CIONET

DISCUSSION SUMMARY

THE CYBERSECURITY CONTROL DILEMMA

Business

On July 2, 2024, CIONET and Telenet Business teamed up again for what proved to be another fascinating Leadership Circle. Moderated by Hendrik Deckers, the CIOs and CISOs around the table took a closer look at the delicate balance between user autonomy and organisational safety. This dynamic tension presents a significant dilemma, particularly when managing device control across diverse technologies and environments.

Network segmentation

Developer freedom is at the heart of organisational security. The desired autonomy includes installing software, accessing websites, and using diverse tools that might not comply with the organisation's IT policies. The main security concerns revolve around unrestricted access and autonomy, which can lead to vulnerabilities. Non-standard software, unpatched systems, and accessing potentially malicious websites can open the door to cyberthreats, including malware, phishing attacks, and data breaches.

The road to "solving" the cybersecurity dilemma is paved with trade-offs that must be made in terms of cybersecurity controls, such as software installment policies, website access management, and monitoring and surveillance. A possible approach, discussed during the roundtable, is network segmentation. Not only does network segmentation enhance security control, it also facilitates developer autonomy by letting developers install software and access various resources within their own segments, reducing the risk of introducing vulnerabilities into production networks. The overall network remains secure through controlled interactions between segments.

VPN-centric versus zero trust architecture

However, opting for network segmentation means you have to make a strategic choice between routing all traffic through a VPN and adopting a zero trust architecture. This exercise falls to the CIO or CISO, who must consider the specific needs, existing infrastructure, and security requirements of the organisation.

On the one hand, a VPN-centric approach comes with unified access control, as it provides a centralised point for monitoring and controlling access, making it easier to enforce security policies. Due to the encryption of all traffic, a VPN provides a secure channel over public or untrusted networks and is therefore well-suited to providing secure access to corporate resources for remote employees. But routing all traffic through a VPN can introduce immense latency and reduce overall network performance.

On the other hand, organisations can be reluctant to adopt a zero trust architecture because of its complexity and due to the thorough understanding of the network, components, and workflows it demands. Every single resource and endpoint must be identified, access-controlled, and monitored. Many organisations find value in a hybrid approach, gradually integrating zero trust principles while maintaining existing VPN infrastructure during the transition.

Dedicated workstations

Another solution that is often looked at are dedicated workstations for developers, as they allow organisations to maintain a secure environment while giving developers the freedom to innovate and experiment. There are definitely benefits to this approach, but it also comes with significant cost implications. Companies often avoid using dedicated workstations for developers working in production environments and utilise separate VLANs (virtual local area networks) instead, for several key reasons related to access control, network performance, and testing and production.

SASE

Does Secure Access Service Edge (SASE) offer a potential solution? It certainly aims to address the challenges of modern cybersecurity by providing comprehensive security while maintaining user autonomy and organisational safety. Especially for dispersed remote and hybrid users, it enables an organisation to safely connect them to nearby cloud gateways and a more dynamic and high-performing network that adapts to changing business requirements and an evolving threat landscape.

But there are also challenges attached to this route, which can increase the barrier to investment and prevent organisations from choosing SASE. The complexity of transitioning to a new security model, dependence on internet connectivity, potential vendor lock-in, and compliance concerns are all important factors to weigh up.

AI to the rescue?

Of course, everyone is looking at AI as a possible solution to reconciling user autonomy and organisational safety through advanced threat detection, automated security processes, and predictive analytics. AI systems can not only help with analyzing vast amounts of data in real-time and accurately identifying anomalies and potential threats, they can also help with automating repetitive security tasks like patch management and incident response.

User behaviour analytics (UBA) and adaptive authentication are two of the possible crucial applications that enhance security without hindering user experience. AI can also potentially play a vital role in managing access controls dynamically, ensuring that permissions are granted based on real-time risk assessments and user behaviour.

On the one hand, AI certainly offers a lot of potential as a solution to the cybersecurity control dilemma, but on the other hand, the CIOs and CISOs at the roundtable were careful not to overestimate the potential of the technology. In particular, when it comes to analyzing codes that developers want to add to the pipeline, they point out that airtight use cases are still lacking.

Rik Bobbaers
Tech CISO at ING Global

ING Global: freeing thousands of developers?

