Whitepaper

De 4 security-uitdagingen voor overheden

Overheden moeten in 2017 alle zaken die ze met burgers en bedrijven doen, digitaal kunnen afhandelen volgens het principe 'digitaal waar het kan, persoonlijk waar het moet'. Verschillende overheden moeten dan als één opereren, zodat het niet uitmaakt bij welke overheidsinstantie een burger of bedrijf aanklopt. Om burgers en bedrijven centraal te zetten in de dienstverlening van de diverse overheden, moeten zij niet alleen de dienstverlening verbeteren en de efficiëntie verhogen. Daarnaast moet de informatie-uitwisseling sneller en eenvoudiger verlopen. Hier is echter een cruciale voorwaarde aan verbonden: de Digitale Overheid moet wel veilig zijn.

Onderzoek onder gemeenten

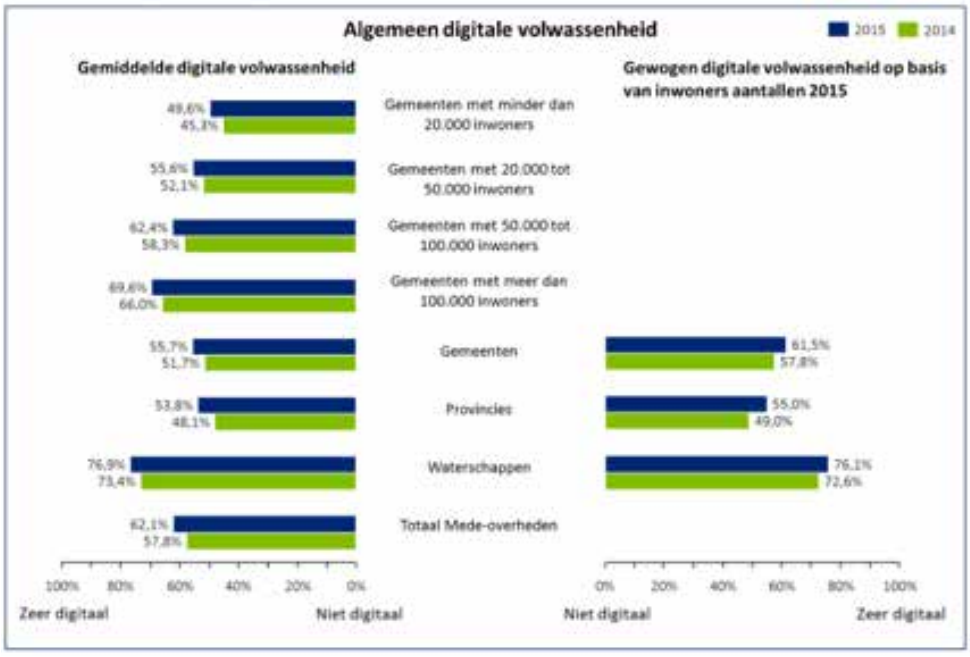
Deloitte deed in opdracht van het ministerie van BZK onderzoek naar de volwassenheid van de digitale dienstverlening bij Nederlandse overheden. Daaruit bleek dat de verschillen in digitale volwassenheid onder gemeenten nog steeds groot is. De hoogste score kwam uit op 87 procent en de laagste op 23,4 procent.

Over het algemeen scoren gemeenten met meer inwoners hoger dan kleinere gemeenten. Toch worden bij de kleinere gemeenten de grootste stappen gezet.

Onderzoek onder provincies

Bij provincies is er eveneens een positieve trend te zien in de mate van digitale volwassenheid. Ook hier geldt dat de variatie groot is. Het verschil tussen de provincie met de hoogste en de laagste digitale volwassenheid bedraagt 42,1 procent.

De waterschappen hebben de hoogste digitale volwassenheid van de onderzochte overheden. Toch zijn de verschillen hier eveneens groot. Het verschil tussen het waterschap met de hoogste digitale volwassenheid (100 procent) en de laagste (33 procent) is 66,7 procent[1].



Bron: Deloitte, Meting aanbod digitale dienstverlening 2015 (2015)

Bij het verkrijgen, verwerken en opslaan van alle gegevens die uit die digitale dienstverlening voortvloeien, is informatiebeveiliging een cruciaal aspect. Zeker in het licht van de nieuwe Nederlandse en Europese privacywetgeving ligt er voor overheden een grote verantwoordelijkheid om veilig met de aan hen toevertrouwde informatie om te gaan.

