Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Uw thuiswerk-faciliteiten zijn nu onmisbaar

Wat doet u bij uitval van uw thuiswerksoftware?

Factsheet FS-2020-02 | versie 1.0 | 1 april 2020

Veel organisaties hebben hun medewerkers opgedragen om thuis te werken na de invoering van de COVID-19-maatregelen. De beschikbaarheid van thuiswerkfaciliteiten is hierdoor opeens kritiek geworden voor de bedrijfscontinuïteit. Eerdere risicoanalyses over de beschikbaarheid van uw thuiswerkfaciliteiten voldoen nu waarschijnlijk niet meer.

Het NCSC adviseert om de kritieke processen van uw organisatie in kaart te brengen en maatregelen te treffen om beschikbaarheids-risico's te beheersen. Met het uitgebreide handelingsperspectief achterin deze factsheet kunt u uw organisatie voorbereiden op dit scenario.

Achtergrond

Na de invoering van de maatregelen voor het bestrijden van COVID-19, hebben veel organisaties hun medewerkers opgedragen om thuis te werken. Organisaties kunnen op die manier blijven doorwerken, zonder dat de fysieke nabijheid van medewerkers leidt tot extra besmettingsrisico. Ook kunnen medewerkers zo zorgtaken op zich nemen voor hun kinderen, die ze in veel gevallen onder schooltijd thuis op moeten vangen.

Doelgroep

Chief information security officers (CISO's), IT-managers, security officers

Aan deze factsheet hebben bijgedragen:

- Belastingdienst
- Nationaal Bureau Verbindingsbeveiliging (onderdeel van de AIVD)
- Schuberg Philis

In januari adviseerde het NCSC organisaties om hun Citrix-thuiswerkfaciliteiten uit te schakelen.[1] Organisaties die Citrix gebruikten om hun medewerkers thuis te laten werken, besloten massaal gehoor te geven aan dit advies, vanwege een ernstige kwetsbaarheid in deze software. De kwetsbaarheid die de aanleiding was voor het advies uit januari, was niet uniek.[2] Elke software bevat programmeerfouten, en alle thuiswerksoftware zou een dergelijke kwetsbaarheid kunnen bevatten. Het bijbehorende advies, om dan maar niet meer thuis te werken, is onder de huidige omstandigheden echter niet acceptabel.

Wat is er aan de hand?

Door de enorme toename in het aantal thuiswerkende medewerkers, is de beschikbaarheid van thuiswerkfaciliteiten voor veel organisaties opeens kritiek geworden voor de bedrijfscontinuïteit. Waar een uitval in thuiswerksoftware eerder misschien als een beperkt risico werd ervaren, vormt zo'n uitval op dit moment een grote bedreiging.

Risicoanalyses die u eerder heeft gemaakt over de beschikbaarheid van uw thuiswerkfaciliteiten, voldoen nu waarschijnlijk niet meer. Deze risicoanalyses hielden immers geen rekening met de grote mate waarin organisaties tijdens de COVID-19-uitbraak steunen op thuiswerkende medewerkers. Als u maatregelen heeft gebaseerd op deze risicoanalyses, dan zullen deze maatregelen in de huidige situatie tekortschieten voor het blijven waarborgen van de beschikbaarheid van uw thuiswerkfaciliteiten.

Ook ondersteunende ICT-processen, zoals de uitgifte van laptops, tokens en andere fysieke ICT-middelen, zijn nu in veel gevallen verminderd beschikbaar. Er zijn veel minder ICT-medewerkers op kantoor beschikbaar om deze uitgifte te verzorgen. Ook kan de fysieke uitgifte van zulke middelen aanvullende risico's voor besmetting met COVID-19 opleveren, waardoor organisaties er voorlopig voor kiezen deze processen in beperkte vorm uit te voeren.

Wat kan er gebeuren?

Als er een ernstige kwetsbaarheid in uw thuiswerksoftware bekend wordt, kan uw organisatie gedwongen worden te kiezen tussen twee kwaden. Als u niets doet, stelt u uw ICT bloot aan aanvallers die ongebreideld hun gang kunnen gaan. Als u wel ingrijpt en de thuiswerkfaciliteiten uitschakelt, brengt u de continuïteit van uw organisatie in gevaar. Voor de meeste organisaties zijn beide scenario's volstrekt onacceptabel.

