https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-254

Towards sector specific security operation

Michael Pilgermann [1]***, Sören Werth*** [2]***, Reiner Creutzburg*** [1]

[1] ***Technische Hochschule Brandenburg, Department of Informatics and Media, IoT and Smart Home Security Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany***

[2] ***Technische Hochschule Lübeck, Department of Electrical Engineering and Computer Science, Mönkhofer Weg 239, D-23562 Lübeck, Germany***

Email: michael.pilgermann@th-brandenburg.de, soeren.werth@th-luebeck.de, creutzburg@th-brandenburg.de

Abstract

Many organisations, especially Critical Infrastructures, are facing an increasingly severe cyber threat situation and are continuously improving their IT-security. We present the state of the art of sector specific security operation of CI operators with the German health sector as an example. To improve the situation we propose several spheres of activity with practical exemplary measures, e.g. for relevant protocols. In this way we help to prepare a CI sector governance with sourcing options for security operation for all relevant actors: from the responsible authorities in the country via a single point of contact in the health sector to hospital centres and the medical practice.

Introduction

Today, cyber-attacks are constantly rising to higher levels of sophistication and hence the IT threat situation remains alarming. Therefore, many organisations are forced to improve their protection. Governments in more and more countries are reacting by adjusting the cyber policy frameworks. Most of these frameworks increasingly include Critical infrastructures (CI).

Although many enhancement can be observed regarding IT-security, on the operational side we are not advanced as we should in 2020. The exchange of security incidents beyond organisational boundaries is often carried out by email. Sophistication is limited to register security incidents on web portals or installing (manually) sector specific proxies. We need a solution to automate the operational side of Information Security Management in Critical Infrastructures.

In the following we give an overview of the policy situation in the European Union and especially Germany. Via the operational status quo of sector specific security operation in the EU and Germany, we present several spheres of activity with a focus on the opportunities of Security Operation Centers.

Policy situation

From a policy point of view it is worth to look from three perspectives: the current threat situation in Cyberspace, the supranational legislative framework for IT-security, and finally the national legislative framework.

Threat situation

The Federal Office for Information Security, Germany (BSI) published its annual report on the "The State of IT-security in Germany" only in October 2019 [9]. The numbers of incidents, which had to be reported to the authority BSI, are alarming: for the 1500 registered CI facilities in Germany, the operators reported 252 security incidents. Out of those, 47 incidents were reported from the health sector.

The BSI explicitly highlighted the cyber threat situation for medical products in its report on the "The State of IT-security in Germany" 2019. The BSI observes an advancing digitalization; mobile solutions is a major driver here. However, mobile solutions are increasingly partnered with medical products such as insulin pumps. Often, cybersecurity is of lower priority for vendors of mobile solutions. The situation becomes more severe due to increasing interconnections as well as penetration. The BSI attests a "critical threat situation" for the security of medical products.

It was only in July 2019 when a group of hospitals from "Deutsche Rote Kreuz" got hit by a RansomWare – regarding the authorities, the most comprehensive attack the German public health sector had experienced so far [29]. The Clinical Center Fürth was the next major victim in health industry when getting hit by a virus in December 2019 [28].

European Union level policy situation

The EU Cybersecurity Act was agreed in December 2018, it stresses the role of cybersecurity certifications, contributing to trust and security in ICT products and services [22]. It is to be understood as the second legislative step after the NIS directive (entered into force in August 2016), being the very first legal act of the EU setting up a global approach to Cybersecurity. The Healthcare sector had been covered by this directive in Annex II, listing the relevant Critical Infrastructures (CI) [23].

Within that new EU Cybersecurity framework the European Union Agency for Cybersecurity (ENISA) proposes security certification opportunities in the healthcare sector [18]. They define the term *Internet of Medical Things*, referring to the IoT technologies in the healthcare sector. For the evaluation during a certification process the report defines among others the following controls:

- Establish procedures for security incident handling
- Participate in information sharing
- Apply appropriate traffic filtering
- Deploy early warning/detection systems

The report on certification opportunities refers in turn to an-

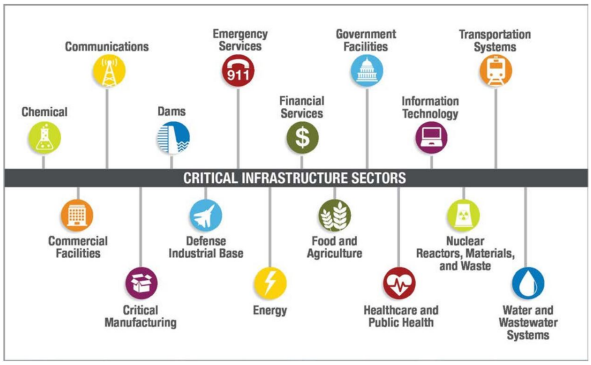


Figure 1. *CI sectors in the US (Image src: US DHS, A Reference Guide for the Critical Infrastructure Community)*

other ENISA study *Smart Hospitals. Security and Resilience for Smart Health Service and Infrastructures*, which was made to identify smart assets in Healthcare organizations [19]. Out of this list of assets, the groups of *Networked medical devices* and *Interconnected clinical information systems* shall be targeted by this paper. The ENISA report states, that these two groups are rated as the most critical ones, based on empirical data. Among the technical good practices stated there, two Cyber security and protection measures are:

- "GP 10 – *Implement monitoring and intrusion detection/ prevention mechanisms.* [...] Violations that are detected are typically reported directly to a member of the IT staff or collected in a central database for further analysis, for instance, by means of a Security Information and Event Management (SIEM) solution. External threat intelligence may be used to improve the analysis."
- - "GP 11 – *Enforce dynamic network segmentation and use of firewalls.* It is important to separate critical parts of the network from non-critical parts. For instance, it is recommended to separate medical devices to the largest possible extent from office components [...]"

