IONOS

IT security in the cloud redefined

Preventing complex network attacks effectively.

IONOS

Contents

IONOS

1 Digitalisation and IT security in the cloud era

Stopping service outage and digital blackmail effectively

As life becomes ever more digitalised, the risks of targeted attacks on systems and devices continue to grow. In this digital world, new Internet of Things (IoT) technologies are becoming more and more essential; they connect countless devices that we use at home every day and are used in machines and sensors worldwide. Although the IoT has been designed to simplify and enrich our everyday lives, systems are being increasingly targeted by attacks due to ever-expanding network connections. Attacks on IT systems around the world are now causing billions of dollars in economic damages.[1] The criminal potential here is so extensive that viruses, Trojans and malware, as well as more complex ransomware and distributed denial of service (DDoS) attacks, are threatening the very existence of companies. They can strike without warning and paralyse entire businesses. Consequently, sustainable, professional IT security is not only gaining in importance but is actually now seen as one of the greatest challenges facing economies and the future world in general. The situation is intensified by the fact that public sector administrations often delay investments and modernisations for considerable periods of time and are therefore particularly vulnerable to attack due to their outdated technology.

5.4 million DDoS attacks were recorded worldwide in the first half of 2021.[2] The number of ransomware attacks is also increasing dramatically. The 2019 Global Risks Report by the World Economic Forum recorded a 97 percent increase in ransomware attacks within two years.

Security providers are constantly striving to master these developments with new security solutions, as this is the only way companies and institutions can protect their IT. Security solutions have improved and become more complex in recent decades, but the threats posed by hackers are also becoming more sophisticated. It is for this reason that security specialists are now also developing cloud-based technologies intended to reliably safeguard companies and institutions against threats within networked systems such as DDoS attacks and ransomware. An exceptionally high degree of protection can be achieved with the help of modern cloud technologies, something that small and medium-sized enterprises (SMEs) and institutions in particular are unable to do themselves. They generally lack the resources and the necessary know-how. Public institutions also stand to benefit from cloud security as this, together with a modern SaaS architecture and the right partner, can ensure data security and sovereignty. But what are the specifics of DDoS and ransomware and what risks do they pose?

1. NETSCOUT (2022): NETSCOUT Threat Intelligence Report, available online at: https://www.netscout.com/threatreport.
2. NETSCOUT (2022): NETSCOUT Threat Intelligence Report,, available online at: https://www.netscout.com/threatreport.

2 Definition of terms – what are we actually talking about?

2.1 Denial of Service (DoS)

Denial of Service (DoS) is exactly that. During a DoS attack, network resources are deliberately restricted; this may be for political reasons or for the purpose of targeted blackmail. The aim of such an attack is to inflict as much damage as possible on a company or institution by massively disrupting everyday processes. To do this, criminals use special DoS software that sends multiple requests to a selected web resource. This increases internet traffic to such an extent that, for example, a company's website can no longer respond quickly enough or crashes completely. In other cases, employees are denied access to their emails or applications run so slowly that they are practically unusable. Online stores, providers of online services and organisations whose success depends on reliable data traffic are particularly affected by this. Attacks on public institutions can also have far-reaching consequences, as a system outage can cause significant political or social damage. Beyond that, most public authorities and a majority of companies work with highly sensitive data that must be available at all times.

A DoS attack can, in actual fact, affect any type of infrastructure that exchanges data via the internet – from a networked manufacturing plant, to a data centre, to individual websites. This means that the risks posed by DoS attacks are almost limitless, given that in our modern, digitalised world, success in business and society is determined by technologies. If these fail, companies, organisations, authorities and individuals are suddenly no longer accessible or only able to function to a limited extent.

A DoS attack can affect any infrastructure that exchanges data via the internet.

But it doesn't end there as standard DoS attacks are now being replaced by DDoS attacks. The potential damage of these attacks is many times greater. A DDoS attack is a distributed network attack that is carried out via multiple computers or devices at the same time. This strategy involves attackers hacking a myriad of systems or machines such as servers and PCs, as well as smartphones and smaller IoT devices, so that they can be networked and controlled in secret. Every infected device becomes a 'bot' or 'zombie' without their users even noticing. The bots then spread the DoS virus themselves and infect other devices. With the help of malware, these connected devices are then remotely controlled by the attacker via a so-called botnet command-and-control server and activated simultaneously if needed. It is therefore easy to envisage that the attack of a large bot army, which can consist of several thousand units, can cause tremendous damage. And that's not all – criminals have now advanced their technologies even further and are in the position to offer illegal bot services according to the individual specifications of a single hacker with a specific target in mind in the form of a rentable service, i.e. ransomware as a service (RaaS). Consequently, the German Federal Office for Information Security (BSI) also makes reference to cybercrime as a service (CCaaS) in its 2021 report.

