10.20378/irb-58523

Port Logistics IT Security Monitoring

Prof. Dr. Wilfried Honekamp

Academy of Hamburg Police, Carl-Cohn-Straße 39, 22297 Hamburg,
wilfried.honekamp@polizei-studium.org

Lars Damm

Hamburger Hafen und Logistik AG, Bei St. Annen 1, 20457 Hamburg,
Damm-L@hhla.de

Torsten Fokuhl

DAKOSY Datenkommunikationssystem AG, Mattentwiete 2, 20457 Hamburg,
Fokuhl@DAKOSY.de

Abstract:

Hackers and cyber-attacks are becoming an increasing threat to the port industry, whose progressive digitisation further increases sensitivity to such risks. An innovative, cross-company linkage of the various existing IT security tools will substantially improve the detection and defence against cyber-attacks on the IT systems of the German port handling companies. Therefore, the partners Hamburger Hafen und Logistik AG (HHLA), DAKOSY AG and Hamburg University as well as EUROGATE and the Academy of Hamburg Police as associate partners have come together in the three-year program "HITS-Moni" to bundle the different competencies and resources to develop new concepts and procedures and to evaluate them with a software demonstrator.

JEL Classification: R49, O33, K39

Keywords: Security, IT, monitoring, deep learning, SmartPort.

1 Introduction

Cyber- and hacker attacks are becoming an increasing threat to companies in the port industry, whose progressive digitisation is further increasing their sensitivity to such risks. By implementing the SmartPort, i.e. the networking of the port and logistics sector with just-in-time production of industry, a cyber-attack can cause enormous economic costs. The shipping company and container terminal operator A.P. Møller Mærsk was targeted at the end of June 2017 by a cyber-attack by NotPetya, which significantly disrupted the operational processes for a period of several weeks. This attack resulted in costs of around USD 300 million.

Port industry companies have numerous powerful IT security tools that do not adequately reflect port-specific security requirements. In addition, coordination of various IT security tools currently cannot be reliably assured. Carefully executed attacks, that are at most visible in a few anomalies, are not or too late detected. The Federal Government has set the framework conditions for the protection of IT in ports with the 2015 national port concept. The aim is to secure business processes and promote international competitiveness. In addition, the ability to analyse and respond on the ground is to be strengthened and law enforcement in cyberspace is to be intensified. Cyber espionage and cyber sabotage should be effectively combated.

HHLA, as a major port and logistics service provider, has numerous IT security tools that show good results in limited areas of responsibility, but are very time-consuming to look after and evaluate while imposing heavy burden on employees. Complex standard IT security products only insufficiently consider port-specific IT requirements. A higher-level, systematic and preferably automatic correlation as well as a coordination of the various IT security tools does not currently take place, but would significantly increase the effect of the entire information security system. Detecting attacks that are made up of different anomalies, each below the triggering threshold of a singular system, are not yet apparent with traditional IT standard solutions, yet can lead to massive disruptions in availability or data integrity.

The German Federal Office for Information Security (BSI) Act requires in §8a (1) that operators of critical infrastructures implement appropriate organisational and technical arrangements to prevent disruptions to the availability, integrity, authenticity and confidentiality of their IT systems, components or processes that are relevant to the functioning of their critical infrastructures. The state of the art should be adhered, too. The implementation of this law will be relevant for HHLA as the largest operator of container terminals in Germany. The BSI is designated as the central reporting office for security in the information technology of critical infrastructures (§8b BSIG). In addition to the compulsory notifications specified in §8b (4) BSIG for certain situations, the BSI is responsible for the creation of the situation report (§8b (2) section 3) as complete, qualified and easily usable as possible, even by companies

whose transport or transshipment volumes are below the threshold values of the BSI-KritisV. With the implementation of this research project, HHLA will be able to send considerably more extensive and qualified data to the BSI. This will hopefully improve the federal situation on cybercrime and substantially support the work of the BSI. In addition, a way will be shown to extend the exchange to other port handling companies (horizontally) or corresponding links in the process chain (vertically, such as IT service providers, authorities, railway operators, shipping companies, haulers). With respect to the above-mentioned challenges the project aims at the following goals:

- early detect and defend port-specific cyber-attacks by monitoring with innovative algorithms
- improve the recognisability of novel attacks
- develop a concept for the ergonomic representation of possible attacks (avoidance of neurostress among employees)
- structure and promote exchanges on cyber-attacks between logistic companies.

