De Verenigde Staten nemen strenge maatregelen voor alle defensie aanbestedingen

Certificering van het maturity level van cybersecurity binnen de defensie-industrie

Vanuit de Verenigde Staten (VS) komt een nieuwe maatstaf over ons heen welke een verplichte certificering eist van de cybersecurity van ondernemingen die leveren aan Amerikaanse defensieprojecten of mee willen doen aan aanbestedingen van de Amerikaanse Department of Defence (DoD). Het betreft de *Cybersecurity Maturity Model Certification* (CMMC). Dit is bedoeld om bescherming van 'Controlled Unclassified Information' en 'Covered Defense Information' te verbeteren. Beoogd is dat deze regels op 20 juni 2020 in werking treden. Is dit van belang voor Nederland? Jazeker, want in Nederland zijn zo'n 350 ondernemingen actief in de defensie-industrie en het betreft jaarlijks zo'n € 5 miljard. De hoogste tijd om hierbij stil te staan.

De defensie & veiligheid industrie kenmerkt zich als een hoogtechnologische sector met brede internationale en civiele verwevenheid. De sector heeft een jaarlijkse omzet van € 5 miljard, waarvan 70% uit export. De DVI is goed voor 110.000 arbeidsplaatsen. 38% van de omzet in de sector zit in onderzoek en ontwikkeling van nieuwe technologieën. www.nidv.eu/de-defensie-en-veiligheidsindustrie-ten-tijde-van-covid-19/

Wat betekent CMMC voor ondernemingen?

Om mee te kunnen bieden op contracten die door de DoD worden uitgezet, zullen ondernemingen binnen de VS en daarbuiten aan de CMMC-vereisten moeten voldoen.
CMMC is een uniforme certificering voor de implementatie van cyberbeveiliging in de gehele defensie-industrie, die meer dan 300.000 ondernemingen in de toeleveringsketen omvat. In Nederland zijn dit zo'n 350 ondernemingen. CMMC is het antwoord van de DoD op belangrijke beveiligingsmaatregelen op het gebied van gevoelige defensie-informatie op informatiesystemen van contractanten.

Eerder waren contractanten reeds verantwoordelijk voor het implementeren, bewaken en certificeren van de beveiliging van hun informatietechnologiesystemen en alle gevoelige DoD-informatie die is opgeslagen op of verzonden werd door die systemen. Contractanten blijven verantwoordelijk voor de implementatie van kritieke cyberbeveiligingsvereisten, maar CMMC verandert dit paradigma door beoordelingen en certificering door derden te eisen van de naleving door contractanten van bepaalde verplichte handelswijze, procedures en processen en deze ook steeds weer aan te passen aan de steeds vernieuwende cyberdreigingen van tegenstanders. Denk bijvoorbeeld aan de cyberaanvallen vanuit verschillende statelijke actoren'.

Het CMMC-raamwerk

Het CMMC-raamwerk stelt vijf certificeringsniveaus vast die de volwassenheid en betrouwbaarheid van de cyberbeveiligingsinfrastructuur van een ondernemingen weergeven met betrekking tot de bescherming van gevoelige overheidsinformatie die zich bevindt in de informatiesystemen van ondernemingen. Ieder niveau bouwt voort op het vorige niveau en per niveau worden de technische vereisten verder aangescherpt. Elk niveau vereist naleving van de vereisten op lager niveau en institutionalisering van aanvullende onderdelen om specifieke op cyberbeveiliging gebaseerde processen te implementeren.

