

Classificatie:
Departementaal Vertrouwelijk

RIVM
Risicoanalyse

Bestelproces COVID-19 vaccins

Auteur: 5.1.2e
Datum: 12 December 2021
Versie: 0.1



Revisieoverzicht

Datum	Versie	Auteur	Bijzonderheden
12-02-2021	0.1	5.1.2e	Opzet voor RA sessie 12 februari 2021; input quickscan BIO bestelproces, systeemdecompositie en lijst met IB maatregelen.



Inhoud

1. Managementsamenvatting
2. Aanpak
3. Risicos
4. Maatregelen

Het bestelproces voor COVID-19 vaccins

- Voor het bestellen en distribueren van de COVID-vaccins zijn drie ketens uitgewerkt. Voor alle ketens geldt dat het om gegevens gaat over hoeveelheid vaccins en toebehoren (optrek/toedieningsnaalden en -spuiten en oplosmiddelen) en NAW-gegevens van de klant (GGD, huisarts, zorginstellingen waar de vaccins bezorgd zullen worden). Er worden geen gegevens van te vaccineren personen gebruikt.

Bestelsystemen:

- De SNPG-webapp wordt gebruikt voor bestellen vaccins, bestellen informatiemateriaal en declareren en melden van vaccinaties. De SNPG-webapp wordt gebruikt door huisartsen, Arboartsen en zorginstellingen. SNPG staat voor: Stichting Nationaal Programma Griepppreventie.

- Formdesk wordt enerzijds als rekentool gebruikt waarmee DVP-medewerkers bij het bestelde aantal vaccins het correcte naalden, spuiten en oplosmiddel e.d. kunnen berekenen voordat ze het in Excel inlezen. In de toekomst kan mogelijk Formdesk als bestelformulier worden gebruikt door externe klanten die nog niet de SNPG Webapp kunnen gebruiken.

- De nog in ontwikkeling zijnde SAP portal biedt de mogelijkheid om vaccinbestellingen rechtstreeks via SAP te verwerken. Enerzijds mogelijk via RIVMtoegang en/of een alternatieve oplossing voor authenticatie.

SAP DVP

- De bestelgegevens vanuit de SNPG-webapp of uit Formdesk worden in SAP-DVP ingelezen. Hieruit worden vervolgens salesorders voor de logistiek dienstverlener Movianto gemaakt die de vaccins naar de klanten brengt.

SAP Movianto

- SAP-Movianto krijgt via beveiligde zorgmail een met password beveiligd Excelbestand van DVP waarna zij de gegevens in hun eigen SAP-systeem invoeren. Met deze gegevens kunnen Movianto-chauffeurs de bestelde vaccins en toebehoren bij de klanten afleveren.

Het RIVM is verantwoordelijk voor het gehele proces/de verwerking binnen de gehele keten.

Scope van het bestelproces voor COVID-19 vaccins

		Bestellen van Covid19-vaccins en toebehoren	***Distribueren van Covid19-vaccins en toebehoren***
		Functionaliteit voor huisartsen, zorginstellingen, ziekenhuizen, arbodiensten en GGD'en om Covid19-vaccins en toebehoren (naalden, spuiten, oplosmiddel) te bestellen.	*Functionaliteit waarmee de vaste logistieke dienstverlener Movianto de bestelde goederen naar de regiokantoren van DVP of naar externe klanten kan distribueren.*
A	***SNPG Webapp***	*Huisartsen en een groot deel van de zorginstellingen plaatsen hun bestellingen via SNPG Webapp. Voor dit proces is een aparte quick scan uitgevoerd.* ***SNPG zal daarom verder buiten beschouwing gelaten worden in de voorliggende analyse.***	
	Formdesk	*Voor GGD'en vult DVP zelf de bestellingen op een Formdeskformulier in.* *Klanten die niet in SNPG zijn opgenomen, kunnen via Formdesk hun bestellingen plaatsen, waarna de gegevens weer in SAP worden ingelezen.* *Op termijn kunnen andere klanten hun bestelling direct in SAP-RIVM-DVP plaatsen.*	
	SAP-RIVM-DVP: - ***SAP/SD voor klantorder*** - ***SAP/MM voor voorraadbeheer***	*Bestelgegevens van klanten die opgenomen zijn in SNPG worden automatisch uit de SNPG Webapp in SAP gelezen.* *Bestelgegevens via Formdesk worden via import/export ingelezen in SAP-RIVM-DVP.*	
	SAP-Movianto		*Movianto krijgt de bestelgegevens in een beveiligde Zipfile via mail.* *De bestelling wordt uitgeleverd door Movianto.*

