Foto's: Mariska Klok

Martijn Hoving (Woonstede):

Managementsteun voorwaardelijk voor informatiebeveiliging

'Informatiebeveiliging naar een hoger volwassenheidsniveau brengen'. Met dat doel voor ogen wil **Woonstede** uit Ede haar organisatie beter beveiligen. Wat houdt het echter in om volwassen te zijn rondom informatiebeveiliging, en hoe richt je je organisatie daarvoor in? CorporatieGids Magazine sprak met **Martijn Hoving**, Informatieadviseur bij de Gelderse corporatie.

Naast informatieadviseur is Martijn ook als Security Officer actief bij Woonstede. "In deze rol functioneer ik namens het management als zelfstandig adviseur op het gebied van informatiebeveiliging," legt hij uit. "Hierbij richt ik mij vooral op de naleving van informatiebeveiliging in de operationele processen. De toegevoegde waarde zit hem in de kennis van de organisatie en afdelingen, en de vertaalslag die moet worden gemaakt van algemene informatiebeveiligingsnormen naar de specifieke bedrijfssituatie."

Logische uitbreiding

De rol als Security Officer ziet Martijn als een logische uitbreiding van zijn functie als informatieadviseur. "In die laatstgenoemde positie ben ik vooral bezig om informatiesystemen goed aan te laten sluiten op onze bedrijfsvoering. Dan moet je denken aan bijvoorbeeld het selecteren, implementeren en inrichten van systemen. Hierdoor heb je een goed overzicht van de processen van Woonstede en het complete applicatielandschap. Door de rol als Security Officer voeg je hier informatiebeveiliging aan toe, wat een logische volgende stap is."

Hoger volwassenheidsniveau

Met als doel om informatiebeveiliging naar een hoger volwassenheidsniveau te brengen, voerde Woonstede afgelopen jaar een nulmeting en phishingtest uit. "De nulmeting was vooral bedoeld om te bepalen in hoeverre we voldoen aan de AVG en BIC (Baseline Informatiebeveiliging Corporaties). Op basis hiervan kunnen we bepalen waar nog aandacht aan moet worden besteed. De phishingtest was onderdeel van onze bewustwordingscampagne onder medewerkers."

Continu aandachtspunt

"Uit de nulmeting bleek onder andere dat we veel zaken al goed geregeld hebben," vertelt Martijn. "De stappen die we nog moeten nemen gaan hoofdzakelijk om het daadwerkelijk opnemen van genomen maatregelen, procedures en richtlijnen in ons beleid. Daar zijn we nu volop mee bezig. Ook rond de AVG hebben wij nu de basis op orde, hoewel dit wel een continu aandachtspunt blijft. We zijn nu bijvoorbeeld de implementatie van nieuwe KCC-software aan het voorbereiden, en hiervoor voeren we onder andere een DPIA uit om de privacy impact te bepalen. Zo zullen er altijd ontwikkelingen zijn waarbij we aandacht voor de AVG en privacy moeten hebben."

Steun van het management

"Een van de belangrijkste pijlers van informatiebeveiliging is de steun van het management," legt Martijn uit op de vraag wat volgens hem de essentie is van goede informatiebeveiliging. "Het management moet het beleid vaststellen, dragen en uitdragen naar de rest van de organisatie. Niet omdat het moet van derden, maar vanuit een oprechte motivatie. Deze steun vormt het fundament en uit zich in het ondersteunen van beslissingen, het dragen en uitdragen van maatregelen, het beschikbaar stellen van financiële middelen, voorbeeldgedrag en het stimuleren van het beveiligingsbewustzijn."

"Ook moet de organisatie informatiebeveiliging zien als een doorlopend proces en niet als project. Een valkuil is het concentreren van de aandacht op enkel de IT-aspecten van informatiebeveiliging of op het vertrouwelijkheidsaspect van digitale informatie. Het gaat echt om informatiebeveiliging in de meest brede zin van het woord. De maatregelen die daarbij getroffen worden, moeten passen bij de organisatie en afgestemd zijn op de risico's die er zijn voor de bedrijfsvoering. Er zal dus een goed inzicht moeten zijn in de bedrijfsvoering, de diverse informatiestromen en de impact van dreigingen. Een adequate beveiliging van informatie is dan ook maatwerk."

