A secure, cyber-resilient data centre is crucial to business continuity. We hear from industry experts about some of the key cyberthreats facing data centres, how these can best be mitigated against and a why BaaS is becoming even more critical.

Securing the data centre

Comport, an industry leader in business backup solutions, held a discussion about the top reasons that BaaS is critical for the security of data centres. With more sophisticated infrastructures creating more opportunities for security breaches, traditional backup may no longer be a viable solution.

"The statistics all point to outsourced backup as the solution that protects against security breaches, insufficient backup testing and a lack of staff or resources," stated Eric Young, Principal Cloud Architect of Comport. "Virtual infrastructures will only become more complex with more data to collect. The time to upgrade is now."

Comport outlined some of the reasons that it considers BaaS critical for data centre security.

Protecting against cybertheft – Digital theft is becoming more of a trend, not less. As organisations grow, they become a more tempting target for cybercriminals, companies without a BaaS solution have more to lose than they can afford.

Fines for data loss – Even if a traditional backup solution is successful at recovering some of the data lost after an incident, it may not be able to mitigate fines or damaging headlines. Inadequate protection of data can cost a company millions of dollars.

Corrupted data – BaaS solutions combined with DRaaS are much more effective at bringing back data in a holistic way. Information loss is the number one cost component of recovering from a cyberattack.

Seamless recovery – The larger a company, the more complex a full recovery can be. Relying on a traditional backup solution gives your IT department the full responsibility for data retention and infrastructure examination.

Industry experts offer their views on the most significant modern threats and what can be done about them.

Felix Rosbach, Product Manager at comforte AG

With an ever-increasing attack surface, security is a constant struggle for data centres. While IoT enables us to analyse data like never before, every device represents a potential attack vector.

Aside from DDoS attacks and other methods of sabotage, the most painful type of cyberattacks are the ones involving theft of sensitive data. Stolen data is not only problematic in terms of reputation and losing IP, in the age of GDPR it can also result in very hefty fines.

There are two main problems:

First is malicious software: this is a battle that is extremely hard to win, especially with the digital workplace and smart devices connected to your data centre.

Second are backdoors: the bad guys always seem to find a way to get in somehow.

Sometimes systems aren't patched or it's simply impossible to patch a legacy system because there are dependencies on older software versions you would never have even thought of. Sometimes the OS is so dated it might no longer have active support available and security patches simply don't exist anymore.

For example, with backdoors on systems that are facing the Internet, attackers are able to launch web attacks like SQL injection, cross-site scripting or cross-site request forgery to gain access to sensitive data.

You can do a lot to protect your network with classic perimeter defence.

Firewalls, intrusion detection systems, patching unpatched systems, identifying servers that are listening on unwanted service ports – these things are still important. The days of 'never touch a running system' are way over – now it's 'you'd better touch a running system.'

But even if you buy every security solution possible you will never be 100% secure. These only protect you against known attack methods. But the more connections you have, the more complex your network is, the less effective is it to build a wall around it. Moving to the cloud, connecting to IoT and having digital workplaces in your enterprise only complicate the situation.

The way to go forward is to implement sophisticated identity access management in combination with data-centric security. With that combination you make sure that only the right people get access and, if somehow the wrong people still manage to gain access, they can't use the data.

Sachin Bhardwaj, eHosting DataFort, Director, Marketing and Business Development

The increasing use of Big Data and the onset of the Internet of Things has only added to the intensity of the need to prioritise cybersecurity within data centres. One is also mindful of the ongoing regulations and compliance needs that have shot up.

This sets the pace for a far more holistic approach to cybersecurity which comprises of a well-rounded security strategy that involves both governance and the operations angles. It includes a combination of information security, information system security as well as physical security. And the framework must be in a strong position to identify, protect, detect, respond as well as recover data.

At a time when attacks are only getting to be more sophisticated and increasing in numbers, there is evidently a gap in the requisite security professionals where

supply does not match demand. It is important that data centres keep pace with the changing threat landscape and minimise the risks.

