Samen strijden tegen cybercriminaliteit

En dan, in één keer, ligt alles plat. Geen toegang tot data, bestanden versleuteld, kortom: computer geblokkeerd. Je bent slachtoffer van gijzelsoftware. Je moet flink dokken om je gegevens weer terug te krijgen. Een horrorscenario. Helaas, is het de praktijk. De dreiging van online-aanvallen neemt schrikbarend toe. Cybercriminelen hebben ook het Nederlandse tuinbouwcluster in het vizier. "Het is niet óf, maar wanneer", waarschuwen deskundigen.

Tekst: Suzan Crooijmans, Fotografie: Glenn Mostert

Om het tuinbouwcluster te helpen in het weerbaar maken tegen digitale spionage en cyberaanvallen, heeft het innovatiepact van Greenport West-Holland het initiatief genomen voor het oprichten van een Cyberweerbaarheidscentrum. Een laagdrempelig centrum dat bedrijven binnen het tuinbouwcluster helpt om zich beter te wapenen tegen cybercriminaliteit. Door het delen van nieuws, praktische checklists, tools, kennis en praktijkvoorbeelden. En waarbij de kennissessies, webinars, trainingen en workshops voor iedereen toegankelijk zijn. Half juli presenteerde het innovatiepact van Greenport West-Holland zijn plannen en vormde ze samen met een aantal ketenregisseurs zoals veilingen, veredelaars en toeleveranciers een 'coalition of the willing'.

Sterk als zwakste schakel

De motivatie om dit met elkaar te doen, is groot. Woody Maijers, programmaregisseur Greenport West-Holland, Marcel Spruit, lector Haagse Hogeschool, Joris den Bruinen, directeur The Hague Security Delta en André van der Linden, CIO Royal FloraHolland, vertellen waarom: "Als het om cybersecurity gaat, is samenwerking de enige sluitende weg. Immers, de hele keten staat met elkaar in verbinding. Er is veel dataverkeer tussen telers onderling, met kopers, handelaren en met leveranciers van technische systemen. Dat maakt de sector in digitale, maar ook in operationele zin kwetsbaar. Het is een complex gebeuren omdat iedereen op een bepaalde manier van elkaar afhankelijk is. De keten is zo sterk als de zwakste schakel." Met zijn hoge graad van digitalisering is er binnen het tuinbouwcluster online veel te halen voor criminelen. De sector is interessant voor de dieven die op zoek zijn naar relevante kennis en technologie, naar intellectueel eigendom, die hen helpen een eigen onderneming te bouwen. Ook voor de groep die uit is op geld, en die systemen gijzelen, is de tuinbouw een gewilde prooi. Alsook voor de vandalen die, met DDoS-aanvallen, de boel willen verstieren en de keten willen platleggen of zomaar om zich heen slaan. "Ondernemers moeten zich bewust zijn van de grote risico's die ze lopen", zeggen de partners die het cyberweerbaarheidscentrum Greenport de komende maanden gaan optuigen.

"Er is werk aan de winkel", concludeert Marcel Spruit, die in opdracht van Greenport onderzoek doet naar de cyberkwetsbaarheid van organisaties en bedrijven binnen het tuinbouwcluster. "Uit een eerste verkennend onderzoek kwam naar voren dat de kopgroep de veiligheid redelijk goed op niveau heeft, de grote middengroep wel wát heeft geregeld en de achterhoede helemaal niet nadenkt over cybersecurity. Hoe gevaarlijk dat is, laat zich makkelijk raden. Zonder bescherming staat de digitale voordeur wagenwijd open en kan de hele wereld bij de knoppen van bijvoorbeeld je klimaatcomputer en zo het kasklimaat ontregelen." De urgentie van cybersecurity wordt door vooral de kleinere organisaties onderschat, weet ook Joris den Bruinen van HSD. "Die denken het zal mijn deur wel voorbijgaan. Een grote misvatting, als je bedenkt dat op jaarbasis, tweevijfde van de ondernemers last heeft van cybercriminele activiteiten. De tuinbouw is daarop geen uitzondering. Internetcriminelen hebben al toegeslagen. Alleen, de getroffen bedrijven houden zich stil. Uit schaamte misschien, omdat ze niet knullig willen overkomen omdat ze hun veiligheid niet op orde hadden." Den Bruinen weet van een geval van CEO-fraude, waarin een medewerker in een mail een vaker voorgekomen opdracht van zijn baas kreeg voor een betaling. Toen de betaling al was uitgevoerd, bleek dat een crimineel het emailadres van de baas had misbruikt, ofwel gespoofd, in cybertermen.

