Digital Trend #4: Cybersecurity

Digital Trends - Cybersecurity

In this article, we will look at what we consider to be the top ten current Cybersecurity threats, and how we think they should be countered.

We also consider the pros and cons of different security sourcing strategies: in-house, outsourcing, or a combination of the two. We also talk about advantages of adopting a truly 'zero-trust' approach to IT security.

Based upon our experiences with other clients, we have also compiled what we foresee may be the potential security challenges at Heineken and offer up some possible solution directions to address these.

The 'unfortunate' trend

We all do it every day, dozens, if not even hundreds of times, in our private and business lives: we login with our personal credentials to enjoy the benefits of digital services. We almost do it automatically. We access our preferable services and data – our social media accounts, our preferred airline accounts, our hotel booking apps, and our online banking and insurance accounts – via our digital devices. We also access our business applications and business data throughout our workday, via our business smartphones, business tablets and business laptops. Sometimes bring-your-own-device concepts make differentiation between business and private usage blurred.

What if you could no longer access all those digital services? If someone had taken control of your account? What would then your day be like? Would your business still operate? Cybersecurity risk is a real threat to any organisation's business continuity in today's digitised world. The question is no longer if an organisation will be hacked, but when. So better be thoroughly prepared.

You are rightly calling it out – cybersecurity is indeed an 'unfortunate' trend, which affects everyone and everybody - in both private and professional lives. A whole industry branch has developed around cybersecurity over the last few decades and is growing, with the goal to fight the ever-changing cyber risk landscape leaving people and organisations vulnerable and exposed to cyber threats. A cyber risk mitigation strategy based on zero trust models is needed for every organisation. On Heineken's journey to connect the best-connected brewer, cybersecurity in all areas – IT, IoT and OT – is inevitable.

EVIDEN

At Atos, under our brand **Eviden** and our Big Data & Security (BDS) business line, we have a particular focus on Digital Security and beyond. Together, Atos and Eviden offer cyber

© Atos 2024 All rights reserved

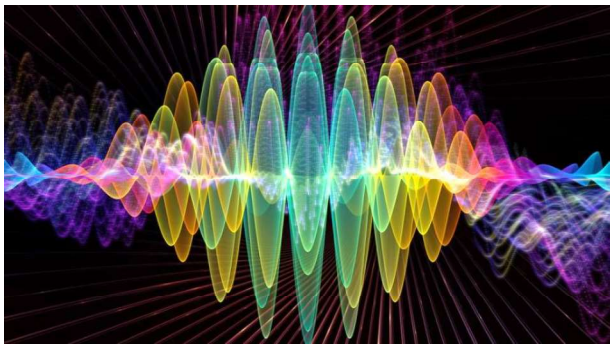
Commercial in Confidence

security services and products as well as capabilities to design, implement and support mission critical systems to a large number of private and public institutions. We are proud to say we are the global #1 supplier of managed security services by revenue (Gartner) – a business that generates €1,4 Bn of revenue through our 9,000 skilled engineers and experts – underlying just how important this aspect of IT services is for everyone.

Top 10 Cybersecurity threats today

As cybercrime continues to evolve and escalate, we have identified the most critical threats that organisations need to prepare for today. 2023-24 was a turbulent time for cybersecurity, with several high-profile incidents that caused significant disruption, damage, and loss. According to Cybersecurity Ventures, cybercrime is expected to cost the world $10.5 trillion annually by 2025, up from $6 trillion in 2021. To help you stay ahead of the curve and protect Heineken from these growing risks, we have compiled the top 10 cybersecurity threats that you need to watch out for currently. We also provide some insights into how these threats will evolve and what you can do to mitigate them.

Threat 1: Quantum disrupting security



Quantum computing is a revolutionary technology that promises to solve complex mathematical problems faster than traditional computers. However, it also poses a serious threat to the security of current asymmetric encryption standards, which rely on mathematical problems that are hard to crack by conventional means. Quantum computers may disrupt the security of these encryption schemes in minutes, rendering them unsecure and exposing sensitive data and communications to hackers.

Quantum computing will become more accessible and powerful, as major players like IBM, Google, Microsoft, and Amazon invest heavily in developing and offering quantum services. According to the 2023 Quantum Threat Timeline report (Global Risk Institute, 2023), we can confidently consider that quantum computers will reach maturity by 2037. Given that nearly all aspects of information systems like networking devices, servers and endpoints, smart devices, operating systems, applications, objects, and IoT and OT will also need to move, this timeline is very short for organisations to prepare, prioritise and execute the complete migration of their digital environment and digital business processes. Also, malicious actors are leveraging now the "harvest now, decrypt later" attack blueprint. Indeed, unfriendly and motivated actors already harvest data in significant volumes. Their goal isn't to know what they harvest, rather betting on the fact of a valuable/critical data be in that set, which they'll soon be able to easily decrypt with quantum computers.

Our prediction: To defend against quantum threats, organisations will need to adopt quantum-resistant encryption algorithms and protocols, such as lattice-based cryptography, and hash-based cryptography. They will also need to monitor the quantum computing landscape and keep up with the latest developments and best practices. The National Institute of Standards and Technology (NIST) released its final post-quantum cryptography (PQC) standards that organisations should adopt. Hence organisations must ask themselves, "To what extent are we ready to implement them?" And the necessary self-audit doesn't stop here.

