CIONET

DISCUSSION SUMMARY

OUTSOURCING CYBERSECURITY

Business

On October 19, 2023, the Telenet Business Leadership Circle, organized and moderated by Hendrik Deckers of CIONET at the invitation of Telenet Business, took a deeper look at the important topic of outsourcing enterprise security. A diverse panel of CIOs and CISOs shared insights into the growing complexity of organizations, the constant challenge to stay ahead of cyberthreats, and the scarcity of available talent. These factors are driving organizations toward outsourcing their cybersecurity to achieve better protection.

Outsourcing cybersecurity has never been as high on the agenda of companies and organizations than it is today. And that's a curious situation when you think about it. Why would you outsource something as vital as cybersecurity? That's why CIOs and CISOs gathered round the table to share their experience, insights, and thoughts on why, what, and how to outsource cybersecurity. They also explored what would be the right timing and where to find the best partners for these tasks.

Outsourcing cybersecurity has become a standard practice for tech-focused businesses, due to several factors. First of all, our CIOs and CISOs agreed that the attack surface is growing, perhaps even exponentially. As technology advances, so do the tactics employed by malicious actors. This has made it increasingly difficult for organizations to keep up with the growing complexity of security threats and to find the necessary talent to defend against them. As a result, more and more organizations are turning to managed security service providers (MSSPs) to bolster their enterprise security.

This is especially true in the Belgian context, where it's becoming increasingly difficult to attract specialized profiles and MSSPs are becoming ever more vital to helping organizations protect their assets and sensitive information. They allow organizations to benefit from the knowledge and experience of security professionals without the hassle of building and maintaining an in-house security team. While the growing attack surface and complexity of cyberattacks and the scarcity of available talent are two key drivers of the move to outsourcing, ongoing compliance challenges and budget are also important factors.

Partnering up

With the outsourcing of (elements of) cybersecurity becoming ever more common, an obvious challenge is finding the right MSSP. This choice is crucial to the security of any organization. While cost might be the most decisive factor, there are many others to consider when choosing an MSSP. Suppliers find themselves in the position where they can afford to pick and choose clients and they are wary of staff augmentation. So it’s important to know your MSSP and be clear about what you – as a client – can offer them and how the partnership fits into their growth strategy. The expertise and reputation of the MSSP is important as well. Ideally it should have a proven track record of success and a strong reputation in your industry.

Organizations need to do their homework to find the best MSSP partner for them. This includes putting metrics in place against which they can judge the potential partner, both during the selection process and the evaluation process after the partnership is up and running. Ideally, this should also include unannounced audits. In this context, for example, a Reddin test offers a range of quantifiable, diagnostic instruments to measure the performance of both individual managers and team performance over a period of time.

Choose wisely

If we broaden this out, CIOs or CISOs do more than play a pivotal role in choosing the right MSSP partner. It’s just as important that they have a say in the choice of software solutions, because this can affect the company’s security landscape in the future.
Some companies are forced to nearshore because of the scarcity of skilled profiles, for specific technologies such as AWS or SAP, for example. So when it comes to choosing a technology or software solution, as a CIO or CISO, it doesn’t hurt to be friendly with the CFO, because the adoption rate of a solution can alter the maneuverability for future decisions and impact the company’s security landscape. As it is often the case, there can be a trade-off between cost in the long run and the short-term contract price.
This brings us back to the previous point of how challenging it is to attract specialized profiles, especially in Belgium, where it’s nearly impossible to find specialists to cover the entire cybersecurity landscape. For companies, it comes down to joining the right ecosystems for their technology and software solutions, as this will impact future options. Microsoft-based companies benefit from an ecosystem that offers nearly everything, while the options for non-Microsoft companies are more limited. So, once again, choose wisely and nudge your CFO in the right direction.

Thomas Colyn
CISO
DPG Media

Cybersecurity as part of an acquisition strategy

It's hard to think of companies that attract more attention than media outlets. This is literally true for DPG Media, which has more than 80 brands operating in Belgium and the Netherlands.
Thomas Colyn, CISO at DPG Media since 2020, gave an interesting insight into the group's cybersecurity landscape. "Media companies are a primary target for cybercriminals," says Thomas. "Since 2017 and 2018 in particular, our attack surface has increased significantly." The group's acquisition strategy is one of the reasons for this, not only leading to an increased attack surface, but also adding to the complexity of cybersecurity tools and increasing the need for flexibility to facilitate integrations.

