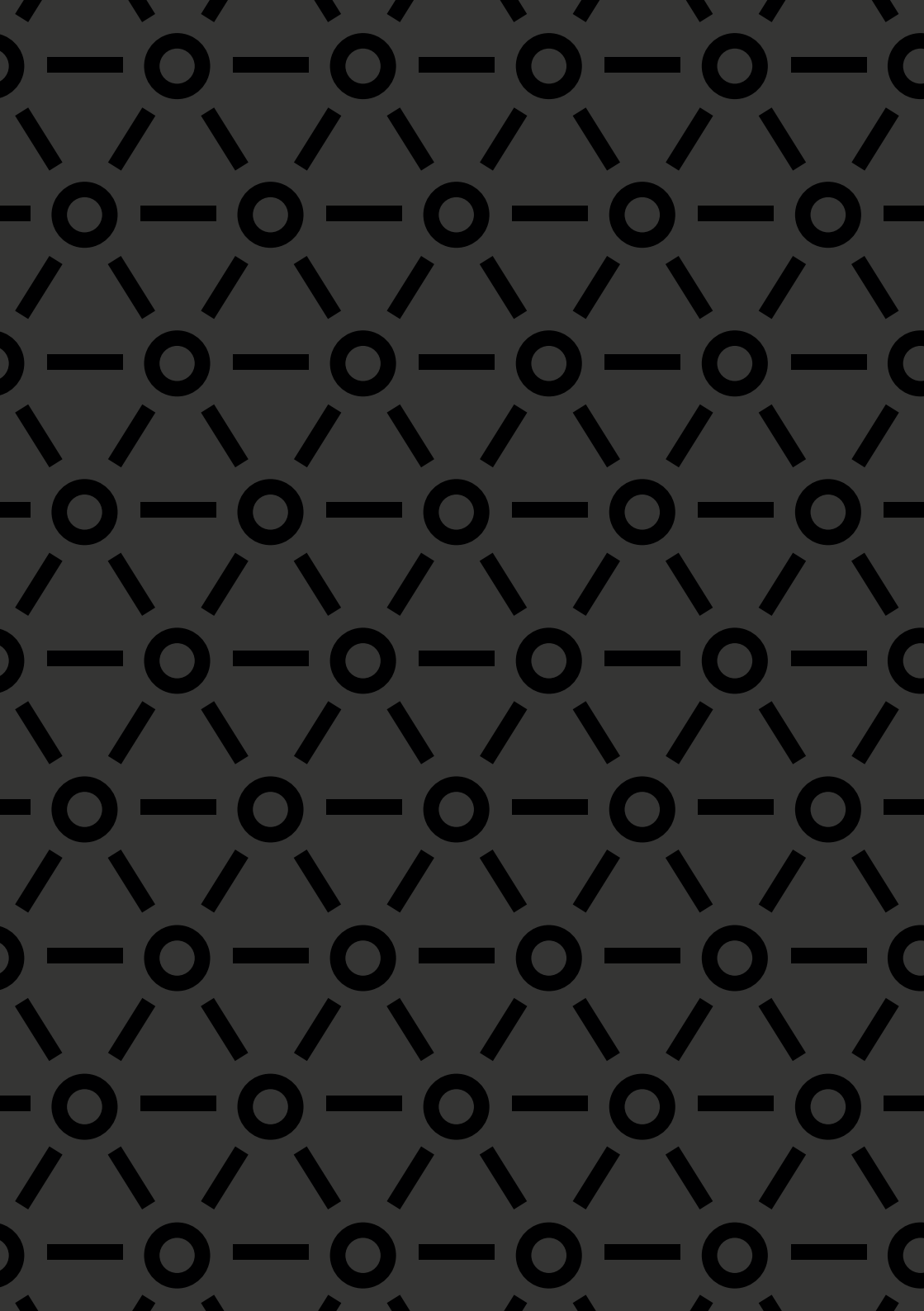
e–shelter security

— Data Center Whitepaper

Multi-faceted Considerations for Data Center Development



— Contents

— Introduction

The structure of data centers has changed quite a bit in recent years. What used to be a hidden facility somewhere in a company's basement or inside a secret building, has now grown into large campuses with multiple, well-secured buildings.

These campuses also utilize complex infrastructure to support many diverse clients. In the past, it was quite typical that each enterprise operated its own data center, filled with individually specialized systems and running on internally developed software. However, advanced communication techniques have made it possible for data center providers, operating from centralized mega sites, to deliver standardized and reliable Software as a Service. As a result, more and more enterprises are using these third-party providers to reduce reliance (and maintenance) on their internal systems, to become more flexible, to saves on costs and to concentrate more on their core competencies.

