Koninklijke VHG adviseert hoveniers om goed na te gaan of hun digitale veiligheid nog op orde is.

VHG waarschuwt: spookfacturen, datalekken en gijzelsoftware bedreigen ook kleine groenbedrijven

Een hack kan ook jouw hoveniersbedrijf stilleggen

Klantgegevens buitgemaakt. Facturen betaald aan cybercriminelen. Bedrijfssoftware gegijzeld. Dit treft niet alleen grote bedrijven. Brancheverenging Koninklijke VHG ziet dat cybercriminaliteit ook de groensector raakt en waarschuwt ondernemers om digitale veiligheid structureel op de agenda te zetten. 'Hackers zoeken geen grote of kleine bedrijven,' zegt Richard Maaskant van Koninklijke VHG. 'Cybercriminelen zoeken en vinden kwetsbare bedrijven.'

Auteur: Frank van de Ven

Op maandagochtend wil een hoveniersbedrijf de systemen opstarten, maar niets werkt. Bestanden blijken versleuteld en op het scherm verschijnt een melding: 'Gehackt'. Daarbij krijgt het bedrijf het verzoek om een bedrag in Bitcoins te betalen om weer toegang te krijgen tot de systemen. Geen planning betekent geen aansturing. Geen urenregistratie betekent geen facturatie. Geen facturatie betekent geen inkomsten. 'Als systemen niet beschikbaar zijn, raakt dat direct de continuïteit van een mkb-bedrijf,' zegt Maaskant. Naast omzetverlies volgen kosten voor IT-herstel, mogelijke meldplichten bij een datalek en reputatieschade. Eén week stilstand kan een klein bedrijf duizenden euro's kosten.

Factuurfraude en slimme phishing

Niet elke aanval begint met gijzelsoftware. Factuurfraude en phishing komen veel voor. Cybercriminelen sturen een factuur of e-mail die nauwelijks van echt te onderscheiden is. Logo klopt. Lay-out klopt. Alleen het rekeningnummer of de link wijkt af. Spam zit allang niet meer vol taalfouten. Berichten zijn professioneel opgesteld en soms vrijwel identiek aan echte communicatie. 'Cybercriminelen analyseren hoe een bedrijf werkt,' zegt Maaskant. 'Zij kijken naar vaste leveranciers en betaalmomenten. Daar spelen cybercriminelen gericht op in.' Steeds vaker wordt kunstmatige intelligentie gebruikt. Berichten worden automatisch afgestemd op de ontvanger. Zelfs telefoontjes kunnen worden nagebootst.

'De stem klinkt overtuigend en het verhaal lijkt logisch,' zegt Marc Derksen. 'Juist daardoor is het risico groter.' In drukke periodes kan een vervalste factuur ongemerkt worden betaald. Het geld is meestal niet meer terug te halen.

Website misbruikt

In de sector werd een webshop van een hovenier gekopieerd. Klanten betaalden via een nagemaakte website. Het geld kwam nooit

> 'Geen toegang tot je systeem betekent geen grip op je bedrijf'

bij het echte bedrijf terecht. 'Dan krijg je boze telefoontjes van klanten,' zegt Maaskant. 'Terwijl het bedrijf zelf van niets wist.' De schade zit niet alleen in omzetverlies. Twijfel over dataveiligheid tast het vertrouwen aan. In een regionale markt kan dat direct invloed hebben op nieuwe opdrachten.

Medewerkers en werktelefoons

Veel hoveniers werken met tablets en telefoons op locatie. Planning en klantgegevens staan op mobiele apparaten. 'Als een werktelefoon wordt gebruikt voor onbetrouwbare apps of het bezoeken van onbetrouwbare websites, kan dat een ingang zijn voor cybercriminelen,' zegt Maaskant. Heldere afspraken over gebruik, versleuteling en het op afstand wissen van apparaten bij verlies zijn noodzakelijk. 'Techniek alleen is niet voldoende,' zegt Derksen. 'Gedrag van medewerkers bepaalt mede het risico.'

'Vertrouwen is snel beschadigd, maar moeilijk te herstellen'

Geen eenmalige actie

Steeds meer hoveniersbedrijven digitaliseren hun processen. Veel ondernemers hebben al beveiligingsmaatregelen genomen. Volgens Koninklijke VHG zit het risico niet in onwil, maar in verslapping. 'Ondernemers zijn ermee bezig,' zegt Maaskant. 'Maar digitale veiligheid is geen eenmalige investering. Je bent nooit klaar.' 'Cybercriminelen gebruiken bots die dag en nacht systemen scannen op kwetsbaarheden,' vult Derksen aan. 'Wie updates uitstelt, laat bekende beveiligingslekken openstaan.'

Cyberverzekering

Steeds meer ondernemers sluiten een cyberverzekering af. Die kan kosten voor IT-herstel en juridische ondersteuning dekken. Volgens Koninklijke VHG is het een vangnet, geen oplossing. 'Een verzekering vervangt geen goede beveiliging,' zegt Maaskant. 'Verzekeraars stellen bovendien eisen aan je digitale maatregelen.'

Marc Derksen

Richard Maaskant

Wat zegt Koninklijke VHG tegen ondernemers die denken dat dit hen niet overkomt?

Veel hoveniers denken dat hun bedrijf te klein is om interessant te zijn voor cybercriminelen. Volgens Koninklijke VHG is dat een misvatting. 'Cybercriminelen maken geen onderscheid,' zegt Maaskant. 'Cybercriminelen zoeken met het oog op hun verdienmodel zwakke plekken.' Ook een klein bedrijf beheert persoonsgegevens en bankgegevens. 'Als jouw planning een week platligt, voel je dat direct in je omzet,' zegt Maaskant. Digitale veiligheid hoort bij professioneel ondernemerschap.

Wat moet je geregeld hebben?

Ondernemers hoeven geen IT-specialist te zijn, maar moeten wel weten of hun basis op orde is en gerichte vragen stellen aan hun IT-leverancier. 'Als je op één van deze vragen geen duidelijk antwoord krijgt, moet je doorvragen,' zegt Derksen.

Samen Digitaal Veilig

Koninklijke VHG wijst ondernemers op het platform Samen Digitaal Veilig en het Digital Trust Center van het ministerie van EZK voor praktische ondersteuning en actuele informatie. 'Digitale veiligheid vraagt blijvende aandacht,' besluit Maaskant. 'Wie pas in actie komt als het systeem niet meer opstart, is te laat. Dan ben je niet alleen je data kwijt, maar mogelijk ook het vertrouwen van je klant.'

Tien vragen voor je IT-adviseur

- Is Multi-Factor Authentication op alle accounts actief?
- Is de back-up getest en werkt herstel aantoonbaar?
- Worden beveiligingsupdates direct geïnstalleerd?
- Is er een concreet stappenplan bij een ransomware-aanval?
- Is toegang tot belangrijke data beperkt tot noodzakelijke medewerkers?
- Worden medewerkers getraind in het herkennen van phishing?
- Zijn laptops en telefoons versleuteld en op afstand te wissen?
- Worden leveranciers gecontroleerd op digitale veiligheid?
- Is recent een penetratietest uitgevoerd?
- Is het bedrijf voorbereid op NIS2-verplichtingen indien van toepassing?

'Een update van vijf minuten is goedkoper dan weken herstel'

BE SOCIAL
Scan, lees & deel!