2 Background

The industry offers a wide range of classic firewalls and anti-virus software products that can generally fend off standardized and untargeted hacker attacks. However, professional IT specialists or job hackers are able to circumvent these well-known individual tools, or deliberately undercut the usual warning threshold. Anomalies in the information system of a company always occur; many are even caused by their own users. Around 20% of the attacks or abuses come from employees within the company, while most of these irregularities or anomalies may occur unintentionally. It has since been found that there are always external cyber-attacks or accesses that are not recognized for a long time, before it comes to the actual attack with visible negative effects. Very often unauthorized external access to an IT system is already established long before detection occurs. According to a recent study a median of 78 days is needed before companies detect such intruders and only then can take countermeasures (FireEye 2019).

Even a vulnerability and risk analysis tailored to port logistics does not currently exist. Software specifically tailored to the needs of port logistics can specifically address the systems used in port logistics and address the specific threats in this industry, such as: moving goods, layer 7 attacks on data elements along the process chain, and interference in payments and politically motivated attacks (hacktivism) focus. Port logistics uses a variety of tools to improve IT security. These include e.g. proxies, mail gateways, virus scanners, USB locks, monitoring, firewalls, and intrusion prevention systems. These different systems require different operators and create diverse, sometimes even contradictory messages. The correlation and coordination of the different messages takes time, which may be missing in the fight against cyber-attacks. Unified

security management tools are available on the market (e.g. Alienvault, LogRhythm), but they have weaknesses, especially in the combination of information and the simplicity of the presentation of results. In addition, port logistics security requirements in the fields of device control and the multi company business process are too short. On the other hand, technologies for processing log files (Graylog, Elasticsearch) are available, but they do not focus on security aspects or ready-made forms of presentation. All available solutions lack the reduction of the number of less relevant messages, the early identification of attack preparations, e.g. automatic baselining, and the identification of novel attack patterns.

Disterer (2015) calls for systematically addressing and differentiating IT security risks in order to be able to plan, develop, control and monitor measures specifically for specific risk areas. The BSI (2012) recommends a vulnerability analysis with the software tool OpenVAS (or the commercial implementation Greenbone). This is now available in version 9. For risk analysis, the BSI (2008) published the standard 100-3 and in November 2017 transferred it to the standard 200-3 into a simplified hazard model. Due to increasing complexity of the systems Schaumüller-Bichl and Kolberger (2016) propagate a scenario-based impact analysis. Different scenarios are thought through and their effects on the protection goals are estimated. However, an industry-specific security standard for critical infrastructure in the transport and logistics sector does not yet exist. Nor is there currently any literature on vulnerability or risk analysis specifically focused on IT in port logistics.

There are a number of Security Information and Event Management (SIEM) tools available for managing IT security information and events. Cam et al. (2016) cite OSSIM, ArcSight, and Splunk as the top three. OSSIM is the open source variant of AlienVault's commercial tool. The implementation and use requires a considerable amount of time and personnel for document verification, communication in AlienVault's online forums and research. However, this effort can be outsourced to external service providers. Hewlett Packard's ArcSight is the most widely used SIEM tool. Like OSSIM, ArcSight is rule-based. Splunk, on the other hand, works with indexed databases that are searched for specific correlation-based patterns based on their own Search Processing Language (SPL). All tools have in common that they only react to known patterns and are not capable of learning.

Detken et al. (2017) also mention the open-source SIEM of rt solutions.de GmbH. However, this does not provide "guaranteed event processing", which raises doubts about reliability. The group is working in the CLEARER project on the development of network access control systems with SIEM functionality for small and medium-sized enterprises. A self-learning SIEM tailored to IT in port logistics does not currently exist.

3 Approaches

In this part the approaches to work on the project goals are described. The chapter starts with the early detection and defence by monitoring with innovative algorithms. Then the evaluation process of novel attacks is described. This is followed by the description of the ergonomic representation of possible attacks. Finally, the data exchanges between companies are depicted.

3.1 Early detect and defend by monitoring with innovative algorithms

In a first step, all internal and external interfaces must be taken into account across the company. It is all about the question of what data is available in the system, can be collected technically and meaningfully processed. This requires a comprehensive analysis of all existing systems supporting the business processes under consideration. These are, among others, services on servers and workstations such as anti-virus programs and firewalls, decentralised (network) intrusion detection systems (IDS) and prevention systems (IPS). Figure 1 depicts an IPS in a company network.

