PLATFORM NEDERLAND


# Cybersecurity: waar begin je?

*En wat valt er verder nog te doen?*

**CEG Information Security**

18 oktober 2018

# INHOUDSOPGAVE

# 1 CYBERSECURITY: WAAR BEGIN JE? EN WAT VALT ER VERDER NOG TE DOEN?

Binnen het CIO Platform Nederland worden het gehele jaar door verschillende kennissessies voor en door de Information Security Officers van onze lid-organisaties georganiseerd, waarbij we herhaaldelijk elkaars best practices bespreken. Zo is er naar aanleiding van het rapport van Herna Verhagen[1] veel gediscussieerd over de '10% maatstaf'; hoe bepaal je wat je in ieder geval aan (cyber) security moet doen en wat het mag kosten? Daarnaast heeft ook het van kracht worden van de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018 de nodige activiteit opgeleverd.

Het CIO Platform Nederland heeft gemeend er goed aan te doen om onze learnings rondom veiligheidsmaatregelen samen te vatten en te delen. Dit ter inspiratie voor organisaties die wellicht minder capaciteit hebben om over veiligheid na te denken, maar hier wel mee aan de slag willen. Ook het Cybersecurity Framework van het Amerikaanse National Institute of Standards and Technology (NIST Framework)[2] kan een handig instrument zijn om in 5 stappen weerbaarder te worden. Deze stappen zijn als volgt: Identificeer, Bescherm, Detecteer, Reageer[3] en Herstel. Hieronder lees je de geadviseerde maatregelen, die we voor de overzichtelijkheid waar mogelijk in de context van het NIST Framework plaatsen.

### Definitie Cybersecurity:

**“Cybersecurity is het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in de ICT opgeslagen informatie of schade aan de integriteit van die informatie.”**

[1] H. Verhagen, Nederland digitaal droge voeten: De economische en maatschappelijke noodzaak van meer cyber security’ Den Haag, oktober 2016. Zie : https://www.cybersecurityraad.nl/binaries/Rapport_Verhagen_NED_DEF_tcm107-314468.pdf

[2] National Institute of Standards and Technology, ‘ Cyber Security Framework’, Gaithersburg, April 2018. Zie: https://www.nist.gov/cyberframework/framework

[3] In de Engelse versie wordt ‘Respond’ gebruikt, wat we hier vertalen als ‘Reageer’. Daarnaast wordt in deze tekst het woord ‘respons’ gebruikt als synoniem voor ‘reactie’, omdat dat nauwer aansluit bij het gebruik in de praktijk.

## 1.1 Waar begin je?

Het veilig houden van een organisatie, haar data en systemen, is een continu proces. Het begint - zoals het NIST Framework al aangeeft - bij het **identificeren** van de systemen, data en andere waardevolle assets die de organisatie nodig heeft voor het behalen van haar doelstellingen. Vervolgens worden de mogelijke risico's voor de beschikbaarheid, integriteit en vertrouwelijkheid van die assets bepaald. In de risk impact assessment plaatst de organisatie de **geïdentificeerde** risico's in een context; hoe erg is het als een bepaald risico zich voordoet? Door het definiëren van de waarschijnlijkheid en de impact van elk **geïdentificeerd** risico, kunnen maatregelen worden bedacht en voorgesteld om dit risico te beheersen.

Dit maakt een rationele afweging mogelijk tussen risico, impact en kosten van de maatregelen. Deze afweging is altijd de verantwoordelijkheid van de eigenaar van het systeem waarvoor het risico geldt. Als dan een plan is gemaakt, moet je het ten uitvoer brengen, checken op de juiste implementatie en effect en vervolgens waar nodig aanpassen (PLAN-DO-CHECK-ACT cyclus).

## 1.2 Hoe houd je data veilig?

Oftewel het '**bescherm**' onderdeel van het NIST Framework. Hieronder volgen enkele praktische invullingen van de **beschermings**maatregelen die kunnen, en soms moeten, worden getroffen.

### 1.2.1 Access management

Access management heeft een belangrijke rol in het veilig houden van data en informatiesystemen en wordt daarom ook in de AVG benoemd. Access management begint met het bepalen van wie toegang nodig heeft tot welke data en systemen, om vervolgens toegangscontroles in te stellen zodat alleen de mensen die daartoe de rechten hebben, bij die systemen en data kunnen komen. Dat beperkt de kans op activiteiten, per ongeluk of opzettelijk, met vergaande vervelende gevolgen voor de organisatie. Een up-to-date HR-proces, met duidelijke in-, door- en uitstroom van de medewerkers, is cruciaal om de rechten up-to-date te houden bij de juiste medewerkersgroepen (role-based). Dit zorgt ervoor dat mensen snel met hun rechten aan de slag kunnen en voorkomt dat mensen die een nieuwe rol krijgen met andere rechten, of die uit dienst gaan, nog met hun vroegere rechten toegang kunnen krijgen tot data en systemen. Als dit wordt gecombineerd met een wachtwoordbeleid, dat sterke wachtwoorden afdwingt, en logging van toegang, is access management een eind op orde. In combinatie met virusscanners, intrusion detection en data leakage prevention, houd je je data en systemen optimaal beveiligd.