Deelprocessen binnen het bestelproces voor COVID-19 vaccins

B1	*Bestellen van Covid19-vaccins en toebehoren*	
	De klant van het proces	- *Huisartsen, zorginstellingen, ziekenhuizen, arbodiensten, GGD'en*
	De output van het proces	- *Een in SAP-RIVM-DVP geplaatste bestelling van het Covid19-vaccin en/of toebehoren met bepaalde omvang voor een specifieke klant.*
	Koppelvlakken met andere processen	- *Voor huisartsen en deel zorginstellingen komt informatie uit SNPG Webapp* - *Resterende zorginstellingen of andere klanten niet in SNPG vullen Formdeskformulier in* - *Voor GGD'en vult DVP zelf een Formdeskformulier in* - *Op termijn kunnen andere klanten hun bestelling direct in SAP-RIVM-DVP plaatsen* - *Zet levering van vaccins en toebehoren door RIVM-DVP in gang via Movianto (SAP-Movianto)*
	Gebruikte systemen	- *SNPG Webapp* - *Formdesk* - *SAP-RIVM-DVP*

B2	*Distribueren van Covid19-vaccins en toebehoren*	
	De klant van het proces	- *Huisartsen, zorginstellingen, ziekenhuizen, arbodiensten, GGD'en*
	De output van het proces	- *Levering van bestelling bij specifieke klanten.*
	Koppelvlakken met andere processen	- *SAP-RIVM-DVP* - *SAP Movianto.*
	Gebruikte systemen	- *SAP-RIVM-DVP* - *SAP-Movianto* - *Zet levering van vaccins en toebehoren door Movianto in gang.*

Systemen binnen het bestelproces voor COVID-19 vaccins

C1	*Formdesk*
Eigenaar informatiesysteem	*CIO-Office/FCC: proceseigenaar* 5.1.2e
De gebruikers van het informatiesysteem	*Medewerkers logistiek bij DVP, later mogelijk ook externe klanten*
De output van het informatiesysteem	*Datafile om in te lezen in SAP-RIVM-DVP*
Koppelvlakken met andere informatiesystemen	- *SAP-RIVM-DVP* - *Geen koppelvlak met CIMS*
Andere processen	*N.v.t.*
Kritische momenten	*Moet laatste week 2020 al beschikbaar zijn*
Soort informatie	*privacygevoelige informatie, commercieel vertrouwelijke informatie*
Data rubricering[1]	*RIVM Vertrouwelijk*
Externe eisen	*AVG, Baseline Informatiebeveiliging Overheid (BIO)*

C2	*SAP-RIVM-DVP*
Eigenaar informatiesysteem	*CIO-Office/FCC: proceseigenaar* 5.1.2e
De gebruikers van het informatiesysteem	*Medewerkers logistiek bij DVP*
De output van het informatiesysteem	*Bestelorder, afleverbon*
Koppelvlakken met andere informatiesystemen	- *SNPG Webapp* - *Formdesk* - *SAP-Movianto (handmatig)* - *Geen koppelvlak met CIMS*
Andere processen	*N.v.t.*
Kritische momenten	*Snelle start per begin 2021.*
Soort informatie	*privacygevoelige informatie, commercieel vertrouwelijke informatie*
Data rubricering[2]	*RIVM Vertrouwelijk*
Externe eisen	*AVG, Baseline Informatiebeveiliging Overheid (BIO)*

