Reference case

# Pinewood biedt Vitens concreet stappenplan naar effectieve informatiebeveiliging




**Waterbedrijf Vitens heeft een passie voor water. De organisatie wint, zuivert en levert drinkwater van topkwaliteit aan 5,4 miljoen klanten in Friesland, Overijssel, Flevoland, Gelderland en Utrecht. Vitens werd in het verleden vanuit regio's aangestuurd, maar inmiddels is overstap naar een centrale procesgeoriënteerde organisatie, Vitens 2.0, gemaakt.**

De nieuwe organisatie vroeg een andere inrichting van de informatiebeveiliging. Een security masterclass van Pinewood legde de basis voor de ontwikkeling van een effectief informatiebeveiligingsbeleid, inclusief een concreet uitvoeringsplan.

"Als waterbedrijf beheren we een cruciale infrastructuur en dat vereist goede informatiebeveiliging", zegt Bert Bannink, Manager Informatie Management bij Vitens. "De huidige informatiebeveiliging is goed op orde, maar we wilden die verder borgen en onderbouwen. Het zwaartepunt lag voorheen bij de techniek. Om naast techniek ook het beleid en de organisatie voor informatiebeveiliging te optimaliseren, wilden we onze situatie inventariseren, een goed beleid opstellen en daar ook een concreet uitvoeringsplan aan koppelen. Op die manier wilden we het informatiebeveiligingsbeleid beter afstemmen op de doelen van onze organisatie en beveiliging beter inbedden."

## Pragmatische aanpak

Om dit proces efficiënt te laten verlopen, zocht Vitens de ondersteuning van een ervaren securitypartner. De masterclass van Pinewood bood een heldere en pragmatische aanpak om snel tot een evenwichtig beveiligingsbeleid te komen, inclusief een uitvoeringsplan. Bannink: "Pinewood heeft aantoonbare ervaring met het ontwikkelen van beveiligingsbeleid. Hun specialisten kennen het proces en samen hebben we alle noodzakelijke stappen doorlopen om een effectief beleid en uitvoeringsplan te maken. ISO 27002 was daarbij de norm. Pinewood kent deze eisen en kan ook inschatten welke inspanningen nodig zijn om hier aan te voldoen. Die kennis en ervaring hebben we benut om snel ons eigen beleid te schrijven."

## Breder kader

Om te onderstrepen dat beveiliging geen exclusief IT-onderwerp is, zijn mensen uit de gehele organi-

satie bij het proces betrokken. Bannink: “Zo werden deelnemers min of meer gedwongen om beveiliging in een breder kader te zien. Dat was nodig om de beschikbare kennis en urgentie naar boven te halen. We hebben gesproken over de verantwoordelijkheid voor specifieke informatie en systemen en wie de beveiliging daarvan op orde moet houden. Als het gaat om systemen met klantgegevens, is dat dus niet per definitie de IT-organisatie. Dat besef is cruciaal voor het bepalen en uitvoeren van de benodigde maatregelen en ondersteunende processen. Door samen over beveiliging te praten hebben we onze eigen prioriteiten gesteld en risicoanalyses gemaakt. Zo zijn we tot het beleid gekomen dat goed aansluit bij onze organisatie en activiteiten.”

## Bewustwording

Bewustwording speelt een belangrijke rol in het succes van informatiebeveiligingsbeleid. Volgens Bannink erkent iedereen bij Vitens het belang van goede beveiliging. Maar als dat het onthouden van meerdere wachtwoorden betekent, is het toch lastig. Het doel is veilig zijn, maar wel met een minimale impact op de bedrijfsactiviteiten. Als die impact onvermijdelijk is, is het cruciaal om het belang van beleid en maatregelen goed kenbaar te maken aan medewerkers en managers. “Voor de autorisatie op specifieke systemen hebben we nu een duidelijke procedure ingericht die samen met de business is bepaald en door hen wordt aangestuurd. De vrijblijvendheid en flexibiliteit van ‘even de helpdesk bellen’ als je een wachtwoord vergeten bent, is daarbij uitgesloten. Een striktere procedure voelt voor veel mensen in eerste instantie minder flexibel. Maar naast een betere beveiliging zijn er zeker praktische voordelen. Een geautomatiseerde procedure voor het aanvragen van een nieuw wachtwoord is bijvoorbeeld 24 uur per dag actief. Dat is efficiënter, maar belangrijker is dat het proces transparant en toetsbaar is.”
Een ander praktisch voorbeeld is de scheiding van de proces- en kantoorautomatisering. “Als waterbedrijf moeten we onze informatie, van de infrastructuur en klanten, goed beheren. We hebben op dat vlak te maken met strikte eisen voor de scheiding van de procesautomatisering en kantoorautomatisering. Maar deze informatie gaat uiteindelijk wel over hetzelfde bedrijfsnetwerk. Het is belangrijk om dat goed in kaart te hebben om passende maatregelen te nemen. Dat inzicht is een belangrijke basis voor effectieve en complete informatiebeveiliging.”

## Uitvoering

De pragmatische aanpak van de Pinewood masterclass past volgens Bannink goed bij Vitens. “We hebben in korte tijd een goed beleid en plan geschreven. Het is nu zaak om dit de komende tijd te implementeren en aan te scherpen. Door de masterclass is het intern besef rondom informatiebeveiliging sterk gegroeid. Bovendien hebben we handvatten om te investeren in gerichte maatregelen.” Bannink vindt het voor de bewustwording belangrijk dat Vitens het proces zelf heeft doorlopen. “We hebben nu echt ons eigen beleid en kunnen deze cyclus ook zelfstandig doorlopen als de omstandigheden veranderen. In eerste instantie was het de bedoeling om de uitvoering van de benodigde maatregelen helemaal zelf te doen. Momenteel beschikken we echter niet over de capaciteit om dit te doen, vandaar dat we daarvoor tijdelijk de hulp van Pinewood inschakelen. Belangrijk is dat we nu zeker weten dat de maatregelen die we implementeren goed aansluiten op het beveiligingsniveau dat bij onze organisatie past. Daarmee is informatiebeveiliging uitgegroeid tot een integraal onderdeel van ons bedrijf, nu en in de toekomst.”

PINEWOOD
Specialist in informatiebeveiliging

Pinewood bv
Delftechpark 57
2628 XJ Delft
**T (015) 251 36 36**
info@pinewood.nl
***www.pinewood.nl***