Menselijke aspecten

Na de nulmeting en phishingtest besloot Woonstede aandacht te geven aan menselijke aspecten als het opslaan en bewaren van gevoelige informatie. "Maar ook andere menselijke aspecten zijn meegenomen, zoals hoe herken je een phishingmail of hoe weet je wie je aan de telefoon hebt en stel je de juiste controlevragen. Er is het afgelopen jaar veel aandacht geweest voor het geheel van bewustwording én bewust blijven. Nu is het zaak deze stappen ook te verankeren in onze procedures en richtlijnen."

Onbewuste handelingen

Martijn noemt de zwakste schakel bij informatiebeveiliging de mens: "Door bewuste, maar vooral door onbewuste handelingen. Techniek kan hierbij goed ondersteunen door ervoor te zorgen dat de kans op fouten geminimaliseerd wordt. Het lastige met deze technische maatregelen is dat deze vaak op gespannen voet met gebruikersgemak staan. Je wilt niet dat de techniek zo onvriendelijk wordt dat mensen er omheen

>>

gaan werken en de inrichting alsnog onveilig wordt. Ik ben ervan overtuigd dat bewustwording voor 'veilig werken' dan ook moeilijker is dan het technisch veilig maken van systemen."

Persoonlijk belang

Bij zowel de nulmeting als de bewustwordingscampagne heeft Woonstede samengewerkt met Audittrail. "Samen met hen hebben wij de campagne uitgevoerd. Dit bestond uit een aantal onderdelen, zoals een bewustwordingscampagne van meerdere maanden, een e-learning training en een lezing door Maria Genova – auteur van 'Komt een vrouw bij de hacker'. We proberen ook de link te leggen naar het persoonlijke belang voor een medewerker. De bewustwording is namelijk niet alleen van belang binnen je werk, maar ook privé."

Regiegroep informatiebeveiliging

Samen met Audittrail heeft de corporatie ook een 'regiegroep informatiebeveiliging' (RGIB) opgericht. "Deze groep is een bewuste keuze om te zorgen dat we als organisatie samenwerken aan informatiebeveiliging. Het is niet een 'feestje' van de Privacy en Security Officer, maar een groep medewerkers vanuit de hele organisatie die vanuit hun functie of interesse een bijdrage leveren. Daar ligt een grote factor van de meerwaarde: informatie is van de gehele organisatie en daarmee is de hele organisatie hier verantwoordelijk voor. Door het oprichten van de RGIB borgen we deze verantwoordelijkheid in de organisatie. De leden van de regiegroep zijn bijvoorbeeld ambassadeur voor informatiebeveiliging en signaleren wanneer er iets mis dreigt te gaan."

Volgende stappen

Om de stappen te verankeren in procedures en richtlijnen maakt Woonstede gebruik van de Baseline Informatiebeveiliging Corporaties (BIC). "De BIC laat zien waar we naartoe moeten, en de nulmeting gaf een beeld van waar we momenteel staan. De resultaten hebben wij verwerkt in het BIC-framework – ontwikkeld door Audittrail – waaraan we ook de informatiebeveiligingsbevindingen van onze accountant en interne auditor hebben toegevoegd. Zo hebben we overzicht van alle activiteiten. Samen met de leden van de RGIB werkgroep zijn we de activiteiten nu aan het prioriteren. Dit leidt tot een jaar- en communicatieplan waarmee we de volgende stappen kunnen nemen. Uiteindelijk levert dit een PDCA-cyclus op en kunnen we aantonen dat we in control worden én blijven."

Need to know principe

Goede informatiebeveiliging zorgt ook voor het borgen van de continuïteit van systemen en betrouwbare informatievoorziening, legt Martijn uit. "Vanuit informatiebeveiliging hebben wij autorisaties opnieuw beoordeeld naar het 'need to know' principe. In andere woorden: alleen hetgeen je

voor je werk nodig hebt, heb je inzage in. Ook het alleen opslaan van data die je écht nodig hebt voor het uitvoeren van je werk, zorgt ervoor dat het werk makkelijker wordt. Het veilig versturen van bestanden met privacygevoelige data is een vraag vanuit de organisatie en komt ook terug in het BIC: dat pakken wij nu als een van de eerste onderdelen aan. Daarnaast was het vastleggen van de beveiligingsincidenten niet goed geregeld en richten wij nu zo in dat we kunnen rapporteren, monitoren en evalueren op deze incidenten."

Inbedden in de organisatie

Martijn sluit af door te stellen dat informatiebeveiliging steeds meer als continu proces wordt gezien. "En zo willen wij het ook inbedden in onze organisatie. Door dit continue proces wordt informatiebeveiliging stap voor stap naar een hoger volwassenheidsniveau gebracht." ■