[1] Meting aanbod digitale dienstverlening 2015, Deloitte (2015)

1 Informatieveiligheid

Betrouwbare beveiliging van gevoelige informatie is een randvoorwaarde voor digitale overheden. Burgers, bedrijven en overheden zelf werken vaak digitaal en delen daarbij belangrijke gegevens. Overheden moeten met die data zeer zorgvuldig omgaan. Burgers en bedrijven moeten erop kunnen vertrouwen dat de systemen van de overheid veilig zijn en weerstand kunnen bieden aan pogingen tot misbruik en aanvallen van binnenuit of buitenaf.

Door het digitale werken, krijgen ambtenaren nieuwe verantwoordelijkheden. Iedere medewerker van een overheidsinstantie moet zich bewust zijn van de waarde van de informatie waarover hij beschikt en daarnaar handelen. Minister Plasterk van Binnenlandse Zaken en Koninkrijkrelaties (BZK) richtte drie jaar geleden de **Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID)** op dat na twee jaar is overgegaan in het digitale platform ibewustzijnoverheid.nl. Op dat platform kunnen alle medewerkers van het rijk, zbo's, gemeenten, provincies en waterschappen terecht voor actuele informatie over het veilig omgaan met gegevens. Bij het platform zijn de VNG, de Unie van Waterschappen, het Interprovinciaal Overleg, CIP en het ministerie van Binnenlandse Zaken betrokken.

In het overheidsprogramma **Digitaal 2017** zijn alle verschillende organisaties zelf verantwoordelijk voor het digitaliseren van hun diensten. Vanuit de rijksoverheid worden daar richtlijnen voor opgesteld, die onder meer in de **Nederlandse Overheid Referentie Architectuur (NORA)** staan.

De digitalisering van de overheid wordt centraal aangestuurd door digicommissaris Bas Eenhoorn. Met zijn Bureau Digicommissaris is hij er met name verantwoordelijk voor dat er een goede gezamenlijke basisinfrastructuur komt waarop alle overheidsinstanties worden aangesloten, de Generieke Digitale Infrastructuur (GDI). De GDI is een geheel van standaarden, producten en voorzieningen waar alle betrokken organisaties gebruik van kunnen maken[2]. Centraal daarbij staan de gegevens van verschillende basisregistraties waarmee gegevens gekoppeld en uitgewisseld kunnen worden. Zoals bijvoorbeeld Suwinet.

Suwinet

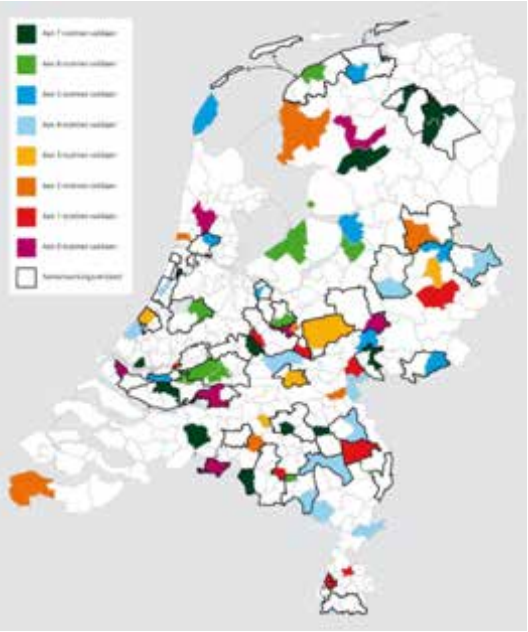
Suwinet wordt door gemeenten , uitvoerings- en overheidsorganisaties binnen het domein Werk & Inkomen – denk hierbij aan het UWV en de SVB – gebruikt om persoonsgegevens van burgers en bedrijven op te vragen. Een handig systeem, dat een zeker risico in zich heeft. Burgers vertrouwen erop dat de gebruikers van dit systeem er alles aan doen om misbruik van hun gegevens te voorkomen en hun privacy te beschermen.

