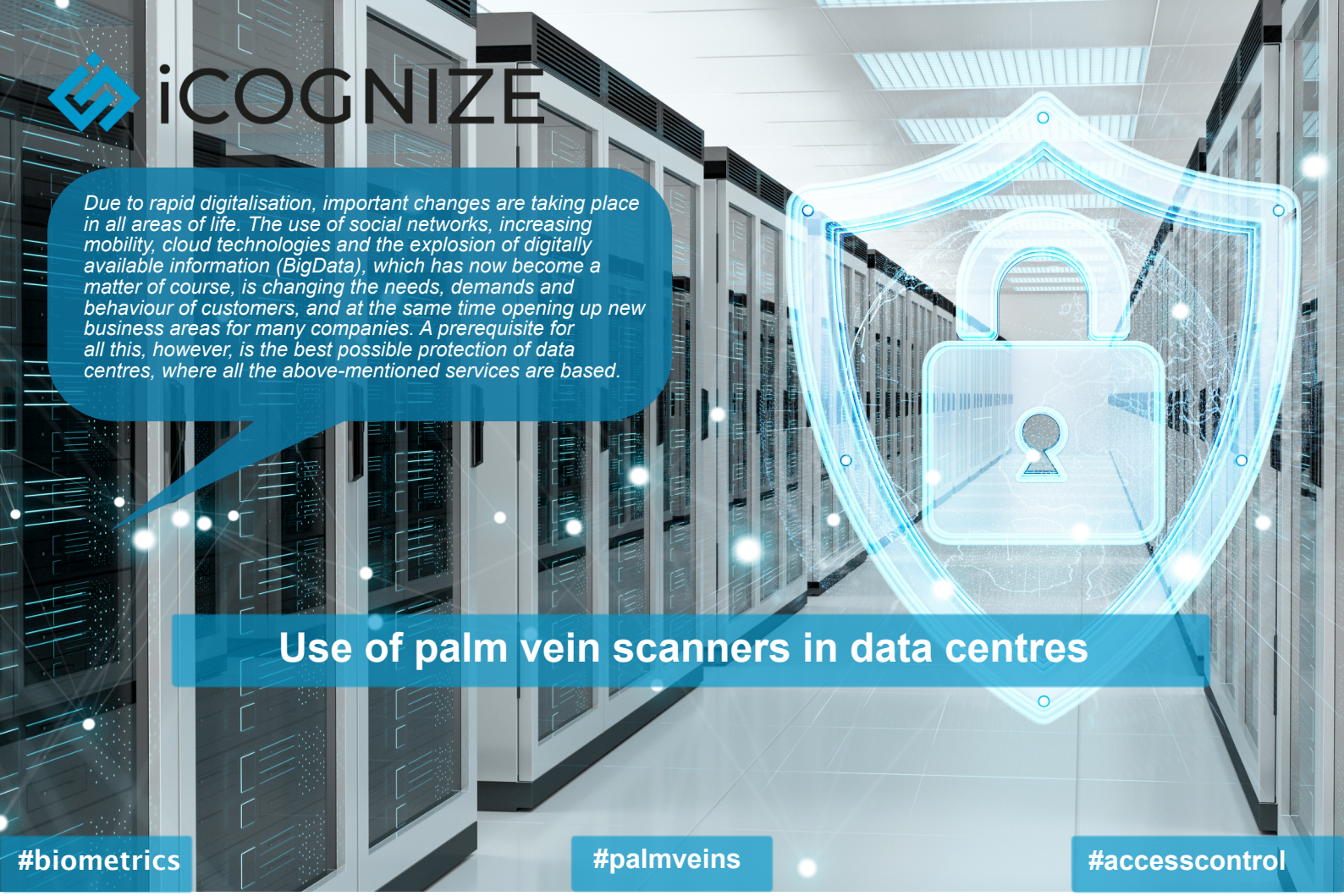

Due to rapid digitalisation, important changes are taking place in all areas of life. The use of social networks, increasing mobility, cloud technologies and the explosion of digitally available information (BigData), which has now become a matter of course, is changing the needs, demands and behaviour of customers, and at the same time opening up new business areas for many companies. A prerequisite for all this, however, is the best possible protection of data centres, where all the above-mentioned services are based.

Use of palm vein scanners in data centres

#biometrics #palmveins #accesscontrol

The challenge

Data centres, with their servers, storage and networks often containing many terabytes of data, form highly critical infrastructures.They are often crucial for the functioning of society, the economy and public life. It is enough to imagine that in the spring of 2020, during the coronavirus crisis, a data centre was paralysed by unauthorised access. The increasing demand resulting from digitalisation means that data – often from the private sector – are increasingly stored on servers in data centres and need to be well protected.

