Overheid

Inzicht in de basismaatregelen cybersecurity en BIO

Veilige informatie voor overheidsinstellingen

In dit document laten wij zien hoe Secquard overheidsinstellingen zoals gemeenten ondersteunt bij het in kaart brengen en verbeteren van hun informatieveiligheid en hoe dit helpt met compliance aan de Baseline Informatiebeveiliging Overheid (BIO).

Door de toenemende digitalisering is het zorgvuldig omgaan met informatie en gegevens van burgers en organisaties ook voor overheidsinstanties van groot belang. Uitval van computers of telecommunicatiesystemen, het gecorrumpeerd raken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de continuïteit van de bedrijfsvoering en het primaire proces. Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening van overheidsinstellingen. Hieraan zijn bestuurlijke consequenties verbonden en het kan het imago van de organisatie en daarmee van de sector in het algemeen schaden.

Onderzoek van TNO geeft aan dat cybercrime de Nederlandse economie jaarlijks ongeveer €10 miljard kost. Deze raming betekent dat de schade door cybercrime voor de overheid naar verwachting zeer significant is. Overheidsinstellingen zijn een target voor cybercriminelen. Daarom is het van groot belang om de cyberweerbaarheid te vergroten. Cyberincidenten hebben negatieve gevolgen voor burgers van gemeenten, maar ook voor leveranciers, partners en de eigen organisatie en haar bestuurders.

Eenvoudige aanvallen

De meeste cybercriminelen maken gebruik van eenvoudige middelen en misbruiken publiek bekende kwetsbaarheden in soft- en hardware.

Deskundigen schatten het aandeel van dit soort eenvoudige aanvallen op ongeveer 90% van het totaal aantal aanvallen wereldwijd. Je kunt deze aanvallen vergelijken met het open laten staan van een raam of deur, terwijl je niet thuis bent. Een passerende dief kan hierdoor makkelijk binnenkomen. Cybercriminelen zijn continu geautomatiseerd op zoek naar dit soort openstaande ‘digitale ramen en deuren’ (Bron: Digital Trust Center).

Helaas zijn dit soort eenvoudige aanvallen zeer succesvol en vallen hier veel nog steeds organisaties en individuen aan ten prooi, ook in de overheid.

Basismaatregelen

Gelukkig maken de grote aantallen eenvoudige aanvallen echter geen schijn van kans als je een aantal essentiële basismaatregelen neemt! Dit kun je vergelijken met het sluiten van je digitale ramen en deuren. Het lijkt misschien vreemd, maar verreweg de meeste organisaties hebben deze nog wagenwijd openstaan. Vaak zijn deze organisaties zich hier niet van bewust en weten zij niet hoe zij deze kunnen sluiten. Toch is het niet moeilijk. Het gaat dan onder andere om basismaatregelen als tijdig installeren van updates (security patches) en het voorkomen van tekortkomingen in configuraties (hardenen, hieronder valt bijvoorbeeld het instellen van wachtwoordbeleid).

Deze basismaatregelen maken ook onderdeel uit van de BIO en helpen organisaties direct om weerbaarder te worden. Deze maatregelen werpen namelijk de eerste barrières op tegen cyberaanvallen, beperken schade bij een incident en maken het herstel makkelijker.

Secquard

De visie van Secquard is dat overheidsinstellingen pas digitaal weerbaar zijn wanneer ze inzicht hebben in de basismaatregelen van hun cybersecurity. Secquard maakt in één oogopslag inzichtelijk welke maatregelen zijn genomen op het gebied van hardening, patching, antivirus en autorisaties. Secquard toetst deze maatregelen aan onder andere de BIO, DigiD, ISO en andere standaarden. Door het volledig geautomatiseerde karakter van Secquard kan meteen worden bijgestuurd als dit nodig blijkt. Daarnaast bieden trendoverzichten inzicht in de status van systemen over langere tijd. Secquard is onbeperkt schaalbaar en dus geschikt voor enkele systemen tot omgevingen van tientallen, honderden of duizenden systemen.

Basismaatregelen helpen overheidsorganisaties direct om weerbaar te worden door de eerste barrières op te werpen tegen cyberaanvallen, schade bij een incident te beperken en herstel makkelijker te maken. Secquard controleert de werkelijke beveiligingsstatus van systemen met de gewenste situatie. Met name voor sectoren die te maken hebben met toenemende wet- en regelgeving helpt onze oplossing omdat wij de configuraties benchmarken tegen de industrie standaarden als BIO, ISO, CIS, NEN, NIST en ENISA. Onze rapportages kunnen gebruikt worden voor verschillende rollen binnen organisaties en geven inzicht aan CISO's, IT-beheerders, managers, controllers en accountants.