2.2 Ransomware

A ransomware attack is by its nature similar to a DoS attack, in that it also uses specific malware to temporarily or permanently prevent certain users from accessing their own systems. As its name suggests, a ransomware attack serves to extort a sum of money. Sensitive data is encrypted or even stolen completely for this purpose with the aim of either selling it back or threatening to make it public (Hive ransomware is a typical example of this) if the victim does not comply with the attacker's demands.

But in practice it doesn't even have to get that far, as immense economic damage can be caused just by the act of blocking a system, or the loss of data, for example by interrupting supply chains or communication channels. Ransomware attacks often hit SMEs or organisations as their systems are often not as well protected and therefore easier to attack. Public services are not immune to ransomware either. The data held is highly sensitive and so of particular interest to criminals.

Similar to conventional computer viruses, ransomware infiltrates targeted computers via everyday processes, such as emails with seemingly genuine invoices, delivery notes or ZIP files attached. But security gaps in standard software, web browsers and file hosting services such as Dropbox and Google Drive are also often easy targets for attackers. Renowned analytics firm Gartner confirms this in a 2021report, in which it is also notes that ransomware is being used more and more frequently as "part of an even more comprehensive attack aimed at compromising critical systems and administrative functions."

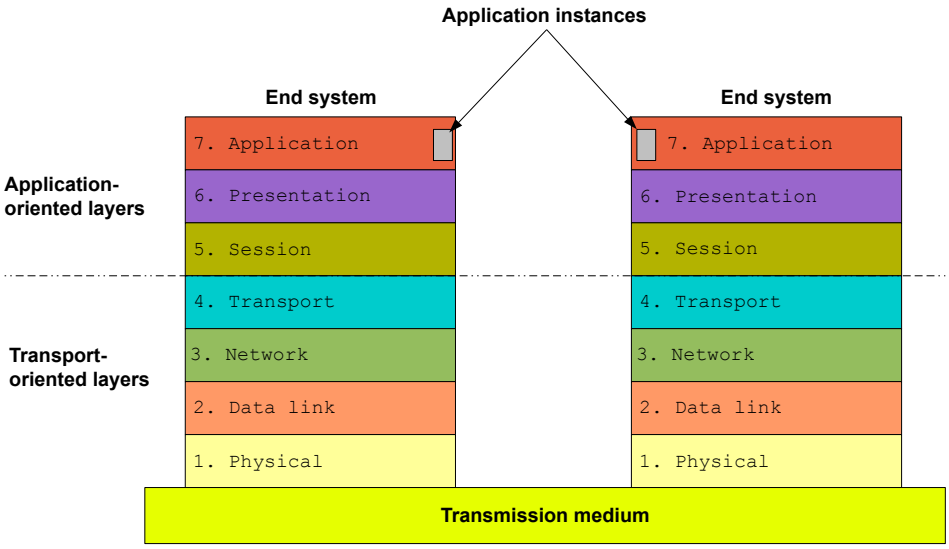
Given the increasing threats posed by DoS and ransomware attacks, reliable protection against these attacks (resilience) should be part of the basic setup of every company and institution regardless of size, industry or region.

3 Real risks – where do threats manifest themselves?

3.1 Types of attacks

If attacks were clearly defined and followed a consistent pattern, reliable protection would be easy to establish. But that is sadly not the case. DDoS attacks in particular usually use several variants at the same time to achieve their criminal goals. For the most part, the types of attack correspond to the individual layers of the Open Systems Interconnection model (OSI model), as summarised in the following graphic. This multi-layer framework is widely regarded as the design basis for manufacturer-independent communication standards. It comprises a total of seven layers, each with its own task.
The model is hierarchical, i.e. each layer accesses the layer below it via an interface in order to make services available to the layer above. In addition to the commonly used OSI model, experts also differentiate between volumetric DDoS attacks, protocol attacks (so called "flooding" such as SYN floods and Smurf DDoS) and application layer attacks (e.g. Ping of Death and LAND attacks).

As attacks are not clearly defined and don't always follow the same pattern, absolute protection isn't possible.



ISO OSI 7-Layer Model (source: Wikipedia)

The seven OSI model layers

- Upper application-oriented layers
  - Layer 7 / Application layer
    This layer establishes direct contact with the user. Email programs, web browsers and other applications receive their additional information here. This process is also referred to as capsuling.

