REGISSEUR VOOR DIGITALE VEILIGHEID

De digitale veiligheid móet beter, samenwerking ís noodzakelijk en het collectieve bewustzijn héέft een zetje nodig. Het is de cybercriminaliteit die dit vereist. Die neemt in omvang toe en het tuinbouwcluster is –door zijn hoge digitaliseringsgraad- een interessant doelwit. Greenport West-Holland, Security Delta, Royal FloraHolland, Interpolis-Achmea, Delphy, Dutch Fresh Port/VBO, Hoogendoorn Growth Management, Glastuinbouw Nederland, Haagse Hogeschool, Provincie Zuid-Holland en GroentenFruit Huis namen het initiatief voor het opzetten van een cyberweerbaarheidscentrum. Komend najaar gaat het open en kunnen ondernemers er terecht voor alle vragen over cybersecurity.

Tekst: Suzan Crooijmans, Fotografie Linda Straathof

Het Cyberweerbaarheidscentrum Greenport is een help- en kennispunt, waar je kunt aankloppen voor informatie en raad, gemakkelijk toegankelijk en bestemd voor alle bedrijven over de hele breedte van het tuinbouwcluster. “Het wordt de plek van waaruit we specialistische kennis gaan delen en bedrijven begeleiden”, zegt Jolanda Heistek, directeur van Greenport West-Holland. “Helpen en voorkomen, dat zijn de kerntaken.” Bert Feskens is programmaregisseur van het Cyberweerbaarheidscentrum Greenport. Hij noemt digitale veiligheid belangrijk op ketenniveau en op individueel niveau en “een absolute randvoorwaarde voor de groei van de sector.”

Heistek en Feskens schetsen de context. “De glastuinbouwsector is onderdeel van een complex ketensysteem met een grote onderlinge afhankelijkheid. Alle schakels –veredelaar, toeleverancier, teler, handel, logistiek- zijn met elkaar verbonden en daarmee tegelijkertijd zeer kwetsbaar. Als door een digitale aanval één onderdeel wegvalt, wordt het hele cluster getroffen.” Ook de hoge standaard van automatisering, robotisering en digitalisering maken systemen kwetsbaar. “Autonome kassen worden digitaal aangestuurd. Gaat er iets mis, dan zijn er nog maar beperkte handmatige terugvalopties. Het is dus ontzettend cruciaal dat die digitale systemen ‘up & running’ blijven.”

Cyberbewustzijn

Des te zorgwekkender is het dat de praktijk de risico’s van een digitale hack schromelijk onderschat. Feskens noemt onwetendheid als oorzaak. Veel bedrijven hebben de digitale veiligheid niet op orde. Om te bereiken dat mensen de dreiging van een cyberaanval voelen, zet het cyberweerbaarheidscentrum sterk in op cyberbewustzijn. In workshops worden confronterende voorbeelden gegeven. “Bijvoorbeeld over het gemak waarmee criminelen ingangen vinden om in een systeem te komen en mee te kijken met een minihack in een kas. Ook signalen dat Russische en Chinese hackers grote interesse tonen voor de agrifoodsector is alarmerend”, zegt Heistek. “Hackers hebben het heus niet alleen gemunt op banken of multinationals. Ze hebben de ketenafhankelijkheid door en weten dat ze de (internationale) tuinbouwketen zwaar kunnen raken met een aanval. Ik hóór lezers denken: ‘hou je mond,

je brengt ze op ideeën.' Maar die ideeën hebben ze al; om ons heen wórden al bedrijven gehackt."

Openheid

Jaarlijks wordt 1 op de 5 bedrijven slachtoffer van een cyberaanval. Het is niet iets waarmee bedrijven snel naar buiten komen. "Toch is openheid belangrijk. Niet alleen omdat er een waarschuwing vanuit gaat, maar ook zodat we samen kunnen zoeken naar oplossingen en verbeteringen", zegt Feskens. Wat de dreigingen zijn? Feskens noemt de drie die er wat hem betreft bovenuit stijgen: "Ten eerste, de bedrijfscontinuïteit. Stel je wordt aangevallen, je systemen vallen plat en je bedrijf ligt een paar dagen stil. Soms is het zo dat als je weer toegang wilt, je een som geld moet betalen. Ten tweede, Intellectueel Eigendom. Interessant voor andere landen om te stelen.
En op drie, frustratie. Bijvoorbeeld van omwonenden die het niet eens zijn met de bouw van een kas. Of van een boze medewerker of een klant die uit is op wraak."

