Inventarisatie corona-gerelateerde informatiebeveiligingsrisico’s

De AFM heeft in april en mei 2020 risico gestuurd een inventarisatie uitgevoerd naar informatiebeveiligingsrisico’s onder 15 (middel)grote financiële ondernemingen en accountantsorganisaties. De aanleiding voor deze inventarisatie was de uitbraak van het coronavirus. De AFM is nagegaan in hoeverre de uitbraak van het coronavirus invloed heeft op de bedrijfsvoering van ondernemingen en hoe ondernemingen omgaan met verhoogde informatiebeveiligingsrisico’s als gevolg van het coronavirus.

Op basis van signalen en in overleg met De Nederlandsche Bank, is een zestal risico’s geïdentificeerd die om extra aandacht vragen van ondernemingen:

- Het risico op datalekken als gevolg van thuiswerken.
- Het risico dat IT-systemen van ondernemingen onveilig zijn door uitstel van de installatie van patches.
- Het risico dat de dienstverlening van ondernemingen vermindert door uitval van medewerkers (key person risk).
- Het risico dat de kwaliteit en continuïteit van de dienstverlening van (externe) service providers afneemt.
- Het risico dat cybercriminelen toegang krijgen tot systemen door phishingactiviteiten.
- Het risico dat ondernemingen slachtoffer worden van DDoS aanvallen.

De AFM heeft deze risico’s met de ondernemingen besproken en de opgedane inzichten zijn in deze bijlage te lezen. Hierbij formuleert de AFM per risico een aantal aandachtspunten waar ondernemingen op moeten letten, voor zowel tijdens de coronacrisis als de periode daarna.

Toename in thuiswerken vraagt om maatregelen op het gebied van informatiebeveiliging

In lijn met de oproep van de overheid werkt het overgrote deel van de medewerkers van de ondervraagde ondernemingen vanuit huis. Dit kan deze ondernemingen extra kwetsbaar maken voor informatiebeveiligingsrisico’s verbonden aan thuiswerken, zoals het lekken van gevoelige informatie door het gebruik van onveilige apparatuur of communicatiekanalen.

Om het proces van thuiswerken in goede banen te leiden maken ondernemingen gebruik van een VPN (Virtual Private Network) of andere beveiligde thuiswerkfaciliteiten. Hierbij is het van belang dat medewerkers worden geïnformeerd over het correcte gebruik van deze faciliteiten. Ook moet worden voorkomen dat medewerkers gebruik maken van niet-beveiligde (privé-)alternatieven.

Door de sterke toename van thuiswerken zijn ondernemingen afhankelijker geworden van de beschikbaarheid van thuiswerkfaciliteiten. De AFM roept de sector op om te anticiperen op deze afhankelijkheid door passende voorzorgsmaatregelen te treffen voor het geval dat de thuiswerkfaciliteiten (tijdelijk of gedeeltelijk) niet beschikbaar zijn[1].

Het risico op datalekken neemt toe bij het thuis printen van documenten met vertrouwelijke informatie. De AFM raadt ondernemingen aan om beleid te formuleren over thuis printen en toe te zien op de naleving daarvan door medewerkers. Uit de inventarisatie van de AFM blijkt dat een aantal ondernemingen hierbij ook kiest voor technische beheersmaatregelen zoals printerautorisatie.

[1] https://www.afm.nl/nl-nl/nieuws/2020/april/alertheid-financiele-sector-gevraagd-voor-cyberrisico-thuiswerken

Het uitstellen van de installatie van kritieke patches leidt tot verhoging van risico's

Security patches worden door ontwikkelaars van software beschikbaar gesteld om bepaalde beveiligingsrisico's, zogenaamde vulnerabilities, weg te nemen. Zolang de patch niet is geïnstalleerd, blijft het systeem kwetsbaar voor deze vulnerabilities. Het niet of niet tijdig patchen van systemen is een van de belangrijkste oorzaken waardoor aanvallers systemen kunnen binnendringen.

De ondernemingen die de AFM tijdens de inventarisatie heeft gesproken, zijn over het algemeen in staat om kritieke patches voor IT-systemen tijdig te installeren. In een aantal gevallen geven ondernemingen aan dat sommige change-initiatieven zijn uitgesteld of dat bepaalde niet-functionele updates niet direct worden geïnstalleerd. Hierbij geven ondernemingen aan dat IT-beheeractiviteiten op dit moment prioriteit krijgen of dat zij bepaalde changes door afhankelijkheden van (externe) ketenpartners te risicovol vinden om op dit moment door te voeren.

De AFM wil aan ondernemingen meegeven dat de installatie van security patches tijdens en na de coronacrisis prioriteit binnen ondernemingen zou moeten krijgen. De AFM raadt aan om security patches zo snel mogelijk na de vrijgave ervan te installeren. Hiermee verminderen ondernemingen de kwetsbaarheid voor dreigingen.

Kleinere ondernemingen extra vatbaar voor key person risk

Als gevolg van de uitbraak van het coronavirus neemt key person risk toe door uitval van medewerkers of door toenemende verantwoordelijkheden van medewerkers in hun thuissituatie. Bij kleinere ondernemingen lijkt key person risk relatief grote gevolgen voor de bedrijfsvoering te kunnen hebben. Kleinere ondernemingen hebben minder schaal en daardoor mogelijk een grotere afhankelijkheid van enkele personen of functies binnen de onderneming.