Begint bij bewustwording

"Iedereen in de keten is verantwoordelijk voor cybersecurity", stelt André van der Linden. "Royal FloraHolland heeft veel aandacht voor veiligheid. Wij zorgen dat onze systemen goed beveiligd zijn. Ook in het belang van onze leden. Ze willen allemaal weten of hun data bij ons wel veilig zijn. Dan leg ik uit welke maatregelen wij nemen. Vervolgens stel ik een wedervraag. Heb jij ook nagedacht over jouw eigen digitale veiligheid? Heb je een alternatief als je internetverbinding uitvalt? Wat heb je geregeld voor het geval iemand toegang heeft tot jouw account? Uit de reacties maak ik op dat het bewustzijn over security best hoog is, alleen het vertaalt zich nog niet zo naar het eigen bedrijf."

Een van de eerste taken van het cyberweerbaarheidscentrum is mensen bewust te maken van de dreiging. Spruit zegt erover: "Zolang je onbewust onbekwaam bent, weet je niet eens dat je een probleem hebt. Voor het stellen van vragen, is een bepaald bewustzijn nodig."
"Als je een IT-er niet vraagt om de restore van een backup regelmatig te testen, dan gebeurt het niet", komt Den Bruinen met een voorbeeld. "Een ondernemer moet vragen stellen!", zegt hij beslist.

Het nadenken over digitale veiligheid, is de eerste stap die ondernemers moeten zetten. "Inventariseer je kwetsbaarheden", zegt Van der Linden. "Wat is belangrijk, wat wil ik beschermen, waar ben ik bang voor, wat mag niet gebeuren, waar liggen mijn risico's, hoe groot zijn die, wat kan ik doen om die risico's te verlagen. Je kunt het vergelijken met de afwegingen en maatregelen die je neemt om je huis te beveiligen."

Den Bruinen wil uit de wereld hebben dat digitale beveiliging een dure aangelegenheid is. "Het kost veel méér geld als je de klos bent. Er zijn bedrijven die over de kop zijn gegaan door een cyberaanval." Hij somt een reeks basisbeveilingsmaatregelen op die niks of weinig kosten en wel op orde moeten zijn: installeer consequent de updates van je systemen, installeer een malwarescanner, maak backups, stel een dubbele authenticatie in en voorkom dat oud-medewerkers nog toegang tot het systeem hebben."

Mentaliteit en gedrag

"Het cyberweerbaarheidscentrum focust op mentaliteit", vult Woody Maijers aan. "Het gaat om verandering van gedrag en het organiseren van bedrijfsprocessen. We willen dat mensen getriggerd worden om digitale veiligheid op de agenda te zetten. Ons doel is dat iedereen zich bewust wordt van de risico's en vervolgens adequate beveiligingsmaatregelen neemt." Maijers sluit niet uit dat klanten eisen gaan stellen dat de cyberveiligheid op orde moet zijn. "Nog niet zo lang geleden lag, door toedoen van een leverancier, de logistiek van Albert Heijn twee dagen plat. Dat moet een waarschuwing zijn."

Na de zomer wordt het cyberweerbaarheidscentrum officieel gelanceerd. Eind van het jaar moet het operationeel zijn. De provincie Zuid-Holland, het ministerie van EZK, Greenport West-Holland en HSD hebben budget vrijgemaakt. Een aantal ketenregisseurs leveren tijd om activiteiten op te starten. "Het is een onderwerp waarop we niet gaan concurreren. Daarvoor zijn de organisaties in de keten te afhankelijk van elkaar", aldus Maijers. "We zitten allemaal in hetzelfde schuitje. Het heeft geen zin als de een het goed geregeld heeft en andere partners in de keten niet. Het gaat echt over awareness en concrete oplossingen", besluit Van der Linden. ■

PAKKET VAN DIENSTEN CYBERWEERBAARHEIDSCENTRUM GREENPORT

- het verstrekken van relevante en duidelijke (dreigings)informatie op strategisch, tactisch en operationeel niveau over actuele cyberdreigingen.
- het opstellen en delen van beveiligingsadvies over kwetsbaarheden in hardware en software.
- het beschikbaar stellen van checklists en tools voor het inrichten van cybersecurity.
- het opstarten van programma's rondom bewustwording en gedragsverandering bij ondernemers en CEO's, managers en medewerkers.
- het oprichten van een digitaal loket voor raad en advies.
- slachtofferhulp.
- het faciliteren van expert-overleggen voor kennisdeling en netwerken.
- het gezamenlijk inkopen van cybersecurity-dienstverlening in de markt.