Quarant verbindt mens en informatie | Solvinity

Informatiebeveiliging onderzoeksrapport

Met concrete adviezen voor gemeenten

> *Informatieveiligheid begint met te beseffen welke risico's je loopt.*

Inhoud

Onderkennen gemeenten de risico's van cyberaanvallen

42% van de gemeenten denkt niet opgewassen te zijn tegen cybercriminelen. Is dat een schrikbarend hoog percentage of getuigt dit juist van realisme? Want heeft die andere 58% de beveiliging echt op en top in orde? Of schatten die gemeenten hun weerbaarheid te hoog in? Bijvoorbeeld omdat dit, ondanks alle alarmerende voorbeelden van datadiefstal, ransomware en dergelijke, gevoelsmatig toch iets blijft dat vooral anderen overkomt?

De eigen mening van gemeenten

Dit zijn enkele van de vragen die naar boven komen als je kijkt naar de resultaten van dit onderzoek over informatiebeveiliging bij gemeenten. Dit rapport is tot stand gekomen in samenwerking met Solvinity. Als Secure Managed IT Service Provider zijn security en compliance randvoorwaarden bij al wat Solvinity doet voor zijn klanten. Quarant, hét onafhankelijke adviesbureau voor de lokale overheid, helpt gemeenten onder andere bij de bewustwording en organisatie van informatiebeveiliging. Onze organisaties vinden elkaar in de aandacht voor de mens bij nieuwe ontwikkelingen die op organisaties afkomen.

De deelnemers zijn afkomstig van 30 gemeenten, variërend van organisaties met minder dan 50 medewerkers tot meer dan 1000. We vroegen hen of ze denken dat hun organisatie cyberaanvallen kan weerstaan. Wat ze doen op het gebied van mens, techniek en organisatie om de informatieveiligheid te vergroten. En wat ze als de grootste bedreigingen zien.

Vergelijking met het gemiddelde in Nederland

Hiermee geeft deze survey een interessant inkijkje in hoe gemeenten zelf vinden dat de informatieveiligheid er in hun organisatie voor staat. Waar dat zinnig is, vergelijken we de uitkomsten met het Solvinity Security Awareness Onderzoek uit 2020. Daar deden meer dan 500 IT-verantwoordelijken van Nederlandse bedrijven met 200 medewerkers en meer aan mee. Zo krijgen we op belangrijke punten ook een idee waar de uitkomsten bij gemeenten afwijken van het gemiddelde in Nederland.

> *"42% van de gemeenten denkt niet opgewassen te zijn tegen cybercriminelen.*

Doen gemeenten het slechter dan gemiddeld of zijn ze realistischer?

We hebben gelijk een opvallend cijfer voor je. In het onderzoek uit 2020 gaf 70% van de deelnemers aan te verwachten dat ze cybercriminelen kunnen weerstaan. Dit percentage is bij gemeenten nu dus lager (58%). Betekent dit dat het bij gemeenten slechter is gesteld met informatieveiligheid dan gemiddeld in Nederland? Misschien. Maar dat hoeft niet. Het zou ook kunnen dat gemeenten een stuk realistischer zijn, bijvoorbeeld als gevolg van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO). Bovendien bleek uit verdere vragen in het onderzoek uit 2020 dat de meeste organisaties de basismaatregelen eigenlijk helemaal niet op orde hadden.

Het begint met weten wat de risico's zijn

Juist een realistische blik op informatieveiligheid is enorm belangrijk. Want informatieveiligheid begint met te beseffen welke risico's je loopt. Alleen dan kun je de juiste maatregelen nemen om die risico's te beheersen. We gaan ervan uit dat de resultaten van dit onderzoek, aangevuld met onze tips en adviezen, daarbij helpen.

Terug naar inhoudsopgave

Breng mens, techniek en je organisatie met elkaar in balans

Gesprekken over informatieveiligheid gaan in de praktijk al snel over techniek. Waarschijnlijk omdat datgene wat hackers en security-experts allemaal uitspoken niet-technici al snel boven de pet gaat. Toch is techniek slechts een deel van het beveiligingsverhaal. Voor een slagvaardige informatiebeveiliging is juist een goede balans tussen mens, techniek en organisatie essentieel.

De mens als zwakste schakel

In de verdedigingslinie tegen cybercriminelen is de mens nog vaak de zwakste schakel. Dat is, op een enkele uitzondering na, geen onwil. Maar zonder structurele aandacht voor informatieveiligheid neemt de oplettendheid bij iedere medewerker af. En een moderne kenniswerker zonder voldoende digitale vaardigheden kun je gerust zien als een tikkende tijdbom voor je informatievoorzieningen. Werken gemeenten actief en structureel aan de versterking van deze zwakste schakel? En zo ja, hoe? In het volgende hoofdstuk zijn dit de eerste vragen waar we aandacht aan besteden.