Now is the time to ensure that data centres equip themselves with Artificial Intelligence (AI) and implement automation processes where the rate of identifying breaches is far higher. This will strengthen their threat detection capabilities, make them quicker to respond to threats and they will also be fortified with an analytical approach to cybersecurity.

It helps in developing a far more effective, efficient and agile security posture with the added ability to forecast future threats. Service providers and end customers are investing heavily in SOC capabilities for creating an enhanced cyberdefence environment against security threats and vulnerabilities. Visibility into the networks and the integration of advanced visual dashboards will enable clarity in what is transpiring between devices, will identify current and possible attacks as well as ensure that compliance requirements are being met.

Higher network visibility will provide greater communication flow between network operations and security operations teams and will be able to proactively identify and mitigate threats. Simultaneously, workloads tend to fluctuate and organisations may not be prepared for scalability which can hinder the security environment. This calls for strong network performance monitoring tools to help reduce threats by alerting security teams of any irregular network behaviour.

While a lot is being done by data centre owners to ensure that the networks, servers and endpoint devices are secured, there is also a need to pay heed to other aspects of security that include the cooling and heating systems, power supplies and the security systems.

Mathivanan Venkatachalam, Vice President, ManageEngine

Digital Transformation in the Middle East is on the rise, sparking the need for data governance and security. Last year, Gartner predicted that the region would reach US$155 billion in IT spending, up 3.4% from 2017, the highest increase for the region in the previous three years.

Cybersecurity has become a top priority for organisations as the average cost of a data breach across the globe was US$3.86 million in 2018. To mitigate these threats, data centres need to have robust security policies in place, improve their cyber-resilience and implement stronger security measures to ensure their customers' data is secure.

Data centres collect and store massive volumes of data from multiple sources, which makes them an attractive target for cybercriminals. DDoS attacks, web application attacks such as SQL injection and cross-site scripting (XSS), disruption of access to DNS servers or poisoning of DNS caches in a data centre, users being prevented from accessing vital services, brute-force attacks due to weak passwords and SSL-induced security vulnerabilities are some of the methods used by cybercriminals to steal data or take the servers offline.

Cyber-resilience mitigates attacks

Given these threats to the data centre network infrastructure, here are some best practices to help defend against cybercriminals.

Monitor the firewall: IT admins need to regularly monitor and analyse their firewall's syslogs and configurations, and optimise its performance to protect the network. Efficient syslog analysis can help identify security threats in real time and effective policy management can help prevent DNS spoofing, DDoS attacks and web application attacks.

Don't stop monitoring at the firewall: To gain insights into potential threats and stop them before they turn into an attack, IT admins need to also look into other log-generating devices in the network such as routers, switches, IDSs, and IPSs, application servers, databases and web servers. It is critical to correlate and analyse logs from all these sources to find security events of interest, such as user access, unusual activities, user behaviour anomalies, policy violations, internal threats, external attacks and data theft. A thorough analysis will help in preventing security attacks.

Keep an eye on configuration changes: The key to efficient network management is using an end-to-end change management tool to track and record all configuration changes made to network devices. Apart from this, security admins also need an alerting system that notifies them of all configuration changes in real time.

Encrypt and inspect your data traffic: Huge volumes of data travel between data centres and to protect this data from being intercepted, security admins need to use strong data encryption, and inspect outbound SSL traffic from internal users, as well as inbound SSL traffic to corporate servers, to identify any suspicious traffic. A combination of encryption and monitoring can save data centres from attacks exploiting SSL-induced security blind spots.

Set up stringent authentication control: Deploying a secure, centralised vault for password storage and access plays a key role in eliminating password fatigue and security lapses. Automating frequent password changes and generating real-time alerts on password access helps keep brute-force attacks in check.

Finally, conducting regular security audits and running regulatory compliance reports to identify and correct security vulnerabilities plays a key role in keeping data centres secure from attacks. ◊