KPMG

Europe at a crossroads

It took the ethical hacker 8 minutes to get in

Rick van Dorp

March 2026

It took the ethical hacker 8 minutes to get in

“Don’t wait until something goes wrong. Always be aware of your role in the chain” Rick van Dorp, Strategic director of Van Dorp

Can you give an example?

"We started a security improvement programme with specialised partners. One of the first things we found out was that an attempted CFO fraud for €40,000 nearly succeeded. Another finding was that quite a few employees clicked phishing links. But perhaps the biggest shock came during a penetration test. We thought we were doing fairly well in securing our systems, but the consultant we hired needed only eight minutes to gain full access."

As a HVAC company, you play a role in the chain and have a responsibility for your clients' cybersecurity. That role may not always be very tangible. Could you give an example of how this responsibility in the chain plays out in your work?

"Certainly. We manage the climate systems of some very prominent governmental offices. This means that you have access to floor plans and know who sits where. That's sensitive information. And perhaps the biggest game changer came during the NATO summit at the World Forum in The Hague. We manage the building management system there too. On the first day of the summit, we got a call from the National Coordinator for Counterterrorism and Security (NCTV), asking us to install a patch immediately. That really sharpened everyone's awareness."

Was it a wake-up call?

"And a blessing in disguise. The urgency became real. The NCTV had noticed a connection from the ministry to us through a vulnerable port. Within minutes, everyone was fully alert. Since then, we've taken compliance and security even more seriously. The entire management team has completed NIS2 training, and we've freed up resources for awareness."

How do you deal with the personal liability for executives that comes with this chain responsibility?

"It's a serious concern following the new legislation. In the end, we are the ones responsible for any fines or damages in the event of a breach. That's a big deal. You install a heat pump, and suddenly you're liable for the fallout of a cyberattack. That's serious. We're a decentralised company with many autonomous branches and a wide range of products and services. That diversity makes things more complex. Our cybersecurity policies have become much tighter. For major clients, we have a checklist that must be completed before we can manage systems remotely. In the past, we mainly advised about cyber. Now we enforce compliance. An example is when we rolled out multi-factor authentication (MFA) on laptops. We experienced a slow adoption. So at a company event with 250 managers, we told them very clearly: if you don't activate MFA today, you'll lose access to your laptop tomorrow. Simple as that."

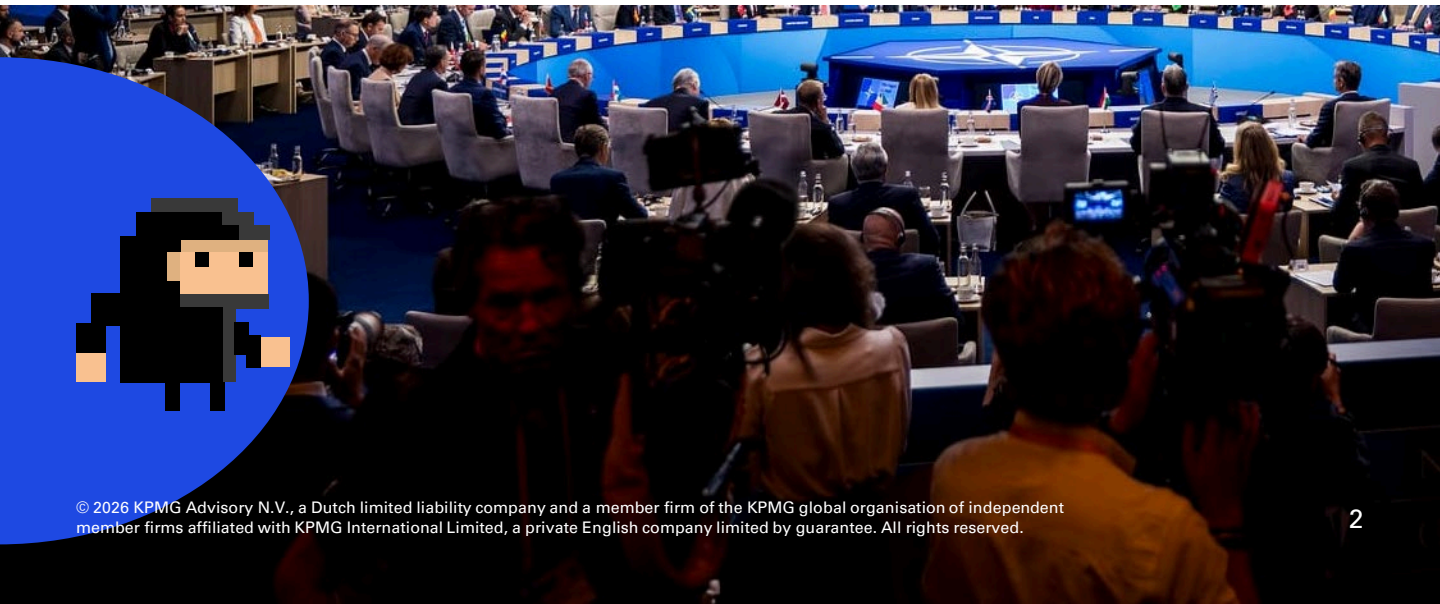
A common complaint is that compliance involves a lot of paperwork, especially because clients ask so many questions and demand reports. How do you handle that?