Firstly, CISOs should identify funding for their post-quantum cryptography migration project from the Board or CFO. Then to evaluate how easy the implementation could go; organisations must build and manage their crypto inventory, so they know where to act. It includes identifying what sensitive and critical data the organisation has, and for all data what security protocols and/or cryptographic algorithm was used and why. Such an inventory should also be used to ensure that all sensitive data are re-encrypted, and all sensitive contracts re-signed with post-quantum cryptography (PQC) and to avoid missing any of their occurrences or copies. After all, a single forgotten RSA encapsulated key could be a major vulnerability. Organisations must also analyse their most critical business processes, so they know where to start in order of priority. Indeed, PQC migration will be a mastodon of a transformation project, meaning critical choices and decisions must be made on whether to migrate highly sensitive data, or take the risk of it being harvested and decrypted. Besides, in terms of supply chain security, CISOs must contact all their software and hardware providers to ask them if and/or when they plan

© Atos 2024 All rights reserved

to deliver a PQC-ready version of their solution. And the list goes on, which highly incentivises organisations to reach for the help of key cybersecurity players like Eviden to properly kick-off their PQC migration.

Consequently, we predict that organisations who do not start acting on their PQC migration in 2024 will be far too late to even be quantum-proof when quantum computers reach maturity. Gear up and start in 2024 to get to PQC readiness on time.

Threat 2: AI-powered attacks

Artificial Intelligence (AI) is another emerging technology that has both positive and negative implications for cybersecurity. On one hand, AI can help improve security by automating tasks, detecting anomalies, and enhancing response capabilities. On the other hand, it can also be used by attackers to create more sophisticated and stealthy attacks, such as deepfakes, adversarial AI, and autonomous bots. The spread of GenAI tools has also enhanced malicious Large Language Models (LLMs), enhancing attackers' capabilities to craft compelling phishing or faster identify attack vectors for released Common Vulnerabilities and Exposures (CVEs). Worm GPT indeed, illustrates the dark side of LLMs when commissioned to hackers' interests.

APT-29 Group is known for using AI to automate tasks and increase the efficiency of their attacks, making them a more sophisticated threat. Okta, an identity and access management company, was breached in 2023 by the hacker group Lapsus$. The hackers used AI to automate their attacks, making them more efficient and difficult to stop.

Our prediction: AI-powered attacks will become more prevalent and diverse as attackers leverage AI tools and techniques to automate and optimise their campaigns. For example, we expect to see more deepfake attacks that can manipulate audio and video to impersonate individuals or spread misinformation, adversarial AI attacks that can fool machine learning models and evade security systems, GenAI prompt injections, and autonomous bots that can perform reconnaissance, exploitation, and propagation without human intervention. To counter AI-powered attacks, organisations will need to invest in AI-based cybersecurity solutions, like Eviden's AI-driven managed detection and response. They will also need to implement robust security controls and policies, such as data protection and identity and access management to counter these threats.

Threat 3: Ransomware

Ransomware is a type of malware that encrypts the victim's data and demands a ransom for the decryption key. It has been one of the most prevalent and profitable cyber threats for years, affecting various sectors and organisations of all sizes. It has also become more sophisticated and aggressive as attackers use more advanced encryption algorithms, target more critical systems and data, and employ more extortion tactics.

The notorious ransomware group BlackCat has filed a complaint with the U.S. Securities and Exchange Commission (SEC) against MeridianLink, a publicly traded software company, for failing to disclose a ransomware attack and not responding to their ransom demands. Russian hackers launched a ransomware attack against a Canadian government service provider, compromising the personal data of 1.4 million people in Alberta. The organisation reportedly paid the ransom, claiming minimal data loss.

Our prediction: Ransomware will remain one of the top threats as attackers innovate and diversify their ransomware operations. For example, we expect to see more ransomware-as-a-service (RaaS) platforms, where attackers offer ransomware tools and services to other criminals for a fee or a share of the profits. We also expect to see more triple or quadruple extortion schemes, where attackers not only encrypt the data, but also steal it and threaten to expose it or sell it, and finally shut down public-facing servers with a Distributed Denial of Service (DDoS) attack, unless the ransom is paid. We also expect to see more ransomware gangs, where attackers collaborate and coordinate their attacks to increase their chances of success and payout. To combat ransomware, organisations will need to adopt a comprehensive ransomware prevention, detection, response, and recovery strategy. They

© Atos 2024 All rights reserved

Commercial in Confidence

will also need to follow ransomware protection best practices, such as patching systems, limiting their network exposure, and educating their users.

Threat 4: Cloud computing

Many companies are now using Cloud computing for the delivery of their servers, storage, databases, and software over the Internet. Cloud computing offers scalability, flexibility, and cost-efficiency. However, cloud computing also poses new security challenges, such as data security, access control, and compliance.