De techniek als vestingwal

Met de juiste technische maatregelen is de kans dat je slachtoffer wordt van een hack, ook in het geval van menselijk falen, een stuk kleiner. En, net zo belangrijk, techniek kan je helpen de impact van een incident flink te verkleinen mocht je toch slachtoffer worden. Cybersecurity en de tools die je daarbij helpen, vragen echter om steeds verregaandere expertise en specialisatie. In het hoofdstuk over techniek kijken we of gemeenten weten waar ze kwetsbaar zijn. Welke middelen gebruiken ze om zich te beschermen? En kunnen ze hiervoor de juiste expertise aantrekken?

De organisatie als controlekamer

Uiteindelijk hoort informatiebeveiliging van iedereen te zijn. Dit vereist draagvlak onder bestuurders en het management over de noodzaak en urgentie van informatieveiligheid. Niet alleen in woord, maar ook in daad: budget, prioriteit en voorbeeldrol. In het hoofdstuk over de organisatie hebben we de deelnemers vooral vragen gesteld over de governance. Zijn de verantwoordelijkheden voor informatiebeveiliging en risicomanagement duidelijk belegd in de organisatie? Op welk niveau van de Baseline Informatiebeveiliging Overheid (BIO) fungeert de organisatie? Op welke onderdelen ervan is het lastig grip te krijgen? En voor welke onderdelen heeft de organisatie hulp van buiten nodig?

De belangrijkste vijf stappen naar een betere informatieveiligheid

In het laatste hoofdstuk benoemen we vijf stappen die (veruit de meeste) gemeenten nog moeten maken. Neem ze ter harte. Zodat informatieveiligheid ook in het DNA van jouw organisatie verankerd raakt.

> ***“ Voor een slagvaardige informatiebeveiliging is juist een goede balans tussen mens, techniek en organisatie essentieel.***

De mens: versterking van je zwakste schakel

Tijdens de bijeenkomsten die we met gemeenten organiseren is er één constante die altijd naar voren komt: de mens is en blijft de zwakste schakel voor je informatiebeveiliging. Je vindt nooit een goede balans tussen techniek en organisatie als eindgebruikers zich niet bewust zijn van het enorme risico dat een gemeente loopt en de rol die zij zelf spelen in het beperken daarvan. Zeker omdat bijna 100% van alle kenniswerkers in een gemeente online werkt. Dit maakt bewustwording en goede digitale vaardigheden twee belangrijke remedies tegen cyberaanvallen.

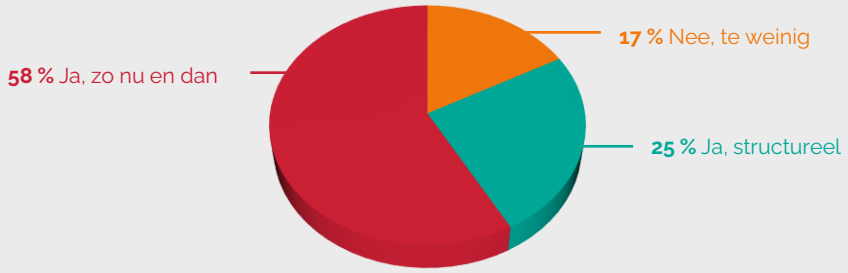
Er is aandacht voor informatieveiligheid, maar meestal niet structureel

Aandacht voor informatiebeveiliging is er bij de meeste gemeenten (83%), maar slechts bij een kwart is die aandacht structureel. Gezien de gevoeligheid van de data waarmee gemeenten werken en de consequenties van uitval is deze vrijblijvendheid anno 2023 redelijk ontluisterend. Hier is nog veel winst te halen, ook als je dit vergelijkt met het gemiddelde in Nederland. In het onderzoek van Solvinity bij alle Nederlandse organisaties gaf 53% aan structureel aandacht aan informatieveiligheid te besteden.

