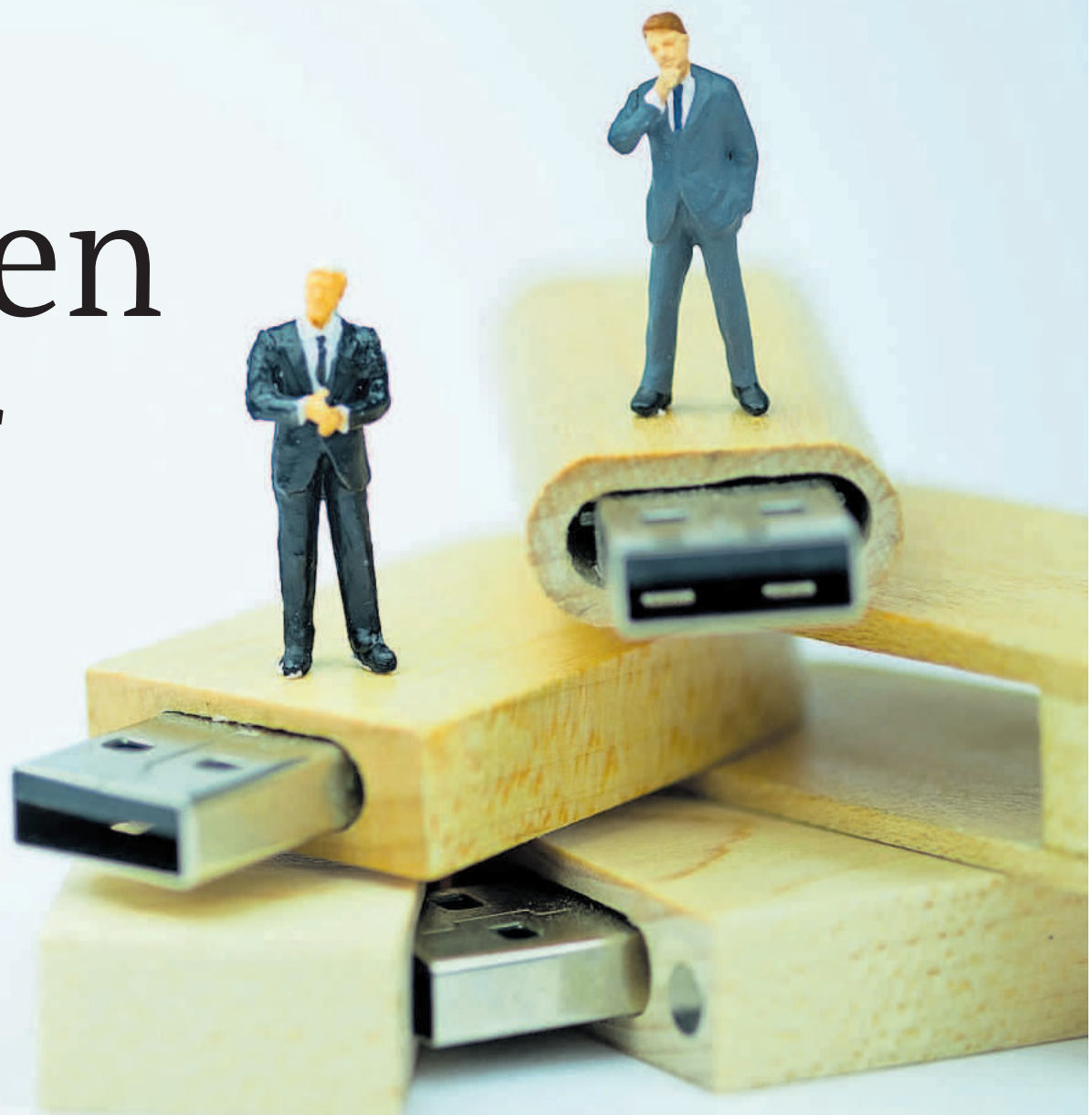
Wat als een makelaar wordt gehackt?



Hoe erg is het als een makelaar wordt gehackt? De MKB Cyber Campus gaat tientallen Friese NVM-makelaars laten zien hoe ze hun digitale veiligheid op orde krijgen.

RENÉ SMID

Natuurlijk kennen de aan- en verkopers van huizen de gevaren. Zij weten ook dat onderzoeksinstituut Wetsus in Leeuwarden eens is gehackt en losgeld moest betalen om de eigen versleutelde bestanden terug te krijgen. Het voorbeeld van leerlingen van CSG Comenius Mariënburg die hun eigen school met digitale aanvallen bestookten, staat velen eveneens nog wel bij.

„Mar ik kin my net yntinke dat soks ek by ús bart'', zegt Willem Donker, voorzitter van de Friese afdeling van makelaarsvereniging NVM. „Want wat falt hjir te heljen? Wy ha gjin foarried en gjin data dy't jild wurdich is. As ik kwea wol en ik wurd ea in hacker, dan gean ik echt net in makelderskantoar besykjen.''