### 1.2.2 Systeem management

Naast het onder controle hebben van toegang tot data en systemen, is het van belang om zicht te houden op de ontwikkeling van het systeem zelf en een proces in te richten om met security incidenten om te gaan. Voor het eerste, de ontwikkeling van het systeem, is het zinvol om een Configuration Management Database (CMDB) in te richten. Daarin wordt bijgehouden hoe het systeem is ingericht en welke instellingen nodig zijn om het naar behoren te laten functioneren. Wijzigingen in het systeem en ervaring met incidenten die zich voordoen vormen input voor de risico inschatting en kunnen leiden tot aanpassen van de te nemen maatregelen.

### 1.2.3 Encryptie van data

Omdat het nooit helemaal valt uit te sluiten dat een onbevoegde derde toch toegang weet te krijgen tot een systeem, of data kan onderscheppen tijdens het transport tussen systemen, is het noodzakelijk om

dataopslag en datastromen te voorzien van encryptie. Voor persoonsgegevens wordt dit ook vereist in de AVG. Encryptie van de data maakt deze data waardeloos voor de derde die er beschikking over krijgt. Encryptie maakt het verlies van gegevens minder problematisch voor het eigen verdienvermogen, omdat een concurrent er niets mee kan, én het kan betekenen dat een datalek niet hoeft te worden gemeld bij de toezichthouder.

### 1.2.4 Monitoring is van belang

Naast alle preventieve en beschermende maatregelen die je treft, zul je ook ervoor zorgen dat je goed in de gaten houdt wat er gebeurt met je data en systemen. Zo kun je nagaan of er op de juiste wijze door geautoriseerde personen en systemen gebruik van wordt gemaakt. Volgens het NIST Framework hebben we het dan over '**detecteren**'. Dat maakt het gemakkelijker om snel en doeltreffend te reageren wanneer iets mis gaat, in de '**reageer**' en '**herstel**' fases van het NIST Framework.

### 1.2.5 Incident respons proces

Voor het geval zich een incident voordoet, dient er te worden **gereageerd**. Er dient een incident **respons** proces te zijn ingeregeld, met duidelijke taken, procedures en escalatielijnen. De verantwoordelijkheid van de uitvoering van deze activiteiten ligt meer en meer bij een Security Operation Centre (SOC). Diverse leden van ons hebben een SOC ingericht, waar de analyses worden uitgevoerd om een dreigingsbeeld te verkrijgen met bijbehorende mitigerende maatregelen. Mocht er geen (financiële) ruimte zijn voor een interne SOC, denk dan ten minste aan een Cyber Security Incident Response Team (CSIRT). Dit team fungeert als de BHV-ers in je organisatie bij calamiteiten op het gebied van informatiebeveiliging.

## 1.3 Herstel na uitval

Mocht er toch uitval zijn van systemen, of verlies van data, dan is het van belang om de operationele processen weer zo snel mogelijk op gang te krijgen. Een vlekkeloos back-up en restore proces, waarmee reservekopieën kunnen worden teruggezet, is onontbeerlijk. Bereid dit proces niet alleen op papier voor, maar test het ook regelmatig in de praktijk. Denk ook na over (interne en externe) meldingen en communicatie rondom dergelijke incidenten, wie moeten op de hoogte worden gesteld?

> **Meest genoemde maatregelen per NIST categorie:**
> 1. **Identificeer: Externe scan laten uitvoeren**
> 2. **Bescherm: Patch management plannen**
> 3. **Detecteer: CSIRT / SOC organisatie optuigen**
> 4. **Respons: Security Incident Management proces inrichten**
> 5. **Herstel: Backup & Restore in orde maken**

## 1.4 Veiligheid in ketens

Externe communicatie is relevant vanuit het perspectief dat organisaties vrijwel altijd relaties hebben met andere organisaties (derden). Daarbij kun je denken aan leveranciers en klanten in de keten, maar ook aan eventuele toezichthouders. Voor cybersecurity ben je bijna altijd afhankelijk van partijen buiten jouw eigen organisatie. Daar moet je dus ook rekening mee houden in je veiligheidsbeleid. Security regel je niet alleen! Dat geldt zeker in de steeds complexere ketens waarin we werken.

