

BMC

YACHT GROUP

Is de informatiebeveiliging bij uw gemeente op orde?

Ontdek hoe u inzicht en grip krijgt



Partners in verbetering

Steeds vaker is informatiebeveiliging bij gemeenten in het nieuws. Denk maar aan de ransomware-aanval op de gemeente Hof van Twente¹ of het rekenkameronderzoek bij de gemeente Utrecht². Voor veel gemeenten is er werk aan de winkel om informatiebeveiliging écht op orde te krijgen. Hoe zit dat bij uw gemeente? Heeft u inzicht in hoe informatiebeveiliging geregeld is? BMC geeft u weer grip.

'Ik was in de veronderstelling dat ik in control was.'³ Dat zei de burgemeester van de gemeente Hof van Twente na de ransomware-aanval. Daar bleek onvoldoende inzicht te zijn in de stand van zaken rond informatiebeveiliging. Daardoor was het college niet in staat om de juiste stappen te nemen en de aanval te voorkomen.

Grote gevolgen van incidenten

Wie hacks en andere cybersecurity-incidenten onvoldoende kan voorkomen, vaststellen en herstellen, riskeert grote gevolgen. Niet alleen de reputatie loopt schade op, ook de dienstverlening aan inwoners komt in het geding. Want in hoeverre is de gemeente na een incident bijvoorbeeld nog in staat om taken rond crisisbeheersing en openbare orde uit te voeren? En zijn de privacy en de beschikbaarheid van gemeentelijke dienstverlening waar inwoners van afhankelijk zijn nog wel te waarborgen? Bovendien zijn er ook nog indirect financiële gevolgen. De kosten van het incident bij Hof van Twente bijvoorbeeld worden geraamd op 100 euro per inwoner⁴.

Verschillende oorzaken

Hoe kan het dat veel gemeenten dat inzicht in hun informatiebeveiliging niet hebben? Daar zijn verschillende oorzaken voor. Om te beginnen gaan de externe audits in het kader van ENSIA alleen over een beperkt aantal toepassingen, zoals DigiD en Suwinet. Die geven dus een verre van volledig beeld⁵. In het kader van ENSIA wordt de landelijke overheidsstandaard voor informatiebeveiliging (Baseline Informatiebeveiliging Overheid, kortweg BIO) alleen geëvalueerd met een zelfevaluatie. Daarbij lijken de criteria bij het invullen van de vragenlijst onvoldoende om blinde vlekken in de implementatie naar boven te halen. Zo scoorde de gemeente Hof van Twente volgens persberichten in 2019 92 procent op de BIG/BIO-vragenlijst⁶. Daarnaast hebben veel gemeenten beperkte kennis van best practices voor informatiebeveiliging. Voor een relatief kleine organisatie is het lastig om actuele kennis en ervaring op het gebied van informatiebeveiliging in huis te hebben en te houden.

¹ <https://nos.nl/artikel/2372868-hack-bij-gemeente-hof-van-twente-veroorzaakt-door-te-simpel-wachtwoord>

² <https://nos.nl/artikel/2375917-rekenkamer-utrecht-informatie-op-stadskantoor-niet-veilig-genoege>

³ <https://www.binnenlandsbestuur.nl/digitaal/nieuws/burgemeester-hof-van-twente-dacht-in-control-te.16475918.lynkx>

⁴ <https://www.binnenlandsbestuur.nl/digitaal/nieuws/burgemeester-hof-van-twente-dacht-in-control-te.16475918.lynkx>

⁵ <https://www.hofvantwente.nl/fileadmin/files/hofvantwente/inwoners/actueel/Te-goed-van-vertrouwen.pdf> par 3.3

⁶ https://www.hofvantwente.nl/fileadmin/files/hofvantwente/inwoners/actueel/Rapport_van_Bevindingen_Raad_defintief.pdf pg 18

Echt in control

Voor u als gemeente is het kortom niet altijd even gemakkelijk om grip te hebben én te houden op de informatiebeveiliging binnen uw gemeente. BMC kan u helpen om écht in control te zijn.

Dat doen wij door gemeenten te ondersteunen bij de inrichting en evaluatie van hun informatiebeveiliging, incidenteel of op structurele basis – net waar uw behoeften liggen. Wij voorzien u van de benodigde actuele kennis en een objectieve blik. Daardoor weet u hoe uw organisatie ervoor staat en bent u in staat om de voor uw organisatie juiste keuzes te maken en prioriteiten te stellen.