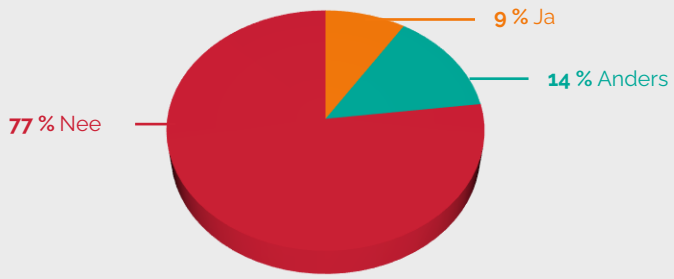
Digitale vaardigheden worden nog te vaak als luxe gezien

In een wereld waarin digitale vaardigheden van medewerkers cruciaal zijn voor de informatieveiligheid van je organisatie, zouden die digitale vaardigheden geen vrijblijvende competentie mogen zijn. Ze zijn echter bij slechts 9% van de deelnemende gemeenten een vast onderdeel van de jaarlijkse beoordelingscyclus. Een iets hoger percentage (24%) meet het niveau van digitale vaardigheden regelmatig. Beide percentages zouden in onze visie flink omhoog moeten. Onder de middelen die ingezet worden om medewerkers digitaal vaardig te maken, zijn vooral e-learnings (ingezet door 65% van de deelnemers) en klassikale (online-)opleidingen (41%) populair.

Figuur 1: structurele aandacht voor informatiebeveiliging



Figuur 2: digitale vaardigheden als onderdeel van het beoordelingsgesprek



Terug naar inhoudsopgave

De techniek: een hogere en dikkere vestingwal

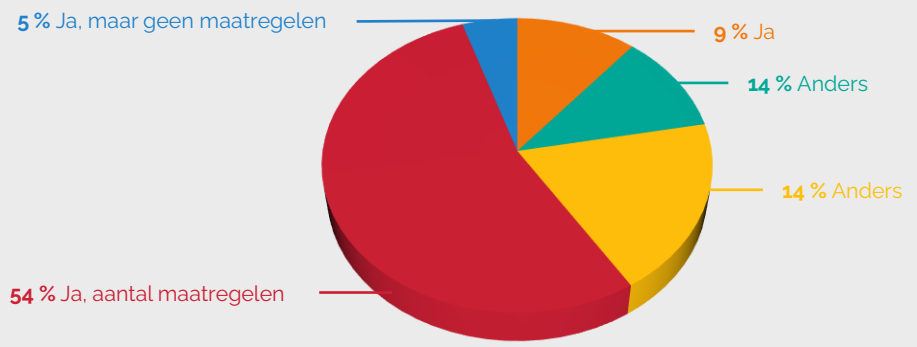
De technische beveiliging van een gemeentelijk IT-landschap is erg complex. Je hebt te maken met meerdere domeinen en afdelingen met eigen applicaties en registraties. Al die systemen, plus de koppelingen ertussen, hebben ieder hun technische uitdagingen als het gaat om informatieveiligheid. Hetzelfde geldt voor alle netwerkapparatuur en werkplekken. Ze genereren ook allemaal hun eigen logs met metadata over bijvoorbeeld het aantal inlogpogingen, opgevraagde informatie, gebruikte data, et cetera. Zorg in die wirwar maar eens voor voldoende overzicht en de juiste expertises om hypergespecialiseerde kwaadwillende buiten de deur te houden.

Driekwart weet waar het pijn kan doen

Inzicht in waar je kwetsbaarheden liggen, is belangrijk als je maatregelen wilt nemen om de informatieveiligheid in je organisatie te verbeteren. Driekwart (78%) van de deelnemers denkt precies te weten waar ze kwetsbaar zijn. Opvallend is dat 5% wel weet waar ze kwetsbaar zijn, maar daar geen maatregelen tegen heeft getroffen. 54% weet niet of de maatregelen die ze hebben genomen voldoende zijn. Slechts 19% van de deelnemers heeft een goed inzicht in de kwetsbaarheden en heeft vertrouwen in de genomen maatregelen.

> ***Slechts 19% van de deelnemers heeft een goed inzicht in de kwetsbaarheden en heeft vertrouwen in de genomen maatregelen.***

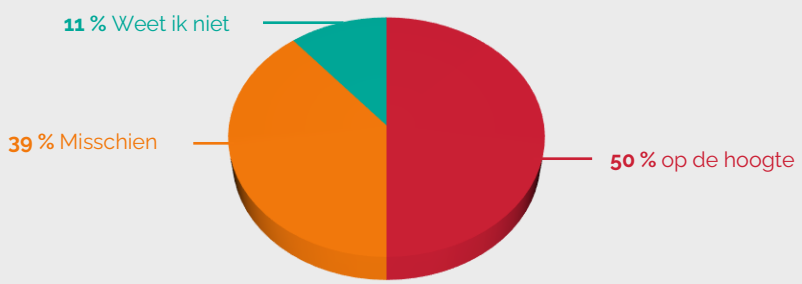
Figuur 3: inzicht kwetsbaarheid eigen IT-infrastructuur



Een groeiend bewustzijn?

