecommunicatie" 31

"Media aandacht" bijvoorbeeld: als uw organisatie recent in het nieuws is geweest wegens verstoring door stroomuitval, dan kan een bestuurder zich niet veroorloven om nog eens zo'n incident te hebben.
Het risico van stroomstoring wordt daardoor groter, omdat de gevolgen van zo'n tweede stroomstoring gevolgen gaat hebben.

Hoogte van risico is gefundeerd op harde cijfers. We zijn niet blind voor risicoperceptie, houden er rekening mee, maar laten ons er niet door leiden.

Raster-methode

3. Risico's

OpStap naar Weerbaarheid 2019 "Vijfstappenplan cyberweerbare telecommunicatie" 32

Voor alle documentatie van Raster zie de website RISICOTOOLS.NL
U kunt daar ook de gratis software downloaden.

4 – Maatregelen

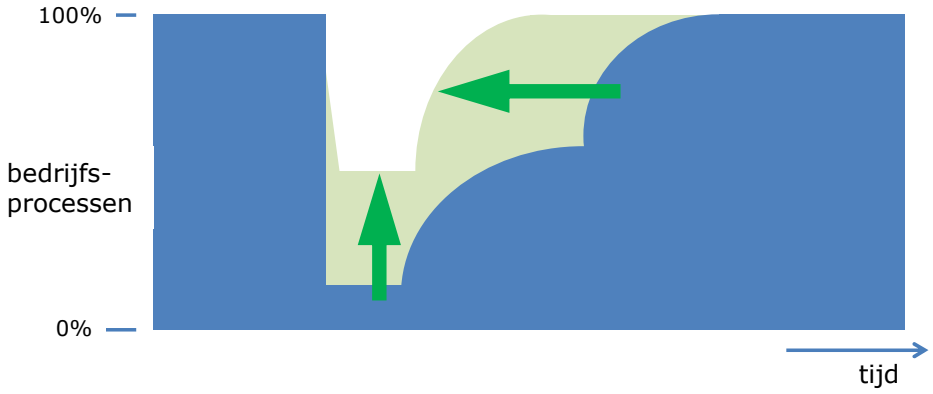
4. Maatregelen

Maatregelen treffen is in onze beleving vaak de minst moeilijke stap.

Het vijfstappenplan is niet zozeer gericht op *preventie*, maar vooral op *weerbaarheid*.
Kijk naar dit plaatje. Horizontaal staat de tijd, verticaal hoe goed onze bedrijfsprocessen lopen (0% = geheel uitgevallen, 100% = alles loopt zoals bedoeld).
Op dit moment ontstaat een incident: bedrijfsprocessen vallen terug.
Stapsgewijs werken we aan herstel.

4 – Maatregelen

4. Maatregelen



Graceful degradation betekent dat je
- minder hard geraakt wordt (“minder diep valt”)
- sneller weer hersteld bent

Het groene oppervlak is de *weerbaarheid* die je wilt organiseren.

4 – Maatregelen

4. Maatregelen

Organisatorisch én technisch

Checklist / tips

- Leg acties bij uitval van telecom vast
- Plaats gegevens in de cloud
- Kies meerdere aanbieders
- Voer aansluitingen dubbel uit
- Maak afspraken en houd instructies actueel
- Bewaar oude werkwijzen
- Werk samen met anderen
- Gebruik sterke wachtwoorden
- Regelmatige software updates

Die weerbaarheid vergt veelal organisatorische maatregelen.

- Papieren kaart (Shell stratenboek)
- In het algemeen: terugvallen op oudere werkwijzen. “Denk jaren 60” – “Gooi je oude schoenen niet weg, zelfs als je nieuwe hebt”
- In de zorg: extra personeel inzetten om uitval van personenalarmering op te vangen.

Soms zijn technische maatregelen nuttig:

- Satelliet-telefoon: onafhankelijk van alle aardse infrastructuren
- Telefoon met tweede SIM-kaart, en neem dan een Belgische of Duitse provider
- Noodcommunicatievoorziening (NCV, het oude “Noodnet”): is die wel op noodstroom aangesloten?

5 – Blijf fit

5. Blijf fit

Herhaal, oefen,

- Incidentenmonitor
- Tips bij Service L
- Serious Game
- Jaarsymposium

Dan de laatste stap.
Innovatie is telecommunicatie gaat echt razendsnel. Dat is bijna een dooddoener, maar vergis je daar niet in. Met 5G kan er vreselijk veel veranderen.
Maar ook organisaties veranderen.

- bedrijfsovernames?
- reorganisaties?

