Rohde & Schwarz Cybersecurity

IT SECURITY IN HEALTHCARE

Investing in the smart hospitals of the future

ROHDE & SCHWARZ

Make ideas real

TABLE OF CONTENTS

INTRODUCTION

The subject of this brochure is the extensive IT security ecosystem in hospitals, composed of infrastructure, software, systems and terminal devices in equal measure. The objective of cybersecurity is to secure the associated components. This brochure is intended to give healthcare employees an in-depth overview of how to achieve and maintain cybersecurity goals. It discusses various topics and regulations, which are in a constant state of change and are only as good as the persons who implement and apply them.

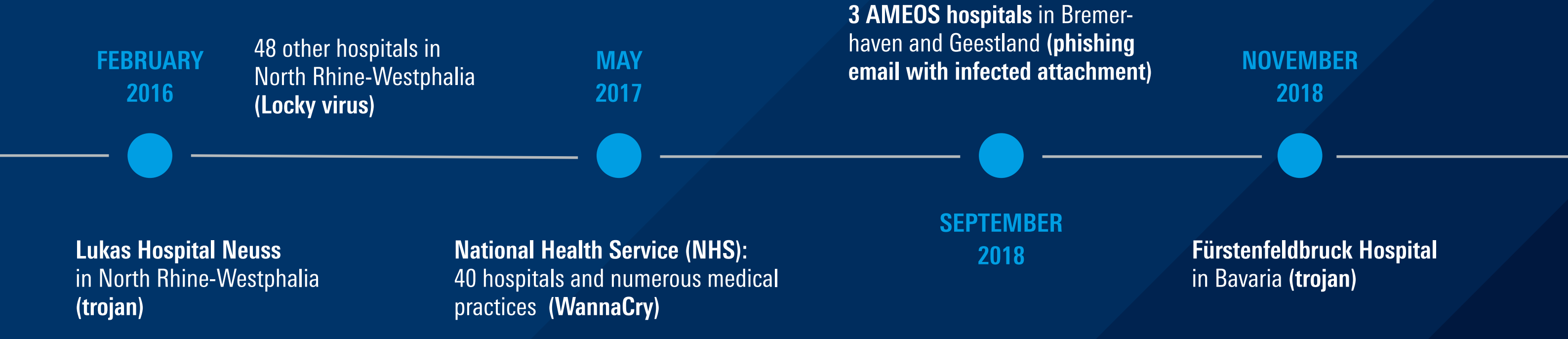
This brochure is aimed at employees working in technical positions in healthcare, in particular those in management positions such as CIO, CISO, CTO and in IT teams, as well as those entrusted with procurement in healthcare organizations.

Hospitals provide medical treatment and nursing care to persons with injuries and illnesses. As institutions with special importance for public health, they are part of the critical infrastructure (CI) of our society. Outage, impairment and disruption of hospitals must be avoided to ensure the availability of services and processes. Modern medical care and digital solutions are an integral part of this. Digitalization offers the healthcare sector more efficient and higher-performance systems. However, these are also subject to attacks that threaten the common good.

Hospitals can be attacked in many different ways. They are vulnerable to the outage of important sources of energy or utilities, such as electricity or water, as well as natural disasters[1]. Modern medical care using IT applications and EHR systems is part of the everyday life of medical practitioners. The goal is optimal care of patients. Protecting these applications is a core concern because they must function reliably in life-threatening situations. This applies, for example, to communications between computer tomography equipment, ventilation equipment, anesthesia equipment and medication control. Ideally, digitalization has the potential to reduce costs and ensure efficiency in hospital processes.

The more areas within a hospital that are optimized by IT systems, the more they become potential attack targets. Hospitals have been specifically attacked in recent years; they are not immune to security incidents and outages.

[1] http://www.tagesspiegel.de/weltspiegel/ueberschwemmungen-chaos-inmittelhessen/753824.html



FEBRUARY 2016

Lukas Hospital Neuss
in North Rhine-Westphalia
(trojan)

48 other hospitals in
North Rhine-Westphalia
(Locky virus)

MAY 2017

National Health Service (NHS):
40 hospitals and numerous medical
practices **(WannaCry)**

SEPTEMBER 2018

3 AMEOS hospitals in Bremerhaven and Geestland **(phishing email with infected attachment)**

NOVEMBER 2018

Fürstenfeldbruck Hospital
in Bavaria **(trojan)**

Fig. 1:

The Electronic Medical Records Adoption Model (EMRAM) describes the degree of digitalization in hospitals. It distinguishes seven stages, ranging from limited supplementary departmental systems to a fully paperless EMR environment.[2]