Vergelijken we deze cijfers met het onderzoek uit 2020 dan valt op dat het aantal organisaties dat inzicht heeft in de kwetsbaarheden én denkt de juiste maatregelen te hebben genomen toen veel hoger was. Nu 19% van de deelnemende gemeenten, toen 49% van de deelnemende organisaties uit alle branches. Dit verschil kan met bewustwording te maken hebben: iedere publicatie van een hack, bijvoorbeeld in Binnenlands Bestuur, zorgt ervoor dat gemeenten weer iets kritischer naar hun eigen situatie kijken. Een positieve ontwikkeling. Een andere oorzaak kan zijn dat gemeenten nog niet altijd in staat zijn de juiste maatregelen te nemen. Bijvoorbeeld 24x7 SOC-diensten zijn best prijzig en nog niet iedere gemeente heeft daar het geld voor gevonden.

Figuur 4: gebruik onveilige software, hardware of diensten



'Het is onveilig, maar we hebben niets anders'

Onveilige software, hardware of diensten wil je uiteraard niet gebruiken. Toch gebeurt dit. Soms omdat gemeenten even geen alternatief voor handen hebben. Soms omdat de IT-afdeling niet precies weet wat medewerkers allemaal op hun laptops hebben draaien. 50% van de deelnemers weet dát en hóe er onveilige software, hardware of diensten worden gebruikt. Nog eens 39% geeft aan dat dit misschien het geval is. En 11% weet het niet. Hiermee scoren de gemeenten ongeveer hetzelfde als alle organisaties in Nederland.

Een rode loper

Bij bijna de helft (44%) van de gemeenten die weten dat er onveilige middelen worden ingezet, is dit een bewuste keuze of wordt er niet op vervangen aangestuurd. De redenen daarvoor zijn divers. Bijvoorbeeld capaciteitsgebrek, verouderde licenties of hardware, plannen om over te stappen naar een andere leverancier of wensen van de gebruiker. Hoe begrijpelijk misschien ook, ons advies is toch echt alles op alles te zetten om onveilige software zo snel mogelijk te vervangen. Want voor hackers zijn onveilige applicaties en hardware niets meer of minder dan een rode loper richting je kostbare informatie.

Updates en patches na weken of maanden

Software, hardware of diensten blijven alleen veilig als je updates of patches installeert zodra ze beschikbaar zijn. Dit kan echter in een groot (en soms ook onoverzichtelijk) IT-landschap best lastig zijn. En dat blijkt ook uit de antwoorden. Bij slechts iets meer dan de helft (56%) van de deelnemers worden updates en patches altijd binnen enkele uren of dagen geïnstalleerd. Bij een derde (32%) duurt dit echter enkele weken tot maanden. Een schrikbarend hoog percentage vinden we. Al lag dit percentage in het onderzoek bij alle Nederlandse organisaties nog op 51%.

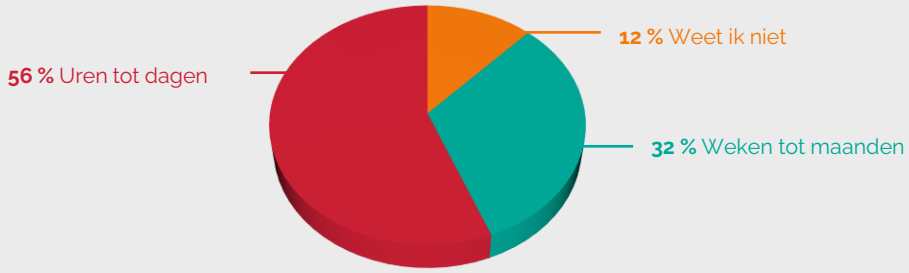
> ***Een derde (32%) gaat pas na enkele weken of maanden over tot het installeren van patches en updates.***

