Woningbedrijf Velsen:

Informatiebeveiliging: de zwakste schakel versterken door medewerkers bewust te maken

Door het toenemende belang van data worden privacy en informatiebeveiliging steeds belangrijker bij woningcorporaties. Bij **Woningbedrijf Velsen** zijn Privacy & Security Officers **Jack Groot** en **Anja Kamphuis** mede verantwoordelijk voor de bescherming van de gegevens van ruim 10.000 huurders. Hoe doe je dat op een goede manier en maak je de medewerkers bewust van de juiste werkwijzen? “Goede informatiebeveiliging beschermt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen de organisatie.”

Over iets meer dan een half jaar - in mei 2018 - worden de wettelijke regels rondom privacy verscherpt en wordt de Algemene Verordening Gegevensbescherming (AVG) van kracht. “Privacy is een onderwerp dat de hele organisatie aangaat,” begint Anja op de vraag wat een Privacy & Security Officer doet. “Vanuit die gedachte is het creëren van bewustwording dan ook noodzakelijk, een belangrijk onderdeel van onze taak. Wanneer iedereen zich bewust is van de eigen verantwoordelijkheden op het gebied van privacy, draagt dit bij aan een betere bescherming van persoonsgegevens.”

Goede informatiebeveiliging

Het waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van informatie is volgens Jack de essentie van goede informatiebeveiliging. “Daarmee bedoelen wij dat de informatiesystemen op de juiste momenten beschikbaar zijn, de informatieverwerking correct en volledig is en dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn. Dit richt zich niet alleen op de geautomatiseerde gegevensverwerking door middel van ICT-systemen, maar ook op de bescherming van niet geautomatiseerde gegevens - zoals fysieke documenten - en bedrijfseigendommen.”

Leidraad

De Wet bescherming persoonsgegevens (Wbp) is bij Woningbedrijf Velsen leidraad geweest voor het werken met gevoelige informatie en persoonsgegevens. Anja: “Hierin staat vastgelegd wat er wel en niet mag gebeuren met de gegevens. Dat begint in eerste instantie met rechten door in de software enkel toegang te verlenen aan de personen die met de informatie werken.” Woningbedrijf Velsen wordt hierbij ondersteund door een outsourcingspartner. “Deze regelt de veiligheid en beveiliging van onze gegevens. We geven onze medewerkers trainingen om hen goed en bewust om te laten gaan met data en zijn we bezig met het afsluiten van bewerkersovereenkomsten met bedrijven die toegang hebben tot onze data. Daarnaast hanteren we een ‘clear desk’ regeling. Dat houdt in dat bij het verlaten van de werkplek het beeldscherm wordt vergrendeld en aan het eind van de werkdag geen privacygevoelige informatie achterblijft op het bureau, op whiteboards of op flip-overs. Ook moet bij het verlaten van het kantoor kasten, lockers en laden dicht zijn, en ruimten met vertrouwelijke documenten moeten op slot.”

Nulmeting

Momenteel is Woningbedrijf Velsen bezig met het realiseren van een privacy-visie. “Naast een heldere visie is het ook belangrijk dat je inventariseert waar je als corporatie staat op het gebied van privacy en security.” Om een beeld van de status rondom informatiebeveiliging te krijgen, voerde Woningbedrijf Velsen een ‘Privacy Plan’ uit. “Dit begon met een Quick Scan waarmee wij in korte tijd tweedimensionaal inzicht kregen waar we stonden, inclusief stappenplan voor de toekomst. Een nulmeting gaf vervolgens inzicht in hoe goed privacy en security binnen de organisatie zijn geregeld. Daaruit hebben wij een goede inventarisatie en evaluatie van alle risico’s op een rijtje gezet. Door deze hoog in de organisatie uit te dragen, werd draagvlak gecreëerd.
Het bestuur of MT zijn hierbij erg belangrijk, zonder ondersteuning van hen is de kans groot dat het plan mislukt.”

