ICTS EUROPE

Data Centre Security of the Future

FICTION MEETS REALITY: EXPECT THE UNEXPECTED

What do most pop-culture instances of data centres have in common? Someone enters the data centre to steal data. How is this achieved?

1. **Intricate Planning:** Data centre incidents in pop-culture typically involve meticulous planning by the perpetrators. They carefully study the target data centre's layout, security systems, and procedures to identify vulnerabilities and exploit them effectively.
2. **Social Engineering:** Social engineering is a recurring theme in pop-culture depictions of data centre incidents. Perpetrators often manipulate or deceive individuals with access to gain unauthorised entry, posing as staff members, maintenance personnel, or other trusted individuals.

Data centres in pop-culture

In the heist film Ocean's Eleven a group of skilled criminals, led by Danny Ocean plans an elaborate scheme to rob multiple Las Vegas casinos, which includes gaining access to a vault that houses sensitive data in one of the casinos. Part of their plan involves posing as maintenance personnel to navigate the security protocols and successfully breach the data centre.

In the action film Die Hard 4.0, John McClane finds himself caught in a cyberattack targeting critical infrastructure. In one scene, a hacker named Matt Farrell impersonates a technician to gain entry into a heavily guarded data centre, intending to disrupt the hackers' operation from within.

In Terminator: Dark Fate the latest Terminator, Gabriel, poses as a security officer who infiltrates a data centre to secure data pointing to Dani Ramos' location.

The above examples highlight the perceived vulnerability of data centres to social engineering and the importance of identity verification protocols. Indeed, data centres are not impenetrable, which is one reason for their multi-layered security measures.

The above remain, nonetheless, fictional scenarios.

How much fiction is actually fact?

In 2008, a group of individuals orchestrated a physical break in at a data centre operated by Payment Card Industry, based in London. The relevant individuals posed as workers from a legitimate maintenance company and gained access by using stolen security badges and uniforms, successfully bypassing all layers of security including alarms and surveillance.

More recently in 2022, pen testers entered a data centre by posing as construction staff who were coming and going through the data centre regularly due to some remodelling work.

Irrespective of the security mechanisms you have in place, there will always be a certain level of uncertainty and unforeseen circumstances. Would your data centre be prepared for a terminator attack or a criminal mastermind? Unlikely. As per the 2021 Data Breach Investigation Report by Verizon, 85% of data breaches involved a human element. This is where fiction meets reality and provides the first brick into building the data centre security of the future.

Data Centre Security of the Future: expecting the unexpected.

Data centres are at the heart of our increasingly connected world, safeguarding vast amounts of critical information. As technology advances, data centre security must evolve to counter emerging threats and address the unexpected irrespective of what form it is presented.

Artificial Intelligence as the Guardian:

The future of data centre security will see AI playing a pivotal role. Advanced AI algorithms are already capable of analysing vast amounts of data in real time, identifying patterns, and predicting potential threats. These intelligent systems will continue to adapt and evolve, continuously learning from emerging risks and improving their defense mechanisms. In fact, AI has been highlighted as one of the most cost-effective and scalable ways to improve resilience in data centres.