Hersteltijd na een cyberaanval

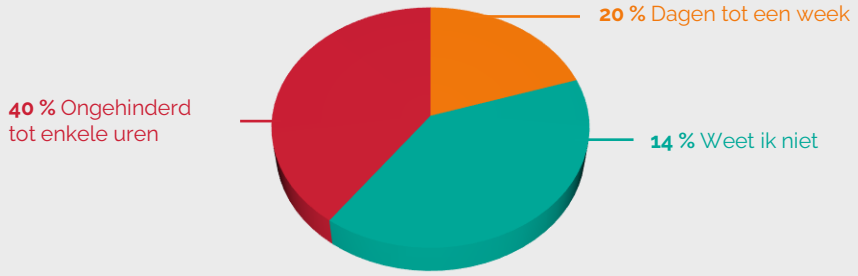
Informatieveiligheid is niet alleen een kwestie van alles op alles zetten om incidenten te voorkomen. Maar je moet ook de juiste maatregelen nemen om de gevolgen van een incident snel te kunnen herstellen mocht je onverhoopt toch slachtoffer worden. Slechts 40% van de gemeenten denkt na een cyberaanval ongehinderd door te kunnen werken of maximaal enkele uren hersteltijd nodig te hebben. Bijna 20% gaf aan dat dit dagen tot aan een week kon duren. Zo'n lange hersteltijd lijkt ons voor de belangrijke taken die gemeenten uitvoeren echt ongeoorloofd. En in de praktijk is dat laatste percentage misschien nog wat hoger, omdat zo'n 40% niet kan zeggen hoe lang de hersteltijd is.

> ***40% kan niet zeggen hoe lang de hersteltijd na een cyberaanval is.***

Figuur 5: duur tot installatie patches en updates



Figuur 6: hersteltijd na een cyberaanval



Hoe zorg je voor de juiste kennis?

Van de deelnemers aan onze survey die denken cybercriminelen van het lijf te kunnen houden, denkt zo'n 40% dit te kunnen doen door te investeren in eigen mensen. Ongeveer 60% denkt hiervoor externen nodig te hebben. We verwachten dat dit laatste percentage in de toekomst nog verder zal groeien. Door onder andere de verdere specialisatie van cybersecurity en het tekort aan deze specialisten op de arbeidsmarkt is het voor gemeenten moeilijk om zelf de juiste technische kennis in huis te halen en te houden. Zeker voor kleine en middelgrote gemeenten. Temeer omdat de specialisten die wel beschikbaar komen meestal met de nieuwste technieken willen werken, bij moderne organisaties en met bijpassende salarissen.

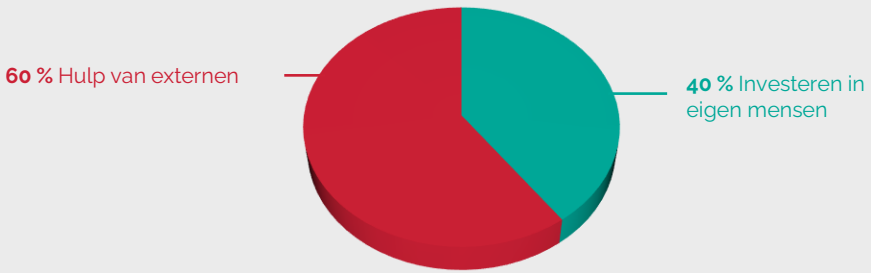
Intelligente monitoring wordt niet automatisch slim

Het gebrek aan specialistische kennis lijkt ons ook een van de verklaringen voor het antwoord op de vraag welke technische maatregelen deelnemers nemen om verdacht verkeer van hun IT-infrastructuur te weren, zie figuur 8.

> ***"Wat opvalt, is dat het aantal organisaties dat actief het verkeer op hun IT-landschap monitort met hulp van intelligente tools erg laag is.***

Wat opvalt, is dat het aantal organisaties dat actief het verkeer op hun IT-landschap monitort met hulp van intelligente tools erg laag is. Daarbij is het belangrijk te beseffen dat bijvoorbeeld een SIEM-oplossing aanschaffen nuttig is, maar dat je er daarmee nog niet bent. Het vraagt ook om voldoende mensen met de juiste expertise om het percentage false positives laag te houden en 24x7 adequaat op meldingen te kunnen reageren. En het vraagt om duidelijke afspraken over de rollen, taken en verantwoordelijkheden voor het monitoren van en reageren op meldingen.

Figuur 7: kennis over weerbaarheid tegen cybercriminelen



Figuur 8: intelligente monitoring

Monitoring tooling	
Firewall	73%
IDS	57%
IPS	49%
SIEM	41%
SOC	27%

Kun je bouwen op je leveranciers?

De beveiliging van diensten die je in de cloud afneemt, heb je niet helemaal zelf in de hand. Bij kleinere leveranciers zul je hier niet alleen eisen aan moeten stellen in je offertes of aanbestedingen, maar daar op een of andere manier ook controle op moeten (laten) uitoefenen. Bij de grote cloudspelers kun je ervan uitgaan dat ze genoeg budget en kennis hebben om flink te investeren in de informatieveiligheid. Maar ook dan blijf je zelf verantwoordelijk voor de data en de manier waarop je de diensten gebruikt. Een bepaald vinkje aanzetten kan het gebruiksgemak flink verhogen, maar ook de risico's of kosten.