National policy situation in Germany

In Germany a comprehensive legislative approach on IT-security was implemented in 2015, when the IT-security law (*IT-Sicherheitsgesetz*) was agreed upon and published [6]. One major focus of this law was the protection of critical infrastructures (CI). Operators of those CIs were to address two major obligations: 1) minimum security requirements and 2) a mandatory security breach notification. The law itself listed seven CI sectors, which are covered (see figure 2 for details). The details on defining what assets in which sectors are concretely to be protected was left to the Federal government using delegated act.

In the meantime those delegated acts have been enacted as well; regarding [9] about 1500 assets have been registered as Critical Infrastructures in Germany by their operators at the Federal Office for Information Security (BSI). For the sector health four so called asset categories have been concretely named as containing critical infrastructures: Clinical medical supply, supply with directly life-sustaining health products, supply with prescription drugs and blood concentrates for humans and laboratory diagnostics. The corresponding delegated act rules in more detail, which

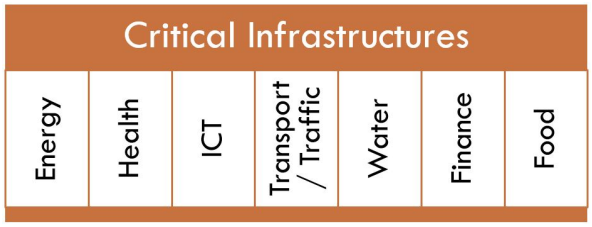


Figure 2. *CI sectors covered by German IT-security law*

assets exactly are covered by the law [8].

Currently, the German Federal Government is preparing version 2.0 of the IT-security law. Drafts indicate the direction of this even more comprehensive approach. Among other, the procedure for protecting CIs shall be extended and even adopted to other, non CI industry sectors. Furthermore, a draft includes an explicit obligation for incident detection when operating a CI.

For supporting the implementation of minimum-security requirements for operating CIs, operators may develop industry sector specific security standards (so-called "Branchenspezifischer Sicherheitsstandard", B3S). The B3S may be presented to the authority BSI, which in turn will evaluate the B3S and will return a verdict on whether it matches the requirements of the law. Since 2015, regarding [9] more than 20 industry sectors have created a B3S or are in the process of doing so.

The B3S for the public health service in hospitals got BSI approval on 22nd of Oct. 2019 [26]. The document describes a comprehensive set of security requirements for running a hospital in Germany. Regarding operational IT-security, a few requirements as shown in table 1 are of relevance.

Policy situation outside the European Union

Although, countries pretty much agree in what infrastructures are to be considered as critical, the concrete sector definitions are different depending on the geographic location. For the US, the sectors were defined in 2013 by the *Presidential Policy Directive 21 (PPD-21)* (see figure 1) [7]. This work has been taken further by US DHS CISA Cyber Infrastructure (`https://www.cisa.gov/critical-infrastructure-sectors`).

Operational status quo

The transposition of the NIS directive into European Member States legislation had a remarkable impact on the incident response capabilities. In November 2019 ENISA presented an incident response development status report [23] and 3 out of 7 key findings support the need to improve the sector-specfic security operation:

- In Key Finding #5 they note that "sector-specific regulations which include guidelines and requirements for reporting and management of incidents are crucial to enhance capabilities at the sectoral level".
- In Key Finding #6 they regret that many sectoral cooperation and information-exchange initiatives often lack visibility or resources to sustain their efficiency.
- In Key Finding #7 it is explicitly stated that "training at sectoral level is key to foster and enhance preparedness".

But sector-specific cooperation of the CI operators faces a lot

Selected requirements from B3S for the public health service in hospitals

ID	Requirement (author's translation)
ANF-MN 28	Operators MUST report incidents, which have yield or may yield to outage or disturbance of the functioning. The operator MUST implement a reporting procedure, which allows for the identification, analyzation and decision on incidents.
ANF-MN 29	In case of an incident, the event MUST be reported without culpable delay.
ANF-MN 73	Critical IT-systems MUST incorporate logging- and audit functionality for supporting the identification and tracking of security incidents.
ANF-MN 93	An adequate segregation of networks MUST implemented [...].
ANF-MN 106	A SYSTEM for prevention and detection of unauthorized accesses to network and IT systems shall be implemented, which also examines generally authorized traffic.
ANF-MN 138	A central logging infrastructure SHALL log general operational events next to security relevant events

of challenges. Without a single point of contact within a sector, there is a decentralized organisational structure. Therefore you have independent choice and operation of communication tools of each operator. This affects the hosting, compatibility between operators and compatibility within the IT of an operator. Nonetheless you need an end-to-end encryption in order to exchange the highly sensitive security information with a revisable key management. Furthermore, the communication solution needs encrypted group messages, has to feature an archive and document storage in order to benefit from lessons learnt. ENISA published a comparison of existing solutions in order to underpin the cooperation of incident response teams in Europe [19]. Due to different requirements of different communities there is not a single jack of all trades solution and ENISA proposes to use an encrypted email mailing list and an encrypted group communication tool and name suitable tools, especially OPENPG/MIME for mailing lists, both Matrix and XMPP for group communication. In Addition to that they note recent ideas as the web key directory for OPENPGP, which may yield more suitable solutions in future.