Uit onderzoek van het ministerie van Sociale Zaken blijkt dat bij 83 procent van de gemeenten niet voldoende beveiligingsmaatregelen worden getroffen voor het opvragen van gegevens via Suwinet. Bij 17 procent is dat wel het geval[3]. Gemeenten werden getoetst op 7 beveiligingsnormen en slechts 1 op de 6 gemeenten bleek aan alle 7 normen te voldoen. Het gaat dan onder meer om het hebben van een actueel, formeel goedgekeurd en uitgedragen veiligheidsplan, het aanstellen van een security-officer, het werken van autorisatiematrixen en controle op het opvraaggedrag.

De 17 procent van de gemeenten die wel voldoende beveiligingsmaatregelen treffen, is een forse stijging ten opzichte van eerder onderzoek. In 2013 bleef het percentage immers op 4 steken. De vraag is of gemeenten de beveiliging hoog genoeg op de security-agenda hebben staan, zeker gezien het feit dat de normen al sinds 2002 gelden.

[2] E-government in Nederland, Herman Heringa, C't, 13 november 2015

[3] Suwinet 'veilig omgaan met elkaars gegevens', Inspectie SZW (2015)



Bron: Ministerie van Sociale Zaken en Werkgelegenheid, Suwinet 'veilig omgaan met elkaars gegevens' (2015)

Privacy

Een van de belangrijkste zaken waar overheden mee te maken krijgen, is het veilig stellen van privacygevoelige gegevens. Digitaal (samen)werken biedt ongekende mogelijkheden en vraagt tegelijkertijd om informatiebewustzijn en informatiebeveiliging. Niet alleen door te zorgen dat er geen gevoelige gegevens onbedoeld naar buiten lekken, maar ook door kritisch te kijken welke medewerkers toegang nodig hebben tot welke data. Uiteindelijk gaat het erom dat informatie vanuit diverse rollen en verschillende verantwoordelijkheden van ambtenaren verantwoord wordt gebruikt.

Overheidsmedewerkers hebben dagelijks te maken met gegevens en informatie. Enerzijds is het noodzakelijk om de privacy van de burger te respecteren en bedrijfsgegevens op een vertrouwelijke manier te behandelen. Anderzijds wil een overheidsmedewerker ook graag een goede dienstverlener zijn en effectief & efficiënt werken. In sommige gevallen staat dit haaks op elkaar.

De verantwoordelijkheid voor het verantwoorde gebruik van beschikbare data ligt bij de ambtenaar. Informatiebeveiliging en privacy zijn nauw met elkaar verbonden. Waar informatieveiligheid zich richt op informatie – dat wil zeggen betekenisvolle gegevens – richt privacy zich op persoonsgegevens. Bij informatieveiligheid gaat het om vertrouwelijkheid van informatie en bij privacy gaat het om het beschermen van de privé-sfeer.

Meldplicht datalekken

Op 1 januari 2016 is de meldplicht datalekken in werking getreden. Deze maatregel is een uitbreiding van de Wet bescherming persoonsgegevens (Wbp) en vereist dat iedere organisatie die privacygevoelige gegevens verwerkt een mogelijk datalek direct meldt bij de Autoriteit Persoonsgegevens (AP).

Als het verlies van gevoelige informatie bewust wordt verzwegen, kan de AP een boete opleggen die kan oplopen tot maximaal 820.000 euro. Alleen dataverlies die ernstige nadelige gevolgen kan hebben voor de betrokkenen moet worden gemeld. Dataverlies kan optreden doordat de overheidssystemen gehackt zijn en er op die manier privacygevoelige data is ontvreemd, maar ook een verkeerd geadresseerde e-mail met gevoelige gegevens of een verloren USB-stick of telefoon waar kwetsbare data op staan, zijn datalekken.

Europese Privacy Verordening

De Europese Privacy Verordening (EPV) lijkt sterk op de meldplicht datalekken, en is eind 2015 op Europees niveau ingesteld. Nadat de verordening is aangenomen, hebben lidstaten nog 2 jaar de tijd om de regels te implementeren. Dat betekent dat deze EPV vanaf eind 2017 daadwerkelijk van kracht wordt.