Data center operators, however, do face challenges. While the failure of an 'enterprise' data center can lead to the interruption of business for that single company, a multi-tenant data center operator supports many customers who critically depend on high availability and security. Depending on the actual supply chain of data centers, cloud and IT service companies and communication network operators, the reliance scheme is much more complicated and requires new definitions for service, security and availability. The objectives must be set in a way to not just satisfy the requirements of a single company, but rather, to have a much more general and inclusive set of services to support a multitude of different clients from various industries. This may also include the need to satisfy external legal and regulatory requirements.

— Requirements for Large Scale Service Data Center Sites

When developing new data center sites, operators require a location that is in the vicinity of business clusters with sufficient demand for IT services requiring safe, secure and available infrastructure. Especially for 'hyperscalers', large and globally operating enterprises who offer various types of cloud services, these companies have strict requirements for both the quality of data center sites (which need to be fulfilled by the operator) and the prices they are willing to pay for various services.

While some companies try to focus on facilities in countries with low energy costs, affordable property and access to international data networks, others look at different requirements. Legal requirements and demands for ultra-fast response times call for locations to be near business clusters, where space and power[1] can be less abundant and more expensive. Also important to many organizations are locations where data networks are dense, distances are small, and the legal regulations match those of the clients. Identifying plots that satisfy the requirements of data center operators (and their present and future customers) is a task for experts with a high degree of local expertise. These companies can be very helpful in identifying such plots, analyzing the environmental situation, planning risk mitigations and helping to master local regulations, which can have a huge influence on how the data center is designed.

Experts have a systematic approach to analyze

— natural risks, like potential sources for flooding, extremes of temperatures, torrential rain, storms, earthquake activity and other ambient conditions, underground structures or soil contamination, buildings and businesses in the neighborhood, industrial risks caused by nearby factories and especially process industries working with large amounts of flammable, explosive, potentially toxic or nuclear materials, sources of electromagnetic radiation, traffic related risks like large roads, freight train tracks or overhead air traffic,
— points of interest that could cause traffic jams, demonstrations, or other large gatherings,
— social situation and criminal hot spots,
— other risks that could affect the operation or also the access.

A concept that defines physical security and availability measures appropriate for the location and based on environmental analysis is a key requirement.

Clients will ask for the levels of control the facility can provide, like
— which measures were implemented to address the risks identified for the location?
— what is the level of resistance against external attacks?
— how is the access to the site managed to guarantee that only authorized persons enter critical areas?

[1] The municipalities of Amsterdam and Haarlemmermeer, for instance, have stopped the development of new data centers due to considerations about energy availability and environmental impact in 2019 – see https://www.amsterdam. nl/nieuwsarchief/persberich-ten/2019/persberichten-ma-rieke-doorninck/regie-vesti-ging-datacenters-amsterdam/ –and released a policy for a very selective growth policy in 2020, see https://www.amsterdam.nl/bestuur-organisatie/college/wethouder/marieke-doorninck/persbe-richten/amsterdam-selectieve-groei-datacenters/

— Availability of Data Centers

Data center operators provide, as core services, resistant and solid buildings, highly available infrastructure for power supply and cooling, security for access protection and reliable processes for access management. In addition, network services are required. Depending on the business model, an operator can provide access to passive networks, or will provide active switching of logical networks within the data center to other buildings or sites, the internet or cloud providers.

Various institutions have created normative frameworks on how resilient a data center is. The Uptime Institute published the Tier specifications, the Telecommunications Industry Association (TIA) describes rating levels in TIA942, and the CENELEC created the norm EN 50600, to name a few. All three institutions defined four levels of resilience with similar but not identical criteria and extensions. Typically, the lowest level describes the absolute minimum required features for data center infrastructure, while the highest level describes the 'perfect' solution without any single point of failure. But 'perfect' also means 'expensive'. Owning the most resilient data center does not mean that clients want to pay the price. The design of a data center must match the client's requirements to have the best cost/performance ratio. Therefore, the interior of a data center needs careful design to match client expectations.

External factors are equally important:

— How reliable is the external power supply? How much power can I use now and in the future, when my demand increases but local or backbone grid capacity can be limited? What do I need to be able to survive power outages? Are diesel generators still the first choice or should I look at other technologies such as fuel cells?
— What level of emissions are allowed when my generators produce noise and exhaust gases?
— Which capacity is available on the data network? Do I have sufficient capacity now and in the future? Are the networks really path redundant or could I experience single points of failure?
— Are my suppliers and maintenance companies readily available when I need support, e.g., in case of incidents, but also in case of regular maintenance activities? Are critical spare parts well managed and readily available onsite to be responsive?