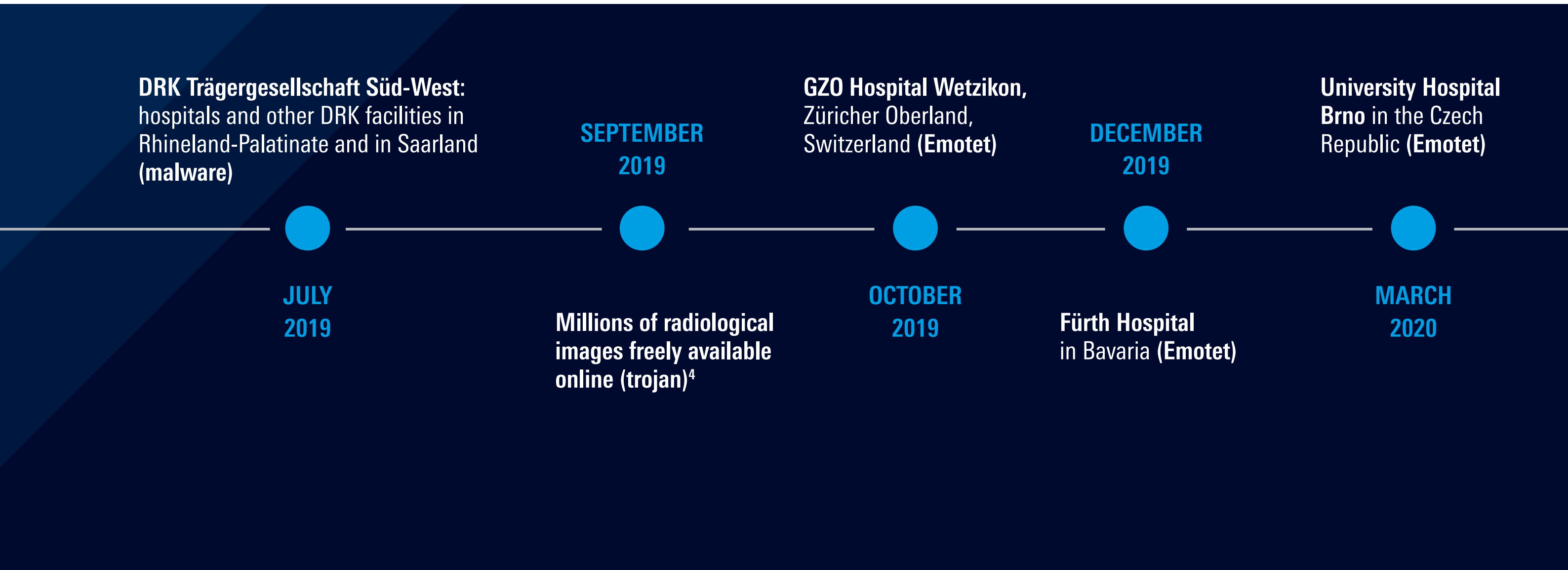
A total of 66 hospitals in Europe are now at EMRAM Stage 6 or Stage 7, including 6 in Germany, Austria and Switzerland.[3]

STAGE 7	Seamless ePA integrates all hospital departments (outpatient, intensive care, emergency, etc. and replaces all (medical) paper documents); deployment of data exchange standards for integrated care; clinical and operational analyses based on a data warehouse
STAGE 6	Clinical documentation integrated with smart clinical decision support (based on discrete data elements) and the presence of an IT based closed-loop medication process
STAGE 5	Integrated image management solution (e.g. PACS) displaces all film based images
STAGE 4	Electronic ordering with clinical decision support (based on a rules engine) in at least one clinical department and for medication
STAGE 3	IT based clinical documentation and deployment of electronic ordering by physicians or care staff; also includes medication documentation (eMAR)
STAGE 2	Electronic patient files (or a clinical data repository) enable the collection and normalization of data from various clinical sources in the entire hospital
STAGE 1	Information systems for major diagnostic and care departments (laboratory, radiology, pharmacy) are installed, or data from external service providers can be processed in electronic form
STAGE 0	Information systems for major diagnostic and care departments (laboratory, radiology, pharmacy) not installed, or data from external service providers cannot be processed in electronic form

[2] https://www.himss.eu/himss-taxonomy-topics/electronic-health

[3] https://www.himssanalytics.org/europe/stage-6-7-achievement

[4] https://www.sueddeutsche.de/digital/patientendaten-netz-sicherheit-1.4604064



JULY 2019

DRK Trägergesellschaft Süd-West: hospitals and other DRK facilities in Rhineland-Palatinate and in Saarland **(malware)**

SEPTEMBER 2019

Millions of radiological images freely available online (trojan)[4]

OCTOBER 2019

GZO Hospital Wetzikon, Züricher Oberland, Switzerland **(Emotet)**

DECEMBER 2019

Fürth Hospital in Bavaria **(Emotet)**

MARCH 2020

University Hospital Brno in the Czech Republic **(Emotet)**

1 MANAGING IT SECURITY IN HOSPITALS

REGULATIONS AND DIRECTIVES

An attack on healthcare equipment, applications or infrastructure would certainly have disastrous consequences for the medical care of societies. Adoption and mandatory implementation of statutory regulations for IT security and data protection are therefore necessary. This includes the development of methods for processing and storing personal data, as well as securing networks, endpoints, clouds and collaboration tools.

Patient care must be reliably ensured, and it is necessary to protect the IT infrastructure as well as patient safety and data. The statutory requirements regarded as especially important for hospitals are described below.

Fig. 2:
Critical infrastructures are subdivided into the following sectors[7]

Critical infrastructure sectors
ENERGY
WATER
HEALTH
Laboratories Pharmaceuticals and vaccines Medical services
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS
FOOD
FINANCE AND INSURANCE
TRANSPORT AND TRAFFIC
GOVERNMENT AND PUBLIC ADMINISTRATION
MEDIA AND CULTURE

Sector-specific security standard for healthcare in hospitals (B3S)

The German Hospital Federation (DKG) presented the security standard B3S[5] for hospitals to the German Federal Office for Information Security (BSI) as a guideline applicable to hospitals with more than 30,000 full inpatient admissions per year. It describes technical and organizational processes as well as more than 160 measures to ensure resilient IT and reliable patient care, such as an information security management system (ISMS) with risk management or process-oriented emergency planning in the framework of business continuity management.

The B3S standard serves primarily to protect the technical infrastructure, which enhances achievement of security goals as well as patient security and treatment effectiveness.

The recommended actions are guided by the BSI provisions and aligned to the requirements of the international standards for information security ISO 27001 and ISO 27799, which are valid to 2021-08-16. The B3S document can be downloaded from the DKG website.[6]

[5] https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Was_tun/Stand_der_Technik/B3S/B3S.html;jsessionid=756D3A0E6D47BEF4A4D194ADE2C33DDB.1_cid360?nn=6776460#doc8140926bodyText10

[6] https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/2019-04-02_B3S_KH_v1.0_-_Gesamtdokument.pdf

[7] https://www.kritis.bund.de

According to the German federal government, all facilities whose outage or impairment would result in persistent care shortages, considerable impairment of public security or other dramatic consequences, are critical infrastructure according to the definition of the national strategy for the protection of critical infrastructure.[8]

Critical infrastructures | Classification in the hospital sector

Self-classification is legally required, which means that hospital operators must decide whether they belong to vital critical infrastructure as part of the healthcare sector subject to the legislation. For hospitals, the defined threshold for critical care infrastructure is 30,000 full inpatient treatment cases per year. This encompasses several hundred hospitals in Germany.

