Cyberrisico’s en de uitbraak van het coronavirus

Door de bezorgdheid over de verspreiding van het coronavirus is thuiswerken nog nooit zo bespreekbaar geweest. In deze risicowaarschuwing benoemen wij een aantal praktische maatregelen die organisaties kunnen nemen om ook tijdens een dergelijke crisis cyberweerbaar te blijven.

De uitbraak van COVID-19 heeft geleid tot een aanzienlijke ontwrichting bij bedrijven en tot een zekere mate van bezorgdheid bij veel werknemers. Bedrijven in Azië en over de hele wereld hebben noodplannen voor de borging van de bedrijfscontinuïteit in werking gesteld en hebben medewerkers toegestaan of opgedragen thuis te werken om zo de verspreiding van het virus te helpen tegen gaan. In een nieuwe realiteit waarin miljoenen mensen op afstand werken, zijn beveiligde cyber-verbindingen en een veilige manier van werken extra belangrijk. Aon raadt bedrijven aan de volgende maatregelen te nemen om duurzaam operationeel te blijven en veilig te werken.

• Wees alert op phishing aanvallen

Kwaadwillenden zullen inspelen op de enorme aandacht voor het virus en de bijbehorende angst en paniek. Beveiligingsonderzoekers hebben al geconstateerd dat er (soms sterk gerichte) phishing berichten worden gestuurd met waarschuwingen over COVID-19. Deze e-mails bevatten doorgaans schijnbaar nuttige informatie, links en/of bijlagen over de virus uitbraak of updates over hoe ontvangers veilig kunnen blijven. Vanuit bezorgdheid en of nieuwsgierigheid worden cyberrisico’s over het hoofd gezien en wordt een phishinglink aangeklikt of document met malware geopend.

Organisaties wordt sterk aangeraden hun medewerkers hiervan extra bewust maken en te waarschuwen dat criminelen juist nu hun slag proberen te slaan. Medewerkers moeten de oorsprong van berichten goed controleren vooraleer e-mails te openen of op links of bijlagen te klikken. Dit bewustzijn kan worden vergroot en tegelijk worden getest door een phishing-campagne te simuleren. Ook op vlak van cybersecurity kunnen maatregelen worden getroffen tegen phishing aanvallen door gebruik te maken van up-to-date antivirus, email bescherming en monitoringtools te gebruiken.

• Test werking en capaciteit van systemen

Wanneer mensen massaal gaan thuiswerken, krijgen organisaties te maken met een ongekende hoeveelheid verkeer die vanaf afstand toegang zoekt tot het bedrijfsnetwerk. Bedrijven met een flexibel thuiswerk beleid hebben zich al wat beter voorbereid op dit soort situaties en hebben de middelen om de netwerkintegriteit te handhaven via versleutelde VPN-verbindingen op basis van multifactor-authenticatie. We raden bedrijven aan om hun IT/cybersecurityteams extra te laten monitoren op aanvallen via thuiswerkers, aangezien de computers van medewerkers vaak een zwakke schakel vormen waarmee aanvallers al te gemakkelijk toegang krijgen tot bedrijfsdata en -systemen. Het uitrollen van de meest recente patches (zoals bijvoorbeeld op Citrix systemen) is daarbij uiteraard ook van groot belang.

Voor bedrijven die minder ervaring hebben met thuiswerken, is COVID-19 een uitdaging. Het risico bestaat dat door het toegenomen volume aan netwerkverkeer de IT-systemen en -medewerkers overbelast raken ofwel dat werknemers via onvoldoende beveiligde netwerken of apparaten toegang krijgen tot gevoelige gegevens en systemen. We raden deze organisaties aan om zo snel mogelijk de normen voor werken op afstand en BYOD (Bring-Your-Own-Device) te implementeren en monitoring te verscherpen. Daarnaast moeten bedrijven hun VPN systemen tijdig patchen (een gemiste patch voor PulseSecure VPN van april 2019 bijvoorbeeld, leidde in december bij veel organisaties tot ransomware) en hun netwerken testen om zeker te zijn dat alle systemen het toegenomen verkeer kunnen verwerken.

• Wees voorbereid op disruptie

Door thuiswerken kost het IT meer moeite om cyberdreigingen te signaleren en in de kiem te smoren. Wanneer een bedreiging wordt gedetecteerd in een bedrijfsnetwerk, dan kan IT het apparaat nog vrij

gemakkelijk in quarantaine plaatsen en het in beslag nemen voor onderzoek. In het geval van thuiswerk is dit minder gemakkelijk en zijn de consequenties al snel groter omdat veel kostbare tijd verloren kan gaan bij het fysiek moeten aanpakken bij de bron. Indien laptops en andere apparaten van de juiste (EDR) software zijn voorzien, dan kunnen deze ook op afstand in quarantaine worden geplaatst en geanalyseerd waardoor het netwerk beter kan worden beschermd tegen cyberaanvallen.

Aangezien het ontstaan alsmede de impact van cyberrisico's niet alleen technisch zijn, moeten organisaties verder uitgaan van een bedrijfsbrede risicoaanpak (ERM). Hierbij heeft bijvoorbeeld de simulatie van een crisissituatie toegevoegde waarde om de bedrijfscontinuïteitsplannen (BCM) en de reactie van het senior management te testen en te trainen. In geval van cyberscenario's als ransomware, pandemieën of combinaties ervan, met alle bijbehorende gevolgen voor automatisering, connectiviteit en cyberbestendigheid maakt deze ervaring al snel het verschil tussen erop of eronder.

Bedrijven kunnen zich ook beschermen tegen dit soort risico's op digitale disruptie door middel van een goede cyberverzekering. Als systemen bijvoorbeeld uitvallen, kan een cyberverzekering dekking bieden voor verliezen door bedrijfsonderbreking en de kosten voor forensisch onderzoek en herstel door technisch experts. COVID-19 stelt bedrijven voor een reeks uitdagingen, maar door de technologische ontwikkelingen sinds de SARS-uitbraak zijn bedrijven in staat operationeel en flexibel te blijven in tijden van onzekerheid. Verlies daarbij de voortdurende cyberbedreiging echter niet uit het oog!