C3	*SAP-Movianto*
Eigenaar informatiesysteem	*Movianto*
De gebruikers van het informatiesysteem	*Werknemers Movianto*
De output van het informatiesysteem	*Bestelorder, afleverbon*
Koppelvlakken met andere informatiesystemen	*N.v.t., krijgen gegevens via mail in beveiligde Zipfile*
Andere processen	*N.v.t.*
Kritische momenten	
Soort informatie	*privacygevoelige informatie*
Data rubricering[3]	*RIVM Vertrouwelijk*
Externe eisen	*AVG, Baseline Informatiebeveiliging Overheid (BIO)*

Aanvankelijk zat de SNPG webapp nog niet binnen scope. Dit omdat het onder een ander centrum valt; het Centrum voor Bevolkingsonderzoek (CvB)

Impact bestelproces COVID-19 vaccins

I	Samenvatting											
	STAP 1		STAP 2			STAP 3						
	(X)	Rubricering	(X)	Classificatie proces	(X)	Classificatie systeem	(X)	B	(X)	I	(X)	V
		Openbaar		Ondersteunend		Nuttig		Laag		Laag		Laag
		RIVM Intern (besloten)		Bijdragend		Belangrijk		Midden		Midden		Midden
	X*	RIVM Vertrouwelijk	X	Strategisch	X	Vitaal	X	Hoog	X	Hoog	X	Hoog
	X*	Departementaal Vertrouwelijk		Kritisch strategisch								
		Staatsgeheim Confidentieel										
		Staatsgeheim Geheim										
		Staatsgeheim Zeer Geheim										

BBN *1, 2, 3 of VIR-BI*	*BBN3*	*Voor de Covid19-vaccinvoorziening geldt: commercieel vertrouwelijke informatie, leveranciersinformatie, grootschalige opslag, beheer en vervoer. Voor statelijke actoren of criminelen is het interessante informatie welke bestellingen/voorraden er waar zijn. Daarom wordt BBN3 als passend beschouwd.*

*Update: voor de gehele keten is het uitgangspunt Departementaal Vertrouwelijk

Proces: Beide deelprocessen (zowel het bestellen als het distribueren van Covid19-vaccins en toebehoren) zijn als strategisch (S) geclassificeerd omdat zonder een goed ingericht proces van het bestellen en de distributie (inclusief voorraadbeheer) het Covid19-vaccinatieprogramma direct schade oploopt.

Systeem: De onderliggende systemen zijn als vitaal (V) geclassificeerd.

Het bestelformulier in Formdesk is nodig om foutloos juiste hoeveelheden toebehoren te berekenen a.d.h.v. de bestelde hoeveelheid vaccin. Tevens is het de back-up voor als niet alle zorginstellingen bestellen via de SNPG Webapp.

SAP DVP omvat de complete boekhouding rond bestellen, uitgifte en voorraadbeheer wordt door de desbetreffende modules in SAP ondersteund.

Zonder SAP Movianto kunnen de vaccins en toebehoren niet aan de klanten uitgeleverd worden.

Fasen in uitvoeren risicoanalyse (regulier)

Fase I	Fase II	Fase III	Fase IV	Fase V
CONTEXT	IMPACT	DREIGINGEN	WEERBAARHEID	RAPPORTAGE
Situatieschets van locaties, systemen, informatie & toegang	*Classificatie van proces, systeem en informatie (BIV) & BBN niveau*	*Inzicht in dreigingen & kwetsbaarheden, de consequenties en kans dat het zich voordoet*	*Inventarisatie huidige maatregelen & voorstel aanvullende maatregelen*	*Vastlegging van risico's, maatregelen & terugkoppeling*

Risicoanalyse – gevolgd proces

Fase I	Fase II	Fase III	Fase IV	Fase V
CONTEXT	IMPACT	DREIGINGEN	WEERBAARHEID	RAPPORTAGE
1. Systeemdecompositie *-SNPG webapp* *- Formdesk*	*1. Vaststellen classificatie van het bestelproces, en gerelateerde systemen en informatie:* *- Rubricering: DepV.* *- BIV: HHH* *- BBN: dreigings-niveau BBN3*	*1. Inroepen BBN3 dreigingsniveau*	*1. Totaal overzicht aan IB maatregelen* *- GAP analyse op basis van rubricering (DepV.) op gerelateerde systemen* *- Maatregelen uit (niet afgeronde) RA SNPG webapp* *- Bevindingen pentest SNPG webapp* *- Afgestemde maatregelen vanuit site visits Movianto* *- Eigen set aan maatregelen opgesteld voor BBN3*	*1. RACC:* *- 30-12-2020* *- 18 -02-2021* *- 28-01-2021 (tot 1 maart)*
2. Systeemdecompositie bestelproces (integraal): *- SNPG webapp* *- Formdesk* *- SAP DVP* *- SAP Movianto* *- en overige systemen*		*2. Uitvoeren risicoanalyse voor vaststellen onder-liggende risico's.*	*2. Herschikken IB maatregelen*	*2.Risicoacceptatie met risico's en openstaande maatregelen*