De MKB Cyber Campus wil bedrijven in Noord-Nederland waarschuwen voor de gevolgen, op het moment dat zij hun digitale deur wagenwijd open hebben staan. Vooral kleinere bedrijven hebben niet de kennis om zich te wapenen tegen cybercrime. Daar wil de campus bij helpen.

Onlangs zijn ongeveer zeventig makelaars bijgepraat over het onderwerp. Zij kregen allen een cyberscan aangeboden die inzicht biedt in de digitale weerbaarheid. Zijn de wachtwoorden goed op orde, is er een back-up en zijn alle belangrijke bestanden versleuteld? Na de scan ontvangen de makelaars een rapport met aanbevelingen om de systemen veilig te maken en te houden. Dit doet de MKB Cyber Campus ook al met de agrarische sector en binnenkort de watersportbranche.

Makelaars hebben veel gegevens die privacygevoelig zijn: namen, adressen en woonplaatsen van klanten en kopieën van identiteitsbewijzen. Als deze data door een hack op straat komen te liggen, heeft een makelaardij te maken met een datalek en dat moet worden gemeld bij de Autoriteit Persoonsgegevens. „Daarnaast draait het hele aan- en verkoopproces van huizen in systemen die de NVM faciliteert'', weet Erik Miedema, mededirecteur van de campus. „Daar moet je wel goed mee omgaan.''

Bij makelaar Donker, die samen met partner Jan Jouke Kraak in Heerenveen een kantoor heeft, is vorige week zo'n scan gedaan. Daar zijn geen gekke dingen aan het licht gekomen, aldus Donker. Bij zijn makelaardij worden alle gegevens opgeslagen zoals dat hoort en hij werkt met diverse systemen van andere partijen.

Bovendien ligt de beveiliging van de Tiara-database – waarin de huizen die op de markt komen worden aangemeld – niet bij de makelaars zelf. „Wy geane dêr net oer.'' Bij individuele kantoren kan dus weinig gebeuren, zegt Donker. „Mar se ha wol tsjin ús sein dat jo in goeie back-up ha moatte.''

Miedema ziet dat makelaars hun beveiliging doorgaans goed op orde hebben. Hij stelt dat bedrijven die hackpogingen goed doorstaan. Eigenlijk beschikken ze allemaal over een fatsoenlijke back-up van hun gegevens: zowel in de *cloud* – via internet opgeslagen – als lokaal op een eigen opslagmedium dat niet gekoppeld is aan het internet. Daarbij valt te denken aan een usb-stick of een externe harde schijf. „Op deze manier heb je altijd twee verschillende back-ups beschikbaar. En deze oplossingen zijn voor kleine mkb'ers betaalbaar.''

Makelaar Ben Roerig van Dijkstra Heida Makelaars Taxateurs in Drachten is jaren geleden eens gehackt, maar hij kon dankzij een goede back-up snel anticiperen. „Drie of vier jaar terug kreeg ik een mail met de melding dat het hele systeem op slot werd gezet, op straffe van een boete van 300 euro'', vertelt Roerig.

„Maar wij maken elke nacht een back-up en dus heb ik mijn automatiseringsman gevraagd om die van de dag ervoor terug te zetten. We hebben nooit betaald en de data staan nu decentraal, dus buiten de server. Spannender kan ik het eigenlijk niet maken.''

De MKB Cyber Campus blijft de makelaars achter de broek zitten. Tijdens bijeenkomsten wordt vaak de urgentie van digitale veiligheid ingezien, maar terug op de werkvloer overheerst de waan van de dag en blijft het vaak liggen. Miedema: „We bellen twee weken na de scan en dan gaan we verdere stappen zetten. Als het ze zelf niet lukt, dan gaan we daarbij helpen. We laten ze niet zomaar los.''

'Se ha wol tsjin ús sein dat jo in goeie back-up ha moatte'

Scans bij boerenbedrijven

MKB Cyber Campus, onderdeel van de stichting Cyber Safety Noord-Nederland, heeft de afgelopen twee jaar tweehonderd agrarische bedrijven gescand. Wat daar opviel is dat de boeren behoorlijk zijn gedigitaliseerd, maar dat bijvoorbeeld wachtwoorden op de melkrobots makkelijk te raden en daardoor dus hackgevoelig zijn. ,,Een hacker kijkt waar hij naar binnen kan en doet dat dan ook'', zegt Miedema. ,,Wat moet je met melkrobots? Als je de hele melkvoorziening wilt platleggen en je kent de wachtwoorden, dan kan dat.''

,,We hoorden ook eens van een boer die trots een hek liet zien dat om zijn bedrijf heen stond'', vervolgt Miedema. ,,Daar kwam je niet overheen, maar de wifi stond wel 'open', want dat zou handiger zijn wanneer er iemand langskwam. Dan blijft het digitale hek dus openstaan.''

Op boerenbedrijven wordt weleens GPS-apparatuur uit trekkers gestolen. Deze apparatuur is duizenden euro's waard. Een boer die deze diefstal meldde, dacht niet te zijn gehackt maar achteraf bleek dat zijn camera's al twee dagen uit stonden. ,,Die waren door een hacker op zwart gezet'', weet Miedema. ,,De meeste camera's hebben een standaard wachtwoord, daar kan een hacker makkelijk bij.''