    - Layer 6 / Presentation layer
      This layer translates local data into standardised formats. The presentation of emails, including the format of attached files (jpg, MPEG4 etc.) is determined here, as is the type of compression.
    - Layer 5 / Session layer
      The session layer is also referred to as the communication layer. Special control mechanisms work to establish and regulate a connection between the upper layers.

- Lower transport-oriented layers
    - Layer 4 / Transport layer
      The transport layer is the central link between application-oriented and transport-oriented layers. A logical end-to-end connection between the communicating systems is established via this transmission channel. The data packet, which has been extended by a specific header in the application-oriented layers, also receives an extra transport header here. Moreover, this is where the data packet is assigned to a specific application.
    - Layer 3 / Network layer
      Here, data transfer reaches the internet. Logical addresses are created for the end devices, which includes the assignment of unique IP addresses. The data packet receives a network header with information on routing and data flow control. Routing protocols such as IP, ICMP, X.25, RIP and OSPF or TCP/IP are used for this purpose.
    - Layer 2 / Data link layer
      This data link layer is primarily concerned with error detection, error correction and data flow management. As a result, transfer errors are largely avoided. The data packet, including application, presentation, session, transport and network headers, is framed by a data link header and data link trailer. In addition, MAC addresses are assigned as hardware addresses. Access to the medium is regulated by protocols such as Ethernet or PPP.
    - Layer 1 / Physical layer
      This base layer focuses on bit transfer. Here, the individual bits of a data packet are converted into a physical signal that can be transferred via a medium, e.g. copper wire, fibre optic cables or air. Protocols and standards such as DSL, ISDN, Bluetooth, USB (physical layer) or Ethernet (physical layer) are used for this purpose.

Data packets pass through each layer in the OSI model. This applies to the sender system as well as the target system. All other devices (e.g. router) that a data packet passes on the way to its destination are only connected to layers 1 to 3.

As a general rule, data packets are transported via router. This process involves the router accessing the incoming information in order to make a forwarding decision. But to do so, a router first has to unpack the individual data packet (a process known as decapsulation) and then capsulate it again later for forwarding. This is the point where IT security experts can directly access the traffic and remove harmful content.

3.2 Which systems are particularly affected?

Attackers are no longer just hacking individual computers or data centres. Because of the IoT, billions of internet-enabled devices all over the world are now an integral part of a completely new threat. Digital viruses lurk everywhere: in smartphones, routers, surveillance cameras and even digital video players. Even a house's smart lighting can carry dangerous malware without its owner being aware. The reality is that the network resources of any networked device can become a silent part of a bot army.

This already major problem became even more acute through the outbreak of Covid-19 and the consequent massive increase in remote working. Endpoint security took on a whole new level of importance. Since 2020, innumerable notebooks, tablets and smartphones, which cannot be secured and monitored as effectively as within a company or a data centre, have been connected to company headquarters and local offices all over the world. By its very nature, this interconnectivity harbours vulnerabilities. The State of Ransomware Readiness Report, published in 2021, also addresses this issue. In Mimecast's study, 47 percent of respondents said that the security of their web technologies was one of the biggest challenges in protecting against the threat of ransomware – closely followed by endpoint protection, which also featured prominently at 45 percent.

On top of this comes the enormous complexity and diversity of potential attack vectors. According to a 2021 study conducted by Osterman Research for example, around 85 percent of companies and organisations had initial experience with at least one critical type of attack (they were presented with a list of 17 key threats in total), but less than a third of respondents had experience with four or more of these. In other words, the majority of companies and organisations had no practical experience in dealing with 13 out of 17 challenges. This is not enough to ensure effective risk management. No wonder then that most respondents in the Osterman study rated ransomware-related issues as "concerning" or "extremely concerning". 61 percent assumed that ransomware attacks would damage their company data. 59 percent were of the opinion that ransomware attacks could lead to their endpoints being infected. If these figures are combined with the results of the How to Prepare for Ransomware Attacks report by Gartner (November 2020), the severity of the problem becomes all the more apparent. The Gartner analysts suggest that the costs in the event of a successful ransomware attack far exceed the ransom that is usually demanded. This is by no means a recommendation to pay the ransom, as doing so would further fuel the attackers' criminality. Instead, when planning their protective measures, users should be aware that the outages, which often last several days or even weeks, recovery costs as well as reputational damage can be 10 to 15 times more serious than the actual ransom in the case of this type of attack alone. Therefore, preventive protection is invaluable.

85 percent of companies and organisations have initial experience with at least one critical type of attack.