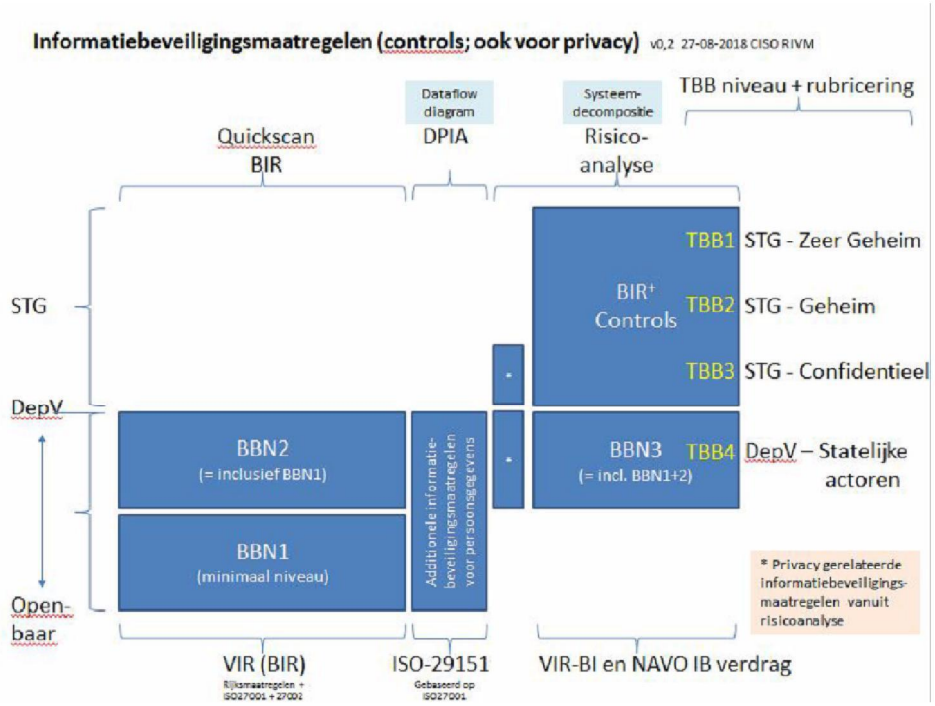
Overzicht IB maatregelen - initieel

1. Op basis van de rubricering Departementaal Vertrouwelijk (DepV) zijn GAP-analyses uitgevoerd voor de verschillende systemen.
   - SNPG webapp 26 maatregelen
   - Formdesk 5 maatregelen
   - SAP DVP 20 maatregelen
   - SAP Movianto 13 maatregelen
2. Maatregelen uit (niet afgeronde) risicoanalyse SNPG webapp
3. Bevindingen pentest SNPG webapp
4. Afgestemde maatregelen vanuit site visits Movianto
5. Eigen set aan maatregelen opgesteld voor BBN3

Aantal van ID		Status				
Systeem	Indicatie doorlooptijd	Gereed	In uitvoering	Te plannen	(leeg)	Eindtotaal
Bestelproces	Maanden		3	7		10
	Weken		2	15		17
Formdesk	Dagen	1				1
	Weken		4			4
SAP DVP	Maanden				1	1
	Weken	4	4		11	19
SAP Movianto	Dagen		3			3
	Maanden		3			3
	Weken		22			22
SNPG webapp	Dagen	9	8			17
	Geen actie	3				3
	Maanden		5	2	2	9
	Weken		9	2		11
Eindtotaal		17	63	26	14	120

Dreigingsniveau BBN3

De BIO (Baseline Informatiebeveiliging Overheid) stelt dat BBN3 van toepassing is op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheidslagen, waarbij weerstand tegen statelijke actoren of vergelijkbare dreigers nodig is.