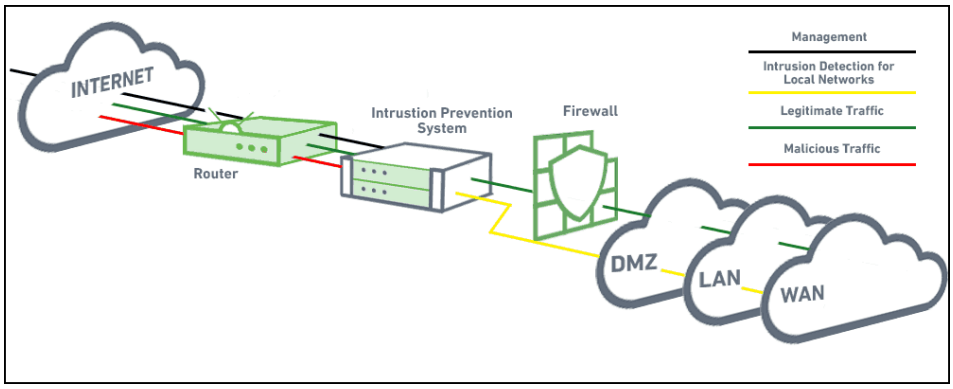

Figure 1: Intrusion prevention system (Borkar 2019)

Furthermore, information, that can be collected, has to be assessed and analysed for its relevance to incident detection and investigation within and for the systems under consideration, as well as how data collection and storage may affect the usability of the systems to users at runtime. This assessment is supported by the identification of potential vulnerabilities in the overall system, which already provides evidence of critical parts of the system and thus show the significance of the monitoring data of these parts of the system.

In a second step, the data must be reduced to the essentials so that forensic investigations become possible. For comprehensive analysis of all data of the individual sending IT elements it is mandatory to set up a common database with a uniform format for all data. In particular, the semantics of the field names must be uniform, so that comprehensive analyses can be meaningfully carried out. The existing data of all IT elements involved must be examined for structure and content, and data elements important for IT security monitoring must be identified. In addition to collecting low-

level technical elements, the performance and health data of the relevant business processes (within IT systems) must be observed and aggregated in the same way. Then, for each IT element, a process must be developed that receives and extracts the necessary content from the raw data, transforms it into the common format, and submits the record to the database. The entries of this database can then be used as input vectors of a multilayer neural network establishing deep learning. Figure 2 maps deep learning into machine learning and artificial intelligence.

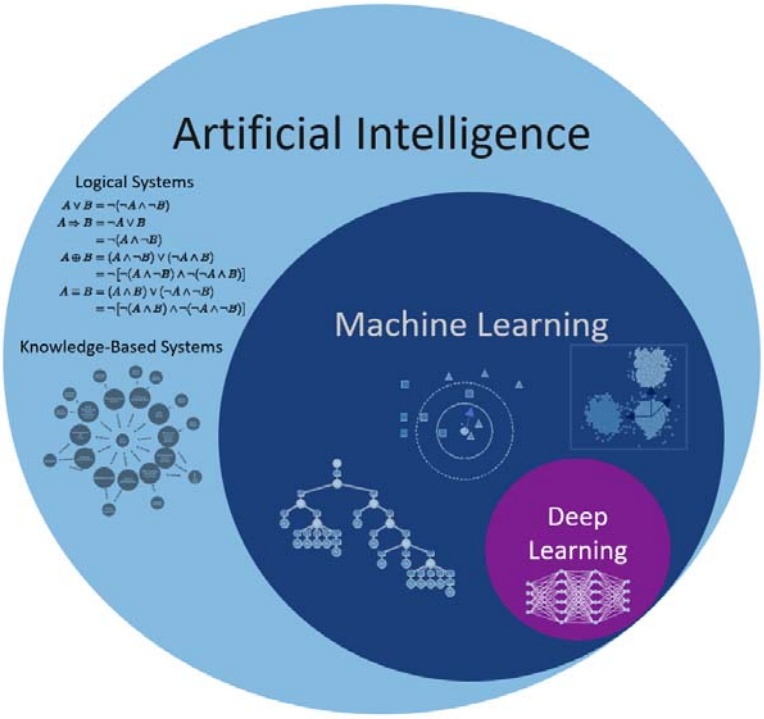

Figure 2: Artificial intelligence, machine learning, and deep learning (Aunkofer 2018)

This approach allows additional correlation of the data and possibly results in an alert. Thus, despite expected flood of data, it will be possible to detect attacks early and precisely.