Ook andere scenario's vormen een risico voor de beschikbaarheid van uw thuiswerkfaciliteiten. U kunt daarbij denken aan overbelasting door een sterke toename in het aantal gebruikers, een tekortschietend aantal licenties of accounts, DDoS-aanvallen op de toegangspunten tot uw netwerk, of onbedoelde verstoringen in de onderliggende systemen. Al deze risico's bestonden ook al voor de grootschalige uitbraak van COVID-19, maar sindsdien zijn de gevolgen ervan sterk toegenomen.

Als thuiswerkfaciliteiten niet beschikbaar zijn, zullen medewerkers geneigd zijn gebruik te maken van andere middelen waarmee ze bekend zijn, bijvoorbeeld in een privécontext. Bekende voorbeelden zijn gratis e-maildiensten of cloudplatforms voor samenwerking en bestandsuitwisseling. Als uw medewerkers dergelijke software gebruiken buiten de reguliere processen voor risicomanagement om, dan kan dat leiden tot flinke extra beveiligingsrisico's, bijvoorbeeld het lekken van informatie. In sommige gevallen kunt u het gebruik van zulke diensten toch accepteren, als u daarmee een groter onheil afwendt. Door nu vast na te denken over het gebruik van zulke privémiddelen, kunt u bij onbeschikbaarheid van uw thuiswerkfaciliteiten een overwogen keuze maken, en die duidelijk communiceren aan uw medewerkers. Het handelingsperspectief biedt u daarvoor verdere handvatten.

Wat adviseert het NCSC?

Het NCSC adviseert om de kritieke processen van uw organisatie in kaart te brengen, zodat u maatregelen kunt treffen om beschikbaarheidsrisico's te beheersen. Natuurlijk is elk onderdeel van uw organisatie belangrijk, maar het is te kostbaar om bij een ingrijpende verstoring alles in stand te houden. Door zich te richten op die zaken die strikt onmisbaar zijn voor de organisatiedoelen, zorgt u voor gerichte aandacht op die plaatsen waar het echt telt.

Ga voor elk kritiek proces van uw organisatie na in hoeverre het steunt op de thuiswerkfaciliteiten. Voeren medewerkers dit proces nu bijvoorbeeld uit met behulp van een samenwerkruimte, of door gebruik van webmail of een werkplek-op-afstand? Maak een lijst van alle thuiswerkfaciliteiten die voor een of meer kritieke processen van belang zijn. Natuurlijk steunt een kritiek proces niet alleen

[1] Zie https://www.ncsc.nl/actueel/nieuws/2020/januari/16/door-citrix-geadviseerde-mitigerende-maatregelen-niet-altijd-effectief.

[2] Zie bijvoorbeeld https://www.ncsc.nl/actueel/nieuws/2019/oktober/18/pulse-secure-en-fortigate-nog-veel-organisaties-in-nederland-kwetsbaar.

op thuiswerkfaciliteiten. Dit advies gaat echter uit van een situatie waarin andere betrokken ICT-systemen vóór de COVID-19-uitbraak al voorzien waren van passende maatregelen. Speelde een bepaald systeem al voor de COVID-19-uitbraak een sleutelrol in een kritiek proces, dan is het via regulier risicomanagement al voorzien van passende maatregelen.

Inventariseer de beschikbaarheidsrisico's voor de thuiswerkfaciliteiten waarop kritieke processen steunen. Welke problemen zijn te voorzien bij elk van deze systemen, en op welke manier bedreigt dit risico de uitvoering van de kritieke processen die op het systeem steunen?

Tref vervolgens maatregelen om de geïdentificeerde risico's te beheersen. Deze maatregelen zullen in twee categorieën uiteenvallen. Enerzijds treft u maatregelen om bestaande faciliteiten beter te beveiligen, en anderzijds treft u maatregelen die uw kritieke processen minder afhankelijk maken van de beschikbaarheid van deze thuiswerkfaciliteiten. Het handelingsperspectief biedt voorbeelden van dergelijke maatregelen.

