Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Handreiking
Cybersecuritymaatregelen

Stap voor stap naar een digitaal veilige organisatie

Nederland digitaal veilig

Installeer software-updates

Zorg dat elke applicatie en elk systeem voldoende log-informatie genereert

Pas multifactorauthenticatie toe waar nodig

Maak regelmatig back-ups van uw systemen en test deze

Bepaal wie toegang heeft tot uw data en diensten

Versleutel opslagmedia met gevoelige bedrijfs-informatie

Segmenteer netwerken

Controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze

Aanvullende informatie vindt u op ncsc.nl/aandeslag

Inleiding

Stap voor stap naar een digitaal veilige organisatie

Elk jaar vinden wereldwijd veel cybersecurityincidenten plaats bij organisaties. Bij deze aanvallen wordt bijvoorbeeld gebruikgemaakt van ransomware of phishing. Het Cybersecuritybeeld Nederland (CSBN) beschrijft en duidt een aantal incidenten die een relatie tot Nederland heeft.

Het CSBN 2021 concludeert dat uit incidenten blijkt dat de weerbaarheid onvoldoende op orde is en basismaatregelen veelal ontbreken. In deze handreiking vindt u maatregelen die elke organisatie zou moeten treffen en die helpen cyberaanvallen zoals het CSBN die beschrijft tegen te gaan. Ga na of uw cybersecuritybeleid deze maatregelen bevat. En gebruik deze handreiking als beginpunt voor gesprekken met uw leveranciers over hun digitale veiligheid.

Hoofdstuk 1 beschrijft de context waarin u deze maatregelen toepast: hoe is de verantwoordelijkheid voor cybersecurity in een organisatie belegd? Hoofdstuk 2 legt uit hoe deze maatregelen regulier risicomanagement ondersteunen, maar er niet voor in de plaats komen. In hoofdstuk 3 staan de acht maatregelen opgesomd die elke organisatie zou moeten nemen voor een digitaal veilige organisatie. Heeft u de maatregelen toegepast en wilt u verder, dan biedt hoofdstuk 4 u hiervoor aanknopingspunten.

Voor wie?

Deze handreiking is gericht op personen in uw organisatie die verantwoordelijk zijn voor cybersecurity.

1.

Organisatorische inbedding van de maatregelen

De maatregelen in deze handreiking kunnen u helpen bij het voorkomen van incidenten. Om deze maatregelen effectief in uw organisatie in te zetten, is het nodig dat u de organisatorische kant van cybersecurity goed geregeld hebt. Het is van belang dat u bewustzijn creëert voor de risico's van cybersecurity op alle niveaus in de organisatie, inclusief gebruikers. Beleg daarnaast verantwoordelijkheden juist.

Directie

Omdat incidenten zich overal in de organisatie kunnen voordoen is cybersecurity een uitdaging voor de gehele organisatie. Om ervoor te zorgen dat de organisatie deze uitdaging aankan, is de juiste sturing vanuit de directie nodig. De belangrijkste cybersecuritytaken van de directie zijn het beleggen van eigenaarschap en verantwoordelijkheid voor informatie en processen.

Informatiesystemen (IT) zijn hierbij ondersteunende middelen. Immers, IT-systemen zijn een middel om informatie te verwerken en om processen die bijvoorbeeld gebruik maken van operationele systemen (OT) aan te sturen. Na het beleggen van deze verantwoordelijkheden ziet de directie ook toe op een goede uitvoering ervan. In deze tijd zijn IT- en OT-systemen, net als geld en personeel, bedrijfsmiddelen waar een organisatie van afhankelijk is. Om die reden is het lijnmanagement de aangewezen plek om deze verantwoordelijkheid te beleggen. De directie dient te zorgen dat de juiste functionarissen beschikbaar zijn om lijnmanagers bij deze verantwoordelijkheid te ondersteunen. Voorbeelden zijn een Chief Information Security Officer (CISO), een Functionaris Gegevensbescherming (FG), Chief Information Officer (CIO) en/of een informatiemanager, een IT-manager of een OT-manager. Echter, de hoogstgeplaatste persoon binnen de organisatie (directeur, bestuursvoorzitter, secretaris-generaal) is en blijft eindverantwoordelijk.

Lijnmanagement

Lijnmanagers hebben de verantwoordelijkheid om voor de IT- en OT-systemen waar zij het eigenaarschap van toegewezen hebben gekregen, de bijbehorende risico's inzichtelijk te (laten) maken, een eindoordeel te geven over het wel of niet accepteren van restrisico's en toe te zien op een juiste implementatie van de mitigerende maatregelen. Lijnmanagers zullen in veel gevallen geen cybersecurityexpert zijn. Daarom wordt een lijnmanager ondersteund door de adviezen en diensten van een Chief Information Security Officer (CISO), een Functionaris Gegevensbescherming (FG), een Chief Information Officer (CIO) en/of informatiemanager, een IT-manager of een OT-manager.