Actoren

	Actorgroep	Toelichting	Motivatie	Possible consequencies
A.	Staten/staatsgelieerd	Staten voeren digitale aanvallen uit op andere landen, organisaties of individuen uit primair geopolitieke motieven. Zij hebben als doel de	Competitive advantage Economic espionage	• Advanced Persistent Threats (APT's) - Defence advantage - Political advantage - Economic exploitation
B.	Criminelen	Actor die aanvallen pleegt met economische of financiële motieven.	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	- Computer crime (e.g. cyber stalking) - Fraudulent act (e.g. replay, impersonation, interception) - Information bribery
C.	Terroristen	Actor met ideologische motieven die maatschappelijke veranderingen probeert te bewerkstelligen, bevolkingsgroepen angst wil aanjagen	Blackmail Destruction Exploitation Revenge	- Bomb/Terrorism - Information warfare - System attack (e.g. distributed denial of service) - System penetration
D.	Hacktivisten	Samentrekking van hacker en activist: actor die uit ideologische motieven digitale aanvallen van activistische aard pleegt. De gehanteerde betekenis van hacker is iemand die met kwaadaardige bedoelingen probeert in te breken in ict-systemen	Beproeving van fysieke, technische en elektronische weerstand Challenge Ego Rebellion Status Money	- Hacking op afstand - Social engineering - System intrusion, break-ins - Unauthorized system access
E.	Cybervandalen/scriptkiddies	Actor met beperkte kennis die hulpmiddelen gebruikt die door anderen zijn bedacht en ontwikkeld, voor digitale aanvallen, om kwetsbaarheden aan te tonen of voor de eigen uitdaging.		• Opzettelijk menselijk handelen
F.	Insiders	Een interne actor die met toegang tot systemen of netwerken van binnenuit een dreiging vormt, met als motief wraak, geldelijk gewin of ideologie. Een insider kan ook worden ingehuurd of opgedragen van buitenaf.	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g. data entry error, programming error)	- Onopzettelijk menselijk handelen - Assault on an employee - Blackmail - Browsing of proprietary information - Computer abuse - Fraud and theft - Information bribery - Input of falsified, corrupted data - Interception - Malicious code (e.g. virus, logic bomb, Trojan horse) - Sale of personal information - System bugs - System intrusion - System sabotage - Unauthorized system access
G.	Niet opzettelijk handelen	Interne actor		

Dreigingsbeeld Statelijke Actoren 1/2



AIVD: staten blijven Nederlandse systemen succesvol binnendringen

vroeg 29 april 2020, 15:18 door Redactie, 10 reacties
Laatst bijgewerkt: 29-04-2020, 17:11

Hoewel er de afgelopen jaren is geïnvesteerd in de digitale weerbaarheid van publieke instellingen blijven statelijke actoren, zoals Chinese, Iraanse en Russische, zeer succesvol in het binnendringen van Nederlandse (overheids)systemen, zo stelt de AIVD in het vandaag verschenen jaarverslag over 2019 (pdf).

Volgens de inlichtingendienst blijkt uit onderzoek dat meerdere Nederlandse topsectoren vorig jaar doelwit zijn geweest van digitale spionage. Daarbij wordt er vooral gewezen naar China, dat zich aan cyberspionage zou schuldig maken. "Een groot deel van de (digitale) spionageactiviteiten van China is gericht op het verbeteren van de eigen economische ontwikkeling", zo laat het jaarverslag weten.



Inlichtingendiensten willen hoger budget voor hackers en ict-systemen

donderdag 11 februari 2021, 09:59 door **Redactie**, **4 reacties**

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) willen een hoger budget voor het inhuren van hackers en aanschaffen van ict-systemen. Dat laten de diensten tegenover het **Financieele Dagblad** weten. Vorige week kwamen de AIVD, MIVD en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) met het **Dreigingsbeeld statelijke actoren** (DBSA).

