Zuidelijke Rekenkamer

Startnotitie Informatieveiligheid van de provincies Limburg en Noord-Brabant

1. Inleiding

De ruggengraat van elke organisatie is de informatie waar zij over beschikt. Het is belangrijk dat die informatie veilig is. Onder veiligheid van informatie wordt verstaan dat deze vertrouwelijk (exclusief), betrouwbaar (integer) en beschikbaar is. De Zuidelijke Rekenkamer heeft de afgelopen jaren geregeld conclusies getrokken over de betrouwbaarheid en beschikbaarheid van de provinciale informatie. Relatief onderbelicht is de vertrouwelijkheid ervan.
De provincie beschikt over veel informatie waarvan het niet de bedoeling is dat deze zonder meer op straat komt te liggen. Te denken valt aan bedrijfseconomische gegevens van de provincie zelf, persoonsgegevens van haar medewerkers, en gegevens van bedrijven en organisaties waar de provincie een financiële binding mee heeft. Daarnaast is het niet de bedoeling dat derden onbevoegd toegang hebben tot de informatiesystemen van de provincie en zo het geheugen van de organisatie kunnen herschrijven of de voortgang van lopende projecten beïnvloeden.
Inbreuken kunnen leiden tot financiële en/of materiële schade en tot reputatieschade voor de provincie. Afgelopen jaar zijn ook in Nederland veel organisaties het slachtoffer geworden van cyberaanvallen en hacktivism. Voorbeelden hiervan zijn de gijzelingssoftware WannaCry, die computers onbruikbaar maakte, en de wereldwijde hack die een maand later weer voor enorm veel schade zorgde.
Informatieveiligheid richt zich op de beheersing van bovenstaande risico's.
De Zuidelijke Rekenkamer onderzoekt de informatieveiligheid van de provincies Limburg en Noord-Brabant.

2. Doelstelling en vraagstelling

De Zuidelijke Rekenkamer wil met haar onderzoek aanbevelingen doen die bijdragen aan een verbetering van de informatieveiligheid van de provincies Limburg en Noord-Brabant, door op zoek te gaan naar kwetsbaarheden in de verdediging van de vertrouwelijkheid van de informatie waar de provincie over beschikt.
De centrale vraag van het onderzoek is welke kwetsbaarheden de beveiliging van de vertrouwelijkheid van de informatie van de provincies kent. We onderzoeken daartoe enerzijds de mate waarin het *systeem* voor onbevoegden toegankelijk is en anderzijds de mate waarin de *medewerkers* handelen op een manier die de informatieveiligheid bewaakt. Daarnaast beschrijven we het *beleid* en de *organisatie* van de informatiebeveiliging.

a. Het systeem: penetratietesten

Er zijn ten minste drie manieren om in het informatiesysteem van de provincie te komen. Alle drie worden getest.
Externe toegankelijkheid. Bij beide provincies is het voor medewerkers mogelijk om vanuit thuis of een andere locatie in te loggen op het netwerk. Kunnen kwaadwillenden ook op afstand in de informatiesystemen van de provincie komen?
Interne kwetsbaarheden. Wat zijn de gevolgen van een aanval op het systeem vanaf het eigen netwerk van de provincie, bijvoorbeeld door medewerkers met slechte bedoelingen of hackers die zich toegang hebben verschaft tot het interne netwerk? Welke interne barrières zijn er ter bescherming van de vertrouwelijkheid van de gegevens?
Wi-Fi. Beide provincies hebben een Wi-Fi-netwerk voor medewerkers en een Wi-Fi-netwerk voor gasten. Hoe stevig is de beveiliging tussen intern en extern?

b. Het gedrag: Social engineering

De mens is doorgaans de zwakste schakel van elk beveiligingssysteem. Er zijn verschillende manieren om te testen hoe sterk het veiligheidsbewustzijn van de provinciemedewerkers is, en in welke mate er in dit opzicht juist wordt gehandeld.
Phishing. Dit is een manier om, meestal via e-mail, in één keer bij een grote groep mensen te proberen om ze naar een site te lokken en te verleiden om daar inloggegevens in te voeren. Vaak wordt daarbij gebruik gemaakt van URL-spoofing: het nabootsen van het adres van bijvoorbeeld een bank. Herkennen medewerkers deze mails en gaan ze er goed mee om?
Spear phishing. Hier wordt geen sleepnettechniek gebruikt, maar ontvangt een select aantal medewerkers een gepersonaliseerde boodschap. Hier staan bijvoorbeeld concrete namen, e-mailadressen en telefoonnummers in. Ook hier wordt geprobeerd om controle te krijgen over het persoonlijke account of de computer van het slachtoffer. Herkennen de medewerkers *spear phishing* als het ze overkomt?
Oplettendheid. Provinciehuizen zijn openbare gebouwen waar iedereen naar binnen moet kunnen, maar niet overal bij moet kunnen. In een *inlooptest* wordt gekeken in hoeverre onbevoegden zich fysieke toegang kunnen verschaffen tot het provinciehuis en welke informatie ze daarbij kunnen vinden.

c. De organisatie: taakverdeling en verantwoording

In dit derde deel van het onderzoek brengen we in kaart in hoeverre de provincie de sturing op, de beheersing van en de verantwoordelijkheid voor informatieveiligheid goed heeft verankerd. Ook kijken we op welke wijze Provinciale Staten worden geïnformeerd over informatieveiligheid.

3. Looptijd en publicatie van het onderzoek

De Zuidelijke Rekenkamer is haar onderzoek gestart medio 2017. Om de testfase van het onderzoek zo effectief mogelijk te kunnen uitvoeren (inclusief een ‘verrassingseffect’), hebben wij het onderzoek niet aangekondigd, en niet in ons Werkprogramma 2017 opgenomen.
In beide provincies hebben we de commissaris van de Koning/gouverneur en de provinciesecretaris/algemeen directeur wel vertrouwelijk vooraf op de hoogte gesteld.

We verwachten de resultaten van ons onderzoek begin 2018 te publiceren.