In Germany, the IT-security law commit the operators to report incidents to the BSI [6]. Unfortunately, there is no sophisticated technical solution for the notification at the moment. At the moment, it is a manual implementation of breach notification. There is a webportal and in addition to that, e-mails and telephone are the solely used tools [13]. The BSI is working on improving the situation.

Within each CI sector, there is a concept for single points of contacts in Germany [25] by BSI and the Federal Office for Civil Protection and Disaster Assistance. It is intended that Operators take the role of SPOC in their sector. There are SPOCs in Transport/Traffic, Finance and ICT, but in other sectors there are no SPOCs at the moment, especially in the health sector.

Perspective of a comprehensive approach for security operation

The operation of security is tackled in different ways today, but most larger organizations, like operators of Critical Infrastructure, have some kind of security center. Their different embodiment and tasks are mirrored by the different names like Information Security Operations Center (ISOC), Network Security Operation Center (NSOC), Security Analytics Center (SAC) or Infrastructure Protection Center (IPC) and so on. Nonetheless, the basic concept is mostly similar. We use the term Security Operation Center (SOC) and will describe our expectations of its main tasks:

- **Process Management**: The SOC is responsible for the implementation of the Information Security Management System.
- **Logging**: The SOC ensures the collection of all machine data needed for security reasons.
- **Monitoring**: The SOC analyzes all machine data with tools in real time and provides alerts and details of suspicious activity.
- **Incident Response**: The SOC reacts to all reports from monitoring, employees, CERTs, etc. with a defined incident management process. They choose the proper security measures in order to stop malicious behavior and to prevent further damage as well as to mitigate incurred damage and to recover the system.

All in all, we understand a Security Operation Center as a solution, which enables organizations to standardize and automate the operational side of Information Security Management. For more information on logging and monitoring, we refer to the "Cyber Security Logging and Monitoring Guide" from CREST [10].

Security information and event management

As a technological base for a SOC a so-called Security information and event management (SIEM) is indispensable. The terminus SIEM was introduced in 2005 by Mark Nicolett and Amrit Williams. In general, security information and event management combines the technologies of SIM (security information management) and SEM (security event management). It provides real-time analysis of security alerts. For proper functioning reporting data from several security systems such as firewalls, IDS, authentication servers as well as from appliances and applications are to be integrated in a SIEM. The capabilites of SIEM products usually include data aggregation, correlation, alerting, dashboards, compliance and retention [35].

Monitoring within organizations

Operators of Critical Infrastructures, no matter what CI sector they belong to, face similar challenges here: network infrastructure devices such as routers and switches, security systems such as firewalls and IDS as well as outstanding other IT systems (such as industrial control systems or VPN endpoints) must

be enabled to report relevant audit trail information to a central database. Moreover, smart configuration must be applied to choose which audit data is to be gathered and passed on to the SIEM for all those sensors in the network (an example from health industry will be introduced below).

Share monitoring information beyond organizational boundaries

Usually, the automated processing of audit trail information is limited to organizational boundaries. This is due to the extreme sensitivity of the audit data and the risk to share information that could harm the image of the organization. Approaches have been researched in the past to overcome this conflict by introducing trust relationships between organization and overcoming the confidentiality issue by introducing measures for anonymizing communication partners and sanitizing relevant pieces of information. Communication protocols to semantically transport this kind of information such as the Intrusion Detection Exchange Protocol (IDXP), the Incident Object Description and Exchange Format (IODEF) and the Intrusion Detection Message Exchange Format (IDMEF) have been established decades ago [33]. A sector specific SOC shall address this mutual communication between operators from a CI sector or even across sector boundaries. As a first step, organization and processes must incorporate this interface - communication itself will remain rather manual for a while. In future, however, this interface should be part of the integrated and automated tool landscape of a SOC.

An additional communication partner enters the scene as soon as reporting of security incidents becomes an obligation by law. As described above, operators of Critical Infrastructures all over the European Union have in the recent past been obliged to report security incidents to their national authorities. In Germany, for most CI operators the Federal Office for Information Security (BSI) acts as the authority in question. To avoid the passing on of relevant security incidents via Email, the BSI has set up a "Registration and Reporting Portal" ("Melde- und Informationsportal", `https://mip.bsi.bund.de/`), where operators register their CIs in the first place, and report on security incidents from there on-wards. SOC processes and thresholds must taken into account those obligations. The authors believe, that with growing maturity of those interfaces, the level of automation should also be increased - an enhancement by introduction of an API is suggested by the authors as part of their conclusion.

Sector SOC in health industry

The authors chose the CI sector *health* as it is covered by the IT security law and, additionally, is heavily penetrated by digitization. Still it does not look back to a long lasting history of IT security regulation as other CI sectors do.

The choice for a concrete scenario within that sector does not heavily impact the research on network security, as the respective protocols are widely deployed no matter of what service within the sector is being analysed - being it either hospitals or laboratories.