CISO

De CISO heeft, als kenner van cybersecurity, een adviserende, coördinerende en controlerende rol. De CISO heeft geen zelfstandige verantwoordelijkheid voor de cybersecurity van de organisatie. De CISO is namelijk geen eigenaar van IT- of OT-systemen. Die rol wordt altijd belegd bij het lijnmanagement van de organisatie.

2.

Risicoanalyse

De maatregelen uit het volgende hoofdstuk ondersteunen uw reguliere processen voor risicomanagement, maar het blijft van belang een eigen risicoanalyse te doen en zelf aanvullende maatregelen te selecteren.

Een belangrijk onderdeel van risicomanagement is het inzichtelijk maken van de risico's voor een organisatie. Op basis van de ingeschatte risico's kunnen maatregelen bepaald worden. Het CSBN duidt de digitale dreiging en incidenten die zich hebben voorgedaan en identificeert risico's voor de nationale veiligheid. Voor deze dreigingen heeft het NCSC een selectie van acht maatregelen gemaakt. U vindt deze in het hoofdstuk 'Maatregelen'.

Het NCSC adviseert u al deze maatregelen binnen uw organisatie toe te passen. Daarnaast adviseert het NCSC om een eigen risicoanalyse uit te voeren. Zo kunt u verdere maatregelen identificeren die helpen de specifieke risico's voor uw organisatie te beheersen. Ook als u nog geen eigen risicoanalyse heeft uitgevoerd, is het verstandig de maatregelen uit deze handreiking toe te passen. Het zijn algemene maatregelen die ook uit uw eigen risicoanalyse zouden moeten volgen.

Eigen risicoanalyse

Het NCSC benadrukt dat deze maatregelen de noodzaak tot het zelf doen van risicoanalyses niet wegneemt. Zie deze maatregelen als basismaatregelen, waarvan het altijd verstandig is om deze op orde te hebben. Echter, elke organisatie is uniek. Ook uw organisatie kent daarom waarschijnlijk specifieke digitale risico's. Het NCSC adviseert om deze inzichtelijk te maken en met passende maatregelen te beheersen. Dit is maatwerk en een continu proces. Zowel dreigingen als de te beschermen belangen van uw organisatie kunnen namelijk veranderen.

Verder lezen

Meer over de rol van de CISO en de inrichting van risicomanagement is te lezen in de factsheet *Risico's beheersen: de waarde van informatie als uitgangspunt van het NCSC*:

https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing

3.

Maatregelen

Dit hoofdstuk somt acht basismaatregelen op die volgens het NCSC noodzakelijk zijn om u te beschermen tegen actuele digitale dreigingen.

Installeer updates

Software bevat programmeerfouten. Zulke fouten kunnen leiden tot kwetsbaarheden. Leveranciers brengen updates uit om kwetsbaarheden in hun software te verhelpen. Zorg voor een proces dat updates voor uw software identificeert, test en installeert. Breng hierbij alle software en systemen binnen uw organisatie in kaart, ook webbrowsers en plug-ins.

Voor de meeste systemen is het van belang om deze updates zo snel mogelijk te installeren. Sommige software biedt de mogelijkheid deze automatisch te laten updaten: maak hier gebruik van. Voor kritieke systemen is het raadzaam de update eerst in een testomgeving uit te voeren, voordat u deze implementeert in de productieomgeving.

In sommige gevallen is een update voor een kwetsbaarheid nog niet beschikbaar. Tref in zulke gevallen mitigerende maatregelen. Vervang software en apparaten die niet meer door de leverancier ondersteund worden.

Verder lezen

Naar aanleiding van recent gevonden kwetsbaarheden of geconstateerde dreigingen publiceert het NCSC beveiligingsadviezen.

Zorg dat elke applicatie en elk systeem voldoende loginformatie genereert

Logbestanden spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Door te zorgen dat applicaties en systemen voldoende loginformatie genereren voorziet u uzelf van voldoende informatie.

Bepaal welke logbestanden nodig zijn. Denk hierbij aan systeemlogging, netwerklogging, applicatielogging en cloudlogging. Stel waar nodig alertering in. Denk bijvoorbeeld aan notificaties van verdachte inlogpogingen op basis van een analyse van logbestanden. Zorg dat uw systemen logbestanden in een bruikbaar bestandsformaat opslaan, en dat de opgenomen tijdsinformatie nauwkeurig en in de juiste tijdzone gesteld is.