> ***"Een bepaald vinkje aanzetten kan het gebruikersgemak flink verhogen, maar ook de risico's of kosten.***

Van beleid tot controle

Deze aandachtspunten zien we ook terug in de antwoorden op de vraag wat gemeenten als security-uitdagingen ervaren in een multi-cloud omgeving, zie figuur 9. Deze aandachtsgebieden vragen om specialistische kennis. Niet alleen op het gebied van security en de controle daarop, maar ook om bijvoorbeeld bij service integratie de afstemming tussen alle IT-leveranciers te regelen. We durven wel te stellen dat die kennis in het merendeel van de gemeenten momenteel niet te vinden is. En dat je die kennis ook niet zomaar even van de arbeidsmarkt plukt.

Figuur 9: uitdagingen van de multi-cloud

Uitdagingen	
Consequent beleid	62%
Inzicht	58%
Monitoring	49%
controle	59%

De organisatie: meer sturing vanuit de controlekamer

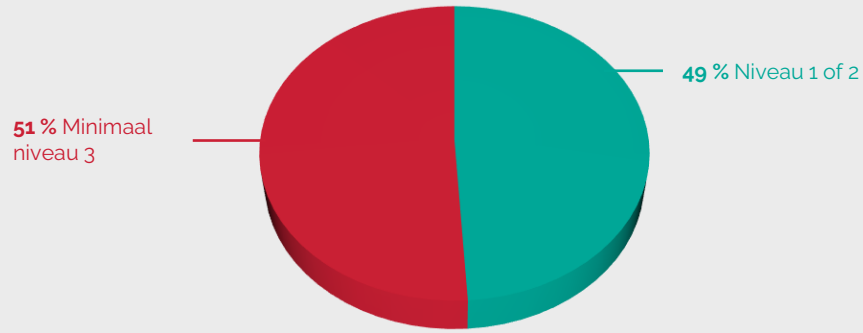
Het samenspel tussen mens en techniek werkt alleen optimaal als je beide voldoende faciliteert. Het gaat erom dat informatieveiligheid in de hele organisatie bij ieder proces, applicatie en verandering scherp op het netvlies staat. En dat bij de verdeling van middelen voldoende oog is voor informatieveiligheid, zowel de technische als de menskant ervan. Dit alles vraagt om zichtbare en actieve betrokkenheid van degenen die eindverantwoordelijk zijn voor die keuzes. En om controle of de gemaakte keuzes ook daadwerkelijk in de praktijk worden gebracht. En of ze leiden tot de verwachte resultaten of vragen om bijsturing.

De helft van alle gemeenten werkt op het geadviseerde veiligheidsniveau

Gemeenten leggen verantwoording af over de staat van hun informatiebeveiliging op basis van de Baseline Informatiebeveiliging Overheid (BIO). Doordat de BIO uit verschillende onderdelen en niveaus bestaat, kun je gemeenten hierin met elkaar vergelijken. Het advies aan gemeenten is om te zorgen dat ze minimaal niveau 3 halen. Uit deze survey blijkt echter dat maar 51% dat haalt. De overige 49% fungeert op niveau 2 of 1. Dat viel ons ruim drie jaar na de introductie van de BIO, en de urgentie van het onderwerp, enigszins tegen.

> *“Het gaat erom dat informatieveiligheid in de hele organisatie bij ieder proces, applicatie en verandering scherp op het netvlies staat.*

Figuur 10: volwassenheidsniveau volgens de BIO



Terug naar inhoudsopgave

De schouders van bestuur en management

We vroegen de deelnemers ook op welke onderdelen ze steun ervaren van het management en bestuur bij de implementatie van de BIO. En op welke onderdelen niet. De steun wordt wel gevoeld als het gaat om:

1. het vergroten van het bewustzijn van informatieveiligheid in de organisatie;
2. het bevorderen van een open en veilige cultuur waarin mensen risico's en misstappen durven te melden;
3. het inrichten van een risicoteam waarbinnen bijvoorbeeld het bestuur, CISO, FG en Controller samenwerken.

In de meeste organisaties is er vanuit het bestuur echter minder aandacht voor de borging van het risicomanagement als een cyclisch, iteratief en terugkerend proces. Hetzelfde geldt voor de borging en controle op het informatieveiligheidsbeleid.