We hebben onze ondersteuning ingedeeld in verschillende modules. Die lichten we hieronder toe.

Jaarlijkse check-up

We onderzoeken bij de inrichting van informatiebeveiliging in uw organisatie in welke mate de BIO-maatregelen zijn geïmplementeerd. Ook kijken we naar de opvolging van bevindingen uit eerdere audits en onderzoeken. Dat doen we door documentatie te bestuderen en interviews af te nemen. Op basis daarvan geven we tips om de maatregelen effectiever te maken en concrete adviezen voor de verdere implementatie of verbetering van maatregelen. De check-up geeft u een genuanceerd, objectief en onderbouwd inzicht in de stand van zaken van de beheersing en de implementatie van de BIO.

Risicoanalyse

In een workshop maken wij samen met uw medewerkers een risicoanalyse. Daarbij nemen we actuele bedreigingen mee. Denk bijvoorbeeld aan de aspecten die hebben bijgedragen aan de ransomware-aanval bij de gemeente Hof van Twente. Een rondgang door uw gebouw is daar ook onderdeel van. Verder kijken we naar de kwetsbaarheid van de gemeente, voor zover die op basis van publiek beschikbare informatie te achterhalen is. Voor een hacker is het immers efficiënter om de meest kwetsbare organisaties aan te vallen.

Jaarplan en roadmap

Op basis van de resultaten van de check-up en de risicoanalyse ondersteunen we uw CISO bij het opstellen van een jaarplan én een roadmap voor de daaropvolgende jaren. Daarbij werken we niet alleen de doelen uit, maar zetten we ook uiteen wie wat wanneer moet doen. Zo wordt ook duidelijk welke capaciteit en expertise nodig zijn om de doelen te halen en in hoeverre die intern aanwezig zijn. Het resultaat is een haalbaar plan om de urgente risico's voor uw organisatie effectief aan te pakken.

Workshop informatiebeveiliging

Twee keer per jaar organiseert BMC een workshop voor uw medewerkers informatiebeveiliging, waarin we actuele ontwikkelingen en een specifiek onderwerp uitlichten. Zo blijft de kennis van uw medewerkers informatiebeveiliging actueel.

Expert on demand

Voor professionals binnen gemeenten kan het prettig zijn om complexe inhoudelijke vragen met iemand anders af te stemmen. Maar soms is dit binnen de eigen organisatie niet mogelijk, bijvoorbeeld omdat specifieke kennis over het onderwerp ontbreekt. Dan is het prettig om die afstemming te zoeken met een onafhankelijk persoon van buiten de eigen organisatie. Wij bieden onze top-adviseurs aan als sparring-partner op het moment dat u die nodig heeft. U heeft daarmee altijd toegang tot actuele en gespecialiseerde kennis en ervaring.

Ondersteuning in de uitvoering

Wij bieden u praktische ondersteuning in de uitvoering van de informatiebeveiligingstaken, zowel bij de implementatie als bij de jaarlijks terugkerende taken, zoals voorbereiding van audits en het actualiseren van documentatie.

Meer weten?

BMC is expert op het gebied van informatie-beveiliging en privacy bij gemeenten en kent de processen en dilemma's binnen gemeentelijke organisaties. Dat maakt dat we gemeenten praktisch toepasbare aanbevelingen kunnen doen.

We bieden de diensten die in deze brochure beschreven staan niet alleen aan als losse modules, maar ook in de vorm van een check-up- en ondersteuningsabonnement.

Kiest u voor zo'n abonnement, dan profiteert u van een vertrouwde adviseur die uw organisatie goed kent en daardoor op maat kan adviseren.

Ook voor privacyvragen bieden wij structurele ondersteuning. Meer daarover vindt u [hier](#).

Meer informatie & contact

Wilt u meer informatie of een vrijblijvend gesprek? Neem dan gerust contact op met:



Julius Duijts
managing consultant
julius.duijts@bmc.nl
06 - 29 52 55 31



Amy den Broeder
directeur domein
Data & Dienstverlening
amy.den.broeder@bmc.nl
06 - 53 60 59 94



Ilhame Hajji
commercieel manager
ilhame.hajji@bmc.nl
06 - 83 13 78 61



Cem Canan
account manager
cem.canan@bmc.nl
06 - 57 14 44 04

Kijk voor meer informatie ook eens op onze website www.bmc.nl