"If you look at the number of tools we have in place and the 2 terabytes of security logs we generate every day, it goes without saying that we have a lot of in-house expertise around cybersecurity." The cybersecurity strategy of DPG Media is mainly one of mitigation and reaction. "The challenge is to combine all the tools we have in place to find that one needle in the haystack. But for a group that uses technology as much as ours, outsourcing is indispensable."

Generative AI and behavior-based malware

A company's security landscape isn't evolving only through the move to outsourcing; the increasing complexity of cyberthreats is also having an impact on the situation and is increasing the attack surface. One threat is behavior-based malware, a form of malware that is more difficult to detect with conventional solutions as it operates from a deeply hidden position within a company's systems. It can change code and appearance and deploys evasion techniques, such as code obfuscation and anti-analysis measures, to avoid detection by security solutions.

The evolution of generative AI and behaviour-based malware go hand in hand. That's why many specialists point to the disruptive potential of generative AI for the whole cybersecurity landscape, as it enables cybercriminals to develop tailor-made malware and continues to lower the threshold in this regard. Thanks to AI, cybercriminals only need a vulnerability profile of their target to enter into the generative coding model, together with the variables. The output is a tailor-made, behaviour-based malware model that demands no coding from the cybercriminals themselves.

Arms race

Organizations will need to adapt and react to this disrupted cybersecurity landscape. The answer will involve more complex mitigation and even more specialization. But again, specialized skills are scarcer than ever. So it's predicted that organizations will evolve toward a cooperative model wherein they bundle their cyber-capabilities — a united front, if you will.

The weaponization against AI-based cyberattacks will undoubtedly involve investing in tools and security systems, for example security solutions that employ behavioural analysis to detect and prevent behaviour-based malware, paired with the implementation of strong network security measures to filter out malicious traffic and prevent malware from reaching your systems. Based on the principle that security is only as strong as its weakest link, educating users about the risks of downloading untrusted software or clicking on suspicious links remains crucial, paired with an effective incident response plan.

But on the brighter side, the evolution of AI also offers more tools to strike back. For example, machine learning models can be trained to detect patterns and behaviours associated with malware. These models can adapt and improve over time as they encounter new threats, making them a valuable tool for behaviour-based malware detection. AI also offers more heuristic analysis capabilities, such as identifying potentially malicious behaviours or patterns within software. It focuses on identifying actions that are indicative of malicious intent, such as unauthorized system changes, data exfiltration, or privilege escalation.

Robin Heylen
Team Manager of the Cybersecurity Operations Center (SOC) and Cybersecurity Incident Response Team (CSIRT)
Telenet

Outsourcing and business continuity

For Telenet, one of Belgium's major telcos, business continuity has a very direct impact on customer satisfaction and loyalty. Each minute without service access due to a cybersecurity incident results in customers departing. "That's why our cybersecurity strategy focuses on business continuity and recovery, as well as event and incident management," says Robin Heylen, Team Manager of the Cybersecurity Operations Center (SOC) and Cybersecurity Incident Response Team (CSIRT) at Telenet.

When it comes to that last issue, the options for outsourcing are limited. "We divide events and incidents according to certain gradations, with level 1 or 1.5 incidents allowing for outsourcing. However, level 2 and 3 incidents call for in-house action, as they don't happen often and require our very specific expertise."

The outsourcing of cybersecurity also depends on whether the company is under attack or not. "Our MSSP mainly supports our business during peacetime and takes care of the forensics part. During a malware attack, for example, our own cybersecurity experts are in control, and we rely on our in-house capabilities. No one can leave the ship in that situation."

Conclusion

The complexity of organizations, escalating cyberthreats, and the talent shortage have led to outsourcing of cybersecurity becoming almost standard practice today, especially for tech-focused companies. This strategic shift is driven by the need to keep pace with the ever-expanding attack surface and evolving threat landscape. Choosing the right MSSP is critical, and organizations should conduct thorough research and establish solid evaluation metrics. The expertise and reputation of the MSSP, as well as its alignment with an organization's technology and software solutions, are crucial factors to consider. CIOs and CISOs not only influence MSSP selection but also play a pivotal role in choosing the software solutions that can impact a company's security landscape.

The evolution of cybersecurity threats, including behaviour-based malware and the rise of generative AI, presents new challenges. These developments demand continuous adaptation and specialization in the security landscape. Cooperative models and investment in advanced security tools and systems are expected to counter AI-based cyberattacks. On the positive side, AI also offers opportunities for cybersecurity.

CIONET

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

Business

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

Copyright 2023

CIONET

DISCUSSION SUMMARY

OUTSOURCING CYBERSECURITY

Business