In het dreigingsbeeld wordt gesteld dat China, Rusland en Iran offensieve cyberprogramma's hebben gericht tegen westerse landen, waaronder Nederland en dat er een toename is van spionageactiviteiten bij Nederlandse topsectoren en kennisinstellingen uitgevoerd door China en Rusland. Het DBSA noemt ook vijftien doelwitten van statelijke actoren, zoals democratische processen, adviesorganen, onderwijsinstellingen, internationale organisaties in Nederland, bedrijfsleven, vitale infrastructuur en voor Nederland cruciale internationale verbanden.

"Er is een nieuwe wapenwedloop gaande. Daarin past geen naïviteit. Het nationale verdienvermogen wordt bedreigd", zegt directeur-generaal Erik Akerboom van de AIVD. Volgens Akerboom lopen 'alle kroonjuwelen' van de Nederlandse economie gevaar. MIVD-directeur Jan Swillens spreekt van een 'imminent threat' uit Rusland en China. "Ze willen het, ze kunnen het en ze doen het", merkt hij op.

Het dreigingsbeeld statelijke actoren (DBSA), 3 februari 2021, is opgesteld in samenwerking tussen Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)

Bron: https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/dreigingsbeeld-statelijke-actoren

Het DBSA beoogt te informeren over zowel actuele als potentiële dreiging door statelijke actoren; niet alleen inhoudelijk, door uitleg over de aard van het fenomeen en de voorstelbare verschijningsvormen, maar ook over de wijze waarop deze dreiging de nationale veiligheidsbelangen raakt of kan raken.

Dreigingsbeeld Statelijke Actoren 2/2

Dreigingen door statelijke actoren manifesteren zich op verschillende wijzen, waarbij zowel de frequentie als de hoeveelheid actoren niet per se iets zeggen over de ernst van de dreiging. Gevolgen van ingezette middelen hoeven niet direct zichtbaar te zijn, maar kunnen ook pas op een later moment zichtbaar worden. De schade die op die manier sluipenderwijs ontstaat kan grote impact hebben.

Inzet digitale middelen: digitale middelen (kunnen) worden ingezet voor spionagedoeleinden en als voorbereidingshandelingen op en daadwerkelijke verstoring en sabotage van vitale infrastructuur.

Beïnvloeding, inmenging en desinformatie: statelijke actoren ontplooien beïnvloedings- en inmengingsactiviteiten, waarbij een onderscheid valt te maken tussen statelijke actoren die deze activiteiten primair richten op hun diaspora en statelijke actoren die juist de Nederlandse samenleving in den brede willen beïnvloeden. Hoewel er veel manifestaties van informatieoperaties bekend zijn, zoals het verspreiden van desinformatie, is het aantal statelijke actoren waarvan onderkend is dat zij dit instrument structureel en centraal aangestuurd inzetten beperkt.

Spionage: diverse landen voeren spionageactiviteiten uit die gericht zijn op het vergaren van politieke inlichtingen. Een aantal landen bespioneert de eigen diaspora en dissidenten in hun verblijfslanden, of doet aan spionage ten behoeve van de eigen economische, technologische en militaire ontwikkeling.

Inzet van economische instrumenten: bij de structurele en centraal aangestuurde inzet van economische instrumenten is het aantal actoren beperkt, met China als veruit de belangrijkste. Monopolie posities of economische machtsposities kunnen als strategisch middel worden ingezet, waardoor ongewenste afhankelijkheden kunnen ontstaan.

Militaire instrumenten: de waargenomen manifestaties van inzet van militaire instrumenten kunnen Nederland raken doordat schade wordt toegebracht aan bijvoorbeeld de internationale rechtsorde, bondgenootschappelijke cohesie, of indien militaire activiteiten leiden tot een conflict waarbij artikel 5 van het NAVOverdrag in werking kan worden gesteld.