A misconfigured Microsoft Azure Blob Storage account exposed 2.4 TB of data belonging to an unnamed customer, including sensitive information such as personal identifiable information A misconfigured Samsung cloud storage bucket exposed the personal identifiable information (PII) of over 100,000 customers, including names, phone numbers, and email addresses.

Our prediction: Cloud threats will become more complex and sophisticated as attackers exploit the vulnerabilities and gaps of the cloud environment and infrastructure. For example, we expect to see more attacks on cloud data, such as data breaches, data leaks, and data tampering that can expose or alter sensitive data stored or processed in the cloud. We also expect to see a rise in attacks on cloud access, such as account takeover, credential theft, and privilege escalation, that can abuse or misuse the access rights and permissions of cloud users and administrators. We also anticipate more attacks on cloud compliance, such as regulatory violations, contractual breaches, and audit failures that can result in fines, penalties, and lawsuits. To protect cloud services, organisations will need to adopt cloud-specific security measures, such as encryption, authentication, and backup. They should also implement cloud security solutions, such as cloud access security brokers (CASBs), cloud security posture management (CSPM), and cloud workload protection platforms (CWPPs), to protect their cloud environments or may opt for end-to-end cloud-managed security solutions like the one offered by Eviden.

Adhering to cloud security standards and frameworks, such as ISO 27017, CSA CCM, and NIST SP 800-144 will not only help with compliance but also improve security posture.

Threat 5: Decoding 5G risks

5G is the fifth generation of mobile network technology that offers faster speed, lower latency, and higher capacity than previous generations. 5G enables new applications and use cases, such as the Internet of Things (IoT), smart cities, autonomous vehicles, and telemedicine. However, it is not secure by default – 5G security protocols are in the hands of the customer and need to be configured and deployed with security risks in mind.

Overall, 5G has increased the attack surface and complexity of the mobile ecosystem, as more devices, networks, and services are connected and exposed to cyber risks. A 2022 study by GlobalData, commissioned by Nokia, found that nearly three-quarters of 5G network operators surveyed had experienced up to six cyberattacks or security breaches in the past year. These incidents resulted in network downtime, customer data leaks, financial losses, and reputational damage. Researchers discovered multiple vulnerabilities in 5G core networks, including the Next Generation Core (NGC) and the evolved Packet Data Serving Node (EPDN), that could be exploited to disrupt network operations or intercept sensitive data.

Our prediction: 5G threats will become more common and severe as attackers exploit the vulnerabilities and opportunities of the 5G infrastructure and environment. For example, we expect to see more attacks on 5G devices, such as smartphones, tablets, wearables, and IoT devices, that can compromise their functionality, data, and privacy. There may be more attacks on 5G networks, such as base stations, edge servers, and cloud platforms, that can disrupt their availability, performance, and integrity. We also expect to see more attacks on 5G services, such as streaming, gaming, and e-commerce, that can affect their quality, reliability, and security. To defend against 5G threats, organisations will need to adopt 5G-specific

© Atos 2024 All rights reserved

Commercial in Confidence

security solutions like the one offered by Eviden. They will also need to implement 5G security standards and frameworks, such as 3GPP, GSMA, and NIST.

Threat 6: Supply chain attacks

Supply chain attacks target the suppliers or partners of an organisation rather than the organisation itself. By compromising the supply chain, attackers can gain access to the organisation's systems, data, and customers, and cause more damage and impact.

Supply chain attacks have become more frequent and sophisticated, as attackers exploit the increasing complexity and interdependency of the supply chain ecosystem.

A supply chain attack targeting the MOVEit file transfer solution compromised several MOVEit customers, including major US government agencies. The attackers gained access to MOVEit source code and injected malicious code into the software, allowing them to intercept and modify files transferred through the system. A supply chain attack targeting Applied Materials, a major supplier of semiconductor manufacturing equipment, disrupted the company's operations and caused delays in chip production. The attackers compromised a third-party software provider used by Applied Materials and injected malicious code into its software.

Our prediction: Supply chain attacks will continue to be a major threat, as attackers target more suppliers and partners, and use more advanced techniques and tactics. For example, we expect to see more attacks on software supply chains, such as software development, distribution, and update processes that can inject malicious code or backdoors into software products and services. We may also see more attacks on hardware supply chains, such as chip design, manufacturing, and delivery processes, that can implant malicious components or firmware into hardware devices and systems. We can also anticipate more attacks on service supply chains, such as cloud, managed, and professional services that can compromise the security and quality of the service delivery and outcome. To prevent supply chain attacks, organisations will need to enhance their supply chain security by conducting regular risk assessments, enforcing security standards, and implementing security monitoring and incident response. They will also need to establish supply chain security policies and procedures, such as supplier vetting, contract review, and incident response.

Threat 7: Insider threats

Insider threats originate from within the organisation, either by current or former employees, contractors, or partners, who have legitimate access to the organisation's systems, data, and resources. These types of threats can be either malicious or accidental, depending on the intent and behaviour of the insider. They can cause significant damage and loss as insiders can bypass security controls, exploit privileged information, and evade detection.

Two former Tesla employees leaked thousands of personal records to a German news outlet, including the names, addresses, and Social Security numbers of current and former Tesla employees. The employees were reportedly motivated by frustration with the company's management.