> ***"In de meeste organisaties is er vanuit het bestuur echter minder aandacht voor de borging van het risicomanagement als een cyclisch, iteratief en terugkerend proces.***

Doen we het juiste?

Kort samengevat lijkt het erop dat de drang om iets te doen aan informatiebeveiliging er vanuit het bestuur en management zeker is, maar dat er minder structurele aandacht is voor de vraag of datgene wat wordt gedaan echt werkt, voldoende is en na een tijdje nog steeds het juiste is. Ook vinden de meeste deelnemers dat hun organisatie nog te weinig samenwerkt met partners en leveranciers als het gaat om het beheersen van veiligheidsrisico's en het nemen van slimme maatregelen.

De lastige onderdelen van de BIO

We vroegen de deelnemers ook met welke onderdelen van de BIO ze moeite hebben. In de antwoorden valt op dat de onderdelen die te maken hebben met een goede veilige digitale werkomgeving voor veruit de meeste organisaties geen struikelblokken meer zijn. Daar heeft het verplicht thuiswerken tijdens de coronacrisis ongetwijfeld een flinke bijdrage aan geleverd. Tegelijkertijd valt ook hier op dat veel gemeenten (49%) het lastig vinden om leveranciers te monitoren, beoordelen en auditen. En ook als het gaat om maatregelen die de bedrijfscontinuïteit moeten garanderen, vinden veel gemeenten (49%) het lastig te voldoen aan de BIO.

De meeste gemeenten kunnen hulp van buiten gebruiken

Net als voor de technische kant, denken veel deelnemers dat hun gemeente ook voor de organisatorische kant van informatieveiligheid (zo nu en dan) wel wat hulp kan gebruiken. 70% bijvoorbeeld als het gaat om maatregelen te nemen die ervoor moeten zorgen dat de continuïteit niet in gevaar komt. Maar ook voor controle of de genomen maatregelen effectief zijn, zet 51% externe expertise in. Geen verrassend cijfer aangezien gemeenten zich moeten verantwoorden op dit gebied. 27% van de deelnemers heeft hulp nodig om alle ontwikkelingen op het gebied van informatieveiligheid bij te kunnen houden. Dit speelt vooral bij de kleinere gemeenten.

> ***"Net als voor de technische kant, denken veel deelnemers dat hun gemeente ook voor de organisatorische kant van informatieveiligheid (zo nu en dan) wel wat hulp kan gebruiken.***

De vijf belangrijkste stappen naar een betere informatieveiligheid

Zoals gezegd is het voor informatiebeveiliging belangrijk dat je continu zoekt naar een goede balans tussen mens, techniek en organisatie. Informatieveiligheid moet in het DNA van de hele organisatie komen. Kijken we naar de uitkomsten van deze survey, dan raden we gemeenten aan de volgende verbeterstappen te zetten:

1

Bestuur

Stel voldoende en de juiste middelen ter beschikking en geef security een plek op strategisch niveau aan de bestuurstafel.

2

Medewerkers

Investeer structureel in next level kennis en (digitale) vaardigheden, en maak security onderdeel van de taakomschrijving.

3

Techniek

Zorg voor inzicht met tools voor 24/7 intelligente monitoring van je IT-landschap. Als je zelf de expertise daarvoor mist, kies dan voor een managed service variant, zodat je 24/7 beschikt over ondersteuning. Want cybercriminelen doen niet aan sluitingstijden. Zorg er verder voor dat je de basismaatregelen op orde hebt, zoals een tijdig en gestroomlijnd patch- en updatebeleid, immutable backups en een getest disaster recovery plan.

4

P&O

Kijk eens naar de kwetsbaarheid van je organisatie op personeelsvlak. Hoeveel mensen hebben ergens verstand van? Welke expertises mis je of ga je binnenkort missen? En hoe vul je die gaten op? Dit moet je regelmatig voor alle vakgebieden doen, maar zeker ook voor informatieveiligheid. Vanwege het specialistische karakter van het onderwerp is het verstandig je informatie op dit vlak eens door externe specialisten te laten doorlichten..

5

Samenwerken

Maak (meer) gebruik van kennis en ervaring op de markt, van zowel partners als collega-gemeenten. Je kunt (zeker als kleine of middelgrote gemeente) niet alles zelf bijhouden. En je hebt ook niet alle kennis en vaardigheden fulltime nodig.