3.3 It can happen to anyone – examples of attacks

It's not difficult to find examples of DDoS or ransomware attacks. One such example is the automotive supplier Eberspächer, which became the victim of a ransomware attack in October 2021.[3] The family-owned company was suddenly cut off from the public; all phone connections were severed for days. The targeted attack focused on the company's IT systems.

Another case occurred in November 2021 at MediaMarkt Saturn, one of Europe's biggest consumer electronics retailers. A hive ransomware attack encrypted the company's retail management system. From one second to the next, checkout systems and various store services became limited in usability. Following the targeted attack, it took almost a week for the company's computer specialists to identify the affected systems and repair the damage caused. The cost of this work and the loss of sales alone proved enormous, not to mention the demand for a 240 million dollar ransom.[4]

In addition to the losses incurred, the attackers demanded a ransom of 240 million dollars.

3. Álvarez, S. et al. (2021): Will car radiators and exhausts now be in short supply?, available online (in German) at: https://www.wiwo.de/technologie/digitalisierung-der-wirtschaft/nach-hackerangriff-auf-eberspaecher-werden-jetzt-heizungen-und-auspuffe-fuer-autos-knapp/27769800.html.

4. Focus Online (2021): Cyber attack on MediaMarkt and Saturn paralyses systems: more than 3000 servers affected, available online (in German) at: https://www.focus.de/finanzen/boerse/webshops-nicht-betroffen-cyber-attacke-auf-mediamarktsaturn-legt-systeme-lahm-ueber-3000-server-betroffen_id_24407981.html.

The public sector has not been spared either. In October 2021, an encryption Trojan paralysed large parts of city administration in Schwerin, Germany. Due to the attack on a municipal IT service provider, the entire system had to be shut down and all public offices closed. According to the broadcaster NDR, this attack was not random. The perpetrators targeted a critical infrastructure and wanted to obtain high-value data.[5] The attack on Schwerin's administration is by no means an isolated case. As a survey by BR and Zeit Online from 2021 shows, more than 100 IT systems of authorities, local governments and other state and public agencies have been attacked and encrypted in the past six years.[6]

4 Efficient protection against DDoS and ransomware

4.1 Protection as a service

Due to the growing threat, preventive protection against DDoS and ransomware attacks is becoming ever more important, which the Osterman Report clearly confirms. Survey respondents in fact named all the essential protective measures themselves:

- Multi-factor authentication (78%)
- Security awareness training (62%)
- Fast patching of potential weak spots (64%)
- Offsite or cloud backup (62%)

These measures can, without doubt, protect companies and organisations against DDoS and ransomware attacks, whereby multi-factor authentication and security awareness training should be integrated as core measures across all levels of a secure network structure. In terms of backup, however, there are various options available, which are largely determined by the philosophy underlying decentralised or centralised (cloud-based) architecture. Whatever the case, a strategic combination of measures is key here, with endpoint security becoming an increasingly important focus, especially because of the shift in working locations. It is now no longer only a question of protecting a self-contained corporate network with clearly defined core technologies against external attacks, but increasingly also about protecting the rapidly expanding network edge (endpoints), which encompasses countless local devices and clients where the user is situated as well as mobile technologies.

5. Scheller, M. (2021): Attack on data in Mecklenburg-Western Pomerania: How the criminals operate, available online (in German) at: https://www.ndr.de/nachrichten/mecklenburg-vorpommern/Angriff-auf-Daten-in-MV-So-gehen-die-Kriminellen-vor,itausfall110.html.

6. Zierer, M / Tanriverdi, H. (2021): More than 100 authorities blackmailed, available online (in German) at: https://www.tagesschau.de/investigativ/br-recherche/ransomware-103.html.

This is where modern cloud technologies can provide sustainable security. The reasons why are clear. If a company or institution networks its own systems by means of a central cloud, it moves the data worth protecting and a considerable part of the critical (i.e. vulnerable) traffic to a system that is protected and monitored by experts. This central location allows all data traffic to be protected cost-effectively around the clock with professional security tools, such as extensive encryption and a reliable backup service. Moreover, these tasks are some of the core competences offered by cloud providers. No on-premises user could ever manage this to the same extent.

4.2 What role does the cloud play?

Given this context, cloud-based IT security shines in a completely new light, as the number of potential points of attack shifts from a multitude of individual systems lacking optimal security to a single central solution that offers impressive professional protection. This can make all the difference, especially in the case of complex DDoS and ransomware attacks as the cloud is no longer concerned with defending a large number of devices against a large army of bots, but with countering attackers with a well-protected 'fortress' and an army of extremely well-trained 'soldiers'. A cloud-based security strategy therefore ensures that critical services continue to be available even after a serious attack and that decentralised or less important data can be quickly restored as required.