Secquard is van toegevoegde waarde bij vraagstukken in relatie tot strategie en risico, compliance en cyberweerbaarheid. Onderstaand een overzicht hoe Secquard uw organisatie kan ondersteunen.

	Inzicht en bewustwording	Groei naar volwassenheid	Volwassen en weerbaar
Compliance	Waar sta ik nu, welke basisprincipes heb ik op orde en welke (nog) niet? Secquard	Hoe voldoe ik aan best practices en certificeert mijn organisatie naar mijn klanten en partners? Secquard	Hoe weet ik zeker dat mijn cybersecurityprogramma voldoet aan gestelde eisen en welke stappen moet ik zetten om compliant te zijn? Secquard
Strategie en risico	Hoe creëer ik bewustwording in mijn bestuur en directie, zet ik cybersecurity op de agenda, en zorg ik voor voldoende budget? Secquard	Hoe maak ik een helder cybersecurityprogramma?	Hoe verkrijg ik inzicht en zekerheid over de weerbaarheid van mijn organisatie tegen aanvallen of verstoringen? Secquard
Cyberweer-baarheid	Hoe creëer ik meer securitybewustzijn bij mijn werknemers?	Hoe maak ik kwetsbaarheden in mijn infrastructuur zichtbaar? Secquard	Hoe kan ik mijn organisatie testen op volwassenheid en weerbaarheid, zodat ik bestaande maatregelen kan aanscherpen? Secquard

De BIO

De basismaatregelen spelen een essentiële rol in de BIO. De BIO is bedoeld om:

- Overheidsinstellingen op een vergelijkbare manier efficiënt te laten werken aan (de inrichting van) hun informatiebeveiliging.
- Een hulpmiddel te bieden om aan alle eisen op het gebied van informatiebeveiliging te kunnen voldoen.
- De auditlast te verminderen.
- Overheidsinstellingen een aantoonbaar betrouwbare partner te laten zijn.

Kort samengevat helpt de BIO u bij het verhogen van de informatieveiligheid van uw overheidsinstelling én het voldoen aan wet- en regelgeving. Voor nadere toelichting op de BIO verwijzen wij u graag naar het document “Baseline Informatiebeveiliging Overheid”. Dit bestand kunt u vinden via deze link.

Door Secquard in te zetten kunt u een flink aantal essentiële onderdelen van het technische deel van de BIO geautomatiseerd, frequent en consistent in kaart brengen. U toont u hiermee de feitelijke werking van maatregelen aan, in plaats van alleen opzet en bestaan. Daarnaast weet u precies met welke handelingen u en uw collega’s úw specifieke situatie op zeer efficiënte wijze verbetert.

Directie: verantwoordelijkheid en betrokkenheid

De BIO schrijft voor dat de directie verantwoordelijkheden verdeelt en betrokkenheid toont op gebied van informatieveiligheid. Vaak zijn maatregelen en rapportages zeer technisch waardoor directie beperkt geïnformeerd en betrokken is. Met Secquard genereert u management rapportages over de essentiële basismaatregelen waarbij, ook zonder kennis over cybersecurity, de relatie tussen risico en beveiligingsstatus begrijpelijk wordt weergeven. Tevens maken trendrapportages onderdeel uit van de rapportage.

Doordat de directie de risico's nu beter begrijpt, krijgen CISO's en IT-management de directie sneller aangehaakt bij de security-uitdagingen, en worden deze leidend in de discussie over de risico's en vervolgstappen; het accepteren van de risico's of deze mitigeren. In laatste geval moeten mogelijk additionele middelen beschikbaar worden gesteld.

Ondersteuning van Secquard bij BIO

Secquard rapporteert de technische basismaatregelen die betrekking hebben op een aantal belangrijke maatregelen uit de BIO. Onderstaande figuur geeft de relatie tussen Secquard en BIO weer. Zoals u in de figuur hierboven kunt zien is autorisaties niet opgenomen in de CIS, maar wel onderdeel van de Secquard rapportage én ISO, en dus ook de BIO.

Onderstaande tabel bevat een aantal van de belangrijkste bepalingen van de BIO waarover Secquard rapporteert. Secquard helpt bij het implementeren van deze besturingselementen en het voldoen aan BIO. De Secquard rapportage op hieronder beschreven procedures en hoofdstukken garandeert niet dat de BIO volledig wordt nageleefd voor betreffende hoofdstukken.

