duiding

“Land- en tuinbouwers extra gevoelig voor cybercriminaliteit”

duiding

Boeren en tuinders lopen een bovengemiddeld risico om slachtoffer te worden van cybercrime. Dat vertelt Kurt Callewaert, verbonden aan de hogeschool Howest en benoemd tot cybersecurity-onderzoeker van het jaar. Hij reageert op een recente hack bij een tuinbouwbedrijf. “Land- en tuinbouwers zijn vaak niet ICT-onderlegd en bovendien is het een sector die onder druk staat waardoor bedrijven niet uitgerust zijn met de nieuwste digitale veiligheidssystemen.”

25 JUNI 2024

Jerom Rozendaal

Lees meer over:
landbouw algemeen

“Hallo, kan ik met je praten? Per email?” Deze e-mail ontving onze redactie onlangs van een contact in de tuinbouw, van wie het e-mailadres gehacked bleek te zijn. “Alle mensen waar ik in het verleden e-mailcontact gehad heb, hebben zo'n bericht ontvangen. Ik word om de haverklap gebeld”, vertelt de tuinder aan de telefoon.

De tuinbouwer blijkt het slachtoffer te zijn van e-mailspoofing, vernemen we van Kurt Callewaert, verbonden aan Howest en benoemd tot cybersecurity onderzoeker van het jaar 2023. “Dat is een soort van identiteitsdiefstal waarbij de hacker inbreekt in het emailsysteem en berichten uitstuurt naar contacten. Daarbij probeert hij het vertrouwen van de ontvanger te winnen en geld af te troggelen.”

Volgens Callewaert is e-mailspoofing schering en inslag. De cybercriminelen bevinden zich in landen als China, Rusland en Iran en door middel van artificiële intelligentie (AI) wordt hun werkwijze zeer verfijnd. “Ik heb recent een geval gehad waarbij een vader door zijn dochter was benaderd dat zij in nood zat en dringend 2.000 euro nodig had. Het bericht was zo geloofwaardig dat de vader meteen het geld heeft overgemaakt.

Wake-up call

De identiteitsdiefstal heeft volgens de tuinder niet tot schade geleid bij zijn contacten. Hij is desondanks ontdaan en wil liever anoniem blijven. “Ik ben een tuinder en heb nooit stil gestaan bij mogelijke cyberrisico’s. Wat dat betreft is dit een goed wake-up call. Het is misschien goed om van tijd tot tijd een expert uit te nodigen om de cyberveiligheid op het bedrijf door nemen.” Van zijn e-mailprovider heeft hij het advies gekregen om af en toe zijn paswoord te veranderen.

Dit is volgens Callewaert het minste wat gedaan kan worden. “Inbraken in mailboxen ontstaan vaak als je op verschillende podiums inlogt met hetzelfde emailadres en wachtwoord. Denk bijvoorbeeld aan reisbureaus, internetwinkels, enz. Deze platforms kunnen gehacked zijn en dan zit de cybercrimineel in jouw mailbox”, vertelt de professor die ook het gebruik van multifactorauthentificatie aanraadt om cybercriminelen buiten te houden. Dat is een methode om de authenticiteit van een gebruiker te verifiëren op meer dan één enkele manier.
Alhoewel het voorval van de tuinder niet specifiek sectorgelinkt is, zijn land- en tuinbouwers volgens Callewaert bovengemiddeld gevoelig voor cybercriminaliteit. “Land-en tuinbouwers hebben een druk bestaan en zijn bovendien vaak niet erg ICT-onderlegd. Daarbij is het een sector met de nodige problemen waardoor computersystemen niet zijn uitgerust met de modernste veiligheidssystemen.” Hij pleit voor een sensibilisering over de gevolgen van cybercriminaliteit door de landbouworganisaties.

Phishing en spoofing

In het geval e-mailspoofing kunnen cybercriminelen ook de facturatie onderscheppen en zodoende financiële schade berokkenen aan de boer. Andere vormen van cybercriminaliteit waar boeren en tuinders, net zoals gewone burgers, slachtoffer van kunnen worden, zijn phishing, website- en telefoonspoofing. Bij dat laatste nemen de oplichters een ander bestaand telefoonnummer aan van bijvoorbeeld de bank en proberen een overboeking af te dwingen.
Wat betreft de grote vormen van digitale criminaliteit, zoals bijvoorbeeld het kapen van computersystemen door het plaatsen van ransomware om losgeld te eisen, ziet Callewaert geen bijzonder risico’s bij boeren en tuinders. “In deze gevallen gaat het vaak om miljoenen euro’s om vervolgens een internetsysteem vrij te geven.”
De agrovoedingsindustrie in bredere zin is volgens de wetenschapper wel een mogelijk doelwit voor digitale struikrovers. “In het verleden zijn al voedingsbedrijven gekaapt zoals bijvoorbeeld De Keyser-Ossaer (vleesverwerker), Ranson (bakkerijproducten), Beyers (koffie) en Duvel (bier).” Omdat voedingsbedrijven gelden als een strategische sector zijn ze onderhevig aan de NIS2-wetgeving (Europese richtlijn rond Network and Information Security, red.), die dit najaar van kracht wordt. Deze wet verplicht bedrijven aanvullende cyberbeveiligingsmaatregelen te nemen.

Ingebouwde veiligheidssystemen

Callewaert stelt verder dat IT-systemen op boerderijen, denk aan bijvoorbeeld melkrobots en klimaatsturing van serres, door de leveranciers beveiligd worden. Hierdoor ziet hij met de oprukkende digitalisering in de landbouw in het achterhoofd ook geen extra risico’s voor de sector. Eén van deze leveranciers is ook DjustConnect, een platform dat digitalisering en het digitale datadelen in de sector in Vlaanderen faciliteert en stimuleert. “Cybersecurity heeft onze hoogste prioriteit en wij volgen hierbij de geldende richtlijnen”, vertelt Stephanie Van Weyenberg, DjustConnect coördinator bij ILVO.
Multilayerbeveiliging moet voorkomen dat kwaadwilligen tot de data doordringen en boeren moeten zich bij het aanmelden bijvoorbeeld identificeren met hun ID-kaart, wat neerkomt op dezelfde veiligheid als bijvoorbeeld bij het internetbankieren.

VILT vzw

Bd Simon Bolivar 17
1000 Bruxelles

Contact

M • info@vilt.be

Volg ons op:

screenreader.visit us on our facebook page: https://www.facebook.com/vilt.nieuws/
screenreader.visit us on our linkedin page: https://www.linkedin.com/company/vilt-vzw/
screenreader.visit us on our instagram page: https://www.instagram.com/vilt.nieuws
screenreader.visit us on our x page: https://x.com/vilt_nieuws
screenreader.visit us on our bluesky page: https://bsky.app/profile/viltnieuws.bsky.social

---