Patient data, as a form of personal data, especially needs protection, making data protection in hospitals essential. Subjects such as digital patient files are therefore at the center of public perception with regard to IT security in hospitals. From a CI perspective, however, the main concern is not data protection, but instead ensuring secure medical care.

This means that hospital operators have a special duty of care with respect to the population. This includes knowledge of processes in the event of a loss of functional capability – such as emergency plans.

GDPR

The European General Data Protection Regulation (GDPR) has been in force for more than two years, and the healthcare sector is basically subject to the same data protection rules as other sectors. However, requirements for confidentiality and data protection are higher for hospitals and medical facilities.

Processing of personal data is an essential part of the activities in hospitals and healthcare facilities. From a data protection perspective, according to Article 9 of the Data Protection Regulation this belongs to a special category of personal data and therefore needs special protection. This means that as a rule this data can only be processed with the consent of the person concerned. According to Article 32 of the GDPR (Security of processing), appropriate technical and organizational measures must be taken to ensure an appropriate level of protection.

[8] https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html

Technical and organizational impact of digitalization in hospitals – GDPR (extract):

- Pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- No unauthorized system use, secure passwords, automatic blocking mechanisms, two-factor authentication, encryption of data storage media
- Permission concepts and need based access permissions, logging of accesses
- Separation control
- Separate processing of data collected for different purposes, e.g. client capability and sandboxing
- Transfer control
- Determination of whether and by whom personal data is entered, modified or deleted in data processing systems, e.g. logging and document management
- Protection against accidental or intentional destruction or loss, e.g. backup strategy (online/ offline; on-site/ off-site), uninterruptible power supply (UPS), antivirus, firewall, and emergency plans
- Resilience

If the requirements are not fulfilled, the GDPR provides for fines up to EUR 20 million or, in the case of an enterprise, up to 4 % of total worldwide sales revenue in the previous fiscal year, whichever is higher, and in Germany EUR 50,000 for NIS violations.

Directive to ensure high security of networks and information (NIS Directive)

To harmonize regulations for cybersecurity within the European Union, the Directive on the Security of Networks and Information (NIS Directive) was adopted in 2016. The objective is to achieve a high level of security for IT systems, compliant with the state of the art, in order to limit technical outages and attacks.

All essential information systems within a hospital must be protected in a separate area of the information system.

If these applications are stored outside the hospital, they must be authenticated, data transmission must be encrypted, and stored data must also be encrypted.

As operators of designated essential services, entities in the healthcare sector, which means hospitals and private clinics, are subject to the NIS Directive. The previously mentioned regulation for the determination of critical infrastructure (CI) complements this directive and defines specific application areas. All essential information systems within the hospital must be protected in a separate area of the information system. If these applications are stored outside the hospital, they must be authenticated. Data in motion (transmitted data) and data at rest (stationary data) must be encrypted.

Cloud Act

The US Congress adopted the Clarifying Lawful Overseas Use of Data Act (Cloud Act) in early 2018. This act primarily deals with the transfer of data to foreign countries, with the protection of personal data defined as a secondary consideration

– even when this data is stored in countries outside the USA.

This contradicts the GDPR, which says that protection of personal data is the highest priority. To avoid violating this directive, hospitals and all healthcare facilities that make use of cloud computing and SaaS services should employ European processors that are not subject to the Cloud Act.

Technical and organizational impact of digitalization in hospitals – NIS

Hospital operators must take IT security measures conforming to the state of the art, which includes the use of cloud computing services and reporting disruptions of these services with considerable impact on availability. Individual security measures are defined at the national level.

In contrast to periodic checking of compliance with the NIS Directive by CI operators every two years, providers of digital services are subject to monitoring after the fact, which means only after specific indication of noncompliance with security requirements.

In Germany, emergency teams for disruptions are identified as Mobile Incident Response Teams (MIRT) under the jurisdiction of the German Federal Office for Information Security (BSI). In specific cases, CI operators must request support from the BSI to restore the security and functional capability of their IT systems. The BSI can formally request the cooperation of hardware and software manufacturers for the restoration of IT systems.

Hospitals are additionally subject to the provisions of BSI IT Basic Protection or ISO 27001 and ISO 80001. Each requirement includes measures that must be implemented. These requirements for information security, data protection and IT emergency planning pose major challenges for project owners and managers in the healthcare sector.

