nederlandse vereniging
bestuurders woningcorporaties

Sfeerimpressie zomerbijeenkomst en masterclass

‘What the hack!?’

Een normale zondag in maart, je ontvangt een telefoontje “We zijn gehackt”. En vanaf dat moment sta je aan en raakt alles in een stroomversnelling…

Dagvoorzitter Wendelien Wouters schetst hoe de situatie start voor 8 bestuurders van woningcorporaties in het laatste weekend van maart 2022. Een ingrijpende ervaring die nu, ruim een jaar later, heeft geresulteerd in een evaluatierapport met daarin de geleerde lessen, beschikbaar voor de sector. Want een hack kan echt iedereen gebeuren en het is goed om op de situatie voorbereid te zijn.

Guido van Woerkom (voorzitter VTW) wordt uitgenodigd om dit rapport in ontvangst te nemen, uitgereikt door Annelies Barnard, voorzitter van de NVBW. Hij benoemt de lastige positie waarin bestuurders, maar ook leden van de raden van commissarissen, zich bevinden op het moment dat een hack plaatsvindt. Er wordt immers een beroep gedaan op alle facetten van het bestuurderschap ineens. “Maar”, richt Van Woerkom zich tot de getroffen bestuurders, “het is goed dat jullie dit hebben meegemaakt. Dan kunnen wij ervan leren".

Bewust onbekwaam

“Wie denkt klaar te zijn voor een hack?” Deze vraag van Wendelien Wouters roept verschillende reacties op in de zaal. Van “Ja, voor zover mogelijk” tot “Er is veel geregeld, maar het voelt onrustig te weten dat het misschien toch kan gebeuren en je niet alles hebt afgedicht". Bewust onbekwaam dus, daar komt het vaak op neer. We weten dat een digitale inbraak, ondanks voorzorgsmaatregelen, iedereen kan overkomen én dat er vast ook nog verdere acties te ondernemen zijn om eventuele vervolgschade te beperken.

Big business

Pim Takkenberg, directeur van Northwave Nederland, neemt de zaal mee in het proces van een hack. Wat gebeurt er, wie zijn er betrokken en hoe kun je het beste handelen. Kortom; wat doe je

bij het ontvangen van een digitale 'ransom note'? Bel je direct de politie? Leg je het hele systeem plat? Trek je de stekker uit het netwerk of stel je meteen een crisisteam aan?
Na een korte discussie wordt geconcludeerd dat eigenlijk alle genoemde opties zinvol zijn, behalve het bellen van de politie. Daarvan wordt gezegd dat het in ieder geval niet in het eerste stadium prioriteit heeft. Handiger is het om een externe partij te betrekken die je met raad, daad en onderhandelingsvaardigheid kan bijstaan.
Takkenberg presenteert met luchtige toon een serieuze boodschap. Hij legt uit dat het de hackers echt *business* is. Zakelijk dus. Het is een economisch model met verschillende samenwerkende groepen. Vaak zijn dat professioneel ingerichte bedrijven die zelfs over een Klantenservice beschikken. Want hackers zijn servicegericht: als je niet weet hoe je in Bitcoins moet betalen, dan zijn zij graag bereid je daarbij te helpen. En tegen een extra 'kleine vergoeding' willen ze je achteraf ook nog vertellen waar de kwetsbaarheden in je systeem zitten. Alles bij elkaar is de vraagprijs voor een hack gemiddeld zo'n 2% van de jaaromzet van het getroffen bedrijf. Van de gechanteerde organisaties betaalt uiteindelijk bijna de helft.

De afweging die je als bestuurder moet maken, zorgt voor praktische en morele dilemma's. Met de praktische kant kan een onderhandelaar helpen, de morele overweging maak je, met behulp van je achterban, zelf. Als je besluit te betalen, betekent dat dat je je laat chanteren door criminelen, door terroristen. Als je *niet* betaalt, ligt gevoelige bedrijfsinformatie evenals persoonsinformatie van je medewerkers en van je huurders misschien zo op straat. Of in ieder geval op het *dark web*. Onmogelijke afwegingen?