Smart city

Gemeenten worden in toenemende mate slimmer, doordat ze gebruikmaken van sensoren en verschillende informatiebronnen met elkaar combineren. Die enorme poel aan data (ook wel big data genoemd) brengt ongekende mogelijkheden met zich mee. Nieuwe dienstverlening, efficiëntie en kostenverlaging zijn een aantal voordelen. Toch moeten gemeenten zich ook op dit vlak bewustzijn van de mogelijke risico's die onvoldoende beveiliging van deze data met zich meebrengt.

Diverse gemeenten zijn al druk bezig met een plan voor hun smart city en sommige experimenteren al volop. Denk hierbij aan projecten met sensoren die de drukte in fietsenstallingen meten en op geautomatiseerde wijze mensenmassa's tijdens evenementen in de gaten houden[4]. Maar aan deze digitalisering zit een keerzijde. Zo kunnen sensoren, besturingssystemen en infrastructuur worden gehackt, waardoor gemeenten kwetsbaar worden. We kennen inmiddels talloze voorbeelden van slimme straatverlichting die door hackers op afstand kon worden bediend nadat ze zich onrechtmatig toegang hadden verschaft tot de systemen die de verlichting regelen.

Het beveiligen van al deze systemen en data is cruciaal voor het slagen van smartcityprojecten. In de praktijk blijken vooral de kleinere gemeenten niet altijd over de juiste hoeveelheid middelen en kennis te beschikken om dit te voorkomen.

[4] Hoe een slimme stad een dom idee kan worden, Wouter van Noort, NRC, 17 oktober 2015

2 Cybercrime

Cyberdreigingen nemen alsmaar toe. Iedere dag vinden er hackpogingen, aanvallen en andere incidenten plaats. Daarom is het noodzakelijk om permanent te werken aan informatieveiligheid - aan zowel weerbaarheid als herstelvermogen. Overheden moeten aanvallen snel in kaart kunnen brengen en analyseren. Alleen zo is een snelle en correcte afhandeling van incidenten mogelijk.

Om data en informatie zo goed mogelijk te kunnen beschermen, moet een overheidsorganisatie weten welke informatie voor hen van cruciaal belang is. In de markt worden deze data ook wel de 'kroonjuwelen' van een instantie genoemd. Dat kunnen privacygevoelige gegevens zijn, maar ook procesbeschrijvingen voor een vitale infrastructuur of andere kennis en informatie. Op basis van deze kroonjuwelen kunnen instellingen vervolgens een plan opstellen en uitrollen waarmee ze effectief kunnen worden beschermd.

In dit plan moeten zij ook stilstaan bij de interne organisatie, de rollen en verantwoordelijkheden van de ambtenaren. Hoe specifieker de toegang wordt geregeld tot alleen de data die nodig zijn voor de eigen werkzaamheden, hoe kleiner de kans dat zich een lek voordoet. Het spreekt voor zich dat het plan ook de processtappen bevat voor het geval er toch een incident plaatsvindt.

DDoS

Regelmatig komen er gemeenten en andere overheden in het nieuws als ze slachtoffer zijn van een zogenaamde distributed denial of service-aanval (DDoS). Bij een DDoS-aanval worden grote hoeveelheden data naar servers gestuurd zodat die overbelast raken. Het gevolg is dat het netwerk of een deel daarvan plat ligt en gemeenten, provincies en waterschappen digitaal niet meer bereikbaar zijn voor burgers en bedrijven.

Ransomware

Ransomware is kwaadaardige software die vaak via e-mail een overheidsinstelling binnenkomt. Als de e-mail of bijgevoegde bijlage wordt geopend, versleutelt de software alle belangrijke bestanden waar de ambtenaar toegang tot heeft. Vervolgens verschijnt er een melding op het scherm waarin wordt gemeld dat de bestanden versleuteld zijn en dat tegen betaling de encryptiesleutel wordt geleverd. Vaak staat er ook een aftelklok bij om aan te geven hoeveel tijd er is om te betalen. Kiezen gedupeerden ervoor om niet te betalen, dan worden de bestanden na het aflopen van de tijd vernietigd.