De AFM ziet dat ondernemingen verschillende maatregelen treffen om key person risk tijdens de coronacrisis te verminderen. Wat nagenoeg alle ondernemingen hebben gedaan, is een onderscheid maken tussen kritieke en niet-kritieke functies. Sommige ondernemingen hebben dit gedaan als gevolg van de uitbraak van het coronavirus, voor een aantal andere ondernemingen maakt het onderscheid tussen kritieke en niet-kritieke functies deel uit van het reguliere risk management framework. Onder de kritieke functies binnen de reikwijdte van deze inventarisatie vallen onder meer functies zoals IT-helpdesk en medewerkers die door hun functie fysieke toegang tot IT-infrastructuur nodig hebben.

Veel ondernemingen kiezen binnen hun kritieke functies voor het verspreiden van medewerkers. In een aantal gevallen wordt gewerkt met verschillende varianten van A/B-teams waarbij een deel van het team op de kantoorlocatie werkt en het andere deel thuis. Ook zijn er ondernemingen die hun medewerkers over verschillende locaties binnen Nederland hebben verspreid.

Daarnaast kiezen veel ondernemingen er ook voor om extra aandacht te geven aan het opvangen van mogelijke uitval van individuele medewerkers. In een aantal gevallen wordt er actief opvolging gegeven aan kennisoverdracht tussen medewerkers en sommige ondernemingen kiezen ervoor om (tijdelijk) extra autorisatie-rechten toe te kennen aan medewerkers zodat kritieke processen doorgang kunnen blijven vinden. Ook hebben sommige ondernemingen contact gezocht met partners die op korte termijn gespecialiseerd personeel kunnen leveren om uitval van medewerkers op te vangen.

De AFM raadt ondernemingen aan om periodiek een risicoanalyse uit te voeren om kritieke functies of personen in de organisatie te identificeren en maatregelen te treffen om de afhankelijkheid van deze functies of personen te verminderen.

Service providers vragen doorlopend om aandacht

Uit de inventarisatie van de AFM blijkt dat (externe) service providers in veel gevallen in staat zijn om ondanks de uitbraak van het coronavirus hun diensten te leveren. Sommige ondernemingen geven aan dat service providers minder snel reageren op niet-urgente verzoeken dan gebruikelijk. Uit de gesprekken met de ondernemingen is niet gebleken dat er kritieke processen onder druk zijn komen te staan als gevolg van problemen bij service providers. Toch blijft de AFM vragen om waakzaamheid van ondernemingen omdat de afhankelijkheid van service providers is toegenomen.

Ondernemingen kiezen er steeds vaker voor om delen van hun dienstverlening uit te besteden. Bij uitbesteding blijven ondernemingen onverminderd verantwoordelijk voor de kwaliteit van hun dienstverlening. Dit betekent onder meer dat ondernemingen moeten toezien op de kwaliteit van de beheersmaatregelen rond informatiebeveiliging die de service provider heeft getroffen. De AFM geeft ondernemingen mee dat het noodzakelijk is om de dienstverlening van de service provider te monitoren en regelmatig contact te hebben met de service provider over de geleverde diensten. Dit is van belang tijdens de periode waarin maatregelen rond het coronavirus van kracht zijn, maar zeker ook daarna.

Cybercriminelen spelen in op informatiebehoefte over het coronavirus

Een aantal van de ondernemingen die de AFM heeft gesproken, ervaart een toename in phishing activiteiten. Phishing is een aanvalstechniek van cybercriminelen die erop is gericht om het slachtoffer te verleiden tot (onbewust) schadelijk gedrag, zoals het installeren van malafide software. Hierbij wordt vaak gebruik gemaakt van e-mail. Sinds het uitbreken van het virus gebruiken cybercriminelen het coronavirus vaak als thema voor phishing e-mails in hoop dat de geadresseerde zich laat verleiden door zijn nieuwsgierigheid naar het onderwerp.

Veel ondernemingen hebben technische beheersmaatregelen zoals e-mailfilters ingericht om te voorkomen dat phishingberichten hun medewerkers bereiken. Ondanks deze maatregelen slagen cybercrimelen er in sommige gevallen toch in om medewerkers te bereiken. Daarom kiezen de meeste ondernemingen ervoor om naast technische beheersmaatregelen ook organisatorische beheersmaatregelen in te richten.

Om medewerkers bewust te maken van de risico's omtrent phishing hebben ondernemingen sinds het uitbreken van het coronavirus diverse awareness programma's geïnitieerd. Deze programma's zijn erop gericht om medewerkers in staat te stellen phishing te herkennen en op een veilige manier af te wenden. Ook zijn er enkele ondernemingen die zelf phishing aanvallen simuleren om (op een veilige manier) te toetsen hoe medewerkers reageren op dergelijke situaties. De AFM is positief over dergelijke initiatieven, maar wijst op het belang van een werkomgeving waarin medewerkers zich veilig voelen om incidenten te melden.

Verhoogde alertheid op DDoS aanvallen

Cybercriminelen kunnen ook gebruik maken van Distributed Denial-of-Service (DDoS) aanvallen om ondernemingen te ontregelen. Bij een DDoS aanval proberen aanvallers de capaciteit van online diensten, servers of netwerkapparatuur te ontregelen. Als gevolg hiervan kan de beschikbaarheid van diensten voor medewerkers of klanten in het geding komen.

De meeste ondernemingen hebben geen significante toename geobserveerd in het aantal DDoS aanvallen sinds de uitbraak van het coronavirus. Wel zijn ondernemingen extra alert op dit risico, omdat de potentiële impact groter is door de toegenomen afhankelijkheid van systemen sinds de uitbraak van het virus. De AFM verwacht van ondernemingen dat zij passende maatregelen treffen om het risico van DDoS aanvallen te beheersen.