Het perspectief van de bestuurders

Als bestuurder kom je in een dergelijke situatie steeds voor belangrijke en moeilijke afwegingen, dilemma's en beslissingen te staan: betaal je wel of niet, wie licht je in en op welk moment? Trekken we samen op of liever individueel?

Het antwoord op die laatste vraag is evident; deze bestuurders zijn complementair aan elkaar. Iedereen had al snel zijn of haar eigen rol in de groep en dat is ook duidelijk te zien als zij met elkaar voor de zaal plaatsnemen.
Aanwezig zijn zes van de acht bestuurders die tegen wil en dank ervaringsdeskundig zijn. De informele voorzitter van de groep, Karo van Dongen (Alwel), vertelt over de 3 fases; eerste 24 uur, eerste week en tenslotte de daaropvolgende periode. De andere bestuurders, Annelies Barnard, Jan Leo van Deemter, Jan Wim Franken, Dennis Gerlof en Jessie Bekkers van Rooy, vertellen op vraag van de dagvoorzitter over hun persoonlijke ervaringen in deze tijdvakken. Deze ervaringen zijn net zo divers als de verschillende karakters van de bestuurders en als de unieke omstandigheden van iedere corporatie. Het maakt namelijk uit of de gegevens van jouw corporatie gestolen zijn of niet. Of je verzekerd bent tegen dergelijke schade of niet. Het maakt uit of je een stevig management hebt en of je het vertrouwen van je RvC geniet. Het maakt uit of je bij iemand je verhaal kwijt kunt.

De hele ervaring wordt door verschillende bestuurders omschreven als een achtbaan. En waar de een gek is op de daarbij behorende spanning en sensatie, raakt de ander van slag als niet te voorspellen is of je uit de bocht zal vliegen of niet. In de opeenvolgende fases (eerste 24 uur, eerste week en de periode daarna) maakt iedereen diverse emoties en stemmingen door. Van vastberadenheid tot woede en moedeloosheid en weer terug.

Hoewel de bestuurders ieder zo hun eigen, persoonlijke ervaring en verhaal hebben, zijn er veel overeenkomsten. Ze zaten in hetzelfde schuitje. De groep kwam dan ook tot de afspraak ‘wat we doen, doen we samen'. Een afspraak die niet altijd gemakkelijk te houden bleek, want de belangen zijn niet voortdurend voor iedereen gelijk. Toch bleven zij met elkaar, met hun medewerkers en Raden van Commissarissen in gesprek en hebben zij zowel intern als naar de buitenwereld weten te verantwoorden dat zij de keuze hebben gemaakt om als groep NIET toe te geven aan de eisen van de hackers. Dat besluit namen zij niet *ongeacht* de consequenties, maar *rekening houdend met* de consequenties.

Aan de bak

Na de eerste schok is iedereen direct in de *aan-de-bak-stand* gegaan. De primaire processen moeten altijd doorgaan en dit werd met veel creativiteit (denk aan het begin van de coronaperiode) opgepakt. Het was moeilijk, maar het lukt iedereen om vrij snel de dienstverlening weer op niveau te krijgen. Wel heeft het heel erg lang geduurd voordat alle systemen weer naar behoren werkten en alles weer op de rit stond.

De bestuurders vertellen: “Medewerkers zetten zich enorm in en de solidariteit was heel groot. Dit zorgde voor een grote motivatie van allen, samen als bedrijf. Die hackers zouden ons er niet onder krijgen”. Tegelijkertijd zorgde de hele situatie, omdat het zo veel langer duurde dan verwacht, voor problemen bij veel medewerkers. Dit varieerde van irritatie, verdriet en tijdelijke vermoeidheid tot echt serieuze klachten. Zeker bij de medewerkers die zich om wat voor reden dan ook in zekere zin verantwoordelijk voelden voor wat er gebeurd is. Het ziekteverzuim is als gevolg van de hack aanzienlijk gestegen.

Zichtbaar

Annelies benadrukt dat het heel belangrijk is om zichtbaar te zijn voor je medewerkers. Jan Wim vult aan: ”Het is zaak om als bestuurder naar je medewerkers toe ‘cool, calm and collected’ te blijven. Je wilt naar je medewerkers uitstralen dat het goed komt. De verantwoordelijkheid die je als bestuurder voor je organisatie hebt, voelt en is gewoon heel groot”.