An IT worker in the United Kingdom was jailed for impersonating a ransomware gang and extorting his employer. The worker sent a threatening email to the company demanding a ransom payment of £50,000, warning that if the company did not pay, he would delete all of their data. The worker was caught after the company reported the incident to the police.

Our prediction: Insider threats will become more challenging and costly, as organisations face more internal and external factors that can influence and trigger insider actions. For example, we expect to see more insider threats driven by economic hardship, social unrest, political polarisation, and personal grievances that can motivate insiders to sabotage, steal, or leak sensitive data or assets. We can also expect more insider threats enabled by remote work, cloud migration, and digital transformation that can create more opportunities and avenues for insiders to access and compromise critical systems and data.

© Atos 2024 All rights reserved

Commercial in Confidence

To deter insider threats, organisations will need to adopt a holistic insider threat management approach, that includes monitoring, training, and auditing, and implementing insider threat detection and prevention solutions, such as user and entity behaviour analytics (UEBA), data loss prevention (DLP), and privileged access management (PAM) to protect their assets from insider threats. They will also need to implement insider threat policies and programs, such as background checks, access control, and awareness training.

Threat 8: Phishing for vulnerabilities

Phishing is a type of social engineering attack that uses fraudulent emails, messages, or websites to trick the victim into revealing sensitive information, clicking malicious links, or downloading malicious files. While it is one of the oldest and most common cyber threats as it is easy to execute and effective in exploiting human vulnerabilities, phishing is also a gateway to other attacks, such as malware, ransomware, and account takeover.

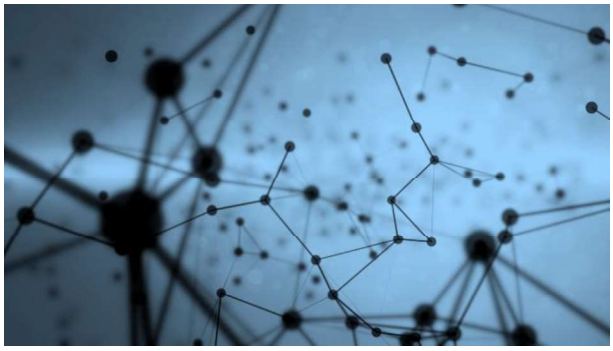
A South Korean government-affiliated institution was reportedly the victim of a phishing scam that resulted in the loss of 175 million won (approximately $131,000). This incident is said to be the first phishing attack against a South Korean government public organisation.

Hackers used an SMS phishing attack to target Activision employees, gaining access to their email addresses, cell phone numbers, salaries, and work locations. The attack was reportedly not detected by Activision until February 2023, despite occurring in December 2022.

Our prediction: Phishing will continue to be a widespread and persistent threat as attackers refine and diversify their phishing techniques and tactics. For example, we expect to see more spear phishing and whaling attacks, where attackers target specific individuals or organisations with personalised and convincing messages. We also expect to see more vishing and smishing attacks, where attackers use voice calls – including AI-generated voices use – or text messages to deliver their phishing content. In the future, more phishing attacks will leverage current events and trends, such as Gen-AI, the metaverse, and the Olympics to increase their relevance and appeal.

To prevent phishing, organisations will need to adopt phishing prevention solutions such as secure web gateway (SWG), secure email gateway (SEG), and phishing simulations. They will also need to educate their users on how to spot and avoid phishing, such as checking the sender, the content, and the URL of the message or website.

Threat 9: Unravelling IoT



The Internet of Things (IoT) is a term that describes the network of physical devices, such as sensors, cameras, smart appliances, and wearables, that are connected to the Internet and can collect and exchange data. This wide spectrum offers many benefits and opportunities, such as improving efficiency, convenience, and innovation. However, the IoT also introduces new security risks, such as data privacy, device security, and network security.

Cybersecurity firm Mandiant warned of a new ransomware strain that specifically targets IoT devices. The ransomware, known as 'Mallox,' encrypts files on infected devices and demands a ransom payment in exchange for the decryption key.

Hackers exploited a flaw in an industrial control system to cause widespread power outages in several countries. The attack highlighted the growing threat of cyberattacks against critical infrastructure.

Our prediction: IoT threats will increase in number and impact as more IoT devices are deployed and used in various domains and scenarios. For example, we expect to see more attacks on consumer IoT devices, such as smart TVs, smart speakers, and smartwatches that can compromise their functionality, data, and privacy. We also expect to see more attacks on industrial IoT devices, such as sensors, controllers, and actuators that can disrupt their operation, performance, and safety. There will be a rise in the attacks on healthcare IoT devices, such as pacemakers, insulin pumps, and thermometers that can endanger their

© Atos 2024 All rights reserved

reliability, accuracy, and therefore people's health and safety.

Organisations will need to implement IoT-specific security measures to secure IoT devices. This includes encryption, authentication, and patching, and adopting IoT and IT-integrated security solutions — IoT security gateways and purpose-built platforms — to protect their IoT devices and networks. They will also need to follow IoT security best practices, such as updating their firmware, changing their default passwords, and isolating their IoT networks.

