Rapportage Verhogen Digitale Weerbaarheid

Gemeente Groningen

Verhogen Digitale Weerbaarheid

Basismaatregelen Informatieveiligheid 2022

Uit informatiebeveiligingsincidenten van de afgelopen jaren is één rode draad te ontwaren: Organisaties werden voornamelijk getroffen[1] doordat één of meerdere systemen niet voorzien waren van de benodigde beveiligingsupdates of doordat onvoldoende maatregelen waren genomen om de toegang tot deze systemen te beperken. Hacks en incidenten hebben grote impact op imago, bedrijfsvoering en kunnen behoorlijk wat tijd en geld kosten. De Informatiebeveiligingsdienst (IBD) adviseert daarom bij de implementatie van de BIO om prioriteit te geven aan het op orde krijgen en houden van basismaatregelen en basisprocessen.

Lessen uit incidenten en actuele dreigingen laten zien dat basismaatregelen essentieel zijn voor het beveiligen van informatie. Voor deze basismaatregelen geldt dat deze hoe dan ook van belang zijn, ongeacht de omvang van de organisatie en de risicocontext. Hiervoor heeft de IBD het ondersteuningstraject Verhogen Digitale Weerbaarheid (VDW) ontwikkeld, met in Module-1 de focus op de basismaatregelen en processen.[2] De basismaatregelen hebben nu ook een aparte markering gekregen in de BIO-vragenlijst van de ENSIA-verantwoording. Het doel van deze markering is dat voor zowel bestuurders als professionals bij gemeenten direct inzichtelijk kan worden gemaakt of de basismaatregelen voldoende zijn geïmplementeerd. Kortom, of voldoende effectieve preventieve en impact beperkende maatregelen zijn genomen om informatiebeveiligingsincidenten in de toekomst te voorkomen.

Kanttekening
Informatiebeveiliging valt of staat bij de samenhang aan maatregelen die de daadwerkelijke beveiliging van de organisatie bepalen. Voor een effectieve beveiliging staan maatregelen niet op zichzelf. De momenteel gebruikte set aan maatregelen is specifiek gekoppeld aan de BIO-vragenlijst in de ENSIA-verantwoording en bevat niet alle aspecten van de maatregelen uit de ondersteuning van VDW Module-1. Zoals bij alle onderdelen van ENSIA is een ‘afgevinkte’ maatregel nooit een garantie op veiligheid. Ook is compliance geen vervanging voor het uitvoeren van een risicoanalyse of het zelf te blijven interpreteren of risico’s afdoende worden gemitigeerd. Daarentegen is het ontbreken van een basismaatregel wel een belangrijk waarschuwingssignaal.

1 https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2021-2022/
2 https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/

Managementsamenvatting

Een gedeelte van de vragen die gesteld worden in de BIO-vragenlijst zijn voorzien van het trefwoord ‘VDW-1’. Deze vragen zijn geclusterd in 7 verschillende onderwerpen. In de bijlage zijn de vragen opgenomen die horen bij deze clusters. Op basis van de antwoorden in de BIO-vragenlijst wordt de volgende beoordeling gegeven over de onderwerpen die in het kader van VDW Module-1 relevant zijn:

Onderwerp	Status (<)2020	Status 2021	Status 2022
1. Dringend advies IBD	☹	😐	☹
2. Beheer en bedrijfsmiddelen	☹	😐	☹
3. Toegangsbeveiliging	☹	☹	☹
4. Wachtwoorden	😐	😐	😐
5. Wijzigingsbeheer	😐	😐	😐
6. Back-up & restore	☹	😐	☹
7. Beheer van informatiebeveiligingsincidenten	😐	😐	😐

Legenda:

☺ = goed, geen directe reden voor verbetering nodig

😐 = matig, heeft te zijner tijd aandacht nodig

☹ = slecht, heeft dringend aandacht nodig

Toelichting CISO op de *werking* van de onderwerpen

1. Dringend advies (2-factorauthenticatie & kritieke/hoge kwetsbaarheden tijdig patchen)

Het risico bestaat dat, als 2-factorauthenticatie niet goed is ingevuld, via bruteforce of een gelekte accountinformatie een account gecompromitteerd wordt en gebruikt kan worden voor een datalek of een hack. Het niet binnen een week patchen van kwetsbaarheden met een hoge impact en een hoge kans (high/high) kan ervoor zorgen dat kwaadwillende een kwetsbaarheid misbruiken om in het gemeentelijk netwerk in te breken.

Beide punten zijn zeer basaal ingericht en verdienen de nodige aanscherpingen door onze ICT-outsourcingleverancier(s). Dit heeft de volledige aandacht van de bestuurlijke stuurgroep outsourcing ICT en stuurt op spoedige inrichting.

2. Beheer en bedrijfsmiddelen

Het risico bestaat dat, als deze maatregelen (configuratiebeheer en patchmanagement) niet goed zijn ingevuld en mobiele apparatuur niet is voorzien van de juiste beveiliging, data kan worden gemanipuleerd of gestolen.