Om te zorgen dat ransomware zo weinig mogelijk schade kan aanrichten bij de IT-systemen, is het belangrijk om geen mails of bijlagen te openen die afkomstig zijn van onbekenden. Omdat we niet altijd de afzenders van mail kunnen herkennen, zijn ook technologische voorzorgsmaatregelen nodig. Denk hierbij aan slimme firewalls met antivirusfunctionaliteit en het continu updaten van software. Tot slot is het ontzettend belangrijk om regelmatig back-ups te maken en die goed te testen. Bewaar ze op een veilige plek.

Als een gemeente, provincie of waterschap toch wordt getroffen door ransomware, kunnen zij het besmette systeem het beste direct loskoppelen van de rest van het netwerk. Een tool detecteert en ruimt die malware op het systeem op. Die software zorgt er niet voor dat de gegijzelde bestanden teruggehaald worden, maar kan de ransomware wel van het systeem verwijderen. De ransomware verspreidt zich niet automatisch verder of kopieert zichzelf niet op de systemen.

Omdat ransomware bij alle bestanden en systeeminstellingen kan waar de gebruiker toegang toe heeft, is het verstandig om kritisch te kijken naar de rechten van gebruikers op het netwerk en deze rechten te beschermen. Hoeven bepaalde documenten alleen maar bekeken te worden? Geef een gebruiker dan alleen leesrechten. Zo kan de malware de bestanden wel lezen, maar ze niet veranderen of versleutelen. In de praktijk hebben veel gebruikers volledige administratorrechten en dat maakt een overheidsinstantie kwetsbaar voor ransomware. Het is aan te raden om niemand standaard administratorrechten te geven. Als dat toch wenselijk is, zorg er dan voor dat iemand zich met die rechten kan aanmelden voor bepaalde taken. Op die manier wordt de toegang tot instellingen beperkt, wat gunstig is in het geval van besmetting.

Advanced Persistent Threats

Een advanced persistent threat (APT) is een cyberaanval waarbij een ongeautoriseerd persoon toegang weet te verkrijgen tot het netwerk en daar lange tijd ongemerkt zijn gang kan gaan. Vaak worden organisaties, instellingen of landen getroffen die over waardevolle data beschikken. De aanvaller is volhardend in zowel de pogingen om een organisatie of instantie binnen te dringen als om heimelijk binnen te blijven. Tijdens de APT-aanval verzamelt de aanvaller vooral vertrouwelijke informatie of treft voorbereidingen om de werking van vitale componenten te verstoren. Het merendeel van deze aanvallen is eenvoudig van aard en vooral succesvol door het ontbreken van adequate detectie en beveiligingsmaatregelen.

Het National Cyber Security Center (NCSC) heeft een aantal mogelijke maatregelen opgesteld tegen een APT-aanval. Naast deze maatregelen is het raadzaam om een aanvullende APT-oplossing te implementeren. De adviezen van het NCSC komen in het kort op het volgende neer:

- Detectie: start een onderzoek binnen de (vitale) ICT-infrastructuur op de aanwezigheid van malware, onduidelijke systeemrechten en/of back-doors in hard- en/of software. Monitor al het verkeer, alle services en andere activiteiten op het netwerk.
- Incident response: richt een toegewijd security intelligence/operational center op en stel een team samen dat autonoom en met de juiste bevoegdheden en middelen kan optreden in geval van een APT-incident. Zorg dat dit team zo klein mogelijk is en goede directe contacten heeft met het hoger management. Stel een response-plan op voor incidenten en calamiteiten en test dit regelmatig.
- Infrastructuur en techniek: Blokkeer toegang van vreemde apparaten tot de infrastructuur en sta alleen het uitvoeren van bekende programma's toe. Segmenteer daarnaast de infrastructuur, en zo ook het beheernetwerk. Denk na over het gebruik van standaardoplossingen en inrichtingsmodellen bij het inrichten van de vitale omgeving.
- Governance: maak gebruik van een risicomanagementmethode als ISO27005 en normen zoals ISO27001/2. Onderzoek welke informatie voor aanvallers waardevol kan zijn. Zorg voor verregaande awareness-trainingen en update zo snel mogelijk de componenten binnen de (vitale) omgevingen[5].