Terug naar inhoudsopgave

De tijd van vrijblijvendheid is voorbij

Als Solvinity en Quarant verkondigen we al jaren de boodschap dat, als het gaat om informatieveiligheid, de tijd van vrijblijvendheid absoluut voorbij is. Gelukkig is bij eigenlijk alle gemeenten inmiddels het besef wel ingedaald dat ze heel erg aantrekkelijk zijn voor kwaadwillenden. Desgevraagd zal iedere bestuurder, manager en medewerker het belang van informatieveiligheid dan ook uitvoerig bepleiten. Maar dat is nog wat anders dan weten wat de juiste maatregelen zijn om de kans op incidenten te beperken. En vervolgens ook voor de juiste expertises en voldoende budget te (willen en kunnen) zorgen om die maatregelen daadwerkelijk uit te voeren.

Vragen? Laat het weten!

We zijn ervan overtuigd dat de aandachtspunten uit dit onderzoek en de stappen uit het vorige hoofdstuk praktische handvatten zijn voor gemeenten in hun strijd tegen cyberaanvallen. Heb je nog vragen over dit onderzoek? Wil je inhoudelijk meer weten over een van de behandelde onderwerpen? Of wil je advies over de praktische uitvoering van de verbeterstappen? Neem dan gerust contact met ons op.

Meer weten over Solvinity?
Neem contact met ons op via
+31 (0)20 36 43 600 of
info@solvinity.com
of bezoek onze website
www.solvinity.nl

Wil je nog wat meer informatie of heb je een vraag?
Neem contact op via
+31 85 489 02 16 of
info@quarant.nl
of bezoek onze website
www.quarant.nl

Over Solvinity & Quarant

Over Solvinity

Solvinity levert Secure Managed IT Services aan organisaties met hoge beveiligingseisen. Met innovatieve managed cloud oplossingen ondersteunt het bedrijf de (rijks-)overheid, gemeenten en toonaangevende organisaties in de financiële en zakelijke dienstverlening, zoals het ministerie van Justitie en Veiligheid, Politie Nederland, TransLink (OV-chipkaart), ING en ONVZ. Solvinity adviseert en ondersteunt organisaties in hun digitale transformatie en ontwerpt en bouwt de complexe platformen waarop bedrijfskritische applicaties veilig en optimaal functioneren. Daarnaast levert het bedrijf CI/CD, containertechnologie en 'Stretched' DevSecOps oplossingen voor softwareontwikkelaars.

Solvinity onderscheidt zich op het gebied van cybersecurity met een uitgebreid portfolio aan securitydiensten en -oplossingen en biedt, met een meerderheidsbelang in Securify.nl, aanvullende diensten op het gebied van pentesting, red teaming en agile security. Daarnaast heeft het bedrijf certificeringen volgens (inter)nationale normen als ISO 27001, ISO 14001, ISO 9001, PCI DSS en heeft het als eerste MSP in Nederland SOC 1 en 2 compliance rapporten voor de gehele beheeromgeving van de private én Azure cloud. Solvinity heeft 350 medewerkers en vestigingen in Amsterdam, Assen, Amersfoort en Den Bosch. In 2021 haalde het bedrijf een jaaromzet van 59 miljoen euro.

Kijk voor meer informatie op www.solvinity.nl,
of volg Solvinity op Twitter en LinkedIn.

Over Quarant

Quarant is al 20 jaar hét onafhankelijke adviesbureau voor lokale overheden. De organisatie heeft als doel bij te dragen aan een betrouwbare overheid en veilige samenleving waar burgers prettig kunnen leven, werken en wonen. Lokale overheden creëren daarvoor de randvoorwaarden. Klantgerichte, rechtmatige en doelmatige dienstverlening is nodig om burgers en overheden dichter bij elkaar te brengen. Quarant helpt lokale overheden hierbij door praktisch toepasbare oplossingen te bedenken die echt werken en technologische, wettelijke en maatschappelijke ontwikkelingen te integreren en te verankeren in de bedrijfsvoering en dienstverlening.

Met een effectieve en inspirerende aanpak ervaren en beleven medewerkers niet alleen het eindresultaat, maar raken ook gemotiveerd om daar zelf aan bij te dragen. Quarant neemt het initiatief, maar het gewenste eindresultaat wordt samen bereikt. Zo ontstaat een positieve energie en worden veranderingen blijvend omarmd. Het team bestaat uit een inspirerende club consultants, dat samen een berg aan kennis en ervaring bezit om te delen met gemeentelijke organisaties. Iedere collega heeft zijn expertise. Zo haal je een echte specialist in huis.

Kijk voor meer informatie op www.quarant.nl
of volg Quarant op LinkedIn.

Quarant

verbindt mens en informatie

Fruitweg 36a, 3981 PA Bunnik

+31 85 489 02 16 | info@quarant.nl