For illustrating the comprehensive approach, the authors chose a non-complex set-up within a medical laboratory. We are considering two components in our imaginary set-up:

- a Laboratory Information System (LIS) on IP address 10.0.2.2 in network 10.0.2.0/24, and
- a digital X-Ray apparatus on IP address 10.0.1.2 in network 10.0.1.0/24.

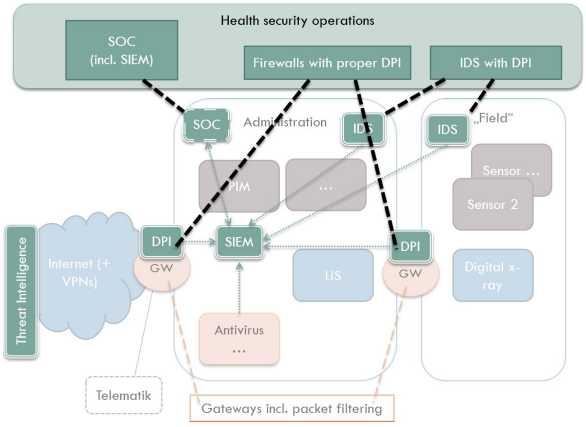


Figure 3. *Overview on health sector SOC*

Listing 1. *SAMPLE MLLP MESSAGE WITH HL7 PAYLOAD (SOURCE [4])*

```
<SB>
MSH|^~\&|ZIS|1^AHospital|||199605141144||
    ADT^A01|20031104082400|P|2.3|||  AL|NE
    |||8859/15|<CR>EVN|A01
    |20031104082400.0000+0100|20031104082400
     PID||""|10||Vries^Danny^D.^^de
    ||19951202|M|||Rembrandlaan^7^Leiden
    ^^7301TH^""  ^^P||""|""||""|||||||""|"" <
    CR>PV1||I|3w^301^""^01|S|||100^van den
    Berg^^A.S.  ^^""^dr|""||9||||H
    ||||20031104082400.0000+0100<CR>
<EB><CR>
```

Both components are being connected via IP / Ethernet. More details on the communication will be provided below.

For our imaginary lab setup, we will focus on the HL7 protocol since this is most widely used for these purposes (following [3] in 2013 90 % of queried US laboratories were using HL7). Although from the 1980's, the version 2 is still the most widely used HL7 version – version 3 is XML-based and has been available for a few years but has not gained enough penetration. Be aware, that with HL7 major effort has additionally be put on so-called semantic interoperability, which however does not impact the network security approach, which the authors address with this paper [3].

The Minimal Lower Layer Protocol (MLLP) is said to be a "minimalistic OSI - session layer framing protocol" and is being used to transport the HL7 messages in networks. In fact, the HL7 payload is encapsulated by special characters in order to form a block. Before the data, a start block character indicates, that data will follow. After the payload, an end block character indicates the end of a block respectively, followed by a carriage return.

Listing 1 provides an example of a simple MLLP message with HL7 payload. Please note, that according to [4] <SB>, <EB> and <CR> are used to denote the non-printable MLLP-

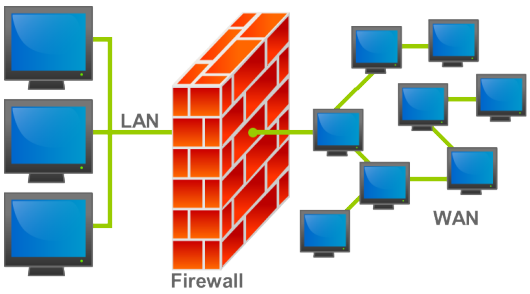


Figure 4. *Scenario for a packet filter between Local and Wide Area Network (Image src: Bruno Pedrozo under GNU Free Documentation License, version 1.2)*

framing single-byte values 0x0B, 0x1C and 0x0D (they are not to be interpreted as XML-tags).

Although, other implementations are possible, for the objectives of our example, we assume the TCP/IP-based MLLP-setup. This way, MLLP directly establishes a TCP/IP-socket. Please also note, that several minor enhancements have been applied with a release 2 of MLLP, which however do not impact the network security in general.

Deploy Sector SOC sensors in the network

In order to allow for sector specific Security Operation the infrastructure must provide relevant raw data from security systems and IT systems in general. In Linux based environments such data is usually based on the Syslog technology [11], other kind of IT systems such as network devices like routers or Windows boxes do provide some similar kind of mechanism to provide an audit trail of the activities, which might be of interest.

Sophisticated added value can be gained by using those security systems once they can analyse the traffic passing by. In the following, the authors will explain sector specific security sensors in nature of a packet filtering system and a network intrusion detection system.

Packet filtering

Packet filters are the least complex Firewall systems (also called first generation firewalls). They act by inspecting packets of the network communication. Depending on the rule-set, packets may be dropped, rejected or passed. Packets may be filtered by source and destination network addresses, protocol, source and destination port numbers (see figure 4 for very plain scenario of a firewall) [30].

The authors chose the *NFTABLES* technology (`https://netfilter.org/projects/nftables/`) for the packet filtering functionality. It is a *Netfilter.org* project and is distributed as part of the Linux kernel and therefore widely and free available.

Rules for packet filtering may be easily defined via a well-defined and documented syntax. The rules also allow for dropping log messages, which contributes to the SIEM, which will be explained afterwards.

Listing 2 provides an example of an extract of a rule for NFTables, which restricts traffic on the corresponding TCP ports to the chosen IP addresses of the X-Ray and the LIS (any other traffic will be dropped). Note the suffixes in each rule for dropping messages to the audit trail.