Critical are suppliers of power and fuel for emergency operations because fuel is limited, logistics can be complicated, and supply can be impossible on holidays or weekends. You want to be sure to make a good investment and have qualified engineers and experts on your side before you make such a big decision.

— Sustainability

100% of the energy consumed in a data center is ultimately converted into waste heat. The energy delivered from the grid comes from a mix of renewable, fossil and nuclear sources. Many clients have set up programs to become carbon neutral and so, data centers need to support this trend. This is asking for concepts to maximize the use of renewable energies, and also to reduce overhead spending and minimize the demand for IT systems operated in the data center. Since the vast majority of waste heat is created at quite low temperatures which makes it hard to reuse, e.g., to heat houses, more general concepts are required. Using local energy production, direct current technology, or high-temperature processors could help to increase efficiency but the hardware industry does not yet provide the required systems in large numbers and at affordable prices.

The environmental impact is just one aspect of sustainability. How do data centers fit into local communities, how well are investments and value of operation balanced – not only for the owners but also for society? How are working conditions in the data center and the supply chain? Is the company considered a 'good citizen'? More and more clients are asking for proof of sustainability principles that are implemented by their suppliers – and data centers are part of most supply chains.

— Security, Access Protection and Management

People are needed at the data center but you would only want authorized personnel to enter and all others to stay outside. With current technology, the protection of a data center can largely become an automated process. 'Intelligent' fences, with video surveillance that detects attackers or other blackguards who try to make their way to the data center, can be designed to a very high level of resistance that also protects against more violent attacks involving cars or trucks. Breakthrough-safe doors, gates, barriers or bollards can help to secure sensitive buildings or installations on the site. And this equipment can all be laid out very discretely or explicitly to show that unwanted visitors are not welcome.

Authorized visitors are welcome at the data center at any time. You want to know who they are, and that, when access is granted, there is no doubt, as to whether they can access the infrastructure and clients' areas. This requires a dedicated and failure-proof process that not only covers clients but considers that clients can have secondary clients, a multitude of service providers are needed for both the clients' infrastructure and the data center operator's systems and that various third parties can require access, too. Depending on the requirements of the operator and the clients, various levels of assurance

can be employed. The more traditional approach is that visitors (as well as onsite staff) have possession of a badge that shows their status and that opens the right gates and doors. However, this can be easily circumvented, but modern identity management concepts require that every individual is in possession of an access medium (i.e., a badge or a smartphone displaying a QR code), knows a PIN or a password, and is identifiable by facial recognition, a fingerprint or other means. Managing logistics is not only a physical task but it also needs to be included in access management to ensure correct and safe storage and correct delivery to authorized parties. While this seems to be complicated, modern technology is available that makes the fully featured access control affordable and, considering that many manual process steps can be avoided, even cheaper, more efficient and extremely effective.

— Operation and Facility Management

Data centers have thousands of components that need to be controlled and permanently monitored. Changing loads in the data center and adjusting ambient conditions influence how parameters are set to create the best possible conditions and balance energy consumption. Incidents must be identified, if possible before they take effect on the client's systems. Most infrastructure systems can be remotely managed by digital control systems that are cascaded into a central Building Management System (BMS).

Similar considerations apply to the security systems. Monitoring the state of doors, gates, barriers and locks is important, along with managing alarms from Intrusion Detection Systems and automated video surveillance systems, responding to alarms from Health and Safety monitoring and fire alarm systems. All these things require central control and consolidation into a Hazard Management System to be able to reduce manual efforts.

Planning regular patrols that check the proper functioning of all operation and security systems is required to keep the data center running. It also requires qualified and well-trained personnel from all areas of electrical engineering, refrigeration technology, facility management, security technology, to name only a few functions. They must also be available 24/7.

— Quality and Process Management

Clients expect an elaborate level of process design and control from the data center operator. In regular operations, many tasks must be executed in a predefined manner that guarantees correct execution and uninterrupted operation. Several examples are the following:

— Standard Operation Procedures (SOP) and Emergency Operation Procedures (EOP) are low-level descriptions of how certain components must be handled during regular operation and in case of possible out-of-line situations. They must be readily available for most activities in the data center.

— Changes are frequent and require appropriate preparation including risk analysis and risk mitigation measures. The Change Management process must also take care of information to clients in case a change will or could impact the client's operation.

— An effective Incident Management process is required to be able to react promptly on events that happen in the data center. Information to clients is again a key component.

— Maintenance management is needed to have full control over the operation of critical infrastructure and to avoid unwanted interruptions that could cause impacts on the clients' business.

— Service Level Management serves to inform clients about all service parameters like power availability and usage, temperature and humidity profiles in the data halls, service requests delivered etc. The summary of service levels achieved is also important internally as a base for improvement of services, performance optimization, especially around energy efficiency. The measurement of the Power Utilization Efficiency (PUE) is key for sustainability but also for the financial position.

