Basismaatregelen voor cybersecurity

RendementOnline

Door redactie FA Rendement

20 april 2022 | 5 minuten

Het Nationaal Cyber Security Centrum (NCSC), een onderdeel van het ministerie van Justitie en Veiligheid, werkt aan een digitaal veilig Nederland.

Door onder andere de toegenomen digitalisering door de coronapandemie, is het belang van digitale veiligheid verder toegenomen. Het NCSC heeft een handreiking gemaakt met basismaatregelen voor ondernemers. Een samenvatting.

De 'Handreiking Cybersecuritymaatregelen: Stap voor stap naar een digitaal veilige organisatie' gaat in op maatregelen die ondernemingen kunnen treffen om weerbaar te worden tegen cyberaanvallen. Volgens het NCSC kunnen ondernemingen acht basismaatregelen treffen om zich te beschermen tegen digitale dreigingen.

2,5 miljoen slachtoffers van online criminaliteit in 2021

Bijna 2,5 miljoen Nederlanders werden in 2021 slachtoffer van online criminaliteit, vooral van oplichting en fraude. Minder dan de helft maakte daar melding van en slechts een kleine 20% deed aangifte.

Phishing

Het Centraal Bureau voor de Statistiek (CBS) meldt in de publicatie 'Veiligheidsmonitor 2021' ook dat er afgelopen jaar ruim 1,5 miljoen Nederlanders slachtoffers zijn geworden van online oplichting en fraude. Er was meestal sprake van aankoopfraude (7%) en hacken (ook 7%). Ruim 100.000 Nederlanders waren gedupeerd door phishing. Ook ontvingen meer dan twee op de drie (68%) van Nederlanders van 15 jaar of ouder in 2021 ten minste één keer een telefoontje, e-mail of ander bericht van een oplichter.

De eerste basismaatregel is het installeren van updates. Is er sprake van programmeerfouten in software, dan kunnen deze leiden tot kwetsbaarheden. Updates verhelpen deze kwetsbaarheden.

Het advies van het NCSC aan ondernemingen luidt: zorg voor een proces dat updates voor uw software identificeert, test en installeert. Alle software en systemen moeten hierbij in kaart worden gebracht, inclusief webbrowsers en plug-ins.

Updates zo snel mogelijk installeren

Het NCSC raadt ook aan om updates zo snel mogelijk te installeren. Automatische updates verdienen de voorkeur. Bij het updaten van kritieke systemen is het aan te raden om eerst een update in een testomgeving uit te voeren. Een andere nuttige tip: vervang software en apparaten die de leverancier niet meer ondersteunt.

Logbestanden bijhouden

De tweede basismaatregel die het NCSC voorstelt is zorgen dat alle applicaties en systemen voldoende loginformatie genereren. Logbestanden zijn namelijk van belang bij het herkennen van cyberaanvallen en het afhandelen van incidenten.

Ondernemers moeten voor zichzelf bepalen welke logbestanden nodig zijn. Denk hierbij aan systeem-, netwerk, applicatie- en cloudlogging. Waar nodig kunnen notificaties worden ingesteld. Door een analyse van logbestanden kunnen verdachte inlogpogingen worden herkend.

Ondernemers moeten ook voor zichzelf de bewaartermijnen van logbestanden bepalen. Het is aan te raden om toegang tot logbestanden te beperken en op te slaan in een apart netwerksegment.

Multifactorauthenticatie combineert een wachtwoord met een token

Voer multifactorauthenticatie in

De derde basismaatregel is: pas multifactorauthenticatie toe bij:

- accounts die vanaf het internet bereikbaar zijn;
- accounts die beheerrechten hebben; en
- accounts van essentiële systemen.

Hackers krijgen zo geen toegang tot een account als zij het wachtwoord hebben weten te achterhalen. Factoren zijn er in drie categorieën:

- iets dat iemand weet (bijvoorbeeld een wachtwoord);
- iets dat die persoon bezit (bijvoorbeeld een token); of
- iets dat die persoon is (bijvoorbeeld een vingerafdruk).

Voorbeelden van multifactorauthenticatie zijn een wachtwoord gecombineerd met een token of gebruik van een vingerafdruk met een eenmalige code.

De 3-2-1-regel voor back-ups

Het maken en testen van back-ups is van essentieel belang als data en systemen zijn aangetast en moeten worden hersteld. De 3-2-1-regel kan helpen bij het inrichten van het back-upproces: er moeten drie versies van de desbetreffende data zijn (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 een back-up op een andere locatie kunnen systemen worden hersteld als een ondernemer door bijvoorbeeld ransomware geen toegang meer heeft tot het bedrijfsnetwerk. Het NCSC adviseert ook om toegang tot back-ups te beperken. Denk bijvoorbeeld aan toegangsrechten.

Goede netwerksegmentatie kan de gevolgen van cyberaanvallen beperken

Segmenteren van het netwerk

De vijfde basismaatregel die het NCSC voorstelt is om netwerken te segmenteren. Door een netwerk in verschillende zones te verdelen, worden de gevolgen van een cyberaanval beperkt.

Zo kan bijvoorbeeld een virus maar een deel van het netwerk treffen. Goede netwerksegmentatie kan de gevolgen van ransomware- of DDoS-aanvallen beperken.

