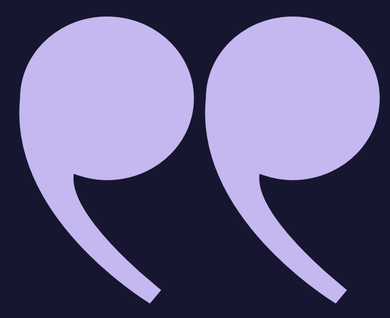

Ruud van den Einden

Verbetering en ondersteuning voor een veilige gemeente

INFINITY IT

Ruud van den Einden is sinds twee jaar als coördinator informatie en CISO verantwoordelijk voor de informatieverwerking, digitalisering en informatiebeveiliging van Gemeente Bergen.

Gemeente Bergen is een kleine gemeente met zo'n dertienduizend inwoners. Twee jaar geleden werkte de gemeente nog veelal op papier, maar dankzij het doorzettingsvermogen van team informatie en de juiste IT partners is de digitalisering van Gemeente Bergen een feit. Via zijn neef Willem Wismans kwam Ruud in aanraking met Infinity IT voor managed services. Van den Einden omschrijft Infinity IT als een uitstekende partner, die geeft om kennisdeling, die buiten de gebaande paden durft te kijken naar innovatieve oplossingen en die bovendien investeert in de IT specialisten van de toekomst door veel samen te werken met Hogescholen. Met Infinity IT ging Ruud ook het gesprek aan over cyber security en sinds april maakt de gemeente voor de SOC/SIEM oplossing gebruik van Arctic Wolf. De combinatie van een Security Information & Event Management en een Security Opertations Centre zorgt voor meer cyberweerbaarheid van de gemeente. Dat is handig om teamleden en het college van B&W van de juiste inzichten en informatie te voorzien en om de data van de Gemeente Bergen veilig te houden. Dat gaat zelfs boven verwachting; van miljoenen logregels, naar dertigduizend threats tot slechts honderd activiteiten die het IT team zelf moet bekijken. Wat geen vreemd gedrag is, wordt aangepast in de software, waardoor het aantal 'normaal gedrag' meldingen steeds verder afnemen en de echte activiteiten die onder de loep moeten worden genomen overblijven. Ruud is van het hele proces enorm onder de indruk en deelt zijn ervaringen daarom open en met veel enthousiasme.

"Normaal praat ik niet over software om de boze buitenwereld niet onnodig slimmer te maken, maar de manier waarop we in dit proces zijn ondersteund verdient de aandacht." Zo begint Ruud zijn verhaal.

"Een militaire operatie die staat als een huis"

INFINITY IT

“Mede door de Baseline Informatiebeveiliging Overheid moeten we als gemeente een SOC/SIEM oplossing hebben, maar als kleine gemeente is dat nogal een uitdaging. Wij hebben daar de mensen en het budget gewoon niet voor. Daarom is er in het verleden een landelijke aanbesteding uitgezet. De gekozen oplossing bleek echter te gecompliceerd en onhaalbaar en is zodoende ontbonden. Wij hebben er toen bewust voor gekozen om niet meer mee te gaan in een nieuwe ronde, maar om voor een eigen oplossing te kiezen. Daarbij hebben we naar verschillende partijen gekeken zoals Darktrace en Arctic Wolf. De keuze is uiteindelijk op Arctic Wolf gevallen omdat zij niet alleen 24/7 ondersteunen, maar ook de oplossing bemannen. Sterker nog, ik heb nu meer ondersteuning voor dezelfde prijs dan dat ik via de aanbesteding of bij Darktrace zou hebben gekregen."