BIO Hoofdstuk		Omschrijving	Secquard
Beheer van bedrijfsmiddelen	8.1.1	Inventariseren van bedrijfsmiddelen	✓
	8.3.1	Beheer van verwijderbare media	✓
Toegangsbeveiliging	9.1.1	Beleid voor toegangsbeveiliging	✓
	9.1.2	Toegang tot netwerken en netwerkdiensten	✓
	9.2.1	Registratie en afmelden van gebruikers	✓
	9.2.2	Gebruikers toegang verlenen	✓
	9.2.3	Beheren van speciale toegangsrechten	✓
	9.2.4	Beheer geheime authenticatie-informatie	✓
	9.2.5	Beoordeling toegangsrechten gebruikers	✓
	9.2.6	Toegangsrechten intrekken of aanpassen	✓
	9.3.1	Geheime authenticatie-informatie gebruiken	✓
	9.4.1	Beperken van toegang tot informatie	✓
	9.4.2	Beveilgde inlogprocedures	✓
	9.4.3	Systeem voor wachtwoordbeheer	✓
	9.4.4	Speciale systeemhulpmiddelen gebruiken	✓
Cryptografie	10.1.1	Beleid cryptografische beheersmaatregelen	✓
	10.1.2	Sleutelbeheer	✓
Beveiliging bedrijfsvoering	12.2.1	Beheersmaatregelen tegen malware	✓
	12.4.1	Gebeurtenissen registreren	✓
	12.4.2	Beschermen van informatie in logbestanden	✓
	12.4.4	Kloksynchronisatie	✓
	12.5.1	Software installeren op operationele systemen	✓
	12.6.1	Beheer van technische kwetsbaarheden	✓
	12.6.2	Beperkingen voor het installeren van software	✓
	12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	✓
Communicatiebeveiliging	13.1.1	Beheersmaatregelen voor netwerken	✓
	13.1.2	Beveiliging van netwerkdiensten	✓
	13.1.3	Scheiding in netwerken	✓
	13.2.3	Elektronische berichten	✓
Acquisitie, ontwikkeling en onderhoud van informatiesystemen	14.1.2	Toepassingen op openbare netwerken beveiligen	✓
	14.2.8	Testen van systeembeveiliging	✓
Naleving	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	✓
	18.2.3	Controle op technische naleving	✓

DigiD

Veel overheidsorganisaties maken gebruik van DigiD. Hiervoor is een norm ontwikkeld waarop jaarlijks een audit wordt uitgevoerd. Wanneer niet aan de richtlijnen wordt voldaan, wordt het gebruik van DigiD verplicht gestopt. Dit kan uiterst vervelende situaties tot gevolg hebben. Zorg er daarom voor dat u alles op orde heeft. Secquard helpt u daarbij een handje.

De “Norm ICT-beveiligingsassessment DigiD” is speciaal bedoeld voor organisaties die DigiD gebruiken en hiervoor jaarlijks een ICT-beveiligingsassessment moeten doen. De norm is een selectie van richtlijnen uit het document “ICT-beveiligingsrichtlijnen voor webapplicaties” van het Nationaal Cyber Security Centrum (NCSC) en vastgesteld door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties in overleg met Logius, Rijksauditdienst en NCSC.