Listing 2. *SAMPLE NFTABLES RULE FOR RESTRICTING TRAFFIC*

```
table inet filter {
  chain input {
[...]
    # accept ssh and MLLP sockets
    ip saddr 10.0.1.2 ip daddr 10.0.2.2 tcp
        dport {1080} ct state new log
       prefix "MLLP Traffic " accept
    tcp dport {22} ct state new log prefix
       "SSH Traffic " accept
    # count and reject everything else
    counter reject with icmpx type admin-
       prohibited
    log prefix "NFTABLES GENERIC DROP "
[...]
}
```

Listing 3. *SAMPLE SNORT RULE FOR MALICIOUS TRAFFIC*

```
alert tcp !10.0.1.2 any <> 10.0.2.2 1080 (
    flags:S; msg: "Access attempt on LIS
    ";)
alert tcp any any -> 10.0.2.2 1080 (content
    :!"<sb>"; depth:1; msg: "Corrupt MLLP
    message ";)
alert tcp any any -> 10.0.2.2 1080 (
    from_end, post_offset -2; content:!"<EB
    ><CR>", distance 0, within 2; msg: "
    Corrupt MLLP message ";)
```

Intrusion Detection

Intrusion Detection Systems (IDS) are hardware or software that monitor a network or systems for malicious activity or policy violations. IDS is a mature approach as first concepts were published as early as 1980 already [31, 32]. Usually, two categories of IDS are distinguished: Host Intrusion Detection (H-IDS) and Network Intrusion Detection (N-IDS) [33]. Although, generally speaking, the Health Sector SOC could also benefit from H-IDS sensors on relevant machines such as the LIS, the remaining paper will only address further integration of N-IDS technology.

The authors chose the *Snort* (`https://www.snort.org/`) software as N-IDS technology as it is, again, freely available. Furthermore, the authors had successfully carried out experiments with Snort in past projects already. Snort's development had been initiated by Martin Roesch in 1998 and since then it has ever grown in popularity. Due to its modular approach with its preprocessors and output plug-in mechanism it can and has been deployed in numerous, diverse employment environments [33].

Listing 3 provides an example of Snort rules, following that a message will be dropped to the audit trail, whenever

- any client other than x-ray contacting port 1080 on LIS
- the payload is not following very basic MLLP specifica-

tions.

SIEM Correlation

As introduced above, the Security information and event management (SIEM) integrates the audit trail information from all relevant network, security and other IT systems. So as a precondition, the sensors must be configured in a way, that the monitoring information is being passed on to the SIEM.

When defining (and continuously improving) the ruleset for a SIEM, security experts generally base their configuration on use cases, which in turn shall be based on the risk situation, the organization faces. As shown in table 2, the authors combined general risk information commonly known for deploying SIEMs (number 4), input from the hospital specific B3S (see [26] chapter 6) (number 1 - 3) and risks directly tailored to the lab environment described before (number 5, 6):

Selected sample use cases based on several risk sources

	Use Case	Short description
1	Outage of medical devices, being a mandatory requirement for diagnostics, therapy or medical care	examination of regular probes from relevant machines, which are part of their audit trail
2	Lack of important medical data for diagnostics or therapy	examine audit trail of backup server, which drops a message whenever a relevant IT system runs a backup
3	Manipulation of relevant medical data for diagnostics or therapy	examine audit trail of integrity checkers and access control facilities from relevant IT systems
4	Detection of Possible Brute Force Attack	multiple login attempts from any it system within the network
5	Infection of Office Environment attempts to infect medical devices	check for high amount of MLLP messages
6	Malfunctioning of medical devices	MLLP messages do not match specifications

The use cases would need to be translated to the specific language of the SIEM product, which is not part of this paper.

SOC organization

Good practices for structural organization and processes of Security Operation Centers are evolving and are usually based on security incident handling [36]. For German speakers, an additional set of good practices is available in terms of the "IT-Grundschutz-Kompendium (IT Baseline Security catalogues)", primarily modules "DER.1 Detektion von sicherheitskritischen Ereignissen (detection of security relevant incidents)" and "DER.2.1 Behandlung von Sicherheitsvorfällen (Reaction to security incidents)" [15, 16].

General organization

Generally speaking the following roles should be assigned in a SOC (be aware, that there is not this single definition on which roles are required, depending on the source of information, the roles might deviate and overlap - finally, the selection must also match the size of the organization and the SOC):