2 RISKS TO IT SECURITY IN HOSPITALS

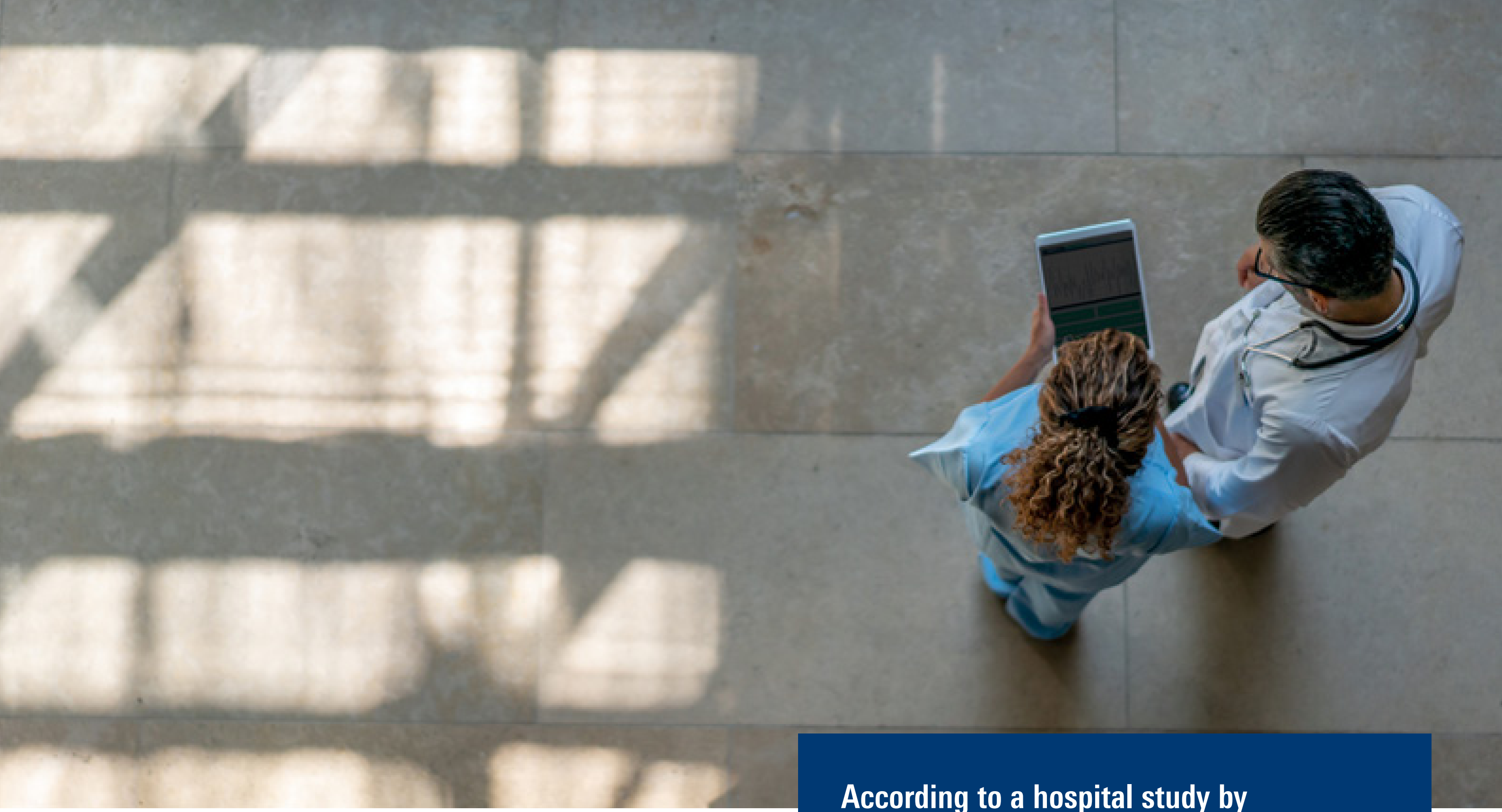
Hospital operators must take IT security measures “conforming to the state of the art,” which is not a legally defined term. For orientation, we have compiled an overview of IT security risks:

- Every networked terminal device in a hospital is a potential entry point for attackers
- Networks and systems that have grown over years and for which IT security is a secondary consideration
- Firmware updates that cannot be installed in operation or that contain harmful code
- IT systems vulnerable to online attack[9] [10]
- Insufficient budget to implement IT security as an essential link between medical and IT equipment
- Lack of awareness of the critical context of operations in the hospital network – and basic care, as well as disgruntled employees
- And the top 10 health technology hazards for 2018[11]
  - Ransomware
  - Missed security alarms due to incorrectly configured secondary notification devices and systems

Fig. 3:
Affected web applications in the healthcare sector

CLOUD-WEBSITES AND APPS	WEBMAIL AND COLLABORATIVE APPLICATIONS	BUSINESS APPLICATIONS	WEB SERVICES AND API
Scheduling Appointments Previous admissions Images Test results	Message handling SharePoint™	Directories Images Biology Pathology Electronic patient file (ePA)	Mobile apps Regional ePA feed Healthcare hosters Medical technology systems

[9] https://www.heise.de/security/meldung/Tausende-medizinische-Geraete-aus-dem-Internet-angreifbar-2831620.html
[10] https://www.golem.de/news/it-sicherheit-lebenswichtige-medizinische-geraete-ungeschuetzt-im-internet-1509-116563.html
[11] https://www.ecri.org/Resources/Whitepapers_and_reports/Haz_18.pdf



Application security in healthcare

IT security gaps in applications in the healthcare sector can have devastating consequences. The more applications are deployed, the greater the potential threat from those that are externally accessible because they can be controlled over the web.

According to a hospital study by Roland Berger in 2017, 64 % of German hospitals have already been victims of cyberattacks. This includes active attacks over the internet as well as incautious use of applications infected by viruses or trojans.[12]

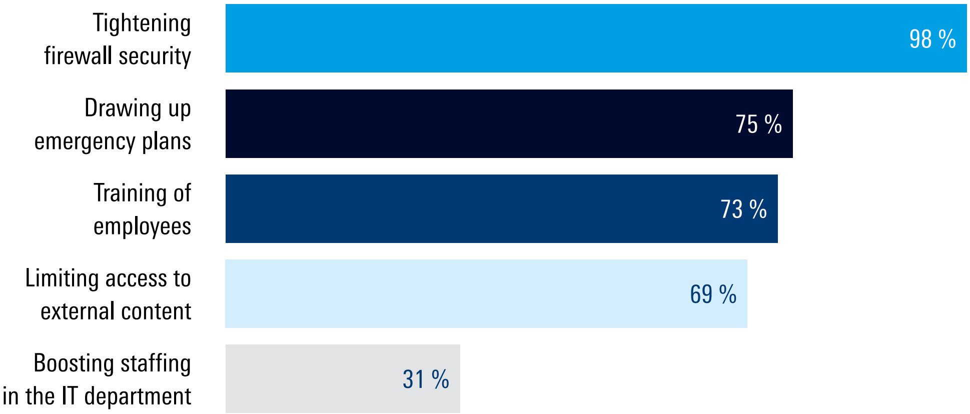


Fig. 4:

Measures taken by German hospitals for protection against unauthorized data access[13]

[12] https://www.rolandberger.com/publications/publication_pdf/roland_berger_krankenhausstudie_2017.pdf

[13] https://www.rolandberger.com/publications/publication_pdf/roland_berger_krankenhausstudie_2017.pdf

TYPICAL VULNERABILITIES

#1 OPERATING SYSTEM COMMANDS

Commands from the host operating system routed via a vulnerable web application.