Maak een afweging over de bewaartermijn van logbestanden. Als u logbestanden lang bewaart, kunt u ook veel later bij incidenten achterhalen wat er is gebeurd. Aan de andere kant bevatten logbestanden mogelijk privacygevoelige informatie en nemen ze opslagruimte in beslag.

Beperk de toegang tot logbestanden en sla deze op in een apart netwerksegment. Incidentenonderzoek is nauwelijks mogelijk als aanvallers de logbestanden hebben kunnen aanpassen of verwijderen.

Pas multifactorauthenticatie toe

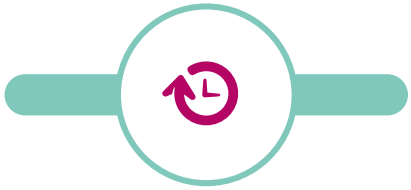
Pas multifactorauthenticatie toe bij accounts die vanaf het internet bereikbaar zijn, accounts die beheerrechten hebben en accounts op essentiële systemen. Het gebruik van multifactorauthenticatie voorkomt dat een aanvaller toegang tot een account verkrijgt door het wachtwoord te raden of te achterhalen. Deze wachtwoorden kan een aanvaller bijvoorbeeld verkrijgen door een phishingaanval uit te voeren.

Een factor is een middel waarmee een gebruiker zich aanmeldt. Factoren worden ingedeeld in drie categorieën: iets dat u weet (bijvoorbeeld een wachtwoord), iets dat u heeft (bijvoorbeeld een token) of iets dat u bent (bijvoorbeeld een vingerafdruk). Logt u in met factoren uit minimaal twee van deze categorieën, dan spreken we van multifactorauthenticatie. Het gebruik van exact twee factoren wordt ook wel tweefactorauthenticatie genoemd. Voorbeelden van multifactorauthenticatie zijn een wachtwoord in combinatie met een token of gebruik van een vingerafdruk in combinatie met een eenmalige code.

Verder lezen

Meer informatie is te vinden in de NCSC-factsheet *Gebruik tweefactorauthenticatie*:

https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-gebruik-tweefactorauthenticatie

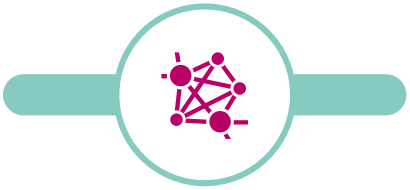


Maak regelmatig back-ups van uw systemen en test deze

Het maken en testen van back-ups is essentieel als uw data en systemen zijn aangetast en hersteld moeten worden. Bedenk van welke data back-ups noodzakelijk zijn en hoelang u deze moet bewaren. Test met regelmaat het terugzetten van uw back-ups zodat u zeker weet dat uw bedrijfsvoering bij dataverlies maar beperkt wordt verstoord.

De 3-2-1 regel kan helpen bij de inrichting van uw back-upproces. Deze regel houdt in dat u drie versies heeft van uw data (uw productiedata en twee back-ups) op twee verschillende media (bijvoorbeeld verschillende fysieke harde schijven) met één kopie op een andere locatie voor noodherstel (bijvoorbeeld fysiek). Door back-ups op een andere locatie op te slaan kunt u, indien bijvoorbeeld ransomware uw bedrijfsnetwerk heeft versleuteld, uw systemen herstellen.

Beperk de toegang tot de back-ups. Denk hierbij aan de toegangsrechten, maar overweeg ook het versleutelen van uw back-ups.



Segmenteer netwerken

Het segmenteren van uw netwerk beperkt de gevolgen van een aanval. Segmenteren betekent dat een netwerk in meerdere zones wordt verdeeld. Netwerksegmentatie voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen beperkt.

Denk bij het segmenteren van uw netwerken na over hoe deze zones ingedeeld en verbonden zijn. U kunt bijvoorbeeld zones definiëren met behulp van firewalls, access control lists (ACL's) en datadiodes. U kunt er ook voor kiezen een netwerk alleen fysiek benaderbaar te maken, een zogeheten *air-gapped* netwerk. Zorg in ieder geval dat kritieke systemen in een eigen netwerkzone geplaatst zijn.

Hanteer het uitgangspunt dat netwerkverkeer in het algemeen niet toegestaan is en voeg vervolgens specifieke firewallregels toe voor verkeer dat wel nodig is. Als u netwerkverkeer al te rigoureus blokkeert, kan dat zorgen voor verstoringen in uw bedrijfsvoering. Dit kunt u voorkomen door eerst het netwerkverkeer te monitoren om te bepalen welke informatiestromen nodig zijn, en daarna pas netwerkverkeer te blokkeren.