- *platform administrator* and *application administrator*: must have sound knowledge about the IT infrastructure that is being monitored including its network topology and its IT systems, components as well as SIEM and monitoring solutions.
- *content engineer*: responsibilities include defining how logs should be parsed, creating new correlation rules, coordinating and conducting event collection, log management, event management, compliance automation and identity monitoring activities. They must have deep understanding of the used SIEM and / or monitoring solution and its capabilities for monitoring as well as for supporting the use case creation.
- *cyber situational awareness analyst*: must be experienced in security and penetration testing for identifying vulnerabilities and investigating as well drafting of (daily) advisories.
- *pen-tester*: must have experience with vulnerabilities and with finding new vulnerabilities in order to check for vulnerabilities in applications and web applications of the organization (using the testing environment).
- *malware analyst*: analyses malware for identifying the respective intentions and analyses new threats, malware mutations and technologies including anti-detection capabilities. must have sound knowledge about software engineering and debugging for reverse engineering and analyzing of malware.
- *IT forensics analyst*: must have experience with creating images from memory or systems and legal experience with handling and preservation of evidence.
- *level 1 analyst* (sometimes SOC operator or triage specialist): responsible for real time monitoring and detection of incidents, the issuing of tickets and the initial reporting and escalation. They must have knowledge about logging and audit trail data as well as SIEM technologies for classification of alarms and identification of false positives.
- *level 2 analyst* (sometimes incident analyst): responsible for in-depth analysis and thereby validation of incidents, ongoing investigations, counter measures, trends and the adjusting of settings. They must have sound and long-standing experience in IT-security with deep knowledge about logging and audit trail data as well as SIEM technologies.
- *level 3 analyst*: similar to level 2, but even more experienced in selected subject areas.
- *SOC Manager*: in charge of the entire management of the SOC, incident resonse oversight, metrics and the assessment of SOC resources as well as capabilities. They must have long-lasting IT experience, very deep understanding of IT-security and its processes, tools and technologies as well as leadership, decision making and communication competences.

Good practices show, that the following processes should be defined and established when operating a SOC: SOC Man-

agement, Detection and Reaction, SOC analysis and monitoring, alarming and notifications, reporting, rule-set engineering, CERT and IT forensics.

Sample incident in sector SOC

In order to provide better understanding of the processes within a SOC an example is provided, showing how an incident is triggered from the security system and, furthermore, how it gets processed by the relevant roles in the SOC.

The raw incidents are being generated at the sensors in the network; for instance the IDS located at the *field* network (figure 3) drops an audit trail entry with content "Corrupt MLLP message" following rule 3 from Listing 3. This messages is passed on to the central SIEM for further analysis.

1. First addressee of an alert is always the Level-1 analyst. On their dashboard (and possibly through additional channels such as Email) an alert will pop up following the rule number 6 from table 2.
2. The Level-1 analyst has to decide, whether the alert is a false positive or whether they expect a potentially harmful alert. Whenever they expect a harmful alert, the incident information is passed on to the Level-2 analyst. Good practice indicate, that the Tier-1 team should hold an incident no longer than 30 minutes.
3. Depending on the severity and complexity of the incident the case could than be passed on to the Level-3 analyst or even a CERT team could be constituted. Additional expertise might be included by pulling in forensic experts, malware analysts or other experts from other departments such as IT operations.
4. No matter where the further incident handling is carried out (level 2 or level 3), the defined procedures must include communication guidelines for both, internal and external communication. Regarding [16] (requirement DER.2.1.A4) internal addressees could be data protection officers, works committee or the compliance department; security breach notification obligations will include addresses outside the organization.
   Therefore, the procedures shall include a check list, which incidents are to be reported to authorities such as the BSI in Germany. Following that, the process description will also include the selection of information, which is included in the breach notification to the authority and to match it with the official requirements of the authority (see [13] for example). Moreover, the approval especially for external communication shall be defined - at least the SOC Manager should be taken into charge here.

Conclusion

Operators of critical infrastructures such as hospitals are providing highly critical services to our societies and are dealing with most sensitive data one can imagine. Strong security controls are thus a must have for running those CIs. Germany, the European Union and also other economies have started to also integrate IT-security obligations in their legal frameworks.

IT protocols used in CI sectors such as health industry are well known. Security technologies such as firewalls with DPI features and Intrusion Detection also with DPI have been available for quite some years already. Security Operations Centers are emerging and good practices for organisation and processes in SOCs are becoming available.

Operators are now facing obligations, which cannot be reasonably addressed regarding the operational duties of IT-security. With the approach of a sector specific SOC, operators are heavily supported in gathering relevant IT-security incident information from their networks. Moreover, through sector wide sharing of relevant information, the rule-sets and threat intelligence is continuously improved. A definition of the corresponding incident response organisation and processes including the interface to authorities such as the BSI (supported by smart semi-automatic tooling) enables operators to react effectively and efficiently and, in the end, improves resilience of CI services for our societies.

Future work

As shown above, the implementation of sector-specific security operation is in progress, but there is still a long way to go. We think that the establishment of a lab to gather more and detailed information would be a reasonable next step to investigate the following issues:

- Consider more relevant protocols in the health sector in more detail and extend the technical aspects of our approach, e.g. for DICOM or SFTP.
- Extend the set the sensors by more sophisticated security systems such as so called next generation firewalls, which are capable of analysing and filtering higher levels of the TCP/IP stack.
- The SIEM needs a lot of attention to establish a concrete, more complete and more refined rule-set than our examples. In the end, the german B3S should be extended with this generic rule set.
- Extend the market survey of the ENISA for secure communication tools to further tools. Compare results of all surveys with the requirements of the users and reach out to to manufacturers of high level network security products, in the end solutions must work nearly out-of-the-box.
- Support BSI in establishing an API of the "Melde- und Informationsportal" to establish a smart semi-automatic tooling. In addition to the tooling, more refined processes to distribute the information to all CI operators in a sector are needed.
- In this way the existing generic concepts should be extended via theoretical work together with the first experience from the lab. We should create a blueprint for other CI sectors in Germany, which are still writing on their B3S, or CI sectors in other countries.