Operationele cybersecurity: ook een kritiek proces

Bedenk bij het inventariseren van uw kritieke processen dat deze processen zelf ook afhankelijk zijn van bepaalde zaken. In het bijzonder vragen we uw aandacht voor het instandhouden van uw operationele cybersecurityprocessen, zoals incidentrespons en netwerkmonitoring. Met deze processen beheerst uw organisatie immers de risico's die ontstaan wanneer processen op alternatieve wijze worden uitgevoerd. Het zal daarom nodig zijn om operationele cybersecurityprocessen uit te blijven voeren, eventueel in een afgeslankte vorm.

Handelingsperspectief

Stap 1: Identificeer de kritieke processen van uw organisatie.	- We spreken van een kritiek proces als de uitval ervan al snel bedreigend is voor het realiseren van de organisatiedoelen. - Het kan verleidelijk zijn om in deze stap veel processen als kritiek te bestempelen. Het is echter nodig om hier keuzes in te maken. Hoe minder processen u als kritiek bestempelt, hoe meer aandacht u kunt besteden aan de paar processen die echt tellen. - Heeft u veel processen die erg belangrijk zijn, breng dan een extra ordening aan. U kunt de prioriteit van een kritiek proces bijvoorbeeld inschatten als 'gemiddeld', 'hoog' of 'top'. Dit helpt u in latere stappen om maatregelen te prioriteren. - Sommige processen zijn met aanvullende maatregelen minder kritiek te maken. Mogelijk kunt u bepaalde dienstverlening bijvoorbeeld uitstellen als u proactief communiceert naar uw interne of externe belanghebbenden.
Stap 2: Ga na in hoeverre kritieke processen steunen op thuiswerkfaciliteiten.	- Bekijk ieder proces zorgvuldig en ga na welke thuiswerkfaciliteiten er op dit moment gebruikt worden voor het uitvoeren van het kritieke proces. - Onderzoek in welke mate dit kritieke proces ongewijzigd uitgevoerd zou kunnen worden als deze thuiswerkfaciliteiten niet beschikbaar zouden zijn. Idealiter gaat het hierbij om vastgelegde en geteste procedures, maar in de huidige situatie zijn ook manieren 'waarop het wel zou kunnen' waarschijnlijk al erg welkom. - Maak een lijst van welke thuiswerkfaciliteiten er op dit moment onmisbaar zijn voor elk kritiek proces.
Stap 3: Inventariseer beschikbaarheidsrisico's van de thuiswerk-faciliteiten waar kritieke processen op steunen.	- Gebruik hiervoor de risico's die staan opgesomd in de sectie 'Wat kan er gebeuren?'. Vul deze aan met risico's die specifiek zijn voor uw situatie, bijvoorbeeld zoals vastgesteld in eerdere risicoanalyses.
Stap 4: Tref maatregelen om de geïdentificeerde risico's te beheersen: probeer onbeschik-baarheid te voorkomen, en zorg dat u er klaar voor bent als er toch verstoring optreedt.	Tref aanvullende maatregelen voor bestaande thuiswerkfaciliteiten. - *Voorbeeld* Zorg dat u het juiste onderhoudscontract voor uw thuiswerksoftware heeft. Heeft u bij storingen of andere problemen directe ondersteuning nodig, dan voldoet een basiscontract niet altijd. Ga na op welke termijn u hulp nodig zou hebben, en waar die hulp uit moet bestaan. Controleer of de afspraken die u met uw leverancier heeft, nog voldoen. - *Voorbeeld* Houd per gebruiker bij vanaf welke IP-adressen deze gebruiker inlogt, of richt een procedure in waarmee gebruikers snel hun IP-adres kunnen achterhalen en doorgeven. Doet zich een ernstige

kwetsbaarheid in uw thuiswerksoftware voor, dan kunt u ervoor kiezen om uw thuiswerksoftware online te houden met gebruik van IP-whitelisting. Daarmee heeft u wat langer de tijd om vervolgstappen te kiezen.

