Foto: Claranet

Eric de Graaf

Twan Willems

Eric de Graaf en Twan Willems (Claranet):

Zoek voortdurend naar security kwetsbaarheden en versterk deze

Woningcorporaties hebben de afgelopen jaren flink getimmerd aan de veiligheid van hun organisatie, zowel fysiek als digitaal. Maar bestaat er een scenario waarin een optimaal security-model is bereikt en je als corporatie achterover kunt leunen, of blijft dit altijd een continu streven? CorporatieGids Magazine ging hierover in gesprek met **Eric de Graaf** en **Twan Willems** van **Claranet**.

Wat zijn de belangrijkste security-ontwikkelingen bij woningcorporaties van de afgelopen jaren?
De belangrijkste recente ontwikkeling is de introductie van de AVG begin dit jaar. Hoewel de introductie feitelijk al in 2016 plaatsvond, is de bewustwording pas rond de handhaving op 25 mei van dit jaar op gang gekomen. Het leek wel alsof er een inhaalslag gemaakt moest worden, want iedereen dook er bovenop met kennissessies, webinars en whitepapers, gevolgd door adviseurs die als paddenstoelen uit de grond schoten op zoek naar AVG-projecten. Het directe gevolg was dat veel stakeholders murw werden van de hoeveelheid informatie die ze voorgeschoteld kregen en veelal nog steeds niet AVG-proof zijn.

Is security een ondergeschoven kindje bij woningcorporaties?
Een ondergeschoven kindje is wellicht niet de juiste benaming, maar het is duidelijk dat databeveiliging zorgt voor een uitdaging. Uit ons onderzoek naar cloudadoptie bij woningcorporaties vorig jaar bleek dat security een van de belangrijkste uitdagingen was, en dat veel organisaties daarom ervoor kozen om toch wat langer gebruik te maken van hun huidige IT-platform.

Daarnaast zien we dat er sprake is van onderschatting door gebruikers. Dit kun je bijvoorbeeld terugzien in de effectiviteit van ransomware-aanvallen. IT-leveranciers hebben vaak hun zaakjes goed op orde, en cyberaanvallen worden daarom vaak gericht op de gebruiker. Omdat ze de gevaren niet goed doorhebben en bijvoorbeeld systemen en software niet updaten, kunnen miljoenen euro's aan data worden gestolen. Iets dat met het simpelweg accepteren van een update of aanbrengen van een patch met grote waarschijnlijkheid voorkomen kan worden.

Jullie vergelijken security met een Jenga-toren, waar zit de overeenkomst?
Security is enorm complex en gaat veel verder dan het plaatsen van een firewall waar je geen omkijken naar hebt. En omdat het zo complex is, heb je expertise nodig die niet altijd voorhanden is. Daarmee wordt het vaak een sluitstuk bij projecten, onder het motto 'we laten er wel naar kijken als de rest bekend is'. En met die instelling loop je achter de feiten aan. Je kan simpelweg niet alleen focussen op groei en veranderingen zonder de gaten te pareren. Hierin zit de vergelijking met de Jenga-toren: de focus ligt op het zo hoog mogelijk maken van de toren, terwijl het spel juist draait om het omvallen van de toren.

Hoe richten woningcorporaties security wél op een goede manier in?
De eerste stap is security meenemen in het design van de IT-omgeving zodat je direct voorbereid bent op veranderingen en groei. En als je daadwerkelijk gaat veranderen, moet je in stap twee zorgen dat de gaten die getrokken worden – kwetsbaarheden die ontstaan – al vooraf geïdentificeerd zijn en meegenomen worden in het project.

Wat is de rol van de cloud bij security voor woningcorporaties?
Veel corporaties denken dat security lastiger wordt omdat ze verantwoordelijkheid uit handen moeten geven. Maar door dit over te dragen aan experts, weet je dat mensen ermee bezig zijn voor wie het hun core business is. Maar het in de cloud beleggen van IT betekent niet dat je gevrijwaard bent van gevaar: zoals eerder gezegd blijft de mens een belangrijk target. Persoonlijk gerichte aanvallen – ook wel spear-fishing genoemd – worden steeds beter uitgevoerd. Voldoende bewustwording bij gebruikers blijft daarom altijd essentieel.

Bestaat er een optimaal security-model voor woningcorporaties, of is dat een continu streven?
Omdat er zoveel geld verdiend kan worden aan de data van woningcorporaties, zullen criminelen altijd creatieve, nieuwe manieren proberen te vinden hieraan te komen. Het 'optimale model' om jezelf hier tegen te beschermen verandert daardoor steeds. Als organisatie moet je daarom zelf continu op zoek naar kwetsbaarheden en deze versterken. Je kan met geautomatiseerde testen jezelf steeds controleren, maar dit vraagt ook om een andere mindset van medewerkers over hoe ze om moeten gaan met bedreigingen van buitenaf. Een klein beetje extra argwaan kan echt geen kwaad.

Wat is jullie propositie in de sector?
Claranet biedt woningcorporaties een volledig pallet aan diensten. Zo bieden wij bescherming op technisch vlak – bijvoorbeeld via firewalls en anti-virusscanners – die shadow-IT buiten de deur houden. Hiermee bedoelen wij het onwenselijke gebruik van niet-standaard diensten op IT-gebied als Dropbox of WeTransfer voor bedrijfsinformatie. Daarnaast houden we met geautomatiseerde kwetsbaarheidscans controle op de beschermmaatregelen en geven we trainingen op het gebied van penetratietesten en bewustwording onder medewerkers.

We nemen hierbij volledige ontzorging voor onze rekening, waarbij we rekening houden met de groei van de organisatie en zorgen dat de flexibiliteit niet in gevaar komt en de beveiliging zo optimaal mogelijk is. ■