Keywords

Cybersecurity, Information Security, Network Security, IT-security, Security Operations Center, SOC, Security Information and Event Management, SIEM, Security Monitoring, Health Care, Critical Infrastructures, Hospitals, HL7, MLLP.

References

[1] David R. Miller et al.: Security Information and Event Management (SIEM) Implementation, ISBN: 978-0-07-170109-9.

[2] Arun E Thomas: Security Operation Center – Analyst Guide, ISBN: 9781533408501.

[3] Mark L. Braunstein: Health Informatics on FHIR: How HL7's New API is Transforming Healthcare, ISBN: 978-3-319-93413-6.

[4] Rene Spronk: Transport Specification: MLLP, Release 1 (https://www.hl7.org/documentcenter/public_temp_2EC646CF-1C23-BA17-0C96EFA7E31E4552/wg/inm/mllp_transport_specification.PDF).

[5] Work Group HL7: Transport Specification: MLLP, Release 2 (http://hl7.ihelse.net/hl7v3/infrastructure/transport/transport_mllp.html).

[6] Bundestag: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Juli 2015 (https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/it_sig_node.html).

[7] The White House Office of the Press Secretary, US: Presidential Policy Directive - Critical Infrastructure Security and Resilience, PRESIDENTIAL POLICY DIRECTIVE/PPD-21, Feb. 2013 (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil).

[8] Bundesministerium des Innern (Federal Ministry of the Interior, Germany): Erste Verordnung zur Änderung der BSI-Kritisverordnung, June 2017 (https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1903.pdf#).

[9] Federal Office for Information Security, Germany (BSI): Die Lage der IT-Sicherheit in Deutschland, 2019 (https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html).

[10] CREST. Cyber Security Logging and Monitoring Guide, 2015. [accessed 17.01.2020.] https://www.crest-approved.org/wp-content/uploads/2015/05/Cyber-Security-Monitoring-Guide.pdf.

[11] RFC 5424 - The Syslog Protocol, 2009 (https://tools.ietf.org/html/rfc5424).

[12] Dalas Haselhorst: Hacking HL7 Data Interfaces in Medical Environments: Attacking and Defending the Achille's Heel of Healthcare, Aug. 2017 (https://www.linuxincluded.com/hl7-medical-attacking-defending/).

[13] Federal Office for Information Security, Germany (BSI): Melde- und Informationsportal (https://mip.bsi.bund.de/).

[14] Federal Office for Information Security, Germany (BSI): Cyber Security Requirements for Network-Connected Medical Devices. Nov. 2018 (https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_132E.pdf?__blob=publicationFile&v=5).

[15] Federal Office for Information Security, Germany (BSI): DER.1 Detektion von sicherheitsrelevanten Ereignissen (IT-Grundschutz-Kompendium) (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_1_Detektion_von_sicherheitsrelevanten_Ereignissen.html).

[16] Federal Office for Information Security, Germany (BSI): DER.2.1 Behandlung von Sicherheitsvorfällen (IT-Grundschutz-Kompendium) (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_2_1_Behandlung_von_Sicherheitsvorf"allen.html).

[17] European Union Agency for Cybersecurity (ENISA): SECURE GROUP COMMUNICATIONS for incident response and operational communities, JULY 2019, ISBN: 978-92-9204-303-2 (https://www.enisa.europa.eu/publications/secure-group-communications).

[18] European Union Agency for Cybersecurity (ENISA): ICT security certification opportunities in the healthcare sector, Dec 2018, ISBN: 978-92-9204-276-9 (https://www.enisa.europa.eu/publications/healthcare-certification).

[19] European Union Agency for Cybersecurity (ENISA): Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures, Nov. 2016, ISBN 978-92-9204-181-6 (https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals).

[20] European Union Agency for Cybersecurity (ENISA): EU MS INCIDENT RESPONSE DEVELOPMENT STATUS REPORT, Nov. 2019, ISBN 978-92-9204-310-0 (https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report/).

[21] ETSI: TR 103 331 - CYBER; Structured threat information sharing, V1.1.1, Aug. 2016 (https://www.etsi.org/deliver/etsi_tr/103300_103399/103331/01.01.01_60/tr_103331v010101p.pdf).

[22] European Union: Cybersecurity Act, 2018 (https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en).

[23] European Union: Directive on security of network and information systems (NIS Directive) (https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive).

[24] PWC (on behalf of Federal Office for Information Security, Germany (BSI)): KRITIS-Sektorstudie Gesundheit, May 2016 (https://www.kritis.bund.de/SubSites/Kritis/DE/Publikationen/Sektorspezifisch/Gesundheit/Sektorstudie_Gesundheit.html).

[25] UP KRITIS: SPOC-Konzept (https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/UPKSPOC/upk_spoc_node.html).

[26] Bundesverband der Krankenhausträger der Bundesrepublik Deutschland: Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, Version 1.1, Oct. 2019 (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/B3S_KH_v1.1_8a_geprueft.pdf).

[27] Jenny Knackmuß, Thomas Möller, Wilfried Pommerien and Reiner Creutzburg: Security risk of medical devices in IT networks - the case of an infusion pump unit, Proceedings of SPIE - The International Society for Optical Engineering, March 2015 (https://www.researchgate.net/publication/273317085_Security_risk_of_medical_devices_in_IT_networks_-_the_case_of_an_infusion_pump_unit).

