Foto: CorporatieMedia

Jorrit van de Walle (Audittrail):

Zorg voor inzicht en overzicht bij informatie- en privacybeveiliging

Informatiebeveiliging en privacy hebben de afgelopen jaren aan urgentie gewonnen bij woningcorporaties. Met de naderende AVG heeft de aandacht voor het goed beveiligen van gevoelige gegevens zijn hoogtepunt bereikt. Maar hoe goed is goed genoeg en hoe houd je dat zo? En op welke vlakken zijn er nog stappen te zetten? Een gesprek met **Jorrit van de Walle**, directeur bij privacy- en informatiebeveiligingsspecialist **Audittrail**.

Zijn corporaties inmiddels voldoende privacybewust?
Dat ligt eraan wat je als 'privacybewust' beschouwt. Wat wij zien, is dat veel corporaties er serieus mee bezig zijn. Corporaties lijken verder dan andere branches. Maar tegelijk komen we ook een behoorlijk aantal corporaties tegen die de noodzaak niet zien en van mening zijn dat de boetes en handhaving wel los zullen lopen.

Wat is volgens jou de essentie van goede privacybescherming?
De essentie is wat mij betreft tweeledig. Ten eerste de perceptie van waarde: persoonsgegevens zijn nou eenmaal heel veel geld waard. Er zijn veel mensen die daar een crimineel slaatje uit willen slaan. Daarbij kan het iedereen overkomen. Op het moment dat alle medewerkers de juiste waardeperceptie hebben, zie je vanzelf dat persoonsgegevens een kostbaar goed zijn. Ten tweede een mate van gezond verstand. Denk goed na over hoe jij kunt voorkomen dat persoonsgegevens in de verkeerde handen vallen.

Zijn corporaties eigenlijk interessant voor hackers?
Niet alleen voor hackers, maar ook voor social engineers als phishers. Een corporatie heeft bovengemiddeld veel persoonsgegevens, van huurders en collega's. Denk aan namen, adressen maar ook inkomensgegevens en soms een BSN. Die zijn op de zwarte markt voor het gebruik bij identiteitsfraude veel geld waard, rond de 45 euro per stuk. Bij een corporatie met 10.000 vhe is er bijna een half miljoen euro buit te maken. Dat kan voor een hacker of social engineer snel verdiend zijn.

Daarnaast zijn corporaties voor hun dagelijkse werk zeer afhankelijk van informatie in hun systemen. Als men slachtoffer is van ransomware of een DDoS-aanval, zitten al gauw veel collega's met de armen over elkaar. Dat is een behoorlijke kostenpost. En dan hebben wij het nog niet eens gehad over de 'hobby-hacker' zoals de boze (ex-)huurder of een verveelde puber.

Zit het snor met de privacybescherming, wanneer een corporatie de informatiebeveiliging op orde heeft?
Ja en nee. Informatiebeveiliging en privacy hebben een nadrukkelijk verband. Maar naast het juist en afdoende beveiligen van gegevens en systemen, zijn er nog meer eisen waar je aan moet voldoen voor je compliant bent aan de AVG. Denk aan bepaalde processen – zoals recht op inzage, wijziging en vernietiging – of eisen aan vastlegging. Met goed beveiligen alleen ben je er dus niet.

Bij informatiebeveiliging is de mens vaak de zwakste schakel, is dat bij privacywetgeving ook het geval?
Privacy is met name een organisatorisch en menselijke opgave. Techniek en ICT spelen wel een rol, maar zijn veel beperkter. Het zijn mensen die het voldoen aan de privacywetgeving regelen in de processen. En het zijn veelal ook de mensen die datalekken veroorzaken. Het vergroten van bewustwording door campagnes en social engineering, training en opleiding zijn dus essentieel.

Over een paar maanden gaat de AVG van kracht: welke stappen moeten veelal nog gezet worden?
Dat is per organisatie natuurlijk verschillend. Een aantal van onze klanten zijn hier al jaren mee bezig, en komen nu op een niveau waarbij het borgen en verbeteren aan bod komt. Andere organisaties beginnen net. Die zijn voornamelijk gericht op het verkrijgen van inzicht in hun stand van zaken en overzicht in wat ze allemaal moeten doen om compliant te raken. De grote middengroep heeft de administratieve basis op orde, en werkt nu aan bewustzijn en het implementeren van de processen.

Zijn corporaties die nu nog moeten beginnen 'te laat'?
Formeel gezien wel, maar dat geldt eigenlijk voor iedere organisatie. Op 25 mei 2016 is de wet van kracht geworden en wij hebben de implementatietermijn van twee jaar al bijna achter de rug. Maar het bijzondere is dat het eigenlijk helemaal niet de AVG is die veel werk veroorzaakt. Het zwaartepunt zit hem in de Wbp, die al sinds 2001 van kracht is en waar heel weinig aandacht voor is geweest. Dus eigenlijk lopen we al zo'n zeventien jaar achter, en moeten wij dit nu 'snel' inhalen. Maar als wij het formele achterwege laten: het is goed dat een organisatie – vroeg of laat – de wens heeft om compliant aan de wet te raken en daar tijd en moeite insteekt. In die zin is het dus nooit te laat.

Corporaties halen door big data, machine learning en IoT steeds meer data binnen. Wat betekent dat voor het risico op datalekken?
Corporaties zullen hierdoor moeten blijven nadenken. De wetgever heeft hierin voorzien; het uitvoeren van een Data Protection Impact Assessment is verplicht voordat je met zo'n traject begint. Ook moet en wil je je houden aan de principes van security en privacy by design, waarbij je aan het begin al rekening houdt met alle eisen aan informatiebeveiliging en privacy.

Wat is jullie propositie in de sector?
Audittrail biedt een breed dienstenpakket in de sector. Van nulmetingen door onze privacyjuristen en securityconsultants tot een helpdeskabonnement waar je alle privacy- en securityvragen kwijt kunt. Heb je ondersteuning nodig in de vorm van een interim privacy- of security officer, of met een kort project, dan kan dat ook. Net als een uitgebreid scala aan awareness activiteiten. Verder beschikken wij over privacy compliance tooling in samenwerking met Mavim. Wij zijn specialisten en daarmee ook een beetje vak-gekken. Daarom maken wij als missie samen de wereld graag een stukje veiliger en mooier.

Wat zouden corporaties omtrent informatiebeveiliging en privacy móeten weten?
Zorg dat je inzicht en overzicht hebt. Weet wat je moet doen en maak een plan. Betrek daarbij iedereen in de organisatie, maar maak het niet te groot en te zwaar. Privacy en informatiebeveiliging kunnen best leuk zijn. Redeneer bij privacy daarnaast vanuit jezelf: wat zou ik ervan vinden als een organisatie op deze manier met mijn gegevens zou omgaan? Wees je bovenal bewust van de risico's en bagatelliseer ze niet. Je wilt niet in het nieuws komen omdat je het 'nog maar moest zien'. ■