Beperk toegang tot data en diensten

Het bepalen wie toegang heeft tot data en diensten, is de zesde basismaatregel die ondernemingen kunnen treffen om zich te beschermen tegen cyberaanvallen. Het NCSC adviseert om werknemers alleen toegang te geven tot de data en systemen die zij nodig hebben om hun werkzaamheden te kunnen uitvoeren.

Deze maatregel beperkt de handelingen van een hacker als hij toegang heeft weten te krijgen tot de administratie van een onderneming.Een bijkomend voordeel van deze maatregel is dat de gevolgen van eventuele fouten van gebruikers worden beperkt.

> **Persoonsgebonden toegang wordt aangeraden**

Verleen minimale toegangsrechten

Het NCSC adviseert ondernemers ook om de toegang van serviceaccounts, machineaccounts en functionele accounts tot het noodzakelijke te beperken. Door toegangscontrole te koppelen aan rollen, wordt het beheer van rechten makkelijker.

Het toebedelen van minimale rechten wordt ook wel het ‘principle of least privilege’ genoemd. Persoonsgebonden toegang, waarbij elke werknemer een eigen gebruikersaccount heeft, wordt ook aangeraden.

Ondernemingen doen er ook goed aan om processen in kaart te brengen voor de indiensttreding, uitdiensttreding en interne doorstroming van werknemers. Ongebruikte accounts moeten zo snel mogelijk worden verwijderd. Serviceaccounts moeten daarnaast alleen worden geactiveerd bij onderhoud.

Versleutel bedrijfsinformatie

De zevende basismaatregel die ondernemingen kunnen treffen om digitaal weerbaar te worden is: versleutel opslagmedia met gevoelige bedrijfsinformatie.

Data worden bij encryptie onbruikbaar als cybercriminelen deze hebben weten te ontfutselen. Door het gebruik van encryptiesoftware kunnen cybercriminelen de data niet inzien. Opslagmedia die in aanmerking komen voor versleuteling zijn:

- harde schijven;
- laptops;
- mobiele apparaten; en
- usb-sticks.

> **Bescherm de apparaten en diensten die bereikbaar zijn vanaf het internet**

Internetverbinding is een risico

De laatste basismaatregel die het NCSC voorstelt is: controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze. Verbinding met het internet vormt een risico voor een onderneming.

Daarom stelt het NCSC voor om alleen toegang tot het internet toe te staan als dit echt noodzakelijk is. Op deze manier wordt het risico dat buitenstaanders ongeautoriseerd toegang krijgen tot apparaten en diensten zoveel mogelijk beperkt.

Beschermende maatregelen die ondernemingen kunnen nemen, zijn onder andere:

- het gebruik van een firewall;
- het uitschakelen van ongebruikte services en poorten;
- zorgen dat software up-to-date is.

Daarnaast is het van belang om apparaten die toegang hebben tot het internet in een apart netwerksegment te plaatsen. Multifactorauthenticatie wordt ook aangeraden voor accounts die via het internet te gebruiken zijn.

Cyber op de agenda

Uit cijfers van de laatste jaren blijkt dat financieel-economische criminaliteit fors toeneemt. Daaronder valt bedrijfsspionage door bijvoorbeeld meekijken via netwerken, fraude en hacken. Cyberveiligheid moet dus hoog op de agenda komen van organisaties. Een tip voor ondernemers: zorg voor een risicoanalyse, indien nodig, en een leesbaar bedrijfscontinuïteitsplan (artikel) dat makkelijk is te actualiseren.

Zorg voor een herstelplan

Met het toepassen van de tips van het NCSC komt een onderneming een heel eind op het gebied van effectieve cyberweerbaarheid (toolbox). Desondanks kan een incident nog steeds plaatsvinden. Een herstelplan (tool) biedt uitkomst.

Voor de cybersecurity is het ook van belang om heldere afspraken met leveranciers en onderaannemers, bijvoorbeeld over incidentmanagement of rapportages, te maken.

Dit is een artikel van de redactie van FA Rendement

FA Rendement is dé informatiebron voor administrateurs, boekhouders, controllers en andere financiële professionals. Wat is er veranderd op het gebied van financieel-administratieve wet- en regelgeving, en hoe kunt u als specialist deze informatie direct in uw dagelijkse werk toepassen? Daarnaast moet u op de hoogte zijn van onder meer de fiscaliteit, automatisering, de loon- en salarisadministratie, sociale voorzieningen, debiteurenbeheer en inkoop.

De onafhankelijke en ervaren redactie van FA Rendement zit bovenop het nieuws en vertelt u als eerste wat de ontwikkelingen zijn. Altijd in heldere taal en met een praktische insteek, zodat u de informatie direct kunt vertalen naar uw eigen werksituatie. FA Rendement is daarnaast multimediaal. De voor uw vakgebied relevante informatie verschijnt:

- ✓ dagelijks op het digitale platform Rendement Online, waar u onder meer het laatste nieuws, checklists, rekentools, maatwerkbrieven en verdiepingsartikelen tot uw beschikking heeft;
- ✓ wekelijks gebundeld in een e-mailnieuwsbrief;
- ✓ maandelijks in het vakblad FA Rendement, boordevol nieuws en achtergrondartikelen, digitaal en op de mat;
- ✓ tweemaandelijks in een handzaam themadossier: een pocketboekje dat iedere editie een complex onderwerp uitdiept.