Huidige situatie

Cyberadvies vanuit AIVD(01-02-2021)

Cyberadvies met betrekking tot compromittering van e-mailomgevingen

Essentie

- Uit inlichtingenonderzoek van de AIVD blijkt dat statelijke actoren hun aanvalsmethodieken om toegang te verkrijgen tot mailboxen en mailomgevingen te hebben uitgebreid.
- Naast *spear phishing* maken actoren in toenemende mate ook gebruik van *brute forcing* en *password spraying* om toegang te krijgen tot mailaccounts.
- Wereldwijd zijn het afgelopen jaar vele overheidsorganisaties, parlementen, non-gouvernementele organisaties en bedrijven slachtoffer geworden van deze spionageoperaties. In Nederland zijn voor zover bekend bij de AIVD ook doelwitten van deze spionagepogingen ook daadwerkelijk gecompromitteerd (geweest).
- De Diensten onderkennen twee belangrijke risico's voor uw organisatie ten aanzien van deze aanvalsmethodieken; Het eerste risico betreft toegang tot gevoelige of vertrouwelijke informatie en persoonsgegevens uit gecompromitteerde mailboxen. Het tweede risico betreft de verdere toegang tot het bedrijfsnetwerk via het misbruiken van inloggegevens. Om deze risico's te mitigeren wordt geadviseerd om preventieve, detectieve en procedurele maatregelen te nemen op basis van een risicoanalyse.
- Door middel van MFA verkleint u de kans significant dat uw e-mailomgeving wordt gecompromitteerd.

Emotet gecompromitteerde accounts, bericht NCSC aan RIVM 11 februari 2021

Op 26 januari jl., tijdens een internationale politieoperatie 'Ladybird', zijn servers uit de lucht gehaald die deel uitmaakten van het wereldwijde botnet Emotet. Bij de internationale politieoperatie waren Nederland, Duitsland, het Verenigd Koninkrijk, Frankrijk, Oekraïne, de Verenigde Staten, Canada en Litouwen betrokken.

Vanuit de landelijke eenheid van de politie is er een dataset met gecompromitteerde persoonlijke accounts gedeeld met het NCSC. Deze dataset bevat de credentials voor meerdere online platformen. Dit betreffen accountgegevens die zijn opgeslagen in de web browser van een door Emotet geïnfecteerde gebruiker. De gelekte accountgegevens kunnen mogelijk misbruikt worden door kwaadwillenden. Echter het is niet inzichtelijk of deze gegevens reeds misbruikt zijn of misbruikt gaan worden.

In de bijlage treft u de door Emotet verkregen accountgegevens die gebruikt worden binnen uw systemen. Het advies is om onderzoek te doen of er verdachte activiteiten hebben plaatsgevonden op deze accounts, monitoring toe te passen en wachtwoorden te resetten.


DDoS-aanvallen op RIVM-website

Eind vorige week is er een aantal gerichte DDoS-aanvallen uitgevoerd op onze website. De IV-organisatie heeft onmiddellijk maatregelen genomen waardoor er geen sprake is geweest van indringing.

Door de maatregelen was de RIVM-website op donderdagmiddag 3 december jl. een uur niet bereikbaar, en een paar keer 's nachts. De maatregelen hebben geholpen: zaterdagnacht stopten de aanvallen. De IV-organisatie doet nu verder onderzoek naar deze aanvallen en houdt de situatie nauwgezet in de gaten.

In december 2020 heeft er 3 x een DDOS aanval op het RIVM plaatsgevonden. Gelukkig waren deze aanvallen kleinschalig. Er is aangifte bij de Politie gedaan.

Huidige situatie





Twee weken geleden gehackte bekend dat het computernetwerk van het Algemeen Medisch Labo in Antwerpen was gehackt. — © BELGA

Cyberaanval legt labo's over heel België plat

De complexe cyberaanval op een Antwerps medisch labo dat coronatests analyseert, heeft ook verschillende andere medische labo's in ons land platgelegd.