The operators of data centres are responsible for the function framework of the data centre, where special security measures begin at the entrance. For security reasons, access to data centres requires structured procedures. Access control should be regulated by several parallel procedures. Suitable access criteria include possession (e.g. ID card), knowledge (e.g. PIN code) and characteristics (e.g. biometric features). All procedures – both successful and unsuccessful – should be recorded and the records stored. Due to data protection requirements, the “Template on Card” method is often used in data centres. It means that the scanned palm vein pattern is stored on the employee's ID card. Data is not stored in a database, so each user always carries their biometric data with them.

It is also important to record both entry to and exit from the data centre, in order to revoke temporary access authorisations and to be able to refuse renewed entry if the exit procedure was not correct. Minimising the risks and preparing data centres for emergency situations as well as complying with legal requirements and

and to be able to refuse renewed entry if the exit procedure was not correct. Minimising the risks and preparing data centres for emergency situations as well as complying with legal requirements and country-specific audit regulations require data centre operators to create a close link between the IT and physical security of the building.

Legal requirements / guidelines

According to §8a BSIG, operators of critical infrastructures (KRITIS) are obliged to prove that their IT security system is state-of-the-art. Increasing numbers of the systems we rely on are digital or are becoming digitally assisted in one way or another. It makes the infrastructure smarter, faster and more precise, but also more vulnerable. According to the Federal Office for Information Security (BSI), operators of critical infrastructure are therefore obliged to provide the highest possible level of security. In terms of data protection, it must be ensured that personal data are stored securely against misuse and are not freely accessible.

iCOGNIZE GmbH
Justus-von-Liebig-Straße 9
63128 Dietzenbach

+49 (0) 6074 310 3600

https://www.icognize.de
info@icognize.de

For the orientation of data centre operators, the European EN50600 standard was created concerning data centre equipment and infrastructure. This European standard specifies the requirements and includes recommendations for operating data centres according to EN 50600-1 and the security systems used in these centres in terms of:
a) unauthorised access, by identifying structuring, organisational
and technological solutions
b) fire within data centres
c) environmental incidents other than fire, including
electromagnetic interference, vibration, flooding, gas and dust hazards:
– inside data centres;
– outside data centres.

Solutions by iCOGNIZE

The security concept of a data centre includes a multi-level, biometric access control. The iCOGNIZE GmbH products and solutions can make an important contribution to the implementation of an advanced security concept.
Contactless access control using palm vein scanning.

The Manuscan Palm Vein Scanner can be installed in the same way as an ordinary light switch: in a standard flush-mounted box. Power is supplied via Ethernet (PoE). The scanners are connected to a top-hat rail capable Authentication Unit (AU) operated from a separate secured IT room, mounted in a 19” rack. It can be easily integrated with existing security infrastructures through all common hardware interfaces and ensures maximum system availability thanks to the in-built software and hardware backup systems. In the case of positive authentication (by scanning the palm veins in connection with RFID and/or optionally entering a PIN code) a compatible signal is given to the existing access control and logging systems as feedback.

“In this way we can secure sensitive doors with palm vein scanners without having to replace the entire access control infrastructure,” Dr. Alexander W. Lenhardt, CEO of iCOGNIZE

With the unique biometric “palm veins” feature, this system offers the user not only maximum security but also the highest level of comfort. The ManuScan indoor palm vein scanner operates without the need for physical contact and in a non-invasive way, while its unique optical hand locating system ensures intuitive use and a high level of user acceptance.

Advantages of the **ManuScan indoor palm vein scanner**

– RGB-LED user guidance
– more reliable than an iris scanner
– FAR < 0.00008% (false acceptance rate)
– FRR < 0.01% (false rejection rate)
– sabotage detection (contact, shock)
– control of rack locks, for example Fath Mechatronics
– easy integration with existing systems
– in-built PIN code reader
– CE- and BSI-certified (components)

The outdoor version of our palm vein scanner is the first palm vein detection solution for outdoor use and meets EMC and EMP military. The V2A housing is resistant to all weather conditions and even sea water, is extremely robust and, with its integrated thermal management, suitable for temperatures from -35° to +85°.

Advantages of the **ManuScan Outdoor palm vein scanner**

– can be used in almost any environment
– very user-friendly
– more reliable than an iris scanner
– FAR < 0.00008% (false acceptance rate)
– FRR < 0.01% (false rejection rate)
– easy integration with existing systems
– IP68 standard
– CE- and BSI-certified (components)

Advantages of using both products

– PIN codes can be stolen or passed on, which cannot happen with the contactless access systems by iCOGNIZE.
– Contactless scanners can also be used with hygiene gloves to ensure a high standard of hygiene.
– Maintenance only once per year.

References

A large number of our products have been installed in the world's largest (in terms of data throughput) Internet node in Frankfurt am Main, significantly contributing to the security of this critical infrastructure. For further information, please contact us at any time.

iCOGNIZE GmbH
Justus-von-Liebig-Straße 9
63128 Dietzenbach
+49 (0) 6074 310 3600
https://www.icognize.de
info@icognize.de