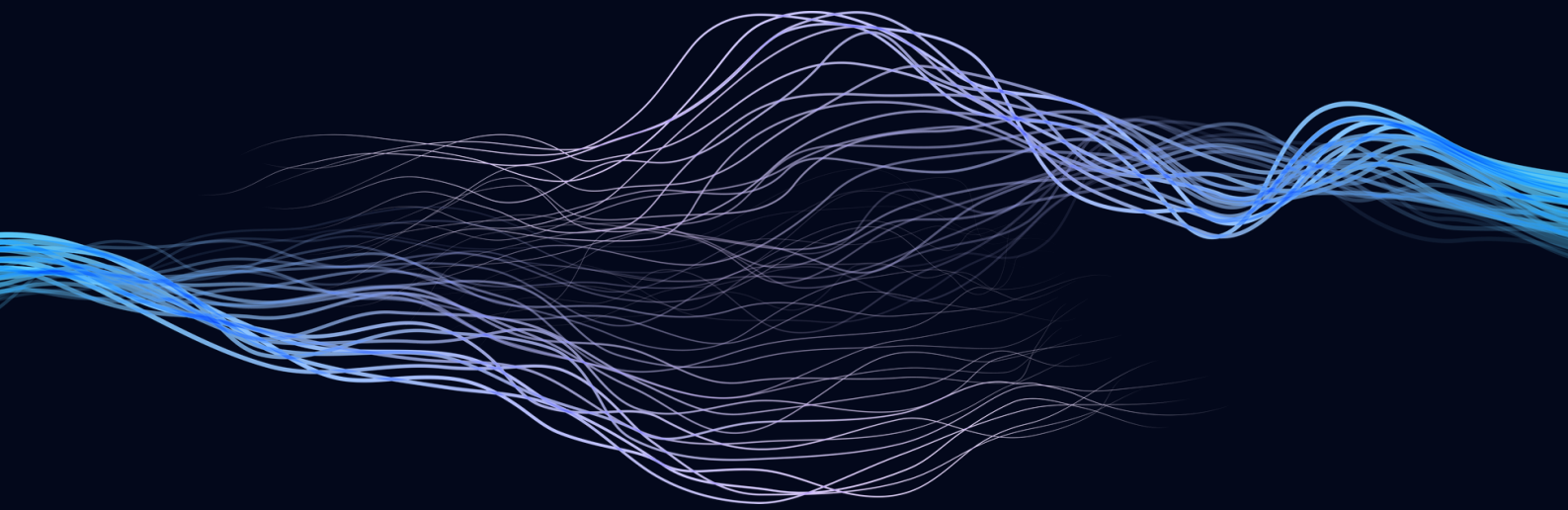
The role of AI will be twofold. On the one hand, AI and machine learning algorithms will continuously monitor, identify anomalous behavior, and predict potential threats. These systems enable proactive defense measures, real-time incident response, and automated mitigation techniques, ensuring data centres are prepared for the unexpected.

On the other hand, Robotic process automation (RPA) and AI-driven algorithms will streamline routine security tasks, enabling security personnel to focus on critical activities. Furthermore, predictive analytics will utilize historical data and real-time threat intelligence to forecast potential security breaches, allowing data centres to stay one step ahead and proactively address vulnerabilities.

Threat Hunting: Predicting and Preventing Attacks:

According to a survey conducted by SANS Institute in 2020 82% of data centres reported that threat hunting improved their overall security posture. The future of data centre security will feature advanced threat-hunting techniques. Sophisticated machine learning algorithms will continuously monitor traffic, analysing data for suspicious patterns and behaviours. This proactive approach will enable security teams to identify potential threats and take preventive measures to safeguard data centres from emerging attacks. This will in turn ensure that they are better equipped to detect and respond to threats before these lead to a breach. Gartner predicts that by 2025 50% of large enterprises will actively implement attack prediction solutions that include machine learning and artificial intelligence algorithms.

Additionally, data centres may employ autonomous surveillance drones or robots equipped with advanced sensors and AI algorithms to patrol facilities and identify potential breaches.



Red Teaming:

Inspired by fiction's portrayal of skilled hackers, data centres will adopt a proactive approach by incorporating red teaming and ethical hacking practices. Red teaming involves independent security experts simulating real-world attacks to identify vulnerabilities and assess the effectiveness of existing security measures. By embracing this practice, data centres can continuously evaluate and enhance their security posture, preparing for unexpected attack vectors and minimising potential risks. This practice is not as prevalent as one would expect. In 2020, it was reported that only 56% of organisations used red teaming to assess their security posture (Ponenon Institute).

Red teaming provides insights into an organisation's incident response capabilities, allowing them to evaluate its ability to detect, contain, and remediate potential security incidents. In fact, in 2019, a well-known technology company conducted a red team exercise on its data centres and discovered vulnerabilities that could have led to unauthorised access to critical infrastructure. The exercise prompted them to implement stronger security controls and revise their incident response procedures.

The ICTS Europe Group has been a trusted security partner to numerous data centres for over a decade. Our security teams operate in over 80 data centre sites across 7 countries. Our emerging technologies and strategy shape the global security landscape and make a difference in the environments in which we operate.