[4] De aanhouder wint, de wereld van Advanced Persistent Threats, Nationaal Cyber Security Centrum (2013)

3 BYOD

Bij overheden doet Het Nieuwe Werken steeds meer zijn intrede. Het tijd-, plaats- en apparaatonafhankelijk werken is bezig met een forse opmars. Dat betekent niet alleen gemak voor ambtenaren, maar ook een uitdaging op het gebied van informatiebeveiliging. Bij BYOD (bring your own device) is het belangrijk dat de apparatuur die wordt gebruikt, ook daadwerkelijk goed beveiligd is als medewerkers naast hun privé-zaken werkgerelateerde data inzien of bewerken.

Wifi

Govroam is een slimme manier om ambtenaren en gasten toegang te geven tot bestaande wifi-netwerken van overheidsorganisaties. Gebruikers kunnen eenvoudig met hun eigen gebruikersnaam en wachtwoord inloggen. De overheid bestaat uit ruim 1.000 organisaties (gemeenten, provincies, waterschappen, departementen, uitvoeringsinstanties, etc), en traditioneel is iedere organisatie gewend om zijn eigen voorzieningen zelf te regelen.

Met Het Nieuwe Werken zit niet iedere ambtenaar dagelijks op kantoor. Dan is het wenselijk om op een andere locatie snel en eenvoudig in te kunnen loggen op het netwerk, zonder dat er aparte wachtwoorden moeten worden aangevraagd of er een (onveilig) open wifi-netwerk gebruikt moet worden. De technische infrastructuur van Govroam bestaat uit een landelijk netwerk van radiusservers en wordt beheerd door SURFnet.

Het is raadzaam om een apart gastnetwerk in te richten voor bezoekers. Op deze manier kan een overheidsinstantie gasten wel internettoegang aanbieden, maar blijft dat verkeer strikt gescheiden van het eigen netwerk waarop bestanden en apparaten beschikbaar zijn.

Verschillende BYOD-scenario's

Technologie verrijkt de digitale overheden, mobiele apparaten kunnen daar een goede bijdrage aan leveren. Dan is het belangrijk dat het (draadloze) netwerk daarop is ingericht. Er is wijdverspreid enthousiasme voor het concept BYOD, waarbij ambtenaren hun eigen apparaten gebruiken. Ook marktonderzoeksbureau Gartner definieert BYOD als belangrijke ontwikkeling. Bandbreedte, netwerkconnectiviteit en beveiliging zijn de grootste zorgen om de impact van BYOD in goede banen te leiden.

We kennen verschillende manieren van aanpak voor het omgaan met zelf meegebrachte mobiele apparatuur.

1. Een overheidsinstelling kan ervoor kiezen om toe te staan dat ambtenaren hun eigen spullen meenemen. Dat betekent wel dat de netwerkomgeving meerdere merken apparaten met bijbehorende besturingssystemen moet kunnen ondersteunen.
2. Een andere mogelijkheid is dat de overheidsinstantie ervoor kiest om medewerkers met mobiele apparatuur uit te rusten. Dat vergt een flinke investering, maar betekent eveneens eenvoudiger IT-beheer en ondersteuning. Bovendien heeft op deze wijze iedere werknemer toegang tot een mobiel apparaat.
3. De meeste overheden kiezen echter voor een hybride aanpak waarbij de twee hierboven beschreven mogelijkheden worden gecombineerd. Daarbij wordt BYOD ondersteund en worden gestandaardiseerde laptops ingezet voor algemeen gebruik.

Voor welke aanpak overheden ook kiezen, het (draadloze) netwerk moet klaar zijn voor het gebruik van al die mobiele apparatuur. Dat kan betekenen dat de keuze maken voor een apart gastennetwerk, waarop bezoekers toegang hebben. Het netwerk voor medewerkers van de overheidsinstelling wordt daarmee afgeschermd. Door verschillende accesspoints te gebruiken kan het dataverkeer eerlijk worden verdeeld. Zware en belangrijke gebruikers kunnen bijvoorbeeld toegang krijgen tot een 5GHz draadloze verbinding, terwijl gebruikers met minder prioriteit toegang krijgen tot een 2,4 GHz verbinding.

Draadloos

Het toenemende gebruik van slimme mobiele apparaten zoals tablets, smartphones en notebooks zorgt voor een enorme BYOD-explosie en stelt daarmee steeds hogere eisen aan draadloze netwerken. Overheidsorganisaties willen de productiviteitswinst die deze apparaten bieden graag benutten, maar tegelijkertijd het netwerk niet in gevaar brengen. Het is belangrijker dan ooit om controle te hebben over het gehele netwerk binnen een overheidsinstantie – zowel bedraad als draadloos.