Een zeer actuele maatregel in dit verband zijn de verwerkersovereenkomsten. Deze zijn verplicht als anderen beschikking krijgen over persoonlijke data waarvoor jouw organisatie verantwoordelijk is onder de AVG. In dit document staan afspraken met deze partners over de wijze waarop er met persoonsgegevens wordt omgegaan. Ook is vermeld hoe er gehandeld wordt op het moment dat een incident plaatsvindt waarbij persoonsgegevens (mogelijk) verloren zijn gegaan of beschikbaar zijn gekomen voor derden. Elke organisatie zal een (flink) aantal verwerkersovereenkomsten moeten sluiten. Daartoe zal men met deze partijen, maar ook met de betrokken afdelingen binnen de eigen organisatie, het gesprek moeten aangaan over cybersecurity en hetgeen is afgesproken daadwerkelijk vastleggen. Dit creëert naast duidelijkheid over wat contractpartijen van elkaar mogen verwachten, ook de nodige awareness voor het veilig werken met de data van of over anderen.

Sowieso is het waardevol om veiligheidsaspecten onderdeel te laten zijn van inkoop- en contractonderhandelingen en deze in de overeenkomst als een zogenaamde “Security Annex” op te nemen. Denk daarbij bijvoorbeeld aan hoe wordt omgegaan met risico evaluaties, te nemen maatregelen, op te leveren rapportages en bewijs van compliancy van de partners en andere derde partijen.

## 1.5 Up-to-date houden van software en systemen

En als dan de assessments zijn uitgevoerd, de overeenkomsten getekend, de maatregelen geïmplementeerd, de specialisten in een SOC alert zijn op incidenten en het oplossen daarvan, dan nog komt er meer bij kijken om secure te blijven….

De snelle ontwikkelingen in soft- en hardware zorgen ervoor dat het noodzakelijk is deze bij te houden. De eigen systemen moeten doorlopend worden gecheckt. Zowel tegen nieuw aan het licht gekomen kwetsbaarheden, als na iedere wijziging in de eigen infrastructuur en systemen. Oplossingen voor gevonden kwetsbaarheden (patches) moeten snel worden doorgevoerd, voordat en zonder dat ze de operatie verstoren. Virusscanners moeten doorlopend worden bijgewerkt en instellingen van soft- en hardware met regelmaat worden aangepast.

Ook is het laten uitvoeren van een externe scan of penetratietest (bijvoorbeeld door een formele audit instantie) aan te bevelen. Daarbij kan worden gekeken of de systemen van binnen- en/of van buitenaf kwetsbaar zijn, of kan over de impact van veranderende wet- en regelgeving worden geadviseerd. Een dergelijke test levert meestal concrete voorstellen op voor het aanpakken van kwetsbaarheden en daarmee veiliger maken van het systeem.

## 1.6 Iedereen heeft een rol en verantwoordelijkheid

Veiligheid blijft altijd een aandachtspunt, je bent nooit ‘klaar’. Want de omgeving verandert voortdurend, de systemen ook en daarmee ook de kwetsbaarheid van de organisatie. En het gaat niet alleen over ICT, tools en systemen en het zijn ook niet alleen de (Chief) Information Security Officers en de Chief Information Officers die hiervoor verantwoordelijk zijn: *Iédereen binnen de organisatie en daarbuiten (in de keten) heeft een rol*. Communicatie daarover in allerlei - op de doelgroepen toegespitste manieren - is noodzakelijk. En doe dat niet alleen incidenteel, maar zorg voor gedoseerde activiteiten gedurende het jaar. Bijvoorbeeld via awareness campagnes en opleidingen voor al het personeel, Dashboard Security Controls voor de Raad van Bestuur, ludieke acties, serious games, oefeningen of een Security talk. Wat je ook doet, zorg dat veiligheid en ieders rol daarbij aandacht blijft krijgen.

## Tot slot

Vanuit de theorie en verschillende inventarisatierondes om input te krijgen voor dit stuk, zijn er 100+ maatregelen te noemen die ingezet kunnen worden om bedrijven meer veiligheid te bieden met behulp van ICT. We willen dus zeker niet compleet zijn in dit verhaal. Wil je eens sparren over de maatregelen binnen jouw organisatie, neem gerust contact met ons op, zodat we je wellicht kunnen introduceren bij één van de CISO's in het netwerk van het CIO Platform Nederland.

### Het CIO Platform Nederland in het kort:

**CIO Platform Nederland is dé vereniging van grote gebruikers van digitale technologie in Nederland. We zijn er voor de CIO/CDO, zijn/haar 'peers' én medewerkers. Wij bieden een makkelijk toegankelijk netwerk, waar de CIO/CDO terecht kan om ambities, uitdagingen, vragen en zorgen te delen. Wij faciliteren actieve samenwerking en het delen van praktische kennis op elk niveau in de organisatie. Dit alles op een vertrouwelijk en integer platform.**

**Kijk voor meer informatie op www.cio-platform.nl.**

## Over deze uitgave



Tekst & redactie
*CEG Information Security, CIO platform Nederland*

Foto Cover
*iStock*

• info@cio-platform.nl
• www.cio-platform.nl