Contact us to find out more about our ever-expanding solutions and to find out how we can redefine your security.

mail@ictseurope.com

www.ictseurope.com
www.ictseurope-viridian.com

In conclusion, the data centre security of the future will have to expect the unexpected. The lines between fiction and reality will be blurred by embracing advanced technologies and innovative approaches to protect critical information. This will be achieved by deploying advanced threat detection systems, leveraging intelligent automation and predictive analytics, and incorporating red teaming practices. By embracing these principles, data centres will stay ahead of emerging threats and ensure their security, integrity, and resilience in a rapidly evolving threat landscape.

STRIKING A BALANCE - DATA CENTRE SECURITY AND GOING GREEN

Data centers are notorious for their substantial energy consumption, particularly for cooling and maintaining servers. It is estimated that these facilities collectively account for nearly 2% of the world's total electricity usage, contributing significantly to global greenhouse gas emissions.

Consequently, the carbon footprint associated with data centers requires immediate attention. More and more data centres are being regulated for their energy consumption and impact on the environment and are currently under a microscope.

Many of them have embraced new regulations by implementing green policies such as renewable energy.

However, what is the impact of physical security on sustainability and vice versa?

The quest for Enhanced Physical Security

Given the increasing threats to data security, organizations continuously invest in advanced physical security measures. These include multiple operation platforms, cutting-edge surveillance systems, biometric access controls, fortified perimeter security, and the employment of dedicated security personnel.

As these become increasingly sophisticated and able to foresee future threats, they pose an additional burden on data centres energy consumption.

One answer might lie with renewable energy, however that requires renewable energy of a large scale which is questionable if smaller data centre operators will be able to accommodate this.

Environmental Damage Affecting Physical Security

The other side to consider in this debate is the impact environmental damage has on physical security. Suddenly, security threats are not limited to intrusions but also the effects of extreme weather patterns.

Floods, fires, power outages directly impact the effectiveness of security systems, leaving data centers vulnerable to physical security breaches. Risk assessments now have to account for things that historically were not perceived a security risk – but how far ahead to you plan?

Are physical security the new keepers of sustainability? Expected to warn of potential extreme weather patterns and fortify data centres accordingly?

If so, how does this change physical security?

It is likely to come in the form of additional training for staff, and technology solutions but one thing is certain, sustainability needs to become an integral part of security, at its very core.

Physical security operational technology will have to adapt to encompass sustainability and staff will have to understand the impact of evolving threats emanating from extreme weather patterns.

AI to the rescue?

As the use of AI further expands, it is likely to have all-encompassing operational systems which address all of a data centres' needs. This would include traditional security concerns but also environmental concerns - such as forecasts, monitoring consumption and raising alerts.

However, AI is energy-intensive. As per the Vrije University Amsterdam's studies, by 2027 will consume annually the electricity of a small country. While the relevant study looked at AI at much larger scale than simply a data centre, it is important to remember that there are approximately 8000 data centres worldwide.

Data Centres already consume massive amounts of energy and with a potential increasing reliance on AI, their will consume even more. Can sustainable resources cover this usage, considering that data centres operate 24/7. As per Vrije University, data centre energy costs will increase by 50% only in terms of cooling.

As per our previous article, physical security will likely become more reliant on AI to address unexpected threats. Unexpected threats now include environmental issues, and energy consumption suddenly sky-rockets.

Physical security is not a mere bystander in sustainability anymore.

Striking a Balance

Striking a balance between security enhancements and environmental sustainability is an ongoing challenge, however the 2 must co-exist.

The first step is a change of mindset - security organisations must be prepared to support clients in their green policies and goals. They need to embrace sustainability in their own plans, monitor their impact and train staff accordingly.

The second step is to determine exactly how to expect the unexpected. As per our previous article, the data centre security of the future will have to expect the unexpected where the line between fiction and reality will be blurred. Expecting the unexpected here comes in a different form - environmental damage and its impact.

Some answers lie with technology but the impact of AI itself on sustainability cannot be overlooked.

The ICTS Europe Group has been a trusted security partner to numerous data centres for over a decade. Our security teams operate in over 80 data centre sites across 7 countries. Our emerging technologies and strategy shape the global security landscape and make a difference in the environments in which we operate.

