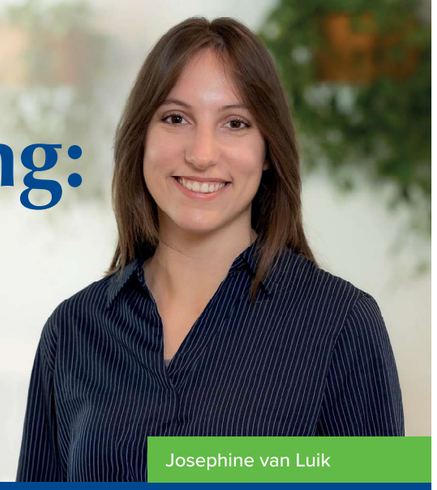
Hack-proof harvesting: digital resilience for growers



Josephine van Luik

Horticulture is undergoing rapid digitalisation by means of robotics, smart sensors and climate control. While this development offers many opportunities, it also makes companies more vulnerable. Cybersecurity therefore requires a systematic approach, not only to prevent unauthorised access but also to avoid confusion about responsibilities. Josephine van Luik, Community Manager at Cyberweerbaarheidscentrum (Cyber Resilience Centre) Greenport, explains the practical steps growers can take to immediately reduce their cyber risks.

Though many are unfamiliar with the term ‘operational technology’ (OT), every grower and supplier deals with it in some way, for example in the form of a greenhouse device such as a conveyor belt or a robotic arm. Previously, ‘office IT’ used to be separate from the installations and cultivation systems in the greenhouse, but those domains now overlap. Josephine sees the risks for growers quickly increasing as a result. ‘The sector is becoming more digital and this makes it more vulnerable. When systems fail, production comes to a halt. Cybersecurity has therefore become a continuity issue.’ Josephine emphasises the need for a combined approach: ‘To enhance your digital safety, you need to address IT and OT at the same time. Keep an eye on which systems are running, how they are connected, and who has access. That makes it easier to identify any vulnerabilities.’

Cybersecurity as a permanent pillar in risk management

Josephine sees cybersecurity as an extension of physical security: ‘You lock the greenhouse, and camera surveillance is already taken for granted as a means of protecting your cultivation and production. Cybersecurity actually deserves the same priority and status within a horticultural company.’ There are many measures that don’t have to be costly or complex to be effective; instead, they rely on attention and discipline. ‘A good password policy costs nothing, and installing updates takes very little time. These simple steps can prevent the majority of modern attacks and significantly contribute to the digital resilience of horticultural companies.’

As strong as the weakest link

In horticulture, companies work with a combination of IT and OT, such as climate computers, irrigation control, sensors, cultivation software, robots and cloud platforms from various suppliers. Criminals deliberately target the least secure component in order to gain entry, and then use that access point to move further through the digital environment of other parties. Josephine: ‘Cybersecurity is therefore not only a business risk, but also a supply chain risk. A company is only as safe as its weakest link. A seemingly small security breach can escalate into a disruption that affects the entire chain, with direct consequences for production processes, logistics and cultivation data.’

Prevention is far better than cure

According to Josephine, suppliers mainly focus on their own piece of technology, while in her experience, cyber risks often arise between different systems due to matters such as connections, outdated updates, weak passwords or unclear responsibilities. She warns against making assumptions about the responsibilities of suppliers. ‘A grower who thinks that the supplier will take care of everything is in for a disappointment. Play an active role in the conversation and make clear agreements,’ she emphasises. In her view, the chain can only operate in a genuinely safe way once roles, responsibilities and security requirements have been made clear.

Cybersecurity becomes legislation

Companies that play an essential role in keeping Dutch society running must comply with the Cybersecurity Act (Cbw) since the beginning of this year. The Cbw imposes clear cybersecurity requirements on companies, including those in the fruit and vegetable sector, so that digital security is permanently embedded in their business operations. That level of attention is just as relevant in practice for organisations without direct legal obligations. Suppliers will also be subject to stricter requirements, says Josephine: ‘Suppliers must demonstrate that they have their digital processes properly in place. The law also encourages horticultural companies to check how digitally resilient their suppliers are.’ Josephine emphasises that this is an essential way to prevent blind spots. ‘If you are unclear about the security measures your suppliers are using, then you will also be unaware of your potential risks,’ she says.

According to Josephine, the key is simple: ‘If you gain insight into your own digital resilience and that of your suppliers now, it will be much easier for you to specifically reduce vulnerabilities and prepare for any future digital challenges!’

Tips from Cyberweerbaarheidscentrum Greenport

What can you do today?

- Create a complete overview of both IT and OT systems.
- Make backups of important systems and test them regularly.
- Use strong passwords and multi-factor authentication (MFA).
- Install software updates as soon as they are available.
- Involve employees actively in cybersecurity.
- The government’s CyberVeilig (CyberSafe) check will help you gain insight into your situation and determine which initial steps are necessary.
- Also check whether your company is subject to the new Cybersecurity Act (Cbw) and take the test at www.ncsc.nl.

If you would like to receive regular practical tips, handy checklists, and current insights into risks and vulnerabilities within the sector, the Cyberweerbaarheidscentrum (Cyber Resilience Centre) Greenport has joined forces with Royal FloraHolland and GroentenFruit Huis to offer free cyber subscriptions for companies in the ornamental horticulture and fruit and vegetable sector. For more information, visit www.cwgreenport.nl.



> Every horticultural business is only as safe as the weakest link in the chain.
>
> – Josephine

Cyberweerbaarheidscentrum Greenport focuses on supporting companies in the horticultural cluster. It is a non-profit organisation and was founded by a large number of prominent organisations: Delphy, Dutch Fresh Port, Royal FloraHolland, Glastuinbouw Nederland, Greenport West-Holland, GroentenFruit Huis, Hoogendoorn Automatisering, Interpolis-Achmea, Anthura, Security Delta (HSD), the NCSC, The Hague University of Applied Sciences, and the Province of South Holland. These organisations are aware of the risks that the chain faces and take the lead, actively contributing to the Cyberweerbaarheidscentrum Greenport.