Amsterdam – 17 april 2020

Probability snapshot

Cybersecurity tijdens en na de coronacrisis

Beste lezer,

Met deze snapshot geven we u inzicht in de risico's en mogelijke beheersing van ICT- en cyberrisico's rondom de situatie die is ontstaan na het uitbreken van het COVID-19 virus en een vooruitblik van deze risico's in het nieuwe normaal. Deze snapshot is voornamelijk gebaseerd op werk dat we de afgelopen tijd hebben gedaan voor en met onze klanten. We beschrijven trends op hoofdlijnen en geven een beeld van onze observaties en aandachtpunten. We geven hierin geen volledig advies, omdat dat instelling-specifiek is en er niet een *one size fits all* oplossing is.

Heeft u hierover vragen of zou u dieper over dit onderwerp in gesprek willen gaan, dan nodigen wij u van harte uit om contact op te nemen met een van onze ICT & Security consultants voor een vrijblijvend gesprek.

Met vriendelijke groet,

Team Risk Management

Probability & Partners

Inleiding

Inmiddels zijn de meesten gewend geraakt aan ‘het nieuwe normaal’ waarbij veel mensen vanuit huis werken. Organisaties zijn de laatste weken creatief geweest bij de invoering van allerlei ICT-toepassingen om dit versneld mogelijk te maken.

Vanuit dit oogpunt heeft de huidige crisis tot een versnelling van de al bestaande trend geleid waarbij werknemers meer en meer op afstand gaan werken. Ook na deze crisis zullen veel van de geïmplementeerde ICT-toepassingen daarom waarschijnlijk in gebruik blijven.

Tijd om ook goed naar de (cyber)risico’s te kijken!

Door de versnelde invoering van ICT-toepassingen en nieuwe manieren van werken met meer digitaal dataverkeer zien we de volgende (bestaande) ICT-/cyberrisico’s versterkt worden:

- Datalekken: informatie wordt ‘gestolen’ of verloren waardoor gevoelige gegevens (met name persoonsgegevens van bijvoorbeeld deelnemers) ‘op straat’ komen te liggen. Dit schaadt het vertrouwen in en de reputatie van het pensioenfonds.
- U kunt niet meer bij de eigen gegevens als gevolg van ransomware, waardoor kritieke processen mogelijk niet meer uitgevoerd kunnen worden. Denk hierbij aan pensioenuitbetaling, salarisbetalingen en processen rondom het vermogensbeheer.
- Ongeautoriseerde wijzigingen in systemen waardoor de datakwaliteit niet meer is geborgd. Dit kan leiden tot bijvoorbeeld onjuiste aanspraken en/of pensioenuitbetalingen.
- Verder in de keten neemt ook het risico op bijvoorbeeld diefstal van pensioenvermogen toe door inbraak of valse orders bij vermogensbeheerders.
- Onterechte betalingen als gevolg van zogenoemde ‘CEO-fraude’.

In deze snapshot lichten wij toe welke ontwikkelingen wij zien die situaties creëren waardoor deze risico’s actueler worden dan pre-corona het geval was.

U als bestuurder blijft daarvoor verantwoordelijk, en de schade is voor het pensioenfonds. Reputatieschade door een datalek lost u immers niet op met bijvoorbeeld een verzekering. Het is verstandig om de bestuurdersaansprakelijkheidsverzekering en een eventuele cyberverzekering hierop na te lopen.

Ontwikkelingen

Bij onze klanten en relaties zien wij de volgende ontwikkelingen die impact kunnen hebben op het risicoprofiel van uw fonds. Doordat uw fonds onderdeel is van een of meerdere ketens neemt de complexiteit en de impact hiervan toe.

Meer en meer elektronische communicatie, zoals online (video-)vergaderen en bestandsdeling

Bij de meeste fondsen zijn op een zeker moment noodprocedures en business continuity plannen inwerking gesteld. Niet alleen voor het fonds zelf, maar ook verder in de keten. Denk daarbij onder andere aan uw fiduciair, custodian, vermogensbeheerders, IT-leveranciers, pensioenadministrateur, bruto/netto-verwerking en alle onderuitbesteders waarvan die organisaties gebruikmaken (kantoorautomatisering, datacenters, externe inhuur). Thuiswerken is normaal geworden en zal dit waarschijnlijk ook blijven. Mensen zien elkaar minder vaak fysiek. Daardoor wordt gebruik gemaakt van verschillende soorten ICT-toepassingen (tools).

Onveilige situaties die hierdoor toenemen zijn:

- Veel van de aangeboden tools voldoen niet aan de beveiligingseisen die hiervoor gewenst zijn, of zoals gesteld vanuit de regelgeving en toezichthouders. Met name gratis tools hebben vaak veel gebreken.
- Er is een kans dat bepaalde tools code bevatten (‘malicious code’) die gegevens verzamelen voor andere doeleinden en eventueel gebruikmaken van zwakheden in de beveiliging om ongeautoriseerde toegang tot vertrouwelijke gegevens mogelijk te maken.
- Inbreken / afluisteren van gesprekken en het onderscheppen van vertrouwelijke gegevens is daarbij een reëel risico en zeker als het er sprake is van persoonsgegevens kan dit een grote impact hebben.