Contact us to find out more about our ever-expanding solutions and to find out how we can redefine your security.

mail@ictseurope.com

www.ictseurope.com
www.ictseurope-viridian.com

In conclusion, the data centre security of the future will once again have to expect the unexpected. In this case, the unexpected will come from the environment. We need to talk about sustainability in the security sector and find a balance between teams, technology and their impact.

By doing this, security teams can not only minimize their own environmental impact but also ensure that data centers stay safe. Remember, what's bad for the environment is likely to also mess with your security.

THE DATA CENTRE WORKFORCE OF THE FUTURE - AI AND EXPERTISE

As data centers (DCs) continue to evolve and expand in the digital age, security will continue to be a critical component of their operations. In this article, we delve into the future of DC security, analyzing the relationship between artificial intelligence (AI) and the DC security workforce. Where does the balance lie between the two?

The Rising Role of AI in DC Security

AI and machine learning have swiftly made their presence felt in the realm of data center security. These technologies bring a new level of automation and intelligence to the table, enabling rapid threat detection, anomaly recognition, and real-time response, as well as comprehensive operational platforms. AI-driven security systems can analyze vast amounts of data in mere seconds, making them a formidable asset for safeguarding DCs against any threat.

However, it is vital to recognize that while AI can enhance security measures, it is not without its limitations. AI systems require precise programming and data training to operate effectively. In addition to this AI, is notoriously power hungry (as explored in our previous article). It can also be susceptible to adversarial attacks, where attackers manipulate input data to mislead the AI. We conclude that it is unlikely for AI to fully remove the need for the human element of security.

The Human Element: Experience and Expertise

In the world of DC security, human expertise will remain indispensable. The security workforce brings crucial intuition, experience, and adaptability that AI alone cannot replicate. Human security professionals are adept at understanding the nuances of a specific data center's operations, recognizing patterns, and responding to emerging threats that may not be captured by AI. However, a challenge lies in human error, which is unavoidable. However, AI can minimise human error by working alongside officers and providing critical real-time information.

The other side of the spectrum is that in a data centre a degree of knowledge and specialisation is needed to effectively safeguard them. Even in the data centre structure - the intricacies of its design alone are numerous.

The Specialization Conundrum

The level of specialization required within the DC security workforce is a subject of debate. Some argue for highly specialized roles, where security experts focus on specific aspects. Others advocate for a broader skill set that encompasses a range of security domains. While some level of specialisation will undoubtedly be prevalent, it is becoming increasingly important for each function to effectively understand all other functions as everything in a data centre is so interconnected.

A small human error such as an open door can cause an outage and a weather issue such as rising temperatures can contribute to overheating. Traditional security training of just covering the site and working in a data centre overall is arguably insufficient moving forward. There will need to be further advanced training accounting for the specific nuances of the data centre environment and the function of AI. This could prove expensive. So, what is the solution?

Recruitment Challenges

Recruitment is a growing challenge for multiple industries, including security. Security companies will have to change their offering to prospective recruits making it a viable, long-term career option rather than a stepping stone. Perhaps what's needed is a reinventing of how we classify the security positions in data centres in the first place. Perhaps another solution is working with universities to create existing, specialised courses which could support people to move into such a profession.

Finding the right balance between specialization and versatility is crucial. Specialization is vital for in-depth expertise in particular areas, but a workforce that is too specialized may struggle to adapt to evolving security threats and technologies. What is needed is a combination of specialisation and knowledge, including understanding how AI works, and how human security works alongside it.

The ICTS Europe Group has been a trusted security partner to numerous data centres for over a decade. Our security teams operate in over 90 data centre sites across 7 countries. Our emerging technologies and strategy shape the global security landscape and make a difference in the environments in which we operate.

Contact us to find out more about our ever-expanding solutions and to find out how we can redefine your security.

mail@ictseurope.com

www.ictseurope.com
www.ictseurope-viridian.com

The Future of DC Security

The future of DC security is a dynamic landscape where AI and human expertise are complementary forces. AI brings speed and precision to threat detection, while human security professionals provide the experience, adaptability, and intuition needed to address complex and evolving security challenges. In this evolving field, a balance between specialization and versatility will be the key to a secure and resilient data center environment