Even though cloud-based security architectures are virtually unavoidable these days, the rationale so far only tells half the story; the real-world scenario is in fact far more complex. For example, IT security that focuses exclusively on cloud protection would hazard the risk of local workstations (clients or endpoints) being infected, something that seems acceptable on the face of things. The reasoning here is that thanks to SaaS, IaaS, MaaS and PaaS, modern cloud systems reduce the role of endpoints to that of a simple user interface. Added to this is the fact that the clients are effectively of no interest to attackers if they do not contain usable data. However, this is not entirely true, as an endpoint is highly vulnerable at the moment of data transfer and becomes a potential weak point in that moment. Therefore, users who rely on professional cloud security must also ensure that their endpoints or clients are secure. The majority of cloud specialists offer corresponding endpoint security solutions with extended client-side security tools for this purpose, which are generally optimally adapted to the respective cloud technologies, centrally managed and do not require any advanced know-how from users at their place of work. Tools and measures provided include:

- An operating system that always has the latest updates
- Specific browser protection with firewalls and intrusion detection as well as anti-virus and internet security tools for mobile devices
- Multi-factor authentication (MFA) with very strong password security guidelines for prevention of unauthorised access

- Removal of software with known security gaps, which is better not used at all
- Specific backup and recovery tools to secure local data on external storage media

Decisive measures are implemented within the cloud to provide efficient protection against large-scale, complex attacks, to detect malicious traffic and to utilise robust defensive measures from the outset. Efficient backup and targeted early detection are of central importance in this respect. This is confirmed by the experts at Gartner in their January 2021 report on backup applications as protection from ransomware. Gartner ascertains that the anti-malware and anti-virus software used by most organisations is not sufficient to achieve true resilience against ransomware. Cloud-based IT security, on the other hand, can provide significantly more security simply through the high capacity and performance of the backend system. Also, when it comes to DDoS, for example, it can play a decisive role in preventing malicious traffic from reaching a website in the first place or in impairing communication via a web API. On this front, cloud providers have a variety of highly efficient tools at their disposal that can cope with the dynamically changing attack vectors of modern DDoS and ransomware attacks. They are therefore in a position to reliably protect users. Cloud customers should therefore make sure that their cloud security package includes the following services in addition to SaaS, IaaS and MaaS features:

- Anomaly detection
- Vulnerability scanning
- Identification of critical IP addresses
- Closing of known security gaps
- Malicious traffic filtering
- DDoS cloud scrubbing
- Integration of the above-mentioned endpoint security tools
- Secure, redundant enterprise-level backup separate from the network

4.3 Backup

A good backup strategy is an essential measure against criminal attacks on corporate networks and is especially relevant in the cloud. When implemented correctly, it can even render the damage of a highly complex DDoS or ransomware attack useless or minimise its impact and make companies or organisations fully operational again in the shortest possible time. In the age of global networking, decentralised installation of protection for each individual device makes little sense, especially in the professional environment. It is far too work-intensive and the number of attack points also increase many times over this way. As DDoS and ransomware attacks by their very nature occur in networked systems, it seems logical, especially in terms of backups, to reduce the potential for attack to a single area. This can be protected with professional know-how and optimised technologies.

Many companies and organisations have already recognised this opportunity and have started to outsource their IT security, including backup, to professional service providers. These are now using future-proof SaaS, IaaS, MaaS and PaaS services, where all critical data is processed centrally anyway. As previously described, only very simple clients remain with users on site, and these are networked display devices without extensive software and data storage.

Returning to the requirements for professional backup in the cloud, the specialists at Gartner have defined a series of critical functions that a professional cloud package should contain. According to Gartner, the following are the most important:

Scalability	The storage and computing capacity of the backup system and the I/O bandwidth should be able to grow with the amount of storage the user has.
Efficiency	The backup system should be efficient in terms of storage utilisation, bandwidth usage and resources.
Performance	The backup system should deliver sufficient performance to carry out backup and recovery processes without delay.
Manageability and user friendliness	The backup system should facilitate the work of the backup administrator, e.g. when creating backup tasks or selectively restoring individual files such as emails or database datasets. Key functions should be automated.
Support for different types of data	The backup system should be able to protect both structured and unstructured data and efficiently back it up centrally on large network-attached storage (NAS) platforms. This also includes data from SaaS applications.
Security	The backup system should include essential security features such as the ability to encrypt during backup operations and support of role-based access control (RBAC), etc.
Protection against ransomware	The backup system should protect backup data from ransomware attacks and enable quick recovery of data if an attack does take place. In addition to this criteria defined by Gartner, the backup system should also offer protection against DDoS attacks.
Reports and analyses	The backup system should inform users about key aspects via regular, easy-to-understand reports. These should, for example, include memory usage, backup job success rates and analysis of the backup system's security status.