#2 BYOD (BRING YOUR OWN DEVICE)

BYOD without rules forms an additional risk.

#3 CROSS-SITE SCRIPTING

Attackers insert a harmful scrip in a vulnerable web application that is displayed to other users. This script can redirect users to other websites or steal login details.

#4 CYBER ESPIONAGE

Competing interest groups ferret out results of clinical research and/ or patient data.

#5 DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

Authorized users are denied access to services. DDoS attacks attempt to slow down or even crash resources hosting web applications or websites, such as servers. DDoS attacks are also used to divert attention from other attacks on networks, which can be much more harmful.

#6 THEFT OF DATA UND ENDPOINTS

Medical devices are expensive, and theft is widespread. Small to medium-size portable devices, such as ultrasound devices, ECG instruments, defibrillators, infusion pumps and vital parameter monitors, should preferably not save any medical data.

#7 DIRECTORY TRAVERSAL (PATH TRAVERSAL OR FORCEFUL BROWSING)

This traversal occurs when an attacker sends an HTTP request using manipulated path data in order to obtain unauthorized access to higher-level directories and view the contents of confidential files.

#8 HIJACKING (CRYPTOJACKING & MEDJACKING)

In cryptojacking, attackers use computers, smartphones, tablets or servers without the consent or knowledge of the user to mine cryptocurrency at the expense of the victim. The difference between cryptojacking and medjacking is that the former uses general IT infrastructure, while the latter uses IT based medical devices.

#9 IDENTITY THEFT

The identities of employees or patients can be stolen. Assuming the identity of a doctor or a nurse, for example, allows fraudulent prescriptions to be issued or carries the risk of false diagnoses. In the latter case, this can lead to social fraud or result in false diagnoses.

#10 DATA LEAKS

These attacks target confidential data that can be displayed by the system, such as error messages and comments in HTML code.

#11 INSIDER ATTACKS

Doctors, nurses, administrators, maintenance employees, and other hospital staff members, as insiders, can pass on patient data, as can patients or visitors because hospitals are open 24/7 and comprehensive physical access control is not possible.

#12 IT SYSTEMS

IT systems in hospitals are highly networked and difficult to separate without impairing functionality.

#13 LOCAL FILE INCLUSION (LFI)

Attackers acquire access to external servers. Attackers send HTTP requests in order to access unauthorized data. Instead of the content of the file, harmful code is executed on the target system.

#14 RANSOMWARE

Infected healthcare infrastructure
1) Software infrastructure is difficult to keep up to date or get slots for downtime
2) Computers running legacy software that only works under specific operating systems or with specific driver versions are easy attack targets.. Outdated devices that can scarcely be updated act as a reservoir for malware distributed in the network.

#15 SOCIAL ENGINEERING (PHISHING)

Compromised emails (phishing, spam and spearphishing) are one of the main attack vectors for malware infections. Many healthcare facilities allow access to personal email web accounts on hospital computers.
Email addresses of doctors can easily be found in public directories of hospitals or existing presentations. This is aggravated by the use of professional email accounts for personal matters and the use of personal email accounts for professional matters.

#16 SQL INJECTION

SQL is a programming language for communicating with databases to retrieve or modify data, for which reason it is often used in web applications. Attacks take the form of SQL entries in text boxes, for example in an online form. The objective is to capture or manipulate data.

#17 WEB BASED ATTACKS

Updates where an attempt is made to retain system configurations in order to reduce downtime make it easier for attackers to exploit vulnerabilities.

#18 XML INJECTION

Like SQL injection, XML injection manipulates a web application by inserting harmful XML code in place of legitimate form data.

Consequences:

- **Loss of reputation due to unavailability or impaired access to systems**
- **Loss of income and care bottlenecks due to outage of critical services**

3 ROHDE & SCHWARZ CYBERSECURITY SOLUTIONS

Although operators of healthcare facilities, in particular hospitals, are aware of the importance of a functional cyber defense system for medical devices, operational implementation is not progressing as quickly as desired.

By strengthening their IT security policy, healthcare facilities can demonstrate compliance with official requirements and fulfill the rising expectations of service providers and their patients.

The solutions from Rohde & Schwarz Cybersecurity cover all aspects of application security, access to healthcare applications, and protection of health-related data.

They ensure easy integration without impacting the productivity of existing systems. With its solutions from a single source, Rohde & Schwarz Cybersecurity ensures the implementation of national and European legal requirements.

Rohde & Schwarz Cybersecurity can support hospitals in four areas with regard to the previously mentioned threats.