Conclusie

Vanaf 2017 moeten overheden alle zaken die ze met burgers en bedrijven doen, digitaal kunnen afhandelen volgens het principe 'digitaal waar het kan, persoonlijk waar het moet'. Daarbij moeten verschillende overheden als één opereren, zodat het niet uitmaakt bij welke overheidsinstantie een burger of bedrijf aanklopt.

Een van de belangrijkste zaken waar overheden mee te maken krijgen, is het veilig stellen van privacygevoelige gegevens. Niet alleen door te zorgen dat er geen gevoelige gegevens onbedoeld naar buiten lekken, maar ook door kritisch te kijken welke medewerkers toegang nodig hebben tot welke data.

De ontwikkeling naar BYOD speelt daarin ook een rol. Ambtenaren krijgen toegang tot overheidsgegevens via hun persoonlijke devices. Het spreekt voor zich dat de beveiliging van zowel die apparatuur als de gegevens cruciaal zijn. Daarnaast nemen cyberdreigingen hand over hand toe. Iedere dag vinden er hackpogingen, aanvallen en andere incidenten plaats. Ook daarom is het noodzakelijk om permanent te werken aan informatieveiligheid.

Producten

WatchGuard biedt diverse productlijnen die onderwijsinstellingen kunnen helpen hun netwerk beter te beschermen tegen cyberaanvallen en ongewenste zaken.

- **Next-Generation Firewall**
  Door het inzetten van een Next-Generation Firewall-oplossing aan de rand van het netwerk, zorgt een organisatie voor zijn veiligheid. Deze productlijn bevat onder meer een intrusion prevention service, application control, data loss prevention en een APT blocker. De functies van deze oplossingen kunnen naar believen worden geconfigureerd. Hierdoor functioneert de firewall naar de specifieke wensen van iedere organisatie.

- **Unified Threat Management**
  Dit alles-in-een security-platform is eenvoudig schaalbaar en betaalbaar. Het bevat, naast de oplossingen uit de Next-Generation Firewall, een gateway antivirus, een spam- en web blocker en reputation enabled defense. Het platform kan zonder al te veel moeite worden gedistribueerd op ieder netwerk van de organisatie.

- **Overige security oplossingen**
  Daarnaast biedt WatchGuard bescherming voor access points en IPSec VPN Clients, maar ook:

  - Dimension
    Kritische besluiten over netwerksecurity moeten vaak snel en met weinig informatie worden gemaakt. Dimension brengt de inzichten van big data naar netwerkbeveiliging. Hierdoor kunnen beslissingen snel, effectief en goed geïnformeerd worden genomen.

  - Secure Wireless
    De huidige digitale bedreigingen beperken zich niet alleen tot de desktop. Dat betekent dat ook de security oplossingen een bredere blik moeten hebben. Deze oplossing breidt de voordelen van het UTM-platform uit naar het draadloze netwerk.

  - Virtual Solutions
    De digitale wereld verandert met een snelheid die nauwelijks bij te houden is. In gevirtualiseerde omgevingen worden data tussen applicaties, divisies en bedrijven heen en weer gestuurd, zonder ooit een fysiek netwerkpad te kruisen. Dat heeft gevolgen voor de beveiliging. Deze oplossing beschermt de interne grenzen van applicaties en organisaties.

Hoe staat het met onze informatieveiligheid?
Steeds meer overheden werken digitaal en wisselen daarbij belangrijke gegevens uit. Het is dus van belang dat overheden zorgvuldig met deze gegevens omgaan en de mogelijke risico's op lekken goed in kaart brengen. Overheidssystemen moeten veilig zijn en weerstand kunnen bieden aan pogingen tot misbruik en aanvallen van binnenuit en buitenaf.

De rijksoverheid heeft via iBewustzijn Overheid een gratis app beschikbaar gesteld die bestuurders, managers en medewerkers concrete handvatten biedt voor het stellen van de juiste vragen over informatieveiligheid. De iVeiligheidsapp is hier voor iOS verkrijgbaar en hier voor Android.