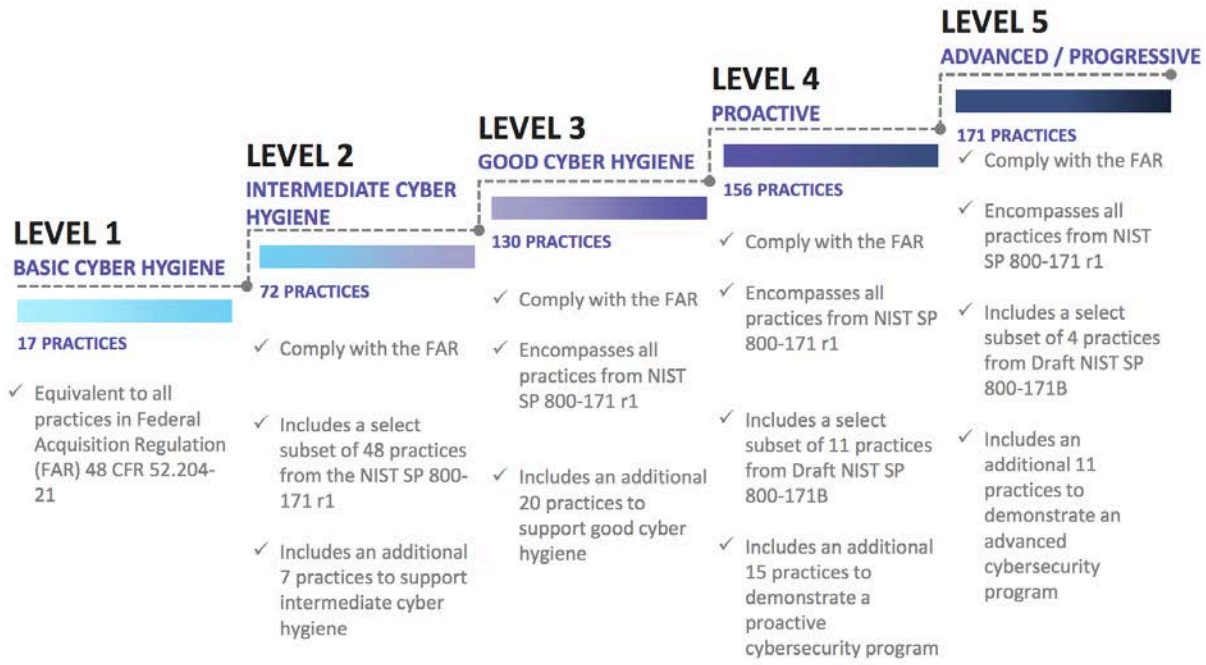
Niveau 1: een onderneming moet "elementaire cyberhygiëne" uitvoeren, zoals het gebruik van antivirussoftware of ervoor zorgen dat werknemers wachtwoorden regelmatig wijzigen om Federal Contract Information (FCI) te beschermen. FCI is "informatie, niet bedoeld voor openbaarmaking, die wordt verstrekt door of gegenereerd voor de overheid op grond van een contract om een product of dienst aan de overheid te ontwikkelen of te leveren." Het bevat geen openbare informatie of bepaalde transactionele informatie.

Niveau 2: een onderneming moet bepaalde "intermediaire cyberhygiënische" documenteren ter bescherming van Gecontroleerde Niet-Geclassificeerde Informatie (CUI) door implementatie van een deel van de Speciale Publicatie 800-171 van het Amerikaanse Department of Commerce National Institute of Standards and Technology (NIST) Revisie 2 (NIST 800-171 r2) beveiligingsvereisten. NB! CUI betreft alle informatie uit wet-, regelgeving of overheid breed beleid, maar omvat niet bepaalde gerubriceerde informatie.

Niveau 3: een onderneming moet een geïnstitutionaliseerd beheersplan hebben om "goede cyberhygiëne" - praktijken te implementeren om CUI te beschermen, inclusief alle NIST 800-171 r2-beveiligingsvereisten en aanvullende normen.

Niveau 4: Een onderneming moet processen geïmplementeerd hebben voor het beoordelen en meten van de effectiviteit van processen, evenals gevestigde aanvullende verbeterde processen voor het detecteren van en reageren op veranderende tactieken en technieken van geavanceerde persistente bedreigingen (APT's). Een APT wordt gedefinieerd als een tegenstander (cybercriminelen, landen op zwarte lijsten etc.) met een hoog niveau van expertise en aanzienlijke middelen die hem in staat stellen kansen te creëren om hun doelstellingen te bereiken door gebruik te maken van meerdere aanvalsmethoden.

Niveau 5: een onderneming moet over de hele organisatie beschikken over gestandaardiseerde en geoptimaliseerde processen en aanvullende verbeterde werkwijzen die meer geavanceerde mogelijkheden bieden om APT's te detecteren en erop te reageren.



Bron: https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

Wie moeten er compliant zijn met CMMC?