Het belang van samenwerking kan niet genoeg benadrukt worden. Uit alle geledingen zijn ketenregisseurs aangehaakt om mee te helpen bij het opzetten van het cyberweerbaarheidscentrum. Dutch Fresh Port is er een van. Bij dit grootste Agro-Vers-Food cluster van Nederland staat cyberweerbaarheid hoog op de agenda. Als internationale draaischijf in de retail van groenten en fruit, waarin jaarlijks 6 miljard euro omgaat, en alle handelsverkeer alsook de communicatie digitaal verloopt, valt er nogal wat te beschermen.

Het wapenen tegen cybercrime binnen het agf-cluster dringt nog langzaam door. "De grotere bedrijven hebben er wel oog voor, daar lopen IT'ers rond. Maar bij de kleinere is de aandacht gering", zegt Johan in 't Veld, projectbegeleider voor DFP. "Daarom zetten we sterk in op communicatie om het belang en de noodzaak ervan te laten inzien. We informeren en schudden wakker en hameren op het nemen van maatregelen. Ook zetten we communities op van bedrijven om van elkaar te leren. Met onze deelname aan het Cyberweerbaarheidscentrum Greenport kunnen we onze ondernemers de ultieme service bieden op het gebied van digitale veiligheid, zoals de bedrijfsscan om te zien waar de zwakheden liggen." In 't Veld noemt het tijdig op de hoogte zijn van cyberdreigingen, een van de waardevolste diensten die het centrum gaat bieden. "Daardoor kun je tijdig maatregelen treffen."

Gedragsverandering

Ook Achmea is, als medeoprichter, nauw betrokken. De verzekeringsmaatschappij, die met de merken Interpolis en Avéro Achmea actief is in de glastuinbouw, wil haar kennis inzetten om bedrijven op de risico's van cybercriminaliteit te wijzen. "Wij willen voorkomen dat bedrijven slachtoffer worden van digitale inbraak of gijzeling", zegt Bart Stengs sectormanager glastuinbouw van Achmea. "We zien de noodzaak om digitale veiligheid te bespreken. Ondernemers hebben nog onvoldoende in de gaten hoe kwetsbaar ze zijn geworden als gevolg van de vergaande digitalisering. Softwaretoepassingen zoals e-mail in de kantooromgeving (IT) zijn vaak niet goed gescheiden van de operationele systemen (OT) waardoor de hacker éénmaal binnen ook de machines en installaties van het bedrijf kan plat leggen. De mens en de organisatie van de beveiliging zijn hierin de zwakste schakels. In onze communicatie sturen we dan óók aan op gedragsverandering, naast preventieve maatregelen. Laat een computer niet onbeheerd achter, verander een wachtwoord regelmatig, installeer een update, dat soort zaken. Met gedragsverandering en preventie is veel te winnen aan bescherming tegen cybercrime, het zijn op dit moment de meest adequate maatregelen voor de bedrijfscontinuïteit.

Laatste hand

Momenteel wordt de laatste hand gelegd aan het Cyberweerbaarheidscentrum Greenport. Bert Feskens: "We zijn bezig met de inrichting van een digitaal loket voor advies en slachtofferhulp en voor het waarschuwen over nieuwe cyberdreigingen zodat bedrijven zich tijdig kunnen voorbereiden. Ook werken we aan de programmering van workshops om deelnemers aan de hand van experts mee te nemen om daadwerkelijk de handelingen te doen. Verder bieden we bedrijven een nulmeting aan, een eerste scan die inzicht geeft in de mate van digitale veiligheid. We willen dat zoveel mogelijk bedrijven zich bij ons aansluiten en van onze diensten gebruik maken. Onze ambitie is het cluster cyberweerbaar te maken én te houden."

Het Cyberweerbaarheidscentrum Greenport is bereikbaar via https://greenportwestholland.nl/cyberweerbaarheidscentrum/

VIJF BASISPRINCIPES VAN VEILIG DIGITAAL ONDERNEMEN

1. Inventariseer kwetsbaarheden
2. Kies veilige instellingen
3. Voer updates uit
4. Beperk toegang
5. Voorkom virussen en andere malware

(bron: digitaltrustcenter.nl)