DR. T. J
GENERAL PRACTITIONER

APPLICATION SECURITY: R&S®WEB APPLICATION FIREWALL

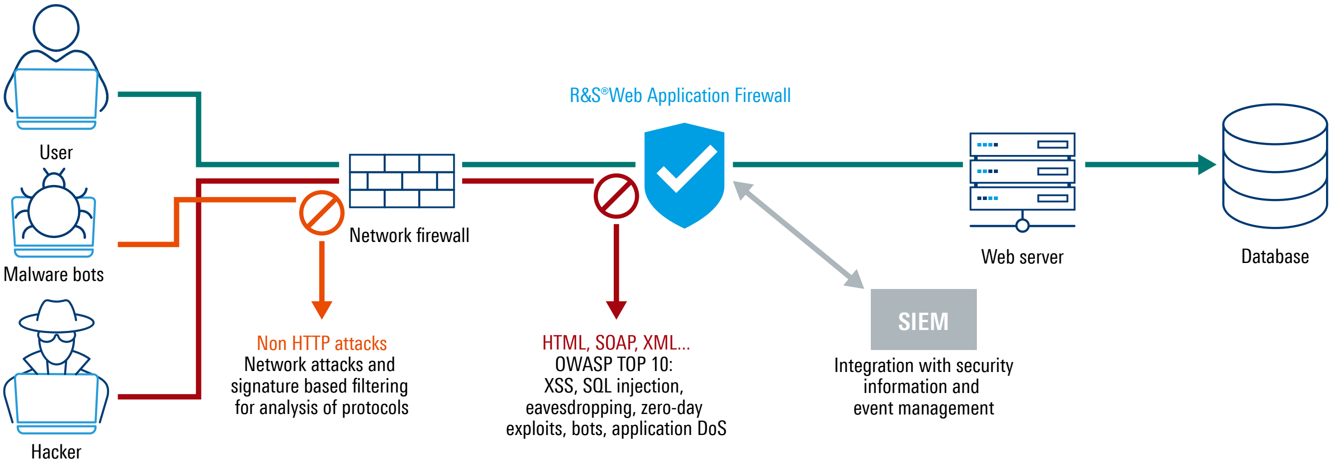
Plays a key role in the definition and implementation of an application security strategy in the healthcare sector. It protects critical web applications (legacy applications), web services (Microsoft® Outlook Web Access™, Exchange™, SharePoint™, SAP) and API against known and unknown attacks, including OWASP Top 10. Certified by the French cybersecurity authority ANSSI.

Its pooling mode allows critical hospital services and systems to be operated in an isolated zone with enhanced security (NIS compliant). The solution is fully scalable, can be implemented locally or in the cloud, ensures that healthcare data storage is stored in compliance with a high standard of confidentiality and integrity, and ensures the safeguarding of web applications and API transactions.

BENEFITS:

- ▶ Protocol layer protection 7
- ▶ Technology independent; allows use of multi-cloud or hybrid cloud deployments
- ▶ Extended API security enables the benefits of modern agile, API based development while remaining secure and compliant
- ▶ Protection against the OWASP Top 10

Fig. 5:
Effective security against a multitude of attacks, including automated attacks (bots)


User
Malware bots
Hacker
Network firewall
R&S®Web Application Firewall
Web server
Database
SIEM
Non HTTP attacks
Network attacks and signature based filtering for analysis of protocols
HTML, SOAP, XML...
OWASP TOP 10:
XSS, SQL injection, eavesdropping, zero-day exploits, bots, application DoS
Integration with security information and event management

NETWORK SECURITY: R&S®SITLINE ETH

Protects sensitive healthcare data against espionage and manipulation. Layer 2 encryption, compliant with modern methods and standards secures communications and data over Ethernet via landline, radio relay and satellite links. The encryptor significantly reduces operating costs while enhancing security.

Ideal for remote diagnostic purposes (real-time application) or as an alternative to data encryption for exchange between different hospital locations

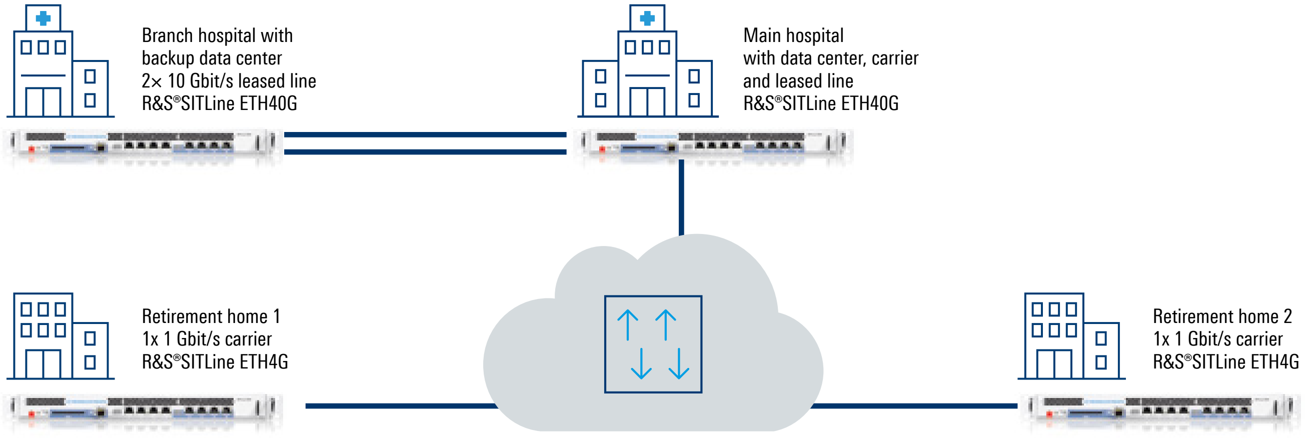
The devices are approved by the German Federal Office for Information Security (BSI) up to security levels NfD, NATO Restricted and EU Restricted.

BENEFITS:

- High speed Layer 2 encryption
- Advanced cryptographic algorithms and standards
- Central network management and monitoring
- Low power consumption and low system costs

Fig. 6:

Preconfigured encryption for leased lines establishes automatically encrypted L2 connections over Fast Ethernet on startup



CLOUD SECURITY: R&S®TRUSTED GATE

Ensures security and data protection in public clouds and collaboration tools. Many healthcare facilities have opted for Microsoft® Office 365™ to benefit from the advantages of the cloud.

Thanks to dynamic encryption technologies and virtualization, the solution fulfills the highest security standards for the protection of health-related data, and it can be used in hospitals and other healthcare facilities in compliance with applicable data protection regulations without compromising performance (secure full-text search) or flexibility.