ING Global comprises 60.000 people who each have their own workstation. Among them are thousands of developers who of course want to have as much freedom as possible on their devices to express their creativity and deliver cutting edge technology to our customers. In terms of ICT management and cybersecurity, this means granting admin-like rights. Everyone is convinced this leads to more creativity and enhanced performance. Developers who want to experiment use platforms such as GitHub to develop their source code. The risks are twofold: the possibility that application codes (possibly with secrets in them) will leak on the one hand, and the possibility of downloading and introducing dangerous code on the other hand.

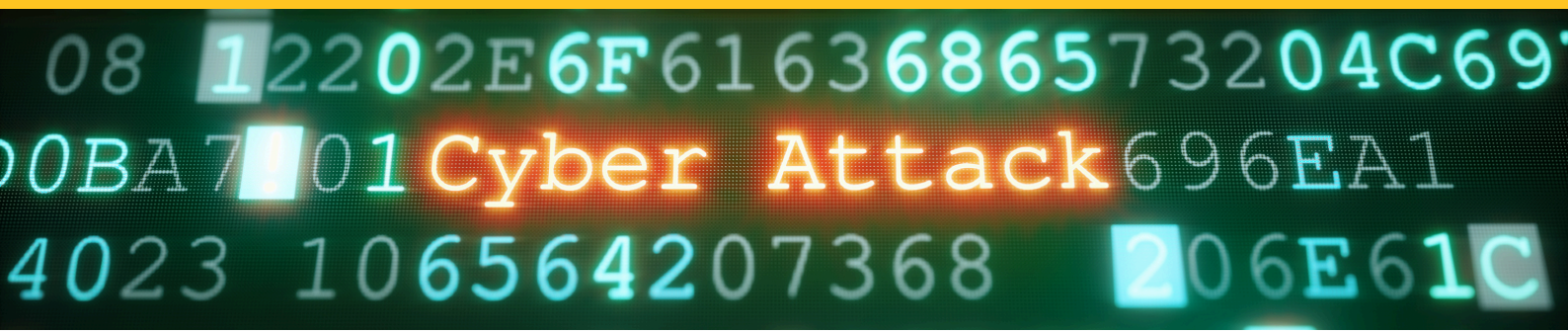
This possibly leads to an increase in your vulnerability and exposure as an organisation, especially when staff members don't only work over the corporate network but also from home or even over public networks. "One of our biggest struggles is exactly that: giving our people, especially developers, the freedom they want while at the same time safeguarding our cybersecurity as much as possible," says Rik Bobbaers, Tech CISO at ING Global.

Zero trust

A fast-emerging paradigm in this context is, of course, zero trust. But when we translate this into a practical context, it becomes clear just as quickly that imposing zero trust has a far-reaching impact on the freedom of movement of employees and the possibilities for developers. Zero trust principles do not solve the problem of accidentally introducing bad code into the pipeline. "That's why we try to emphasise prevention as much as possible." But here too, points of discussion arise. "One of them being the issue of granting developers admin rights for the shortest time possible to limit exposure in time and performing patching of vulnerabilities afterwards each time."

Prevention and detection: a matter of resources

"Prevention is always better than detection," says Rik firmly. But how far can you go in terms of prevention and detection, knowing that a 100% prevention rate is not achievable? In that respect, you can see the cybersecurity control dilemma as a resource allocation issue. At a certain point you have to dare to say that prevention has gone far enough and make the decision not to invest any more in it, but to instead move towards detection.



The current age of cybersecurity

Cybersecurity and regulations naturally go hand in hand, and while everyone agrees that the latter are absolutely necessary, there is some concern about feasibility and possible downsides. The budgetary aspect is one thing, but without the necessary awareness, any attempt at regulation is lost before you even begin. That's exactly where the shoe threatens to pinch. Because of the many laws and regulations that are heading our way, security fatigue is entirely possible. You could compare this to the safety announcement on a plane before take-off — although it's well-intentioned, most of us have become deaf to it.

Everyone agrees that the question is not whether your organisation will be hit by a cyberattack, but when. The key will be to identify the attack as quickly as possible and respond swiftly. Negligence and continuing as though nothing has changed, with a lack of patching and checks on backups, pose a threat to every organisation.