- ***Voorbeeld*** Koop voldoende capaciteit in. De meeste organisaties hebben hun thuiswerkfaciliteiten oorspronkelijk niet ingericht voor het grote aantal gebruikers dat ze nu te verwerken krijgen. Overweeg of de omvang van de faciliteiten nog past bij het huidige gebruik, bijvoorbeeld in het aantal accounts, het aantal licenties of de benodigde bandbreedte.
- ***Voorbeeld*** Tref anti-DDoS-maatregelen op de toegangspunten van uw thuiswerkfaciliteiten. Een DDoS-aanval is eenvoudig uit te voeren. Als uw thuiswerkfaciliteiten hier niet mee om kunnen gaan, zal dit al snel tot beschikbaarheidsproblemen leiden. U vindt meer adviezen over anti-DDoS-maatregelen in de NCSC-factsheet 'Technische maatregelen voor de continuïteit van onlinediensten'.[3]

Richt alternatieven in voor thuiswerkfaciliteiten om kritieke processen te ondersteunen.

- ***Voorbeeld*** Richt een tweede toegangspunt in, op basis van software van een andere leverancier. Dit werkt vooral goed bij VPN-gebaseerde toegang, omdat het dataverkeer via het VPN in principe niet verschilt op basis van de onderliggende software. U kunt er bijvoorbeeld voor kiezen om medewerkers die betrokken zijn bij kritieke processen, alvast ook toegang te geven op basis van het tweede toegangspunt, zodat zij makkelijk kunnen omschakelen.
- ***Voorbeeld*** Sommige applicaties lenen zich ervoor om direct ontsloten te worden via het internet, dus buiten een eventueel portaal of VPN om. Als u hiervoor kiest, houd er dan rekening mee dat deze applicaties elk hun eigen kwetsbaarheden zullen bevatten, en dat deze nu voor een aanvaller gemakkelijker te bereiken zijn. Combineer deze maatregel daarom indien mogelijk met IP-whitelisting, zoals genoemd onder de aanvullende maatregelen voor bestaande thuiswerkfaciliteiten.
- ***Voorbeeld*** Zorg voor de mogelijkheid om kritieke processen in kleine teams op kantoor uit te voeren. Niet elk kritiek proces leent zich ervoor om door een thuiswerkende medewerker uit te laten voeren. Als u medewerkers alsnog naar kantoor laat komen, tref dan maatregelen om het risico op besmetting met COVID-19 te beperken. Stel verschillende teams samen, die elkaars werk in geval van nood kunnen overnemen. Overweeg of u hiervoor vooraf al roosters wilt opstellen, zodat medewerkers snel beschikbaar zijn. Houdt eventueel enkele medewerkers buiten de teams, om als reserve te fungeren. Zorg voor strikte fysieke scheiding tussen de teams. Tref noodzakelijke hygiënemaatregelen op kantoor om besmetting door collega's of via oppervlakken waar mogelijk te voorkomen.
- ***Voorbeeld*** Inventariseer de risico's van het gebruik van privévoorzieningen en adviseer medewerkers hierover. Sommige processen kunnen toch in stand blijven door over te schakelen op zulke alternatieve ICT-middelen. Denk hierbij aan populaire diensten voor bestanduitwisseling en privémail. Inventariseer de risico's als dit zou gebeuren, en weeg deze risico's af tegen de gevolgen van verstoring van uw proces. Stel duidelijke richtlijnen op voor het relatief veilig gebruik van dergelijke middelen. De NCSC-factsheet 'Kies een berichtenapp voor uw organisatie'[4] schetst deze aanpak in de context van berichtenapps. De adviezen zijn ook voor andere typen diensten te gebruiken.
- ***Voorbeeld*** Bereid een stappenplan en communicatie voor om te gebruiken wanneer thuiswerkfaciliteiten niet meer beschikbaar zijn. Sommige medewerkers zullen bijvoorbeeld niet meer kunnen werken. Draag hen op om het werk ook daadwerkelijk neer te leggen, zodat ze niet alsnog met privéfaciliteiten ad hoc samen gaan werken. Leg in het stappenplan ook vast hoe u zorgt voor de omschakeling naar eventuele alternatieve voorzieningen. Houd hierbij in gedachten dat sommige communicatiemiddelen op dat moment niet beschikbaar zullen zijn.

[3] Zie https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-technische-maatregelen-voor-continuiteit-van-online-diensten.
[4] Zie https://www.ncsc.nl/documenten/publicaties/2019/mei/01/kies-een-berichtenapp-voor-uw-organisatie.

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

FS-2020-02 | versie 1.0 | 1 april 2020

Aan deze informatie kunnen geen rechten worden ontleend.