3.2 Evaluate novel attacks

To detect new attack patterns, a robust cyber-attack kill chain analysis is necessary. Figure 3 shows the kill chain first published by Hutchins, Cloppert and Amin (2011). Subsequently, the above-mentioned additions of intelligent components are to make, by which reaction and communication options could be shown. The automated actions of the protection systems are applied in the different phases. In the reconnaissance phase, firewalls and access control lists (ACL) could deny access, web analytics could detect attacks. In the weaponisation phase network IPS and IDS could be effective. The delivery phase can at best be detected by vigilant users (Lovinus 2016). Filters could deny and antivirus systems could disrupt the delivery. By putting software deliveries into monitored queues, an attack could be degraded.

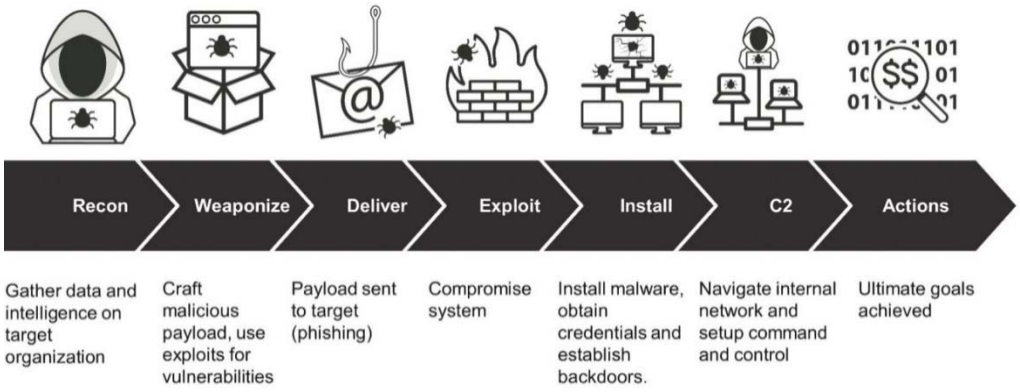

Figure 3: Cyber-attack chain (Lockheed Martin 2018)

The exploitation could be prevented by keeping the system hard- and software up to date, closing known security flaws. Furthermore, exploitation could be detected by host IDS and disrupted by data execution prevention. In the installation phase, the attacker could be kept in a sandbox, e.g. by a chroot jail (Badjatiya 2019), detected by a host IDS or disrupted by an antivirus system. In the command and control (C2) phase, firewalls that control outgoing traffic and ACL could prevent the hostile action. Network IDS and IPS also could be effective. As more and more traffic is encrypted in https a decryption at a central proxy server with forwarding of the payloads to an analysing engine should be evaluated. A tarpit could degrade the attack (Maximov, Sokolovsky, Gavrilov 2017) and a domain name service redirection could deceive the attacker. Finally, the actions on the targeted objectives could be detected by auditing, degraded by quality of service and deceived by honypots. All these measures are initiated only if a single system's detection is sufficiently reliable. Their combination with the broad set of further observed data below the single elements' thresholds could be combined in a system of systems supported by machine learning with deep learning algorithms.

3.3 Ergonomic representation of possible attacks

Ergonomic aspects of information representation have been discussed in science for many years. Bruyas, Le Breton, and Pauzié (1998, p. 412) conclude that graphical "representation of an object should be quickly understood, with no ambiguity, […] when considering the high time constraint context of some situations". Visual representation and interaction mechanisms have been identified as decisive criteria (Luzzardi, Dal Sasso Freitas (2003). In control rooms, where an application of our monitoring system is to be implemented, responsible control system design with implementation of ergonomic aspects according to ISO 9241 is required. Human-centred design is also required (Skřehot, Marek, Houser 2016).

3.4 Exchanges between companies

Threat intelligence is a commodity. There are several threat intelligence sharing platforms with different standards for describing threats. One, the intrusion detection message exchange format (IDMEF) is described in RFC 4765 by Debar, Curry and Feinstein (2007). It is to be evaluated whether this format is suited to share harbour related security information. More recently, the malware information-sharing platform (MISP) has gained in maturity and interest since the beginning of the project in 2011, not least among public IT security authorities in Europe (Dulaunoy et al. 2019). The BSI evaluates operating models to exchange such information with operators of critical infrastructures in Germany (BSI 2019, p. 59).

4 Outlook

In the project, the cooperators work on the above mentioned challenges along the information processing path, beginning with the basic information elements, the aggregation phase and the learning system to the output handling like automated actions, visualisation and situation reporting to third parties. The project is scheduled until February 2022, further results are to be published.

5 Acknowlegements

The project is founded by the German Federal Ministry of Transport and Digital Infrastructure in line with the financial assistance programme for innovative port technologies (IHATEC).

6 References

Aunkofer, B. (2018): Machine Learning vs Deep Learning – Wo liegt der Unterschied? Accessed on 13.10.2019 at https://data-science-blog.com/blog/2018/05/14/machine-learning-vs-deep-learning-wo-liegt-der-unterschied/.