Threat 10: The Metaverse

The metaverse is a term that describes a virtual reality environment where people can interact with each other and digital content in immersive and realistic ways. Now, the metaverse is expected to become the next frontier of the internet as more platforms, applications, and services enable users to create, explore, and share virtual experiences. However, the metaverse also introduces new security challenges, such as data privacy, identity theft, and cyberattacks.

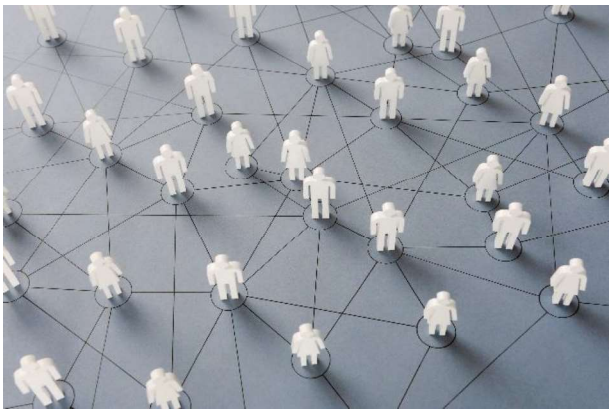
A decentralised finance (DeFi) protocol called Beanstalk Farms was hacked, resulting in the theft of $180 million worth of cryptocurrency. The attackers exploited a flash loan attack to steal the funds. A group of researchers also discovered a new type of malware that can infect VR headsets. The malware is designed to steal users' personal information, such as their credit card numbers and passwords.

Our prediction: The metaverse will attract more users and businesses as well as more hackers and scammers. We expect to see more metaverse threats such as data breaches, account hijacking, phishing, malware, and ransomware. For example, attackers could steal personal and financial information from metaverse users, compromise their accounts and avatars, trick them into clicking malicious links or downloading malicious files, infect their devices and networks with malware, encrypt their digital assets, and demand a ransom.

To protect themselves from metaverse threats, organisations will need to develop metaverse-specific security policies, practices, and tools to protect their users, assets, and infrastructure from metaverse threats. They will also need to follow metaverse security best practices like using strong passwords, enabling multi-factor authentication, verifying the source and content of messages and files, and backing up their data and assets.

In-house vs. outsourcing – or a combination of both?

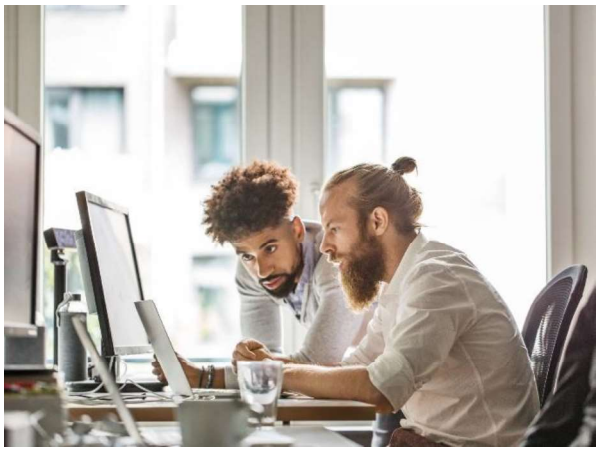
In order to preserve critical systems and sensitive information of our customers, a full-scope, end-to-end trust, business continuity and resilience approach is needed. Organisations must combine logical and physical protection to deliver safety and confidentiality where it matters most.



Today, the world is more interconnected and interdependent than ever before. Enterprises exchange increasing amounts of digital data and their employees are becoming ever-more mobile. Society is asking large organisations to prove they can be trusted with our data, and to demonstrate transparency when aligning with industry regulations. Hence, enterprises have to adapt, to demonstrate compliance without increasing costs and to open their networks in a controlled way. Boundaries are a thing of the past, and so as a consequence, without appropriate risk management, businesses may become more vulnerable. Eviden responds to the new challenges of mobile and "boundary-less business" with a full suite of compliance & security solutions for all industries – from risk management and compliance solutions to fully managed cyber security services. In the process of establishing a cybersecurity organisation, the question always arises whether to perform activities in-house, to outsource certain

© Atos 2024 All rights reserved

cybersecurity activities or combine facets of both.



While both in-house cybersecurity operations and the purchase of outsourced managed cybersecurity services have certain advantages, organisations should carefully evaluate the decision for the optimal operating model. There will be different paths leading to a successful cybersecurity environment, depending on organisation's factors such as its size, markets served, cybersecurity vision and strategy, budget, and top management awareness. To decide on inhouse or sourcing or as a third option – a combination of both, the following advantages and disadvantages should be considered:

a. Manage cybersecurity in-house:

Advantages: Direct reporting lines with short reaction times within one organisation; expert know-how in-house with development of own cyber competence centre with company-specific use cases and direct market access to technology vendors.

