DRACOON

Date: *June 21, 2019*
Source: Krankenhaus IT-Journal: (issue 3/2019 from 21.06.2019)
https://www.dracoon.com/wp-content/uploads/2019/07/190715_Clipping-KH-IT-Journal.pdf

Press Report

A statement by Arved Graf von Stackelberg, Managing Director DRACOON

Regarding the implementation of the CRITIS regulation in the health sector: hospitals must act urgently

On June 30th of this year the time has come: Numerous German clinics must implement the CRITIS regulation of the BSI (Federal Office for Information Security) by this date. The law covers a total of eight industries which the BSI considers to be particularly attack-relevant and worthy of protection due to the operation of critical infrastructures. After all, the term "critical infrastructure" covers organizations that play a major role in the state community.

The BSI-CRITIS Regulation (also known as "Korb I" ("Basket I")) and the first Amendment Regulation (known as "Korb II" ("Basket II")) regulate who exactly the law concerns. Transparent criteria are used here to determine which operators in the fields of energy, water, information technology and telecommunications, nutrition, health, finance and insurance, as well as transport and traffic are obliged to provide the authorities with evidence in accordance with the BSI Act (§ 8a). For the health sector, this means that hospitals with more than 30,000 fully inpatient cases per year are regarded as "CRITIS" operators. Treatment is considered to be fully inpatient if the patient is hospitalized day and night and makes full use of the inpatient services. In Germany, about 33 % of all clinics are affected by this.

A number of requirements must be met by the deadline of just less than two weeks – on the one hand, proof of suitable IT security precautions must be provided every two years. On the other hand, a contact point or a functional mailbox must be designated by the company, and IT malfunctions must be reported to the Office immediately. On a technical level, it must be ensured that the healthcare companies concerned meet the latest technical standards and the testing standards of the federal authorities.

A recent study on IT security in the health sector commissioned by the German Insurance Association (Gesamtverband der Deutschen Versicherungswirtschaft – GDV) shows how important the new regulation is. For example, a test of mail servers with the analysis tool Cysmo revealed that patient data is often not stored securely in German clinics and doctors' practices. A total of 250 clinics and pharmacies were examined in addition to the IT systems of around 1,200 general practitioners. The alarming result was that only 5% of the clinics used a secure encryption standard recommended by the BSI. 31% used the outdated SSL 2 and SSL 3 standards, about 63% the TLS 1.0 or TLS 1.1 standards no longer recommended by the federal authorities. The study's findings that 60% of the clinics e-mail and password combinations were found in the dark net were particularly alarming. Given these figures, it is

not surprising that 64% of the 500 clinics surveyed have already been the victims of a hacker attack, as a large-scale Roland Berger survey published two years ago revealed. These figures indicate that the problem of IT security deficiencies in the healthcare sector is a structural one. In this respect, it is essential that clinics respond and adapt to the new challenges posed by increasing digitization.

Above all, however, with regard to the “state of the art” aspect required by the BSI, German hospitals urgently need to retrofit and implement a uniform contemporary solution. Here, a major role is played by seamless client-side data encryption, which is used to encrypt the information at the end device. This means that not even the manufacturer of the solution has access to stored data. It also makes sense to choose a software solution “Made & Hosted in Germany”. German providers are subject to the strict German data protection laws and at the same time ensure that the solution also complies with the EU GDPR. Corresponding certifications and awards, such as ISO27001, provide additional support for conformity. It is also important for authorized persons to be able to track at any time which data was processed when and by whom. This is the only way to detect and prevent uncontrolled data outflows.

A detailed rights system also regulates who can access and process which data. If the solution has also integrated ransom ware protection, which allows damaged data to be restored promptly, maximum data security and protection is guaranteed. Clinic operators have to take the risk seriously overall and deal with the implementation of a technically up-to-date solution – this way, they are prepared for the future fight against cyber criminals and avoid devastating fines within the framework of the BSI-CRITIS regulation. Even patients can be sure that their sensitive data is in good hands and will not be compromised.

For more information on CRITIS visit: https://www.dracoon.com/de/kritis/