This means that there are high demands on cloud service providers when it comes to providing backup for their customers. External backup not only creates an additional interface that has to be protected against attacks, it also entails an additional risk, in particular when the backup is carried out outside of the EU, that many clients are not aware of. As of 2018, US companies have been obliged by law (US CLOUD Act) to forward their customers' data to the authorities in their country if so required. This means they no longer have control over this data and their customers are not aware of what happens to it. According to the European Court of Justice, the US does not provide an adequate level of protection for personal data, not even for data storage and processing providers with a parent company in the US.

Given this situation, cloud providers should always make it clear to their customers whether they store data externally and what protective measures they offer in relation to the US CLOUD Act. This is the only way they can guarantee a sufficiently high degree of data sovereignty, which is essential for users in the public sector in particular.

The basic purpose of backups is the ability to restore data in the event of loss or unintentional change, such as in the event of a hacker attack. To this end, data is stored securely and protected from unauthorised access. Data encryption and storage separate from the network both play an integral role in this. If they are guaranteed, it is virtually impossible for the data to be used for targeted blackmail as part of a ransomware attack. The experts at Gartner have drawn up useful guidelines on this, which are published in their previously report on backup applications as protection from ransomware. These include:

With the aid of a backup, data can be restored if lost or unintentionally modified.

- Avoiding or eliminating network sharing protocols such as CIFS and NFS
- Ensuring that the backup administration console and copies of backup data are reliably protected
- Securing administrative accounts with multi-factor authentication to prevent unauthorised access
- Carrying out ransomware recovery in an isolated environment to prevent further infections

Notwithstanding these measures, users must always be aware that their backups may potentially be infected, as malware may have entered unnoticed prior to the backup being created. Malware can remain hidden in all kinds of files for long periods of time, waiting to be activated. Even a malware scan when creating a backup cannot guarantee one hundred percent security. This does however, remain strongly advisable. New technologies, such as AI-based technologies, which are capable of further reducing the risk of malware infection, are now also becoming available. While there will always be a residual risk that cannot be completely eliminated, this can certainly be reduced through the use of redundant multiple backups.

But there are also more advanced methods that help to minimise the risk of infection. One of these is immutable file storage, which guarantees a defined retention period. This makes it almost impossible for a dataset to be deleted, modified or overwritten for a specific period of time. If an attack occurs in the meantime, the data continues to be available.

4.4 Recovery

Another critical task is the recovery process. Errors can occur during this process too, and viruses can still infiltrate, especially when it's necessary to restore huge amounts of data from hundreds or even thousands of servers. Therefore, this process needs to be carried out systematically, something experts refer to as 'orchestration'. The primary focus here is on a clearly defined recovery sequence; not all applications can launch at the same time, and in many cases there are also recovery time objectives (RTO) involved. The aim of this process is to get particularly important applications back online quickly, while ensuring that those applications responsible for their security have been launched beforehand. It is also important to take into account the amount of data associated with the application in question and the amount of data that needs to be restored.

Specific data should be clearly prioritised as well. Users need to define in advance which data absolutely has to be preserved in the event of a possible attack and which can potentially be lost if necessary. This recovery point objective (RPO) strategy is designed to specifically accept the loss of data from the last few hours, while master data that is vital to survival is stored several times and protected against changes so that it can be safely restored at any time in an emergency. Realistic backup intervals must be considered in this context in order to define the maximum time a system can be down without a permanent loss of data occurring. RTOs therefore play a key role here too.

In order to ensure that everything is in place in case of an emergency, users should also prepare a disaster recovery plan, which can be activated if necessary. This plan should contain detailed documentation that specifies in minute detail how to proceed in the event of a serious outage and who is responsible for particular tasks. Aspects such as the general layout of the infrastructure, regardless of whether this is on-premises or cloud-based, should be documented in precise detail. In addition, there should also be step-by-step instructions on how to restore services, including all necessary configurations such as IP addresses, DNS configurations, firewalls and routing.

Users should prepare a disaster recovery plan for emergencies, which specifies in precise detail how to proceed in the event of a serious outage.

