IS YOUR DATA CENTRE READY FOR GDPR?

Luca Rozzoni, European business development manager, Chatsworth Products (CPI), discusses methods of ensuring compliance

While security has always been a key consideration for the data centre industry, the upcoming EU General Data Protection Regulation (GDPR) – a strict set of regulations set to protect data privacy – means that data protection and security policies have taken on a new level of priority.

REGULATORY AND COMPLIANCE REQUIREMENTS

The GDPR requirements will come into force on 25 May 2018 and affect organisations worldwide. While EU countries must comply, any organisation collecting or processing data for individuals within the EU should also be developing their compliance strategy. The UK Government has indicated that, even taking Brexit into account, it will implement an equivalent set of legislation and UK organisations must review their security practices in regards to the protection of personal data and consider their own routes to compliance.

HOW SHOULD DATA CENTRES PREPARE?

While organisations are expected to use their own judgment in regards to making sure they have taken the 'appropriate technical and organisational measures' to ensure compliance, Regulation (EU) 2016/679 stresses the need for secure IT networks, and provides an example of 'preventing unauthorised access to electronic communications networks and malicious code distribution and stopping "denial of service" attacks and damage to computer and electronic communication systems.' Put simply, while access control may seem an obvious part of any security policy, data centres must be able to demonstrate that they have the appropriate access policies in place.

Cabinet-level security has always been an important part of data centres' data protection and security policies. Strict regulatory compliance requirements, such as HIPAA in healthcare and PCI DSS in online retail, demand audit logs of every access attempt as part of physical access control to help ensure data privacy and security. Automatic logging of cabinet access is also important, given that a large portion of attacks within these industries (58% in the financial and 71% in the healthcare, to be more precise) are carried out by insiders advertently or inadvertently, according to a 2017 report by IBM X-Force.

This makes sole reliance on mechanical keys not effective at best and, at worst, has the potential of resulting in privacy-related lawsuits.

Electronic access control (EAC) solutions are essential in addressing user access management issues within the data centre and can be an extremely cost-effective method of delivering intelligent security and dual-factor authentication to the cabinet. Here are some of the key features to look out for when selecting an EAC solution...

DUAL-FACTOR AUTHENTICATION

Dual-factor authentication enables data security to be taken to the next level. One of the most secure forms of physical access verification is biometric authentication. However, many organisations have dismissed this in the past due to cost, as it typically requires additional readers to be installed to every cabinet or facility door.

A cost-effective and secure dual-factor authentication solution is a fingerprint-activated card that is able to work with existing EAC or other card-activated locks. A card that is compatible with readers for 125 KHz, HID ICLASS and MIFARE proximity cards and can work with existing campus security systems eliminates the need for expensive deployments and means data centre employees only need to carry a single card.

REMOTE MANAGEMENT AND REPORTING

Using a simple, user-friendly web interface to remotely manage the

Photo: Shutterstock

Luca Rozzoni joined Chatsworth Products (CPI) in 2015 as European business development manager, responsible for identifying and developing products and solutions that will enable CPI to further meet the needs of its customers in Europe. Originally from Italy, Rozzoni moved to the United Kingdom over 20 years ago to begin his career in the telecommunications industry.
Having studied electronic and electro-technic engineering, Rozzoni also holds a business degree in strategy development and implementation and is a BICSI-registered communications distribution designer (RCDD).

CONTACT CHATSWORTH PRODUCTS: 01628 524 834, www.chatsworth.com

networked EAC locks allows the user to remotely monitor, manage and authorise each cabinet access attempt. Crucially, using this type of intuitive interface provides an audit trail for regulatory compliance through log reports. The logging report can be easily exported and emailed to the administrator.

Managing the networked EAC locks through the web interface also reduces the need for wiring the electronic access systems to expensive security panels, which are usually managed through building management systems.

IP CONSOLIDATION

Data centres can realise dramatic savings in networking costs and deployment times through the ability to network several locks through IP consolidation. It is now perfectly feasible to choose a solution that will allow up to 32 EAC controllers (32 cabinets) to be networked under only one IP address.

COMBINING EAC WITH ENVIRONMENTAL MONITORING

Choosing an EAC solution that offers added benefits, such as environmental monitoring, can ensure a much faster return on any initial investment, especially when you consider the savings that can be made by utilising one IP port for an appliance that offers both EAC and environmental monitoring.

There are solutions available that can monitor and manage both temperature and humidity through the same web interface, issuing proactive notifications to help data centre managers ensure service reliability by taking action before issues turn into downtime.

The infrastructure can be badly affected by water, dust and other harmful particles so it is worth looking for a solution that also has the capability to monitor and detect smoke, water and even motion.

THE FUTURE

As outlined in Regulation (EU) 2016/679, 'rapid technological developments and globalisation have brought new challenges for the protection of personal data' and 'the scale of the collection and sharing of personal data has increased significantly'.

As a result, customers' needs and expectations regarding privacy of data have increased, as has the sophistication of the threats now posed. Data centres must look for more powerful and effective methods of delivering peace of mind to the customer as well as compliance to new and emerging regulations and electronic access control (EAC) solutions are a key weapon in their arsenal. Fortunately, delivering intelligent security and dual-factor authentication to the cabinet is no longer out of reach for organisations needing to meet strict budgets.