Werner Rommers, Dirk Coosemans en Steven Leenknegt

Vrijdag 8 januari 2021 om 18:36

08-02-2021 20:37	De Jonge: GGD voldoet niet aan beveiligingseisen DigiD	13 reacties
10-02-2021 21:14	Logius: geen onveilige situatie met DigiD-aansluiting coronatest.nl	12 reacties
04-02-2021 20:37	Politie arresteert vijfde verdachte voor datadiefstal uit GGD-systemen	7 reacties
03-02-2021 17:14	Politie pakt vierde verdachte op voor datadiefstal uit GGD-systemen	7 reacties
03-02-2021 13:32	RIVM maakt zich zorgen over snelle overstap op nieuw GGD-systeem	4 reacties
03-02-2021 11:37	GGD ontslaat dertig medewerkers wegens onrechtmatig inzien persoonsgegevens	13 reacties
03-02-2021 09:54	De Jonge: GGD heeft volledige persoonsgegevens nodig voor taakuitvoering	19 reacties
03-02-2021 09:30	GGD gaat deze week toegang tot systemen en zoekmogelijkheden beperken	4 reacties
02-02-2021 17:37	Politie houdt derde verdachte aan voor datadiefstal bij GGD	4 reacties
01-02-2021 10:49	Rijksdienst: kleine kans op identiteitsfraude door datalek bij GGD	29 reacties
31-01-2021 07:41	GGD schakelt printfunctie uit in coronasysteem wegens datadiefstal	22 reacties
28-01-2021 14:18	Politie houdt meerdere GGD-medewerkers aan voor datadiefstal	25 reacties
29-01-2021 10:41	GGD gaat stoppen met systeem voor bron- en contactonderzoek	20 reacties
29-01-2021 09:23	Autoriteit Persoonsgegevens stelt GGD onder verscherpt toezicht	18 reacties
28-01-2021 16:52	GGD: eind maart automatische en continue controle van systemen	16 reacties
27-01-2021 13:39	Autoriteit Persoonsgegevens eist opheldering van GGD over datalek	12 reacties
27-01-2021 11:32	De Jonge: meer controles op misbruik van privédata in GGD-systemen	17 reacties
27-01-2021 09:56	AP slecht bereikbaar door vragen over handel in privédata uit GGD-systemen	5 reacties
26-01-2021 16:45	GGD-medewerkers opgepakt voor handel in privédata uit coronasystemen	28 reacties

Nog geen misbruik van SolarWinds-backdoor bij overheid ontdekt

maandag 8 februari 2021, 12:55 door **Redactie**, 0 **reacties**

Binnen de Nederlandse overheid wordt gebruikgemaakt van het Orion-platform van softwarebedrijf SolarWinds, maar vooralsnog is er geen misbruik ontdekt van de backdoor die aanvallers door middel van updates aan de software wisten toe te voegen. Dat schrijft minister Grappperhaus van Justitie en Veiligheid in een brief aan de Tweede Kamer (pdf).

De Orion-software van SolarWinds laat organisaties hun it-omgeving beheren. In 2019 wisten aanvallers toegang tot de ontwikkelomgeving van het softwarebedrijf te krijgen. Die toegang gebruikten ze vorig jaar om verschillende updates voor de Orion-software van een backdoor te voorzien. Deze besmette updates werden wereldwijd door zo'n 18.000 organisaties geïnstalleerd, waaronder bedrijven en overheidsinstanties.

Aanvaller steelt scripts, scanners en tools securitybedrijf FireEye

woensdag 9 december 2020, 07:20 door **Redactie**, 17 **reacties**

Een aanvaller heeft ingebroken op de systemen van securitybedrijf FireEye en ze scripts, scanners en tools van het bedrijf kunnen stelen, zo heeft FireEye zelf in een **blogposting** bekendgemaakt. Het gaat om tools die FireEye gebruikt voor het testen van de beveiliging van klanten, zoals scripts voor het automatisch verkennen van netwerken tot exploitatie-frameworks die op CobaltStrike en Metasploit lijken.

Er zijn bij de aanval geen zeroday-exploits of onbekende technieken buitgemaakt. Volgens FireEye zal de diefstal de aanvaller in kwestie dan ook niet veel helpen. Kevin Mandia, ceo van FireEye, stelt dat de aanvaller als primair doel naar informatie over bepaalde overheidsklanten zocht. Er zijn echter geen aanwijzingen gevonden dat er ook data van systemen waarop klantgegevens staan is buitgemaakt.

Te beschermen belangen en kroonjuwelen

Te beschermen belangen	Kroonjuwelen	Dreiging
Bestelproces		
Bestelinformatie		
Vaccins		

Context (systeemdecompositie)