— Complaint and Request Management must react quickly to clients' requirements or critics, provide solutions and work on customer satisfaction.

— Risk Management is a key process, both from an internal view to understand potential technical and administrative failure scenarios, and also from the client's view. Companies from regulated businesses have strong requirements to understand the risks of their business processes. To run IT infrastructure and preserve availability and security of the basic data center infrastructure are important parts, where an operator of these services must be able to demonstrate his risk analyses and implementation of mitigation measures.

— Compliance Management is needed to understand the needs that come from legal regulations, industry standards and special requirements of customers. The Compliance Manager will set rules of behavior, publish and train a code of conduct and audit internal processes to ensure compliance with the rules set. Many companies require that standards are maintained across the complete supply chain. This adds the task to establish a code of conduct also for direct and indirect suppliers and service partners.

In addition, the processes need to be documented and kept up to date. Usually a certification according to ISO 9001 is an absolute minimum standard which, in many cases, must be exceeded to meet customer expectations.

If a serious out-of-line event occurs which cannot be covered by incident management, Business Continuity Management (BCM) processes must be started. Each company should have analyzed critical operations by means of a Business Impact Analysis (BIA) and should have created Business Continuity Plans for the most important event classes that can occur. A special organization that takes over in such events must be defined and regularly trained to be able to react quickly and decisively.

— Business Continuity Management and Disaster Prevention

The better trained the team is and the better the potential risks are addressed, the faster the response to catastrophes and disasters can be handled. The better risk analyses and mitigation are, the less probable are such situations. A comprehensive Business Continuity and Disaster Prevention plan requires experienced personnel within the organization. In addition, various cycles of optimization are needed so that the plan can become effective and also efficient. Organizations can take advantage of expert knowledge for a quick start to reach, at a minimum, a reasonable capability level.

— Internal Controls, Trust and Reporting

All service providers in the IT industry face the challenge of responding to a multitude of audits requested by their clients. These clients want to ensure that the provider is running the business according to the rules set by them in addition to legal and technical standards.

In previous years, standards have been developed that let the service provider demonstrate compliance. With these rules, the process is set to control objectives, define controls that support the control objectives and let the Internal Control System (ICS) be audited by an independent auditor. The summary of how the controls are established is then made available in an audited report that shows the effectiveness and efficiency of the ICS. The major auditing companies have agreed to accept reports audited by another qualified company, which can make it much easier to satisfy requirements in a common approach.

Several standards are available for the establishment of controls, auditing, and reporting.

— ISAE 3402 defines controls that must be maintained to prove that systems relevant for a company's financial statement are reliably operated, and with respect to data centers, are run in a secure and available environment.

— ISAE 3000 is a wider standard that defines audit principles to address areas which go beyond what ISAE 3402 covers. An audit report to check adherence to the Global Data Protection Regulation (GDPR) could be prepared under this auditing standard.

— System and Organization Control (SOC) 1 reports are similar to ISAE 3402, however, they are governed by the SSAE18 standard, which is created and maintained by the American Institute of Certified Public Accountants (AICPA). SSAE18 has become a standard also outside the United States, due to US companies requesting the standard also internationally.

— System and Organization Control (SOC) 2 reports, also a standard of the AICPA, focus on special 'trust' areas, like controls for cybersecurity, availability, information security, or data protection.

These reports are generally available as Type 1 reports where the report focuses on the completeness of the controls set at a defined point in time, while Type 2 reports require proof of effectiveness over a period of at least 6 months.

Effective implementation of an ICS can greatly reduce the need for 3rd party onsite audits and helps to create improved management control over the operation of a data center.

— Summary

Data center development for an operator requires expertise not only in the core areas of business operations but also, in somewhat peripheral fields such as regulations, sustainability, certifications, and high-grade security. In-house proficiency in these areas is not always viable as it is expensive and full-time personnel may not be required throughout the entire data center lifecycle. On the other hand, third party experts are essential as providers select new sites and build them out for operations. Even more indispensable are experts who can provide a holistic view of the entire data center lifecycle from one vantage point.

e-shelter security has more than 20 years of experience in the data center industry. Experienced consultants and engineers, along with qualified partners, help to manage the challenges of planning, constructing, and running a data center. With e-shelter, both operators and their customers are secure that their facility is at the forefront of modern data center technology, where their businesses operate optimally and without interruption.

— Let's get in touch.

T +49 69 247 430 – 000
info@e-shelter.io
e-shelter.io

e-shelter security GmbH
Eschborner Landstr. 100
60489 Frankfurt am Main
T +49 69 247 430 – 000
info@e-shelter.io
e-shelter.io