NOTITIE

Risico-inventarisatie 2018
30 oktober 2018

Risicofactor	Beheersmaatregelen
De Personal Computers en/of servers worden geïnfecteerd met een virus.	Op Personal Computers en servers antivirus geïnstalleerd die elk uur wordt bijgewerkt als er definities uit zijn gekomen. Pc's en servers staan in beheer tooling van beherende partij voor 24 uurs monitoring. Meer thin clients (domme pc's) ingezet en gebruik van Pc's en laptops is sterk afgenomen.
Nieuwe virussen en andere beveiligingsrisico's die via internet of een netwerk worden verspreid.	Windows automatische updateservice. Microsoft (MS)Windows versies inclusief Internet Explorer van Servers en Personal Computers worden automatisch bijgewerkt met de meest recente updates.
Ongeautoriseerde processen starten in de gebruikersomgeving.	RES Workspace manager. Met een extra beheers-schil worden ongeautoriseerde processen verhinderd te starten in de gebruikersomgeving op servers.
Criminaliteit gericht op het ongeautoriseerd verrichten van betalingen ten laste van de opdrachtgever.	Het BNG-betalingsverkeer loopt via MS Internet Explorer. De gebruiker logt in via credentials en een wachtwoord naar de maatstaven van BNG. Voor het betalen zelf zijn twee verschillende gebruikers benodigd.
Onttrekken van persoonsgegevens	Persoonsgegevens en andere vertrouwelijke gegevens worden door dezelfde eerdergenoemde middelen beschermd.
Onttrekken van privacy gevoelige informatie op het gebied van persoonsgegevens (bijvoorbeeld medische informatie).	Deze informatie wordt decentraal beheerd door een gespecialiseerde partij (Iron Mountain).
Criminaliteit gericht op het verwerven van bijvoorbeeld strategische en commerciële gegevens.	Gezien de aard van onze business, rechtsvorm en omgeving is dit niet aan de orde bij WNK. WNK staat voor open en transparant. Hiernaast valt WNK ook onder de Wet openbaarheid van bestuur (Wob), waardoor deze informatie opvraagbaar is.

Voorgesteld wordt om de notitie vast te stellen.