Bepaal wie toegang heeft tot uw data en diensten

Geef medewerkers alleen toegang tot de data en systemen die nodig zijn voor het uitvoeren van hun taak. Dit geldt zowel voor accounts als voor fysieke toegang. Dit beperkt de handelingen die een aanvaller kan uitvoeren indien deze zich toegang verschaft. Ook beperkt het de gevolgen van eventuele fouten van gebruikers.

Beperk ook de toegang van serviceaccounts, machine-accounts en functionele accounts tot het noodzakelijke. Op rollen gebaseerde toegangscontrole kan het beheer van rechten makkelijker maken. Het toebedelen van minimale rechten wordt ook wel het *principle of least privilege* genoemd. Limiteer hierbij ook het gebruik van beheerrechten.

Zorg daarnaast dat toegang tot data en diensten persoonsgebonden is waarbij elke medewerker een eigen gebruikersaccount heeft. Verander standaardwachtwoorden van apparatuur en systemen bij installatie of ingebruikname.

Zorg dat u processen heeft voor de indiensttreding, uitdiensttreding en interne doorstroming van medewerkers. Geef nieuwe medewerkers alleen toegang tot de middelen die ze nodig hebben. Ontneem accounts van vertrekkende medewerkers direct toegang tot data en systemen. Verwijder ongebruikte accounts. Deactiveer serviceaccounts, en activeer deze alleen wanneer onderhoud plaatsvindt.

Versleutel opslagmedia met gevoelige bedrijfsinformatie

Het versleutelen van opslagmedia met gevoelige bedrijfsinformatie maakt de data onbruikbaar als deze in handen van aanvallers valt. Door de versleuteling is de data niet in te zien. Versleutel harde schijven, laptops, mobiele apparaten en usb-sticks die gevoelige informatie bevatten. Gebruik veilige encryptiesoftware om deze media te versleutelen.

Controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze

Het verbinden van apparaten en diensten met het internet vormt een risico. Controleer daarom welke van uw apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze. Sta toegang tot het internet alleen toe indien dit noodzakelijk is. Dit beperkt het risico op ongeautoriseerde toegang. Tref maatregelen om de apparaten en diensten die bereikbaar zijn vanaf het internet te beschermen. Beschermende maatregelen zijn het gebruik van een firewall, het uitschakelen van ongebruikte services en poorten en zorgen dat software up-to-date is. Plaats apparaten die vanaf het internet bereikbaar zijn in een apart netwerksegment. Pas multi-factorauthenticatie toe voor accounts die via het internet te gebruiken zijn.

4.

Aandachtspunten

Met de acht maatregelen uit het vorige hoofdstuk legt uw organisatie het fundament voor effectieve cyberweerbaarheid. Daarnaast adviseert het NCSC om u voor te bereiden op incidenten en in gesprek te gaan met uw leveranciers.

Wees voorbereid op incidenten

Ondanks de genomen maatregelen kan een incident nog steeds plaatsvinden. Bereid u daarop voor. Zorg dat cybersecurityincidenten zijn opgenomen in uw bestaande herstelplan (bijvoorbeeld een Disaster Recovery Plan). Update en oefen dit plan regelmatig.

In gesprek met leveranciers

De cybersecurity van uw organisatie is mede afhankelijk van leveranciers. Maak heldere afspraken met leveranciers en onderaannemers, bijvoorbeeld over incidentmanagement of rapportages. Het NCSC adviseert om op basis van risicomanagement gebruik te maken van bestaande normen en richtlijnen bij de inkoop van producten en diensten. De maatregelen genoemd in deze handreiking kunt u meenemen tijdens het inkoopproces.

Verder lezen

Voor de inkoop van clouddiensten heeft het NCSC de factsheet *5 adviezen voor veilige inkoop van clouddiensten* gepubliceerd:

https://www.ncsc.nl/documenten/publicaties/2020/oktober/29/factsheet-5-adviezen-voor-veilige-inkoop-van-clouddiensten

Andere publicaties

Er zijn meer publicaties die uw organisatie handvatten kunnen bieden om uw cyberweerbaarheid te verhogen, zoals:

- Cyberaanvallen door statelijke actoren – 7 momenten om een aanval te stoppen (AIVD): https://www.aivd.nl/cyberdreiging
- De 5 basisprincipes van veilig digitaal ondernemen (Digital Trust Center): https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen
- In de Tool Handreiking Cyberoefenen van de Cybersecurity Alliantie worden handvatten geboden aan organisaties om oefeningen voor te bereiden en te evalueren. Door te oefenen binnen een organisatie of binnen een keten, kunnen organisaties zich voorbereiden op (eventuele) cyberincidenten. Kijk voor meer informatie op Cybersecurityalliantie.nl.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

juni 2021