Disadvantages: High fluctuation of experts combined with skill and resource gaps in the cybersecurity resource market; high costs for experts; increased effort to stay current with technological changes, or choose technology, engineers/experts with narrow competence on certain technology; organisational change fatigue could lead to outdated cybersecurity solutions and increased risk levels.

b. Buy in managed security services:

Advantages: Fully managed security services allow focus on core activities and delegation of operational tasks; it is cost efficient; the nature of its competitive environment leads to cost efficiency and best practice solutions; it allows to get technology evaluations performed by security providers, the delegation of technology choices and handling of security technology vendors; it includes cybersecurity consulting as part of procurement phase and benefits from cybersecurity partnerships when choosing a strategic managed security services provider.

Disadvantages: Only strategic expert know-how in-house; interaction/governance schemes need to be clearly defined and lead to more management effort; the dependency on providers is high; contractual obligations must be well defined to avoid gaps and unclear actions; there is still the need to supervise suppliers; there is little technology choice, as they are often performed by security service suppliers based on their strategic partnerships, time and resources to handle services procurement.

c. Combinations of both - keeping core/overarching cybersecurity functions in-house and sourcing managed security services:

Advantages: Strategic functions in-house allow for ownership of overall architecture and strategy development while maintaining full transparency; this allows for a focus on minimal operational/ engineering know-how, but rather provide and develop management functions needed; in combining strategic management functions with off-the-shelf and industrialised managed security services, an efficient operating model can be maintained; a cybersecurity partnership when choosing a strategic managed security services provider increases innovation thinking and flexibility to keep up with the current threat landscape; the skill shortage problem can be mitigated.

Disadvantages: Increased dependency on the other party for strategic risks; cybersecurity grows into a complex organisation with multiple stakeholders and management layers; this requires clear expectations and detailed contracts to define areas of responsibility while time and resources to handle services procurement cannot be eliminated.

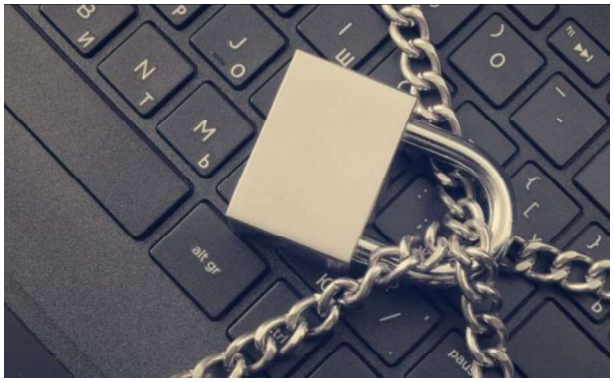
A Zero Trust-based approach

Zero Trust Services secure access to networks, applications, and data by implementing an identity-based approach that combines

© Atos 2024 All rights reserved

Commercial in Confidence

adaptive controls and continuous verification across entire organisation to improve our clients' security postures and to reduce the risk of a breach. The phrase "zero trust" refers to the principle of not providing access to any resources unless a clear business need has been identified, and that the extent of privileges are restricted to only what is absolutely required in order to perform that function or role: "least privilege" access. The shift to remote access and hybrid workplace accelerated the move towards cloud-based services, and a corresponding need to maintain a higher security posture.



Our colleagues in Eviden have designed a Zero Trust Security Umbrella which embraces digital transformation security challenges and accelerates our clients' moves to a data-centric approach, increasing business agility with enhanced data protection. In the process, our learning has been that the main challenges for adopting Zero Trust architectures are:

- Zero Trust architecture doesn't rely on a single solution. It requires the adoption and integration of different technologies.

- Migrating legacy applications and systems to adhere to zero trust principles requires investments in time, resources, and technical knowledge.

We found that implementing a security mesh approach, where different technology parts fit together, effectively utilises the best tools in the best places to eliminate security gaps. This ensures that only securely authenticated users and devices have access (based on the principle of "least privilege") to targeted applications and data. Using as granular as possible access control enforcement ensures the protection of users, applications, and network at every layer, and effectively prevents unauthorised access to data and services.

Zero Trust principles are focusing on shifting from defending not only a single parameter, but to additionally protecting each user, device, and access point.

Using micro-segmentation and security policies applied on identity level, ensures the security of resources no matter where they are located, and no matter as to the changes related to infrastructure. This level of security management requires a long-term commitment and technical expertise. There doesn't appear to be any shortcuts to the establishment of these standards, although they can be simplified once implemented, through the measured use of user profiles aligned to business function roles with common access requirements.

© Atos 2024 All rights reserved

Commercial in Confidence

Potential organisational challenges

Based upon our experiences with other clients, we have compiled what may be the potential security challenges at Heineken and offer up some possible solutions to address these.:

Likely Challenges	Possible Solutions
Creating a trusted collaboration environment • Complexity – how to set up and maintain a set of harmonised multiple security controls in a hybrid and cloud environment. • Ease of use of cybersecurity services – the security services need to be easy to use and maintain.	Developing an end-to-end enterprise security architecture by adopting Zero Trust principles and creating multi-layer defence zones, with a set of effective technical security controls and processes. Carry out risk-based analysis your current security postures, business drivers and ecosystems and mapping them into a Zero Trust Architecture that fits your organisation. Using your Zero Trust Architecture to assess adoption readiness of your People, Process and Technology.
Safeguarding Data and Privacy • Data ownership and encryption – protecting valuable sensitive, data, preserving sovereignty, • Secured data lifecycle management – how to enforce and monitor data security from creation, usage and deletion. • Ethical use of AI – demonstrate how to prevent personal data being used for AI training and big data analytics.	Valuable and sensitive data must be encrypted using your own encryption key under your strict control. This will demonstrate your crown jewel data is safe no matter where it is stored or processed. Effective control of your data lifecycle needs to be understood, documented, enforced, monitored and audited. Data Lost Prevention tooling will enable this. Data Privacy Enhanced Technology (PET) can be set up to ensure private data is anonymised when sharing and being processed .
Protected access to critical data and resources • Hacker is logging in and not breaking in. • Human and Machine Identity Security Management – Demonstrating that you are in control of who has access to what, how to prescribe the access. • Securing privileged access to networks, systems and data.	Identity and Access Management is the core foundation of cybersecurity and building Zero Trust Security. Anything is important to you needs a unique identity, no matter if it is human, machine or a logical entity. Once the unique identity is established, the access between identities can be explicitly specified by prescribing what access privilege is allowed under what conditions.
Monitoring and Response • How to spot any unusual behaviours before it becomes a major security incident • How to apply a set of proactive measures to prevent the cyberattack	Apart from getting various telemetry data sources from your IT infrastructure into a Security information and event management (SIEM), it is vital to determine how to leverage AI and machine learning to analyse the high volume of data, positively identified the security abnormalities. Investing a security orchestration, automation and response (SOAR) will reduce the lead time to respond to security incidents. A well run SOAR capability can also form an effective feedback component when implementing a context-based dynamic access control mechanism often promoted by Zero Trust Security design.

© Atos 2024 All rights reserved

Demonstrate Data Security Regulatory and Compliance • Audit trail and report • Cybersecurity investment vs. Security Posture dashboard in real-time.	With ever-changing security regulations and standards like: GDPR, DORA, NIST, NIS2, it is important to put in governance in place and how to demonstrate compliance is in place. Eviden can provide enterprise security and ROI dashboard to give management real-time visibility of their security posture and return on investment.
Security resources are in high demand • Team capacity is an issue • Need for specialist skills for short periods • Skills keeping pace with market	Apart from building your security function operation with your own resources. It might be useful to supplement your capabilities and capacities during cyberattack and recovery by working with external partners like Eviden.

We encounter many enterprises, which each have varying levels of maturity in their security postures. If we are tasked with improving cybersecurity capabilities, we always tackle the basics first to get companies up to a minimum standard that can be maintained and built upon. In the following section we have highlighted common areas to be aware of when evaluating your own operations. You may well be doing all of these, but sometimes it's still reassuring to get confirmation that what you are doing is aligned to good industry practice. For brevity, we have focused on general considerations, and to align with your Digital Trends, specific aspects associated with Cloud and GenAI.

General Cybersecurity Strategy

Some critical areas Heineken may wish to prioritise in their Cybersecurity strategy:

a. Zero Trust Models

Implementing a Zero Trust approach is essential for mitigating cyber risks. This involves verifying every access request as though it originates from an open network, regardless of where the request comes from.

b. Managed Firewall Services

Ensuring robust firewall management is crucial. This includes managing the technical operation of the firewall and collaborating on functional aspects to maintain security.

c. Next-Generation Firewall Solutions

Upgrading to advanced firewall solutions that in addition to blocking unauthorised access, also offer features for preventing data contamination, and providing integrated security features tailored to Heineken's environment.

d. Cybersecurity in IT, IoT, and OT

A comprehensive cybersecurity strategy should cover all areas, not just IT, including Internet of Things and Operational Technology, to protect the business more broadly against the ever-changing cyber risk landscape.

e. Threat Detection

Improving the detection of emerging threats, such as ransomware, should be a top priority. This involves staying ahead of potential cyberattacks by continuously monitoring and updating security measures. You have already shown a great awareness of this in your article.

f. Gap Analyses

Conducting regular, thorough gap analyses to assess the weaknesses in Heineken's cybersecurity defences and the maturity of your systems. This helps in identifying areas that need immediate attention and improvement.

g. Regulatory Compliance

Ensuring that Heineken's cybersecurity strategy aligns with regulatory requirements and company objectives. This includes staying updated on relevant regulations and incorporating them into the cybersecurity plan, which should be reviewed and updated regularly.

By focusing on these critical areas, Heineken can strengthen their cybersecurity posture and better protect their assets and operations.