5 Secure, sovereign digitalisation – how to make it work

5.1 Data sovereignty is more than just a legal issue

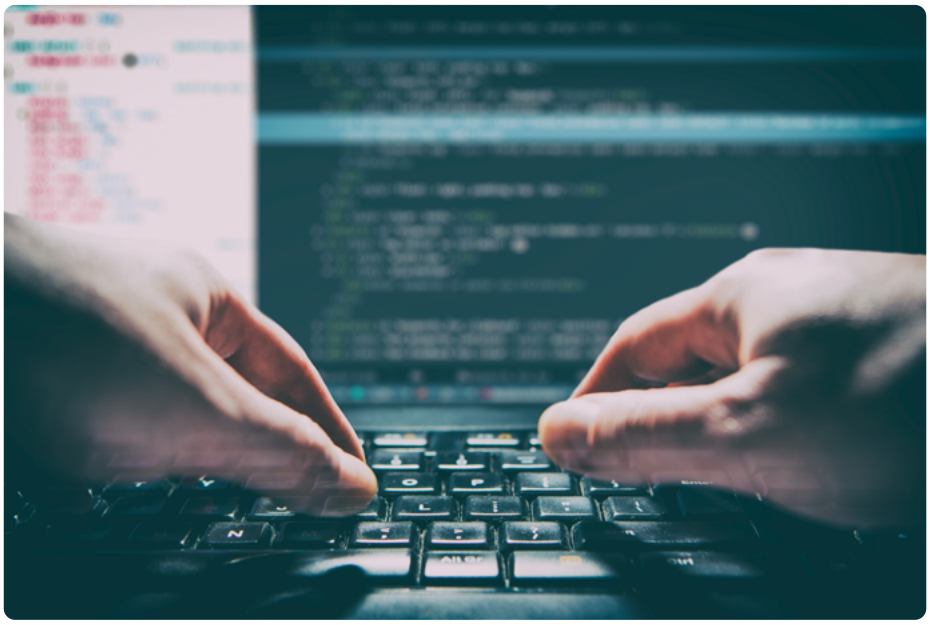
The area of IT security is huge and the market is expanding rapidly. Numerous providers now offer cloud-based solutions that include reliable protection against ransomware and DDoS attacks, including for medium-sized and larger corporations as well as public sector institutions. Providers include Akamai, Bechtle, Bitdefender, Cloudflare, Dynatrace, F5 Networks, Fastly, IONOS, Juniper, Palo Alto Networks, Zscaler, to name just a few. The majority of these providers are based in the US and are therefore subject to the US CLOUD Act, which not only enables but explicitly requires the transfer of stored data to the US – even if the storage itself is not located in the US. To avoid this, users can opt for European providers where the security of customer data is a key priority. In order to provide users with guidance and to support them in selecting the appropriate service provider for their needs, the German Federal Office for Information Security (BSI) has published dedicated guidelines that cloud providers must give binding assurances of to effectively guarantee data sovereignty. These include the following:

- No dependency on foreign interests
- No transfer of data to third countries
- Data processing in Germany
- Transparent system and service description
- Certification by independent third parties
- Support of at least one open standard in the sense of infrastructure as code

The European initiative Gaia-X also offers an interesting approach. In the context of this initiative, companies and experts from business, science and politics are in the process of designing a vital, open and transparent digital ecosystem that can meet the highest demands for digital sovereignty at a European level, and that specifically promotes innovation. Ultimately, the aim is to make data and services accessible, to collate them and share them in an environment of trust. To achieve this, Gaia-X members are focusing on open source solutions as a central foundation for the digital sovereignty of users. Open source is about technical independence and enables self-determined development without users becoming dependent on individual providers. Vendor lock-ins, where users are tied to specific technologies or standards on a long-term basis, are therefore avoided. Moreover, open source systems can be individually adapted and work with a variety of interfaces or even with open, programmable interfaces (APIs).

5.2 What factors should be taken into account when finding the right solution and the right partner?

Even large corporations, which often rely on their own in-house solutions or hybrid architectures, can benefit from cloud-based IT security, as outsourcing this demanding responsibility allows them to concentrate more on their core competencies. Should the need arise, cloud providers also have the right know-how to install customised cloud solutions, which takes the burden off the user while still integrating all local offices into a secure network infrastructure. Users should keep data sovereignty in mind when choosing a cloud partner to ensure that data cannot fall into the hands of third parties.



6 DDoS in practice

This white paper has already outlined several attack scenarios and numerous protective measures. But what does it all look like in practice? What happens behind the scenes when a company or institution decides to work with a professional cloud security provider?

Usually, protection is implemented out of sight within the cloud and, even in the case of an attack, users are only informed about a successful defence. But the actual work of security experts is highly complex and time consuming. In almost all cases, a large team of well-trained network specialists works around the clock to ensure that protective mechanisms are not decrypted, undermined or exploited. This requires complex processes to work seamlessly hand in hand. Not surprisingly, cloud security centres are designed like fortresses – close to impenetrable.