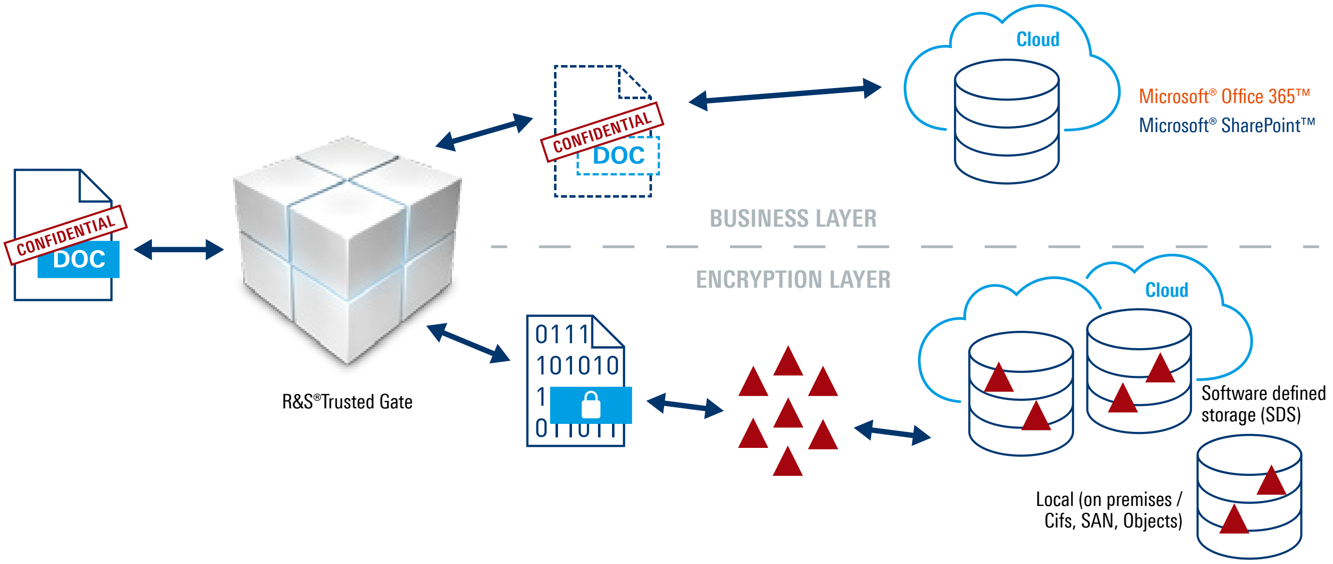
The encryption mechanisms of R&S®Trusted Gate are seamlessly integrated in Office 365™ solutions. Healthcare employees can continue using their apps in Office 365™ as usual.

Fig. 7:

Secure collaboration in the cloud: original data is encrypted and fragmented before it is placed in a configurable storage system

BENEFITS:

- Compliance with data protection requirements when working in a public cloud
- Working effectively and securely in cloud applications
- Solutions for public clouds and collaboration tools
- Infrastructure optimization by virtual mirroring, on-premises or multi-cloud



DESKTOP SECURITY: R&S®BROWSER IN THE BOX

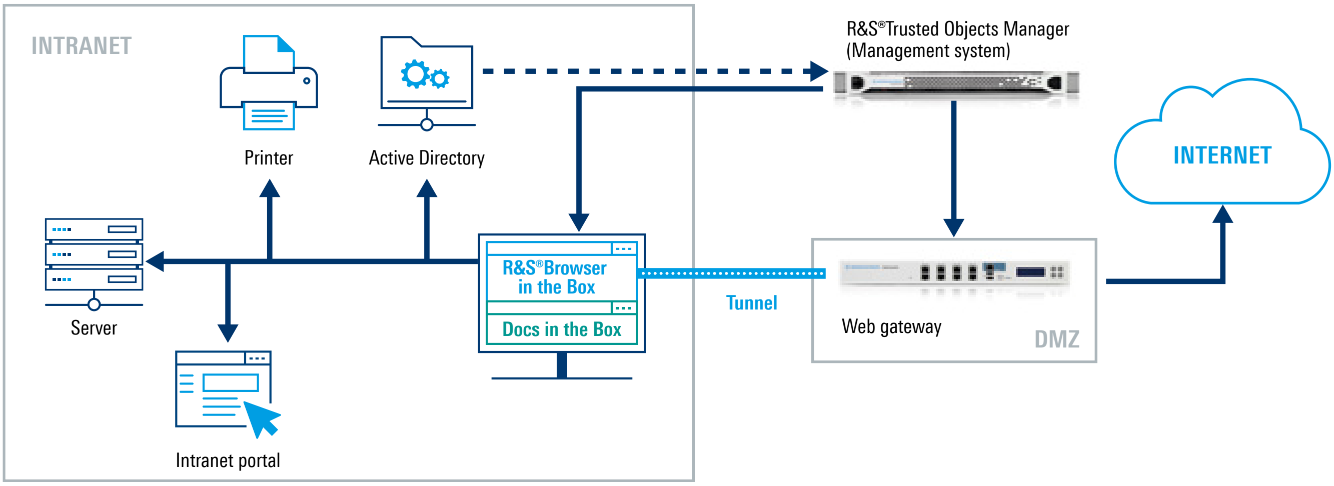
Provides a virtual environment for secure web browsing. Internet browsers are one of the largest weaknesses of endpoints and networks in healthcare facilities. Malware can be introduced into hospitals via emails, applications and collaboration tools used by employees to carry out their everyday work, which can have disastrous consequences not only for data security.

R&S®Browser in the Box protects hospitals against data outflow through remote data in Microsoft® Office™ and Windows 10™, and the viewer function of the Docs in the Box feature allows all attachments of standard Office applications and services with internet access, such as Skype, to be tested in a virtualized environment.

BENEFITS:

- "The most secure browser in the world"
- High security by virtualization and separation of internet and intranet
- Granular allocation of permissions, specified user settings, and unimpaired browsing
- Proactive blocking of all remote services

Fig. 8:
Network separation creates a protected space that prevents malware from reaching local computers or corporate networks



4 IN PRACTICE: IT SECURITY STRATEGIES IN DEPLOYMENT

Web applications require security at several levels. Especially when working with healthcare systems in hospitals, it is important to isolate and individually secure key components of web applications.