Alle DoD-contractanten, behoudens een zeer beperkte uitzonderingsgroep, zullen uiteindelijk een CMMC-certificering moeten behalen. Dit omvat alle leveranciers op alle niveaus in de toeleveringsketen, kleine ondernemingen, contractanten van handelsartikelen en buitenlandse leveranciers. De CMMC-Accreditation Body (CMMC-AB) zal rechtstreeks met DoD samenwerken om procedures te ontwikkelen voor de certificering van onafhankelijke externe beoordelingsorganisaties en beoordelaars die de CMMC-niveaus van ondernemingen zullen evalueren.

Vanaf wanneer worden ondernemingen verwacht CMMC-compliant te zijn?

Het DoD geeft aan dat het al op 20 juni 2020 zal beginnen met het opnemen van minimale certificeringsvereisten in informatieverzoeken (RFI's) en in geselecteerde verzoeken om voorstellen (RFP's) in september 2020. DoD heeft ook aangegeven dat een certificeringsvereiste op primair niveau niet

noodzakelijkerwijs hetzelfde certificatieniveau zal zijn dat vereist is gedurende de gehele supply chain voor een bepaald contract. Verschillende certificeringsniveaus op een enkel contract hebben het potentieel om complexe implementatie-uitdagingen op te werpen voor zowel hoofd- als ondercontractanten.

Waarom zouden ondernemingen volgens DOD aan continuous monitoring moeten doen?

De DoD onderzoekt manieren om de cyberveiligheid van de Defense Supply Chain ("DSC") te verbeteren, inclusief de intermezzo's tussen de normaal verwachte CMMC-certificeringscadans (van de levels 1-5) voor ondernemingen in de DSC. De DoD zou ondernemingen op het hart willen drukken dat ze vigilant blijven en hun cybersecurity constant blijven monitoren. Tijdens die onderbrekingen kunnen er veel veranderingen optreden in de computersystemen van een organisatie, en dit is een mogelijke manier waarop de CMMC-AB kan helpen de beveiligingshouding van de DSC te verbeteren en te behouden en de waardevolle informatie van de DoD beter te beschermen.

Handhaving van de certificeringsvereisten

Hoewel het coronavirus en de impact ervan de laatste tijd hoog in het vaandel stonden bij overheidscontractanten en, inderdaad, de hele wereld, is het ministerie van Defensie (DoD) onverminderd doorgegaan met de geplande implementatie van de CMMC-programma. Hieronder belichten we enkele recente ontwikkelingen, bekijken we aankomende activiteiten met betrekking tot CMMC en geven we enkele aanbevelingen over wat contractanten nu kunnen doen om zich voor te bereiden.
DoD heeft het CMMC-model uitgegeven en bijgewerkt.

Op 4 mei 2020 berichtte de DoD dat de CMMC-AB in plaats is. In januari 2020 werd de CMMC-AB geregistreerd als een Maryland 501 (c) (3) non-profitorganisatie. Het heeft een Raad van Bestuur bestaande uit toonaangevende experts De website is www.CMMCAB.org. De DoD heeft de CMMC-AB belast met het uitvoeren van de operationele aspecten van CMMC, inclusief de selectie en opleiding van personen die CMMC-evaluaties zullen uitvoeren. De relatie tussen DoD en CMMC-AB is vastgelegd in een Memorandum of Understanding dat niet openbaar is gemaakt.

Tot op heden zijn er **geen** gecertificeerde externe beoordelingsorganisaties (CMMC Third Party Assessment Organizations, C3PAO's) geselecteerd of geïdentificeerd. De CMMC-AB heeft echter aangegeven de komende maanden te zullen beginnen met het opleiden van assessoren, waarschijnlijk door een combinatie van online en persoonlijke activiteiten. Assessoren ontvangen een licentie van de CMMC-AB na het voltooien van de vereiste training en het behalen van een examen. De DoD waarschuwt ondernemingen dat er momenteel personen actief zijn die stellen dat zij bevoegd zijn te certificeren, echter die informatie is onjuist.

Sylvie Bleker-van Eyk

Hoogleraar Compliance & Integriteit Management aan de VU (vu.nl/cim)

Senior Director PwC Cyber Forensic & Privacy

sylvie.bleker@pwc.com