Beide punten zijn zeer basaal ingericht en verdienen de nodige aanscherpingen door onze ICT-outsourcingleverancier(s). Dit heeft de volledige aandacht van de bestuurlijke stuurgroep outsourcing ICT en stuurt op spoedige inrichting.

3. Toegangsbeveiliging

Het risico bestaat dat, als deze maatregelen (logisch toegangsbeheerprocessen, waar onder periodieke controle van toegangsrechten en authenticatie van apparatuur) niet goed zijn ingevuld, onbevoegde toegang krijgen tot gemeentelijke data en een datalek veroorzaken. Daarnaast kunnen medewerkers met teveel rechten (onbedoeld) veel schade veroorzaken door verkeerde handelingen uit te voeren of, als het account is overgenomen, kan een kwaadwillende de organisatie bewust schade toebrengen.

Deze punten zijn zeer basaal ingericht en verdienen serieuze aanscherpingen door zowel de gemeente Groningen als door onze ICT-outsourcingleverancier(s). Dit heeft de volledige aandacht van de bestuurlijke stuurgroep outsourcing ICT en stuurt op spoedige inrichting.

4. Wachtwoorden

Het risico bestaat dat, als deze maatregelen (wachtwoordinstellingen) niet goed zijn ingevuld, wachtwoorden niet sterk genoeg zijn en accounts daardoor onvoldoende beschermd zijn. Dit kan leiden tot een datalek of een hack.

Dit punt is basaal ingericht en verdient nog aanscherpingen door onze ICT-outsourcingleverancier(s). Dit heeft de volledige aandacht van de bestuurlijke stuurgroep outsourcing ICT en stuurt op spoedige inrichting.

5. Wijzigingsbeheer

Het risico bestaat dat, als deze maatregelen (formeel goedkeuren van wijzigingen en testen van wijzigingen in separate testomgevingen voor in productie name) niet goed zijn ingevuld, wijzigingen niet of onvoldoende getest zijn, waardoor de dienstverlening mogelijk (langdurige) onbeschikbaar is en/of (onbedoeld) kwetsbaarheden in de productieomgeving geïntroduceerd worden.

Deze punten zijn basaal ingericht en verdienen de nodige aanscherpingen door zowel de gemeente Groningen als door onze ICT-outsourcingleverancier(s). Dit heeft de volledige aandacht van de bestuurlijke stuurgroep outsourcing ICT en stuurt op spoedige inrichting.

6. Back-up & restore

Het risico bestaat dat, als deze maatregelen (maken van back-ups en het periodiek testen daarvan) niet volledig en goed zijn ingevuld, back-ups niet voldoen aan de gewenste eisen en daardoor data onvoldoende gerestored kan worden waardoor gegevens verloren gaan. Hierdoor kan de dienstverlening bij een incident potentieel niet voldoende hersteld worden.

Deze punten zijn zeer basaal ingericht en verdienen nodige aanscherpingen door de gemeente Groningen alsook grote vooruitgang door onze ICT-outsourcingleverancier(s) door het uitvoeren van de volledige uitwijkstest. Dit heeft de volledige aandacht van de bestuurlijke stuurgroep outsourcing ICT en stuurt op spoedige inrichting.

7. Beheer van informatiebeveiligingsincidenten

Het risico bestaat dat informatiebeveiligingsincidenten onvoldoende gemeld, opgepakt en geëvalueerd worden om de incidenten in de toekomst te voorkomen. Het gevolg van het niet tijdig aanpakken van informatiebeveiligingsincidenten is dat dit de impact van datalekken en incidenten kan vergroten en zodoende leidt tot reputatieschade en (langdurig) uitvallen van de dienstverlening.

Deze punten zijn basaal ingericht en verdienen de nodige aanscherpingen door zowel de gemeente Groningen als door onze ICT-outsourcingleverancier(s). Dit heeft de volledige aandacht van de bestuurlijke stuurgroep outsourcing ICT en stuurt op spoedige inrichting.

Verbetervoorstel CISO

Om tot serieuze verhoging te komen van de digitale weerbaarheid van de gemeente dient Gemeente Groningen nog strakker te gaan sturen op informatiebeveiliging.

De grootste uitdaging ligt daarbij momenteel op de sturing van de externe naleving van de gecontracteerde dienstverlening door onze ICT-outsourcingsleverancier(s). In volgorde van prioriteit zou de focus daarbij moeten liggen op het patchen en hardenen van de (kwetsbare) systemen (punt 1 en 2), het aantonen van effectieve processen voor back-up & restore (punt 6) en het periodiek controleren en schonen van oude accounts en autorisaties (punt 3).

Qua interne sturing zou de aandacht in de komende periode grotendeels moeten gaan naar de verbetering van de toegangsbeveiligingsprocessen in het algemeen, maar het periodiek gaan controleren van accounts en autorisaties (punt 3) door alle proces- en systeemeigenaren in het bijzonder.