© Atos 2024 All rights reserved

Commercial in Confidence

Full stack observability in Cloud environments

a. Detecting and mitigating threats in real time

Heineken can use full-stack observability to monitor its cloud infrastructure and applications continuously. By collecting and analysing data from various sources, such as logs, metrics, and traces, Heineken can detect unusual patterns or anomalies that may indicate a cyber threat. For example, if there is a sudden spike in failed login attempts or unusual data access patterns, the observability tools can alert the security team to investigate and respond promptly.

b. Ensuring compliance with security standards

With operations in multiple countries, Heineken must comply with large numbers of international and local security regulations and standards. Full-stack observability can help ensure compliance by providing comprehensive visibility into all layers of the technology stack. This visibility allows Heineken to track and document security controls, monitor compliance with policies, and generate reports for audits. For instance, observability tools can help verify that data encryption is consistently applied across all cloud services.

c. Improving incident response and forensics

In the event of a security breach, full-stack observability can significantly enhance Heineken's incident response capabilities. By having detailed logs and traces of all activities within the cloud environments, the security team can quickly identify the source and scope of the breach. This information is crucial for containing the incident, mitigating damage, and conducting a thorough forensic analysis to understand how the breach occurred and prevent future incidents.

d. Optimising Security Operations

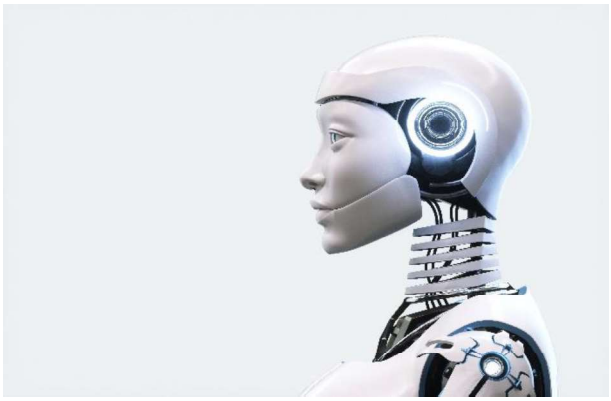
Heineken can use observability to streamline and automate its security operations. For example, integrating your observability tools with your security information and event management (SIEM) systems, can enable automated threat detection and response workflows. This integration can reduce the time and effort required to manage security incidents, allowing the security team to focus on more strategic tasks. Additionally, observability can help identify and eliminate inefficiencies in security processes, leading to more effective and efficient operations.

e. Enhancing Application Security

During the development and deployment of applications, Look to ensure that security is built into the software from the start. By monitoring application behaviour and performance in real-time, developers can identify and fix security vulnerabilities early in the development lifecycle. This proactive approach, known as "shift-left" security, helps prevent security issues from reaching production environments and reduces the overall risk to the organisation.

By leveraging full-stack observability, Heineken can enhance its Cloud-related cybersecurity posture, ensuring robust protection for its digital assets and maintaining the trust of customers and partners.

Cybersecurity and GenAI



We have covered some of these topics in our response to the 'Power of AI' but more generally:

a. Leveraging AI for advanced threat detection

improve threat detection and response capabilities by integrating AI-driven solutions, to automate the identification of potential threats and respond to them more efficiently. This includes using AI for advanced behaviour pattern and anomaly detection, which can help in identifying unusual activities that may indicate a cyberattack. AI in cybersecurity can anticipate, respond, and recover from attacks at a speed humans can't match.

© Atos 2024 All rights reserved

b. Using AI for proactive risk assessment

Implementing AI-powered tools for continuous monitoring and risk assessment can provide real-time insights into the security posture of your IT, IoT, and OT environments. This allows you to proactively address vulnerabilities before they are exploited. Adaptive learning by the AI can use experience from past incidents to provide fast, objective, accurate weakness and threat detection, and suggest a tailored response strategy.

c. Leverage third party managed service offerings to accelerate your own capabilities

Companies like Atos Eviden are able to offer Managed Detection and Response (MDR) services. We are able to provide a next-gen cybersecurity mesh architecture, powered by Amazon's AI Security Lake for intelligent, unified security operations and proactive threat anticipation. Our approach integrates and enhances your existing security tools. Our mesh draws from your cloud, on-premises, OT, and IoT for a holistic, data-powered view of any potential threat. AI helps us spot threats with enhanced speed – up to 90% faster than legacy systems – minimising the impact of any attack. Our AI also acts as an intelligence companion, rapidly generating reports and playbooks, saving valuable time during incident responses.

Our specialised SOC teams add valuable expertise, while industry-specific automation tackles critical applications and business processes. Eviden's 6,500 frontline security experts, across 17 global SOCs, offer 24x7x365 monitoring, drawing on industry best practices for the fastest mitigation with in-built digital forensics and intelligent incident responses. And by productionising these turnkey processes, this frees up Heineken's own IT and security teams focus on innovation, rather than reacting constantly to threat warnings and incidents.

Atos & Eviden – your partner for Cybersecurity

Atos is well placed to assist Heineken on your journey to greater levels of digital security. Third party. Atos is one of the world's largest IT providers, and innovation and expertise is our core business. Atos has considerable skills and experience in developing and implementing relevant and robust Cybersecurity solutions for our customers. In fact, we are ranked Number 1 worldwide in managed security services by revenue. We're also experts in a wealth of linked technologies such as hybrid cloud, infrastructure technology, applications development and support, and IT decarbonisation services. We have been a Gartner Leader for many years in digital workplace services, hybrid cloud infrastructure and datacentre services.

Our 92,000 skilled individuals bring together agility and ability, designing imaginative, creative solutions that help our clients anticipate what matters most to their customers, stakeholders and employees, and create lasting value in today's world.

Security
Experience
Connection
Innovation