This ensures the secure operation of individual protocols, servers, databases and services.

Selected practical examples and tips from our customers are presented below:

- Get an overview of all deployed web applications
- Establish security guidelines and carry out internal audits
- Encrypt this data traffic

CUSTOMER

- A hospital group with four hospitals and 3,400 beds
- Over 12,000 medical and non medical staff and 2,000 doctors
- 125,000 inpatient admissions, 900,000 consultations and 200,000 emergency cases per year

CHALLENGE

- Determining the security levels of the most important business applications
- Identifying potential security gaps in the IT infrastructure supported by these applications
- In addition, compliance with the GDPR and general conditions for quality and cost-effectiveness in health care and nursing
- SSL encryption of mobile apps

SOLUTION

- R&S®Web Application Firewall
- 4,000 IP addresses and 100 applications
- Compliance and ensuring data integrity

CUSTOMER

- Local hospital and healthcare enterprise
- Over 4000 employees

CHALLENGE

- Securing critical web applications against OWASP Top 10 attacks
- Safeguarding an internally developed application for requirements planning and ordering meals from the hospital kitchen. The application switched from the intranet to the internet
- Securing an e-learning application

SOLUTION

- R&S®Web Application Firewall
- (using) virtual machine ware with 20 applications and the Web Access Manager module

CUSTOMER

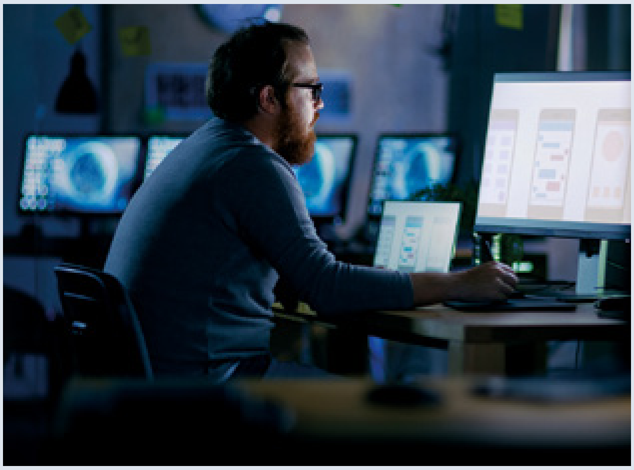
- Over 2,500 medical and non medical representatives
- 845 beds and offices
- 148,437 full hospital days

CHALLENGE

- Secure communications between the data center and the CHPG EHPADs
- Operator Monaco Telecom with limitations related to the MPLS network and the fiber optics operated by Orange
- Technical challenge: multiple VRF, multicast routing

SOLUTION

- R&S®SITLine ETH
- Deployment of four Ethernet encryptors in fiber optics and MPLS networks
- Assured security for communications between EHPAD locations



CUSTOMER

- Public hospital
- 845 beds
- Over 2,500 employees

CHALLENGE

- Secure communications between the data center and the care facilities associated with the hospital
- Telecommunications operator with limitations related to the MPLS network and the fiber optics connection
- Technical challenge: multiple VRF, multicast routing

SOLUTION

- R&S®SITLine ETH
- Deployment of four Ethernet encryptors in fiber optics and MPLS networks
- Assured security for communications between EHPAD locations

CUSTOMER

- Healthcare authority of a state capital

CHALLENGE

- Internet searching is part of daily work
- Separate processing of personal data and health data is required
- Specialized procedures with specific security requirements make data separation necessary

SOLUTION

- R&S®Browser in the Box
- Multi-level encapsulation fulfills statutory security requirements

SUMMARY

In February 2020 the European Union Agency for Cybersecurity (ENISA) published procurement guidelines for cybersecurity in hospitals[14] because the procurement of services, products and the entire infrastructure is a key process in the ICT environment of healthcare facilities, in particular hospitals. This is the start of holistic cybersecurity.

A reliable IT infrastructure is necessary to protect healthcare facilities such as hospitals against manipulation and sabotage, since a broad based attack on the medical infrastructure would certainly have disastrous consequences for public health.

Compliance with rising regulatory requirements for IT security and data protection must equally be ensured, as well as the basic availability of technical systems and healthcare data.

Proactive, future-proof and state-of-the-art solutions are a basic prerequisite to ensure properly functioning healthcare services and secure working in networked hospital operation.

Rohde & Schwarz Cybersecurity supports the healthcare sector with security strategies adapted to individual medical facilities.

INTEGRITY CREATES CONFORMANCE

- Ensure data and files encryption in the cloud by a trustworthy solution
- Enable hospitals to comply with the GDPR and avoid violations
- Make IT security transparent for users – this is the key to acceptance
- Make it easy to work with regulated and unregulated data

[14] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services)

Service that adds value

- ► Worldwide
- ► Local and personalized
- ► Customized and flexible
- ► Uncompromising quality
- ► Long-term dependability

Rohde & Schwarz Cybersecurity

Rohde & Schwarz Cybersecurity is a leading IT security company that protects digital assets of companies and public institutions around the world against cyberattacks. The IT security expert provides innovative data protection solutions for cloud environments, advanced security for websites, web applications and web services as well as network encryption, desktop and mobile security. To prevent cyberattacks proactively, the trusted security solutions are developed according to the security-by-design approach.

Rohde & Schwarz

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, monitoring and network testing. Founded more than 80 years ago, the independent company which is headquartered in Munich, Germany, has an extensive sales and service network with locations in more than 70 countries.

Rohde & Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

Rohde & Schwarz GmbH & Co. KG
www.rohde-schwarz.com

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG
Trade names are trademarks of the owners
PD 3608.4997.62 | Version 01.00 | May 2020 (sch)
IT security in healthcare
Data without tolerance limits is not binding | Subject to change