Technische vragen

Van : PvdA Max de Groot
Datum vraag : 16-5-2022
Onderwerp : Vragen t.a.v. gemeenschappelijke regelingen
Commissiegriffier :
Datum antwoord :

Vragen:

T.a.v. **ODMH**

1. “Ten aanzien van ICT-risico’s zijn diverse maatregelen getroffen om die te verkleinen. Die maatregelen betreffen met name de back-up en de beveiliging van alle systemen. De uitgevoerde actualisatie van de risico-inventarisatie leidt daarom tot een kleiner totaal aan risico’s dan in voorgaand jaar. Ook het gewenste weerstandsvermogen is daarom afgenomen ten opzichte van vorig jaar.”

   Kunt u aangeven welke maatregelen u heeft getroffen om uw systemen te beveiligen en met name hacken/ransomware te voorkomen?

   Antwoord:
   De beveiliging bij de ODMH is dusdanig opgezet dat het reactief acteren tot een minimum wordt beperkt.
   De bij de ODMH in beheer zijnde gegevens worden intern veilig gesteld middels meerdere back-ups. Een serie van deze back-ups wordt extern in een kluis opgeslagen.
   De toegang tot de interne servers is beveiligd middels een firewall constructie. Deze wordt op dit moment geheel vernieuwd. Dit heeft alles te maken met de inrichting van een colocatie. Deze locatie welke zich bevindt in een datacenter in Rotterdam zal een spiegel zijn van de locatie aan de Thorbeckelaan. Als om welke reden dan ook de hoofdlocatie niet benaderbaar is wordt er direct omgeschakeld naar de colocatie. Ook deze locatie wordt beveiligd middels een firewall.
   Daarnaast richt de ODMH een firewall in voor data die in de Cloud wordt opgeslagen. De firewalls zijn altijd voorzien van het antwoord op de laatst bekende bedreigingen. Daarnaast zijn er protocollen die altijd in werking zijn, zoals encryptie, deep pakket inspection (tegen ransomware).
   Ook wordt er gebruik gemaakt van deep learning, een techniek waarbij de firewalls leren van aanvallen en deze in een centrale database met elkaar delen. Hierdoor kan elke firewall direct worden voorzien van beveiliging tegen zich voordoende bedreigingen. Daarnaast wordt er uiteraard constant gekeken naar het dataverkeer waardoor risico's in een vroeg stadium kunnen worden onderkend en geïsoleerd.
   Op lokaal niveau, dus bij de gebruiker, zijn verschillende beveiligingsprotocollen in werking.

	Geen enkel bedrijf kan claimen 100% veilig en niet gevoelig te zijn voor bedreigingen van buitenaf. Je kunt je er wel 100% tegen wapenen en dat is wat de ODMH heeft gedaan en pro actief doet.
Antwoorden:	