"We standardised responses into a single assurance pack aligned to recognised controls: a policy note on our cybersecurity measures, our roadmap to NIS2 compliance, company information, and a statement confirming that we haven't been hacked in the past three years. We only make exceptions for major clients like the Government Real Estate Agency.

For the future, I hope we can get to a standardised report with a rating that shows how well you're managing security, similar to how credit ratings work."

What's your main lesson for other entrepreneurs?

"Find yourself a good partner in the domain of cybersecurity. Don't wait until something goes wrong. And be always aware of your role in the chain, even if you think you don't have one."

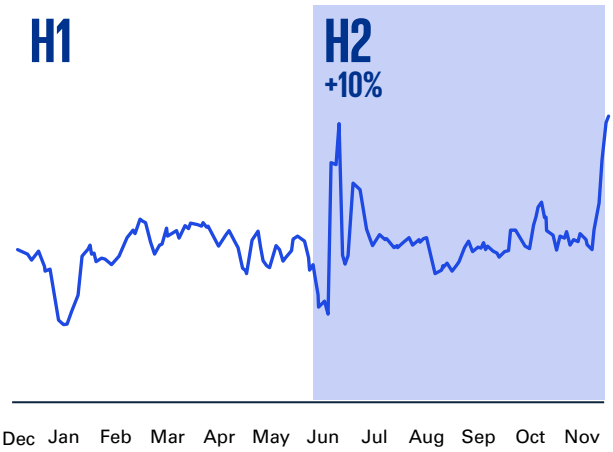


ESET threat intelligence

Rick van Dorp's experience highlights that state-sponsored operations are routinely targeting civilian vital infrastructure. Companies in the installation and logistics sectors have become primary targets in broader conflict scenarios. For C-level executives, the shift toward personal liability under NIS2 is a critical turning point.

Organisations that fail to integrate cyber resilience into their broader geopolitical strategy are ignoring a primary instrument of modern warfare that directly threatens their operational continuity.

Overall threat detection trend in H1 2025 and H2 2025, seven-day moving average



Source: ESET Threat Report H2 2025

Dave Maasland
CEO
ESET Netherlands

Recommendations

Immediate
Organisations need to act and audit critical suppliers for compromise. Prioritise audits in sectors relevant to your organisation, such as telecommunication, energy and logistics.

Mid-term
Implement FIDO2 MFA across infrastructure; eliminate password-based access to sensitive systems.

Long-term
Leadership must implement a long-term policy to also consider where technology comes from, instead of solely focusing on software vulnerabilities. Considering the war on talent, long-term security requires a regional talent pipeline, to ensure critical infrastructure remains resilient during crises when external support might be restricted.