[28] Heise.de: Computervirus: Klinikum Fürth offline und mit eingeschränktem Betrieb (https://www.heise.de/newsticker/meldung/Computervirus-Klinikum-Fuerth-offline-und-mit-eingeschraenktem-Betrieb-4615427.html).

[29] Heise.de: Zurück zu Bleistift und Papier: Schadsoftware legt

Klinikserver lahm (https://www.heise.de/newsticker/meldung/Zurueck-zu-Bleistift-und-Papier-Schadsoftware-legt-Klinikserver-lahm-4473927.html).
[30] KENNETH INGHAM, STEPHANIE FORREST: A History and Survey of Network Firewalls, Technical Report 2002-37, University of New Mexico Computer Science Department (https://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf).
[31] J. P. Anderson: Computer security threat monitoring and surveillance, 1980 (https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf).
[32] D. Denning: An intrusion detection model. IEEE Trans. on Software Engineering, SE-13(2), 1987.
[33] Michael Pilgermann: Inter-Organisational Intrusion Detection System Communication to implement Network Defence, PhD diss., University of Glamorgan (United Kingdom), 2006 (https://www.researchgate.net/publication/338410162_PhD_Thesis_Inter-Organisational_Intrusion_Detection_System_Communication_to_implement_Network_Defence).
[34] David Swift: A Practical Application of SIM/SEM/SIEM Automating Threat Identification, SANS Institute, 2007 (https://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781).
[35] Eva Kostrecová and Helena Bínová: Security Information and Event Management, Indian Journal of Research, Volume 4, Issue 2, 2015, ISSN - 2250-1991 (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.679.2792&rep=rep1&type=pdf).
[36] National Institute of Standards and Technology (NIST): Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology, Special Publication 800-61, Revision 2, Aug. 2012 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf).

Author Biography

Michael Pilgermann has a doctorate in Computer Science with focus on Information Security. He had worked in industry and Federal government, where he gained founded experience in Critical Information Infrastructure Protection. Since 2016 he has been heading the Security Management within the Federal Agency for Public Safety Digital Radio, Germany. Additionally, he has been acting as visiting lecturer at Technische Hochschule Brandenburg in Brandenburg, Germany since 2018.

Sören Werth studied Math and received his doctorate in Computer Science in 2006. He worked at the Federal Office for Information Security on the development and implementation of several cryptographic systems and he worked strategically on the IT-security of critical infrastructures and industry at the Ministry of the Interior in Germany. Since 2017 he has been professor for Applied Mathematics and IT-Security at the Technische Hochschule Lübeck.

Reiner Creutzburg is a retired professor for Applied Informatics at the Technische Hochschule Brandenburg in Brandenburg, Germany. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Device (MOBMU) Conference at the Electronic Imaging conferences since 2005. His research interest is focused on Cybersecurity, Digital Forensics, Open Source Intelligence, Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications.

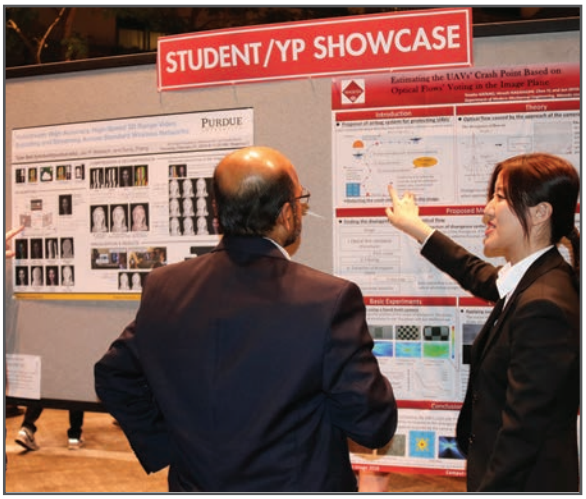
JOIN US AT THE NEXT EI!

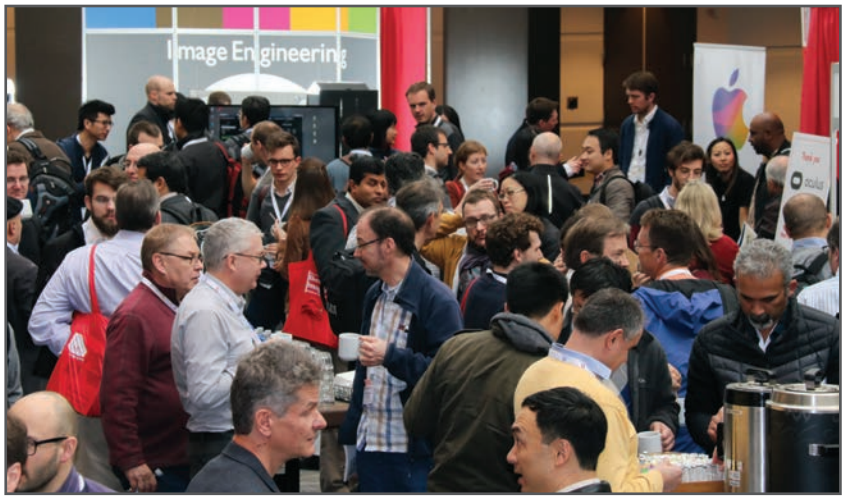
IS&T International Symposium on

Electronic Imaging

SCIENCE AND TECHNOLOGY

Imaging across applications . . . Where industry and academia meet!





• SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •
• INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •

www.electronicimaging.org

IS&T
imaging.org