Almost all of the big cloud security providers are pursuing this strategy, and IONOS is one of them. The network specialist from Montabaur, Germany works with its own backbone and operates eight globally distributed scrubbing centres as well as a DDoS defence platform developed in-house. The entire data traffic of IONOS customers flows through this tightly-meshed system, which gives them a major advantage: IONOS monitors the data traffic of its customers itself and can access anomalies and suspicious content early on during operation in order to further analyse, block or disinfect them. If this data is classified as 'clean' after analysis and cleaning in the scrubbing centre, the system immediately forwards it to the respective responsible data centre and therefore to the corresponding customer. The customer hardly notices the associated delay, as it is minimal and nothing compared to the often week-long outages that a DDoS or ransomware attack can cause.

IONOS works with its own backbone and operates eight scrubbing centres and a DDoS defence platform developed in-house.

Another argument in favour of a cloud security system is its enormous technical potential, which a local security architecture is very unlikely to have at its disposal. IONOS has, for example, sufficient resources of its own to successfully defend against DDoS attacks with a volume of up to 1 Tbit/second. This capacity is far above the usual traffic of a large DDoS attack, which almost always falls well short of 100 Gbit/second. The company also has a number of proven protective measures that it has installed over the years, developed itself and constantly optimised on the basis of its own experience with attempted attacks.

Further information is available in this video.

7 DoS and ransomware protection going forward

In its 2021 study on the state of IT security in Germany, the BSI clearly states that despite all prevention, it will remain impossible to fully protect against attacks in the future. But with the right tools and professional management, the risks can undoubtedly be significantly reduced. Therefore, companies and organisations that work with sensitive data or networked systems need to consider cloud-based security. This approach will enable them to concentrate on their actual business, leaving the demanding task of IT security management in the capable hands of specialists. That said, it is also worth taking a look into the future at this point, as the threat situation is highly dynamic and criminal attackers are constantly developing new methods. In view of the fact that ransomware is now offered as a cloud-based criminal service (RaaS, see above), IT managers in all sectors will need to keep an eye on new attack methods and technologies. There are already signs of various developments in connection with artificial intelligence, cryptocurrencies, deepfakes and shadow IT (see the Sophos Threat Report 2022 and ESET Security Trends 2022).

In addition to these already massive threats, ESET Security also sees a particular risk of an increase in attacks on small and medium-sized enterprises as well as on cities and municipalities, having already recorded a significant increase in attack scenarios at municipal level in 2021.[7] It is precisely the companies and organisations in these areas that often fail to fully exploit their options for protecting their own IT systems and networks.

In view of these developments, monitoring by means of simple security tools will no longer be sufficient in the future. Instead, companies and organisations need to focus on a selective combination of high-performance detection methods and ensure that they are always kept up to date. To this end, cloud-based security that acts as a central fortress, and that professionally monitors and analyses data traffic, can provide the necessary security when it matters most.

7. B2B Cyber Security (2022): ESET SECURITY TRENDS 2022: RANSOMWARE, DDOS & CO, available online at: https://b2b-cyber-security.de/en/eset-security-trends-2022-ransomware-ddos-co/.

IONOS

About IONOS

With more than eight million customer contracts, IONOS is the leading European provider of cloud infrastructure, cloud services and hosting solutions. The company portfolio offers everything businesses need to thrive in the cloud, from domains, websites and do-it-yourself solutions to online marketing tools, fully-fledged servers and an IaaS solution. Products and services are geared towards freelancers, trade professionals and consumers, as well as corporate customers with complex IT requirements.

Our product portfolio includes Compute Engine, an IaaS compute engine with its own virtualised code stack; Managed Kubernetes for container applications; Private Cloud powered by VMware; and S3 Object Storage. Our solutions provide established medium-sized and large companies, regulated industries, the digital economy and the public sector with all the services they need to be successful in and with the cloud.

IONOS was formed in 2018 from the merger of 1&1 Internet and the Berlin-based IaaS provider ProfitBricks. IONOS is part of the listed United Internet AG. The IONOS brand family includes STRATO, Arsys, Fasthosts, home.pl, InterNetX, SEDO, United Domains and World4You.

More information is available at https://cloud.ionos.co.uk

IONOS

Contact

IONOS Cloud Ltd.
Discovery House
154 Southgate Street
Gloucester GL1 2EX
United Kingdom

Phone +44 333 336 2984
Email enterprise-cloud@ionos.co.uk
Website cloud.ionos.co.uk

Copyright