"Arctic Wolf monitort de hele omgeving en stelt ons op de hoogte van de zaken die we moeten bekijken. Dat ontzorgt en bespaart tijd. Er is 24/7 iemand die ons kan helpen bij vragen. De onboarding verliep razendsnel, als een militaire operatie.” Juist omdat hij daar zo van onder de indruk is, vertelt Ruud enthousiast verder: “De begeleiding was echt heel goed. De volledige omgeving is in kaart gebracht om de gehele organisatie veilig te maken. Arctic Wolf heeft daar een zeer uitgebreid draaiboek voor en dat heeft mij ook weer nieuwe inzichten gegeven om de gemeente veiliger te maken. Tijdens de onboarding hebben we bijzonderheden aan moeten geven die we extra in de gaten willen houden. Dat zijn echt niet alleen maar de devices van de burgemeester of wethouders. Iedereen binnen de gemeente is wat dat betreft belangrijk, spear-fishing attacks worden immers steeds beter. Het is dan ook fijn om te weten dat onze data en activiteiten goed gemonitord en gelogd worden.”

"Inzicht in wat er gebeurt om de juiste acties te kunnen ondernemen"

Menselijk handelen is het grootste risico als het gaat om informatiebeveiliging. Ruim 90 procent van de succesvolle aanvallen ontstaan door een phishing actie. Security Awareness staat zodoende op vrijwel iedere boardroom agenda. Binnen de Gemeente Bergen is dat niet anders. "We zijn constant bezig met het creëren van bewustwording bij onze medewerkers en leveranciers. De scheidslijn tussen werk en privé verdwijnt. Dat betekent dat we naar alle devices en omstandigheden kijken qua veilig werken. Natuurlijk wel met optimaal gemak voor medewerkers, door bijvoorbeeld zo veel mogelijk Single Sign On te implementeren. Om de bewustwording te vergroten hebben we een aantal leuke activiteiten bedacht. Informatiebeveiliging is de verantwoordelijkheid van iedereen binnen de gemeente, niet alleen van mij. Zo hadden we onlangs een doos in de gang gezet met de vraag, ‘Wie is er verantwoordelijk voor informatiebeveiliging?’ Als de doos geopend werd zag men een spiegel. Ik vind het belangrijk om op een leuke manier informatiebeveiliging onder de aandacht te brengen. Samen met de burgemeester ga ik deze zomer naar een cyber security game in de regio en we krijgen binnenkort op locatie nog

"Iedere gemeente, ook de grotere, is hierbij gebaat!"

een leuke activiteit. Als alle medewerkers beseffen wat hun rol is in het geheel en wij de bewustwording van alle medewerkers hebben verbeterd, dan hebben we al veel bereikt.” Aldus Van den Einden. Een mooi streven, maar makkelijker gezegd dan gedaan met alle nieuwe wet- en regelgeving als de AVG, BIO, NIS2 etc.etc. Logisch wel, maar ook een uitdaging om goed in te regelen en mensen daarin mee te nemen.

Ruud vervolgt: “Tegenwoordig is remote werken steeds belangrijker. Ik zou zelf bijvoorbeeld nog best wel eens een oude, gele schoolbus willen ombouwen en daarmee gaan reizen en remote werken. Als we technisch alles goed op orde hebben en houden, dan kan dat ook gewoon zonder het risico op een security breach te vergroten. Zo kijken we ook steeds meer naar Software As A Service oplossingen, maar we houden ook een deel op locatie. Er zijn genoeg verhalen te vinden, ook binnen de gemeentes van breaches en de kosten die daarmee gemoeid zijn. Dan hebben we het nog niet eens over de periode van dataverlies en herstel. Wat dat betreft ben ik echt enorm blij met de extra beveiligingslaag en de inzichten die we daaruit krijgen. Een usb stick in een device merken we nog wel op, maar verder is het toch vaak handelen op basis van onderbuikgevoel en karige informatie. Nu kunnen we acties ondernemen op basis van inzichten. Arctic Wolf wijst ons ook actief op verbeteringen en die adviezen helpen enorm. Ik slaap er dan ook echt veel beter van. Alles bij elkaar genomen, het partnership met Infinity IT, de onboarding, de monitoring, de adviezen, rapportages, ondersteuning en inzichten zijn echt enorm goed. Daar zouden andere gemeentes, ook de grotere zeker baat bij hebben. Dat weet ik zeker. Je zou het niet geloven, maar als alle projecten zo soepel en strak liepen dan had ik geen uitdagingen meer over.”