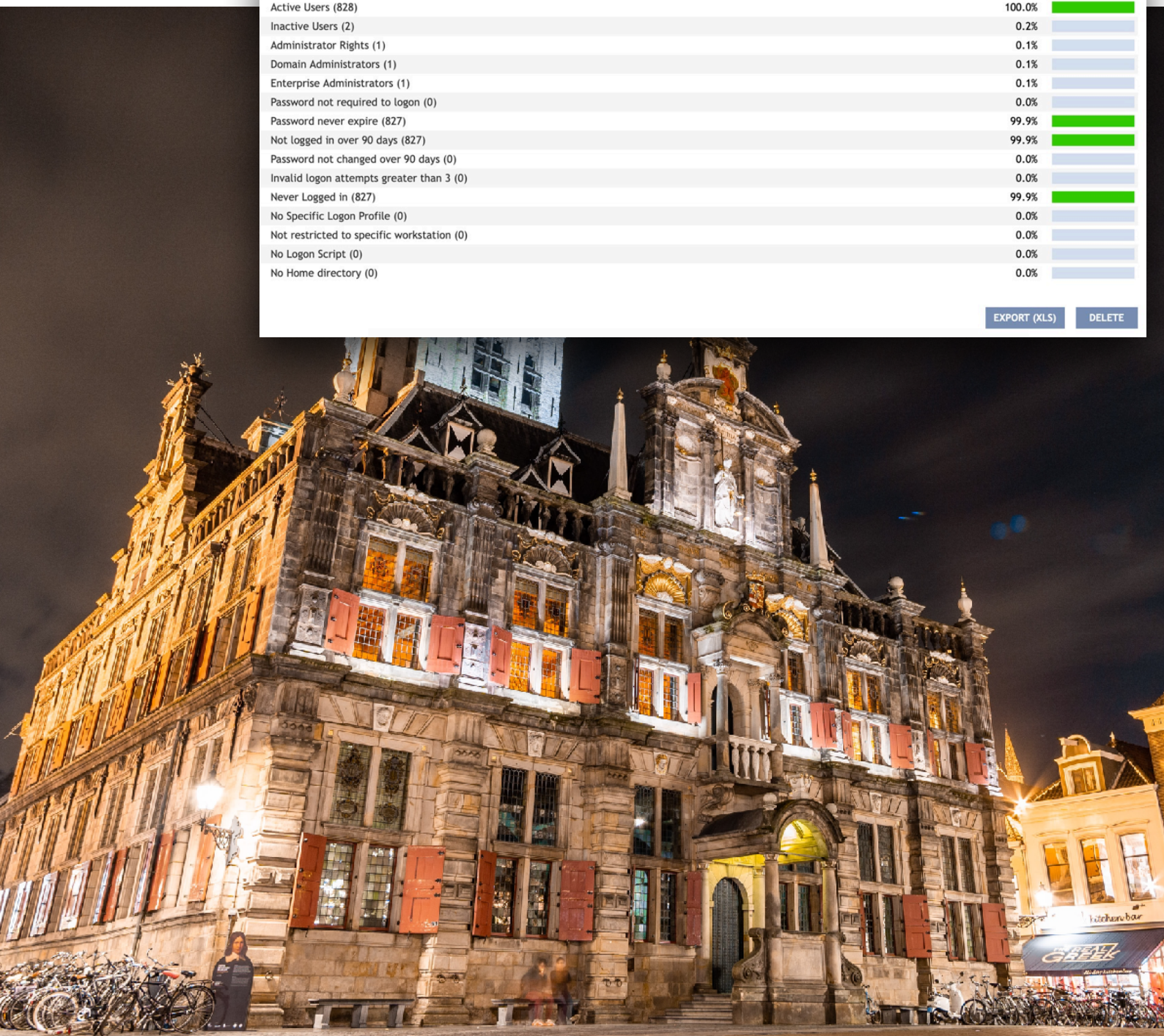
Hieronder een overzicht van de hoofdstukken uit de norm die door Secquard worden ondersteund.

Hoofdstuk	Omschrijving	Secquard	Secquard beleids-document
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	✓	✓
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.		✓
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	✓	✓
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT- componenten van de webapplicatie (scope).	✓	✓
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICTvoorzieningen.	✓	✓

Autorisaties

Het doel van maatregelen onder autorisaties is om systeemaccounts goed te beheren en toegang te verlenen op basis van het principe van minste privileges, zie ook bijvoorbeeld paragraaf 9.2.3. uit de BIO: Beheer van (speciale) toegangsrechten. Hierin wordt bijvoorbeeld voorgeschreven dat gebruikers toegang hebben voor zover dat voor uitvoering van hun taak noodzakelijk is (need-to-know, need-to-use).

Secquard brengt eenvoudig en snel in kaart welke rechten uw gebruikers genieten. Zo ziet u bijvoorbeeld wie (domain) administrator rechten hebben. Daarnaast brengt Secquard in kaart of er inactieve gebruikers zijn of gebruikers waarvan hun wachtwoord niet verloopt. Zie de figuur hieronder voor een volledig overzicht van alle gebruikerskarakteristieken die Secquard toont.



Secquard kenmerken

- ✓ 100% Nederlands product
- ✓ Korte, eenvoudige implementatie en onbeperkt schaalbaar
- ✓ Geautomatiseerde, onafhankelijke audits en rapportages
- ✓ Duidelijk inzicht in technische IT-beveiliging en compliance issues
- ✓ Helpt het beveiligingsniveau te verbeteren en risico's te mitigeren
- ✓ Consistente, periodieke rapportage met trendanalyse
- ✓ Risico assessment ten behoeve van PDCA-cycles
- ✓ Significante verlaging van rapportage-, audit- en compliance kosten

Contactgegevens

Voor meer informatie komen wij graag met u in contact!
U kunt ons bereiken via onze website, met een e-mail, of door te bellen met Marcel Kiffen, Marcel is ook via Whatsapp te bereiken.

Marcel Kiffen
0615044507

www.secquard.com

info@secquard.com