We already referred to the potential role AI could play or is already playing in navigating the changing security landscape. But using AI for development purposes also requires awareness because you want to avoid people developing things using AI if they are not able to explain or comprehend the code behind them. Full documentation of AI will ultimately become necessary, although the European AI act will provide for this.

Sander Wouters
Team Manager & Cyber Catalyst at Telenet

Telenet: the challenges of a tribe-based operating model

Quite recently, Telenet transformed from a traditional, hierarchically structured organisation into a flexible and agile one, with smaller, autonomous teams where possible. The goal was to achieve faster time-to-market, respond better to customer feedback, and create more motivated employees. The organisational model comprises different business circles and tribes, each with end-to-end responsibility for a wide range of operations, including cybersecurity.

“We are convinced that this operational model offers benefits in terms of agility and flexibility, but it also presents certain challenges,” says Sander Wouters, Team Manager and Cyber Catalyst at Telenet. “Friction occurs in some parts of the organisation, as each circle has different interactions, a different security landscape, and a different risk profile. In addition, important questions arise, such as how do you create responsibility in each circle, how and to what extent do you keep control, and how do you keep track of everything?”

Confederalism

These challenges resulted in Telenet developing its own way of working. When you consider Belgian politics, there are quite a few similarities with what might be called a confederate state model: a partnership of various (independent) circles that choose to tackle only a few matters jointly to achieve organisational benefits. “In practice, this means that our central IT department only provides the services that each circle needs. The exercise is to determine how much control they retain.”

Policies and reporting requirements were developed for this purpose. “If cybersecurity were a house, the cybersecurity department constructs the shell, such as the security operation center and the endpoint detection response, because of the benefits of pooling, but this is implemented locally by each circle. The tooling is passed centrally, because we naturally want to keep our finger on the pulse and create economies of scale whenever possible.”

Spotify model

Telenet sought to install a people-driven approach that emphasises the importance of culture and network to increase innovation and productivity by focusing on autonomy, communication, accountability, and quality, known as the Spotify model. "Examples of matters that belong exclusively to the circles are maturity checks, which help to determine how much responsibility and ownership to grant, as well as the fine-tuning of CISD approaches (Critical Incident Stress Debriefing)." Dashboarding, in essence the (real-time) reporting on all cybersecurity parameters, is also an important responsibility of the circles. "Consolidation will be necessary here in the context of NIS2, but the responsibilities of the circles will remain intact."

In summary

Once again, the roundtable provided us with lots of useful knowledge and insights and left us ready to confront the cybersecurity control dilemma within our own organisations:

- In certain organisations, the strong desire for freedom and creative opportunities causes a difficult balancing act between the granting of admin rights and maintaining cybersecurity.
- Zero trust is often looked at as a possible answer but it is not always a complete solution and sometimes does more harm than good to the organisation as a whole.
- A prevention rate of 100% is wishful thinking, which raises the question: at what point have you invested enough in prevention and when does it become time to focus on detection?
- End-to-end responsibly for cybersecurity might have its advantages in terms of agility and flexibility, but it presents new challenges as well.
- The current era of cybersecurity involves strong legislation and regulation. Although this is necessary, there are also downsides: security fatigue threatens to occur.
- The use of AI will undoubtedly have a positive impact on cybersecurity and threat detection, although the real strong use cases are not yet widespread today, but we should also not be blind to possible downsides, such as understanding the mechanisms behind it.

About CIONET

CIONET is the leading community of more than 10,000 digital leaders in 20+ countries across Europe, Asia, and the Americas. Through this global presence CIONET orchestrates peer-to-peer interactions focused on the most important business and technology issues of the day. CIONET members join over a thousand international and regional live and virtual events annually, ranging from roundtables, programs for peer-to-peer exchange of expertise, community networking events, to large international gatherings. Its members testify that CIONET is an impartial and value adding platform that helps them use the wisdom of the (IT) crowd, to acquire expertise, advance their professional development, analyse and solve IT issues, and accelerate beneficial outcomes within their organisation.

cionet.com

About Telenet Business

Telenet Business, part of the Telenet Group, is so much more than connectivity. As a managed service provider they help Belgian companies turn their digital challenges into business opportunities. They support and unburden, large and medium-sized enterprises as well as small entrepreneurs. You can count on them for high-quality managed services such as internet, telephony, solutions to collaborate and communicate digitally, cybersecurity and smart displays.

telenet.be/business