“Alles is nieuw en alles is onzeker”. Je weet dat er risico’s zijn, maar het is niet duidelijk welke risico’s dat zijn. Planningen werken niet. Dit vraagt van alle betrokkenen veel flexibiliteit en een bestuurder die zich zowel vastberaden als eerlijk opstelt, om te voorkomen dat de organisatie zich stuurloos voelt.

Afweging

Er is in het proces diverse malen serieus de afweging gemaakt om wel of niet het losgeld te betalen. En achteraf is ook niet iedereen er van overtuigd dat dit de enige mogelijke uitkomst is en of het het waard is om de gekozen weg te bewandelen. Zij begrijpen dan ook dat er ook situaties zijn waarin er wel betaald wordt door een corporatie.

Lessons learned

Na een korte pauze is er gelegenheid voor de deelnemers aan de masterclass om vragen te stellen aan de ervaringsdeskundigen, die in tweetallen per onderwerp door Wendelien naar voren worden geroepen. Bij ieder onderwerp komen er tijdens de gesprekken vanzelf tips naar voren, waarvan er hieronder een aantal is opgenomen.

Crisiscommunicatie - *Dennis Gerlof en Mechteld van der Vleuten*

- Zorg dat je (thuis) een papieren versie van je actuele crisisplan hebt.
- Communiceer helder binnen je organisatie en naar buiten.
- Laat je niet onder druk zetten door de pers.
- Stel iemand aan als crisis-voorlichter.
- Schakel (gezamenlijk) een communicatie adviseur in.

Stakeholders - *Jan Leo van Deemter en Jan Wim Franken*

- Houd goed contact met je stakeholders. Afhankelijk van hun positie en jullie verhouding informeer je, overleg je en maak je afspraken.
- Vergelijk met elkaar hoe de stakeholders zich opstellen om je positie als bestuurder te bepalen.
- Overleg goed met je accountant over de betrouwbaarheid van gegevens.

Bedrijfsvoering / processen /de organisatie - *Jessie Bekkers van Rooy en Christel van Vught*

- Stel zo snel mogelijk een crisisteam samen.
- Blijf in gesprek met je medewerkers, ook als je niet precies weet waar het naartoe gaat. Zorg voor voldoende mogelijkheden om met elkaar te praten en ervaringen uit te wisselen, zowel over praktische zaken als over de emotionele en onzekere kanten.
- Wees kritisch op het programma van eisen en wensen ten aanzien van je serviceprovider.
- Laat regelmatig je kwetsbaarheid testen door middel van een audit of een ‘pentest’.

Bestuur en Governance - *Annelies Barnard en Karo van Dongen*

- Blijf afwegingen maken en spreek hier vooraf al over met je RvC. (Gaan huurders claimen als je betaalt? Wat betekent het voor je imago? Maakt de hoogte van het bedrag uit?)
- Spreek met mensen die het hebben meegemaakt.

Tenslotte

Deze interessante, leerzame middag heeft de aanwezigen aan het denken gezet. Wat zou ik doen? Ben ik er klaar voor en wat kan ik nu nog doen om de kansen op een hack te verkleinen en de risico’s bij een digitale aanval te beperken. Allemaal zaken om later, thuis of terug op kantoor, mee aan de slag te gaan.
De genoemde tips zijn nog maar een klein voorbeeld van de geleerde lessen. Daarom is het ook fijn dat het gedegen, beknopte rapport ‘Samen uit, samen thuis’ voor alle aanwezigen vanaf nu digitaal beschikbaar is. Dit wordt ter besluit nog eens benadrukt door een videoboodschap van Aedes-voorzitter Martin van Rijn die het rapport van harte en aanbeveelt: “Lees dat rapport!”

Samen uit, samen thuis

v.l.n.r. Dennis Gerlof, Annelies Barnard, Jan Wim Franken, Jessie Bekkers de Rooy, Mechteld van der Vleuten, Jan Leo van Deemter, Christel van Vught en Karo van Dongen

nederlandse vereniging
bestuurders woningcorporaties