Sterke toename van het aantal cyberaanvallen: criminelen zitten niet stil

Kwaadwillenden hebben zich ook aan de nieuwe situatie aangepast en zien nieuwe kansen. Dit blijkt onder andere uit de stijging van het aantal cyberaanvallen en de manier waarop gebruik gemaakt wordt van de nieuwheid en onzekerheid die de huidige situatie voor mensen en organisaties met zich meebrengt (bron: Digital Trust Center ministerie van EZK). Als inbraak of schade bij uw eigen organisatie nog niet erg genoeg is, denk eraan wat de impact is als dit zich verder in de keten voordoet. Bijvoorbeeld als er ongeautoriseerde toegang is tot uw gegevens bij de custodian waardoor uw stukken niet meer op uw naam staan, bij een vermogensbeheerder waardoor er oneigenlijke transacties worden gedaan, bij uw administrateur waardoor aanspraken of uitbetalingen onjuist zijn, of als bij een datacenter iemand (ongeautoriseerd) met een USB-stick bij ‘uw’ servers kan en gevoelige informatie kan kopiëren. Allemaal voorbeelden van zaken die binnen de keten kunnen gebeuren. U blijft daarvoor verantwoordelijk, en de schade is voor het pensioenfonds. Reputatieschade door een datalek lost u immers niet op met bijvoorbeeld een verzekering.

Onveilige situaties die hierdoor toenemen zijn:

- Door minder oplettendheid en het feit dat mensen nu meer berichten van onbekende / minder bekende bronnen krijgen is de kans groter dat mensen reageren op phishing mails / links en gevoelige informatie delen met ongeautoriseerde derden.
- De kans dat een medewerker in een mail trapt van een kwaadwillende die zich voordoet als een hoge functionaris uit de organisatie (‘CEO fraude’) neemt hierdoor toe.
- Veel nieuwe (en bestaande) technologieën kunnen misbruikt worden om (ongewild) kwaadwillende software zoals gijzelsoftware (‘ransomware’) binnen te halen.

Bewustzijn bij de medewerkers/eindgebruiker

Medewerkers en andere betrokkenen van fonds moeten wennen aan de nieuwe toepassingen en de afstand tot de organisatie. Er is een sterke behoefte aan informatie en dit leidt vaak tot een lager bewustzijn als het om de risico’s gaat en verhoogt de kans op onveilige situaties.

Onveilige situaties die hierdoor toenemen zijn:

- Medewerkers zijn zich mogelijk minder bewust van de toenemende beveiligingsrisico’s.
- Ze weten vaak niet goed aan welke regels zij zich dienen te houden ten aanzien van het delen van vertrouwelijke informatie.
- Een wildgroei aan tools en oplossingen maakt de kans groter dat medewerkers informatie verder delen dan bedoelt.
- Het gebruik van ‘eigen’ ICT-apparatuur (tablet, laptop, etc.) met kwetsbaarheden neemt toe.

Terug naar de basis

Als onderdeel van de werkwijze (noodprocedure) die het fonds hanteert is het van belang dat er geen ruis is over wie in de organisatie beslissingsbevoegd is en hoe besluitvorming verloopt.

De invoering van nieuwe ICT-toepassingen ter ondersteuning van het werken op afstand dient vanuit het ICT- en privacybeleid en de bijbehorende gegevensclassificatie (de BIA-scores) bezien te worden. Nieuwe ICT-toepassingen dienen aan dezelfde beveiligingseisen te voldoen als de bestaande ICT-middelen waarbij ook compliance aan wet- en regelgeving en met name de AVG van belang is. Naleving van deze interne en externe regels voortkomt een wildgroei van nieuwe toepassingen en onveilige situaties.

Voor de medewerker is belangrijk dat het duidelijk is aan welke regels en voorschriften hij/zij zich dient te houden als het om gebruik van nieuwe en bestaande ICT-toepassingen gaat. Stel daarom ook online 'etiquette'-afspraken vast die gevolgd dienen te worden (o.a. autoriseren van toegang, check van genodigden, afspraken omtrent het opnemen van gesprekken, welke informatie mag wel/niet getoond worden tijdens een videocall, etc.).

Bij gebruik van 'eigen' ICT-apparatuur zijn onder andere de volgende zaken aanvullend van belang:

- Een recente versie van het besturingssysteem (OS) met support van de fabrikant is geïnstalleerd.
- Daarbij zijn geactiveerd: automatische updates, hardware versleuteling/encryptie en de wachtwoordbeveiliging (met voldoende complexiteit).
- Daarnaast dient gebruik gemaakt te worden van up-to-date bescherming tegen malware (virussen, spyware, adware & andere malicious software).

Dit geldt voor de hele keten, met alle onderuitbesteders die daarbij komen kijken. En blijf u ervan bewust dat dit soort risico's moeilijk afdoende te verzekeren zijn. Controleer daarom uw aansprakelijjkheidsverzekering(en) hierop.

Conclusies

De benoemde ontwikkelingen laten een duidelijke toename van het ICT-, informatiebeveiliging- en cyberrisico voor fondsen zien, zowel in de eigen organisatie als verder in de keten.

De huidige situatie vraagt om heldere afspraken, werkwijze en besluitvorming waarbij de bestaande beleidsregels die uw fonds heeft vastgesteld ook gelden voor nieuwe toepassingen die in gebruik worden en zijn genomen. Op deze wijze kan de meeste zekerheid gegeven worden dat (cyber)risico's beheerst zijn en compliance aan wet- en regelgeving geborgd is.

Dus geen paniek, maar bewaar de rust. Bij vragen adviseren wij u graag verder. Ook als zaken onverhoeds toch mislopen. Mocht u behoefte hebben aan een korte gedachtewisseling dan kunt u contact opnemen met onze consultants:

Jeroen Kinders Vroklage

Risk management consultant
jeroen.kindersvroklage@probability.nl
06 - 51 55 66 53

Renze Munnik

Risk management consultant
renze.munnik@probability.nl
06 - 19 28 06 28

Pim Poppe

Managing partner
pim.poppe@probability.nl
06 - 19 88 34 71