Badjatiya, P. (2019): Linux Virtualization - Chroot Jail - GeeksforGeeks. Accessed on 13.10.2019 at https://www.geeksforgeeks.org/linux-virtualization-using-chroot-jail/.

Borkar, P. (2019): IPS Security: How Active Security Saves Time and Stops Attacks in their Tracks. Accessed on 13.10.2019 at https://www.exabeam.com/ueba/ipssecurity-how-active-security-saves-time-and-stop-attacks-in-their-tracks/.

Bruyas, M.-P.; Le Breton, B. and Pauzié, A. (1998): Ergonomic guidelines for the design of pictorial information. International Journal of Industrial Ergonomics 21 (1998) p. 407–413.

BSI (2008): BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5.

BSI (2012): Schwachstellen-Analyse in Netzen unter Einsatz von OpenVAS. SI-CS 007 | Version 1.00 vom 29.05.2012.

BSI (2017): BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0.

BSI (2019): Die Lage der IT-Sicherheit in Deutschland 2019. Accessed on 13.11.2019 at https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2019.pdf?__blob=publicationFile&v=4.

Cam, H.; Ljungberg, M.; Oniha, A.; Schulz, A. (2016): Dynamic Analytics-Driven Assessment of Vulnerabilities and Exploitation. U.S. Army Research and MIT Lincoln Laboratory.

Cyberwarzone (2014): 8 Steps to perform a successful cyber-attack. Accessed on 13.10.2019 at https://cyberwarzone.com/8-steps-perform-successful-cyber-attack/.

Debar, H.; Curry, D.; Feinstein, B. (2007): RFC 4765: The Intrusion Detection Message Exchange Format (IDMEF). Accessed on 13.10.2019 at https://www.heise.de/netze/rfc/rfcs/rfc4765.shtml.

Detken, K.O.; Kleiner, C.; Rohde, M.; Steiner, M. (2017): IT-Sicherheitsanalyse durch NAC-Systeme mit SIEM-Funktionalität. DACH Security 2017.

Disterer, G. (2015): IT-Risiken systematisch unterscheiden. Wirtschaftsinformatik & Management 6, 2015, p. 92–100.

Dulaunoy, A.; Iklody, A.; Dereszowski, A.; Studer, C.; Vandeplas, C.; Andre, D.; Servili, D.; Wagener, G.; Vinot, R.; Mokaddem, S.; Rommelfangen, S.; Clement, S. (2019): MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. Accessed on 13.11.2019 at https://www.misp-project.org/who/.

FireEye (2019): M-Trends 2019 Accessed on 13.11.2019 at https://content.fireeye.com/m-trends.

Hutchins, E. M.; Cloppert, M. J.; Amin, R. M. (2011): Intelligence driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research 1.1: p. 80.

Lockheed Martin (o.D.) cited in Henkel, M. (2018) Cyber Kill Chain: IT-Infrastruktur gezielt schützen. Accessed on 13.10.2019 at https://www.techtag.de/it-und-hightech/it-security/cyber-kill-chain-it-infrastruktur/.

Lovinus, A. (2016): Vigilant Users Are the Best Malware Tools. Accessed on 13.10.2019 at https://www.neweggbusiness.com/smartbuyer/netsec/vigilant-users-best-malware-tools-10-steps-effective-anti-phishing-training/.

Luzzardi, P. R. G.; Dal Sasso Freitas, C. M. (2003): An Extended Set of Erg.onomic Criteria for Information Visualization Techniques. Accessed on 13.10.2019 at https://pdfs.semanticscholar.org/2d25/2f2216a7a1ab5aa4b3aa16714385b65fb324.pdf.

Maximov, R. V.; Sokolovsky, S. P.; Gavrilov, A. L. (2017): Hiding Computer Network Proactive Security Tools Unmasking Features. Accessed on 13.10.2019 at https://pdfs.semanticscholar.org/2c60/2d31574dcf1514061d3351bac88f7d13ee27.pdf.

Schaumüller-Bichl, I.; Kolberger, A. (2016): Information Security Risk Analysis in komplexen Systemen – neue Herausforderungen und Lösungsansätze. In: Mayr HC und Pinzger M (Hrsg.): INFORMATIK 2016. Gesellschaft für Informatik, Bonn, p. 609–617.

Skřehot, P.; Marek, J.; Houser, F. (2016): Ergonomic aspects in control rooms. Theoretical Issues in Ergonomics Science, p. 1–13.