>>

Foto’s: Ron Pichel Fotografie

Verdwaalde USB-sticks

Zoals veel securityexperts erkennen Jack en Anja dat de mens ook bij Woningbedrijf Velsen de zwakste schakel is. Jack: "Een medewerker die reageert op een phishing mail, zijn of haar e-mailadres op een willekeurige site intikt of een rondslingerende USB-stick zijn slechts enkele voorbeelden van wat in de praktijk kan voorkomen. Dan maakt het niet zoveel uit dat hackers dagelijks aan onze digitale poorten rammelen. Wij proberen met voorlichting over incidenten en actuele bedreigingen preventief onze collega's te informeren over de mogelijke bedreigingen. Niet alleen zakelijk, ook voor thuis geven wij tips mee."

Het blokkeren van websites, de toegang tot USB-sticks aan banden leggen of het automatisch vergrendelen van een computerscherm is niet voldoende, legt Jack verder uit. "Daarom organiseren wij voor onze collega's trainingen en lezingen, plaatsen we relevante informatie op ons intranet en hangen er in het pand diverse posters om de bewustwording te vergroten. Vooral op de door ons gemaakte video's komen veel leuke reacties. Hierdoor kunnen wij merken dat het werkt en goed bekeken wordt."

Medewerkersbewustwording

Om het bewustzijn nog verder te vergroten, wordt Woningbedrijf Velsen ook bijgestaan door audit- en adviesbureau Audittrail. "Zij hebben ons ondersteund en geadviseerd om de medewerkersbewustwording te toetsen en te vergroten. Bijvoorbeeld door middel van een lezing. Audittrail heeft ons daarnaast geholpen met het opstellen van het informatiebeveiligingsbeleid, de nulmeting, het awarenessprogramma en het Information Security Management System ISMS. Dat laatste borgt alle voorkomende maatregelen, procedures en instructies met betrekking tot het waarborgen van informatieverwerking binnen Woningbedrijf Velsen. Door dit in kaart te brengen, kunnen risicoanalyses de nodige organisatorische, procedurele en technische maatregelen worden bepaald en kan de mate van beveiliging worden vastgesteld."

Privacy by design

Op de vraag wat de invloed is van technologische ontwikkelingen op security en informatiebeveiliging, zegt Jack: "Let goed op hoe huidige en nieuwe applicaties zijn ingericht en ontwikkeld. Het feit dat het een nieuwe applicatie is, betekent niet dat deze op de juiste manier is ingericht. Let bij aanschaf daarom op drie dingen: privacy by design, data-minimalisatie en privacy by default."

"Privacy by design is letterlijk: gegevensbescherming door ontwerp. Het idee is om in een vroeg stadium technisch en organisatorisch een zorgvuldige omgang met persoonsgegevens af te dwingen. Bij de ontwikkeling moet er dus al aandacht zijn voor privacy. Data-minimalisatie is daar een

belangrijk onderdeel van. In het ontwerp moet gewaarborgd worden dat er niet meer persoonsgegevens verwerkt worden dan strikt noodzakelijk voor het doel. Privacy by default kan ook gezien worden als onderdeel van privacy by design, en vereist dat de standaardinstellingen altijd zo privacy-vriendelijk mogelijk zijn."

Voldoen aan wetgeving

Op de vraag wat de privacy officers aan collega corporaties mee willen geven, zegt Anja: "Begin bij informatiebeveiliging en privacy met commitment vanuit het management om een draagvlak te creëren. Start daarna met een nulmeting en stel iemand verantwoordelijk en werk volgens de Baseline Informatiebeveiliging Corporaties (BIC) van Aedes en NetwIT. Neem vanaf de allereerste stap jouw collega's mee en maak iedereen bewust over hoe om te gaan met privacygegevens. Omdat de mens de zwakste schakel blijft, maak gebruik van cryptografie. En tenslotte: werk op technisch vlak alleen met gecertificeerde software om zo efficiënt aan de regels te voldoen van het AVG." ■