Wat je wil is dat je organisatie bij al deze veranderingen al rekening houdt met afhankelijkheid telecommunicatie.

Daarnaast moet je bij grote veranderingen je risicobeoordeling herhalen en mogelijk nieuwe maatregelen nemen. Stap 2-3-4 moet een cyclus worden.

Service Level Agreements

5. Blijf fit

Een afspraak tusse
over de kwaliteit a

Valkuilen

- Commercieel, niet technisch
- Onderhandelbaa
- Eenduidig?
- Uitzonderingen?
- Voldoende stimu

99,5%

er maand

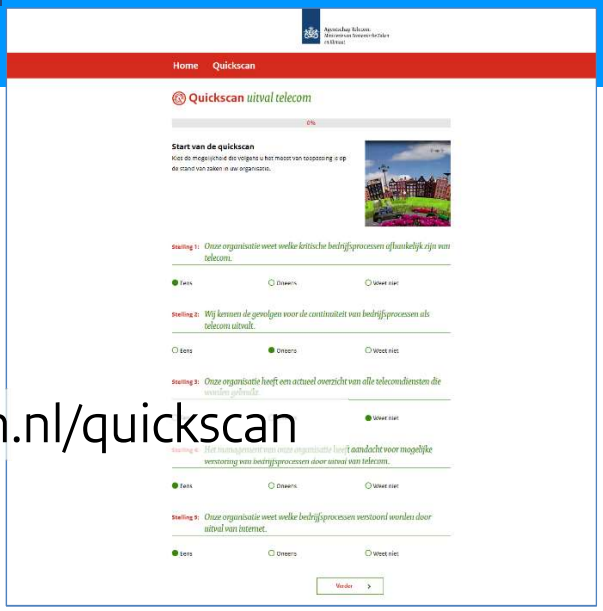
OpStap naar Weerbaarheid 2019 "Vijfstappenplan cyberweerbare telecommunicatie" 37

Tips uit SLA-document:

- Weet goed wat je eisen en wensen zijn
- Zorg dat je de procedure kent, en dat je weet welke oplostijd je hebt afgesproken.
- Weet wat de restricties zijn.
- Staar je niet blind: zelf een SLA kan uitval nooit *voorkomen*

Quickscan Uitval Telecom

https://agentschaptelecom.nl/quickscan



Eén belangrijk hulpmiddel heb ik nog niet genoemd: de quickscan.
Je hoeft niet altijd bij het begin te beginnen.

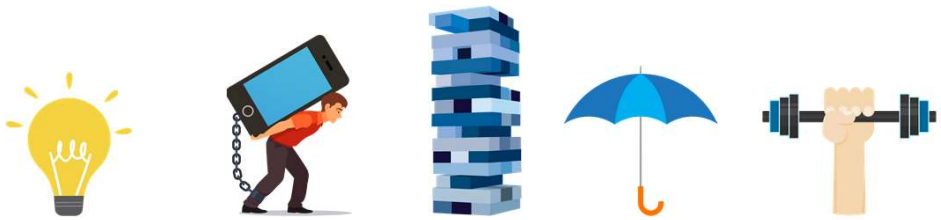
Met de quickscan krijg je snel een inzicht in waar je als organisatie staat, én je krijgt een advies op maat.

De quickscan is volledig anoniem: we vragen geen email-adres, we hoeven niet te weten wie je bent of waar je werkt.

Vul hem eens in. Met een 15-tal stellingen krijgt u misschien een verrassend beeld, en tips waar u wat aan heeft.

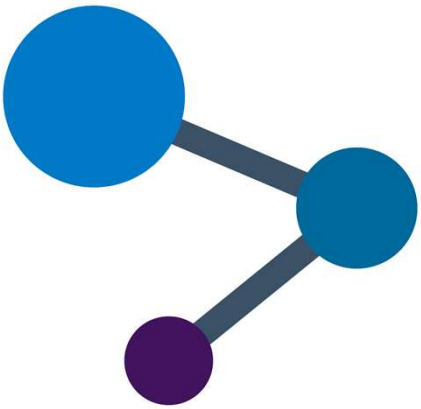
Vijfstappenplan

https://agentschaptelecom.nl/telekwetsbaarheid



1. Bewustwording **2.** Afhankelijkheden **3.** Risico's **4.** Maatregelen **5.** Blijf fit

Dat is in vogelvlucht het vijfstappenplan. Meer informatie vindt u hier.



agentschaptelecom.nl/telekwetsbaarheid

Eelco Vriezekolk

eelco.vriezekolk@agentschaptelecom.nl

https://linkedin.com/in/eelcovriezekolk