Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 190 (2021) 597–603

Procedia Computer Science

www.elsevier.com/locate/procedia

2020 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: Eleventh Annual Meeting of the BICA Society

Network Protection Tools for Network Security Intelligence Centers

Natalia Miloslavskaya*

The National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), 31 Kashirskoye shosse, Moscow, Russia

Abstract

Continuing our research on designing a Network Security Intelligence Center as a combination of a Security Intelligence Center and a Network Operations Center we propose the NSIC's security zone infrastructure with five zones, a few subzones and sandboxing, and network protection tools (NPTs) recommended for use to secure resilient NSIC's operation.

Keywords: network protection tools, Network Security Intelligence Center, information security

1. Introduction

The current state-of-the-art in information security (IS) can be characterized by the following facts. Data breaches are detected in an average of 276 days (versus 197 in 2018) [1]. Insider attacks are detected within a few minutes (22% of respondents), hours (28%), or a day (26%) [2]. Detection of an IS violation is carried out in several months (30% of respondents) and even years (40%) [3]. 81% of IS violations are discovered within days or less [4]. Attacks occur every 39 seconds, on average 2244 times a day [5]. There is a theft of 75 records per second (Source: Breach Level Index). An average of 30,000 websites is hacked every day (Source: Forbes). 300,000 new malware emerges daily (Source: McAfee). At the same time, 73% of hackers said that traditional firewalls (FWs) and anti-virus software are outdated (Source: Thycotic.com). All this leads to the conclusion that it is necessary to effectively and efficiently counter network attacks, the scale and complexity of which is constantly growing, while the use of traditional reactive (not proactive) strategies and systems for IS ensuring and not foreseeing IS threats and incidents

* Corresponding author.
E-mail address: NGMiloslavskaya@mephi.ru

10.1016/j.procs.2021.06.070

cannot provide the required IS level for networks and support properly modern perimeterless network security.

Today's businesses need to enhance their security via quick adaptation to these challenges. Various types of information, services delivered in 24x7 mode, and processes underlying these businesses should be protected. Under the circumstances, the lack of advanced threat detection and response capabilities, as well as busy IS teams, lacked in-depth security expertise, exacerbate the situation. In this landscape, the well-known "Detect-Investigate-Respond" triad must be added by the fourth very critical component named "Adapt", which should be based on Security Intelligence (SI) approach.

After exploring various options, we propose to build a Network Security Intelligence Center (NSIC) as a combination of the Security Intelligence Center (SIC) and Network Operations Center (NOC) for organizations internally. Continuing our research on designing NSICs [6-9], here we describe in detail their security zone infrastructure consisting of five zones (untrusted, demilitarized (semi-trusted), trusted, restricted, and management) with their specific subzones and special sandboxing component. The goal of the paper is to recommend network protection tools (NPTs) for use in these zones to secure resilient NSIC's operations.

2. Related Work

The creation of the innovative NSIC concept, its interpretation, and construction through original research contributes substantially to the modern networks' security, as it extends the forefront of the main security measures and tools used nowadays. The NSIC introduces powerful synergies of SICs and NOCs via people collaboration and toolkits and techniques joint usage. The corresponding structural and logical schema of the research conducted in [6-9] can be illustrated by Fig. 1, where CERTs/CIRTs (Computer Emergency Response Teams/Computer Incident Response Teams) were the structures that were in some sense forerunners for Security Operation Centers (SOCs) regarding its staff. It also emphasizes the main mottos of SOCs (DETECT IS incidents via constant monitoring), SICs (ANALYSE & REACT for real-time IS incident management), and developed NSICs (ADAPT for proactive network security).

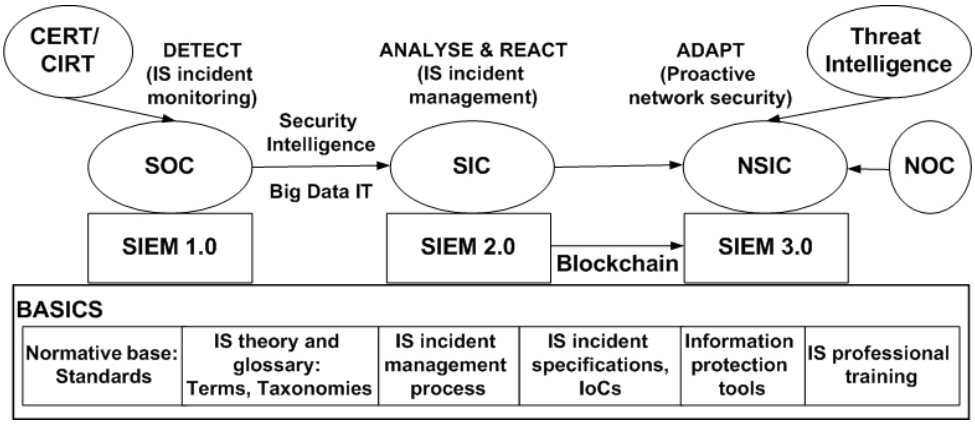

Figure 1. Structural and Logical Schema of the NSIC's development

3. Detailed NSIC's security zone infrastructure

The NSIC's detailed security zone diagram is depicted in Fig. 2 [9]. It contains five foundational layers or dedicated security zones. These security zones can be described as follows.

1) *Untrusted Zone* for intranet's assets not owned by the NSIC and not included into the NSIC itself, but being under the NSIC's control, and remote NSIC's privileged users/developers/administrators (via secure protocols like IPsec (IP Security) or Virtual Private Network using Secure Socket Layer protocol (SSL VPN)). NPTs for securing intranets are here. These tools are the main sources of intranet's IS-related data being transferred to the NSIC for deep analysis and generating feedback in

the form of command information for reconfiguring NPTs and thus strengthening the intranet's network security;

2) *Demilitarized (Semi-Trusted) Zone* (DMZ) [10] as a physical or logical NSIC's forefront subnetwork for external-facing servers and services that are externally shared by the NSIC and organization's intranet as well as remote and infra NSIC's services (like Domain Name System (DNS), Simple Mail Transfer Protocol (SMTP), etc.). Its purpose is to separate the NSIC from the NSIC's Untrusted Zone and, hence, to add an additional layer of security to the NSIC. Users from Untrusted Zone only have direct access to the DMZ, but not to any other "deeper" NSIC's part. It can be divided into two zones, which are physically separated from the NSIC, to provide an additional option to secure NSIC's network-centric applications:
    a. *Demilitarized Zone 1* (External Load Balancing DMZ) with external-facing access to the intranet and NSIC's incoming traffic management based on External Load Balancer (for IS-related data collected from various internal sources and external Threat Intelligence) and its hot standby for operational resilience after the first external front-end FW;
    b. *Demilitarized Zone 2* (Remote Access DMZ) after the second external FW. The main security gateway (with remote entry server) to the NSIC Perimeter is here. For example, encrypted VPN traffic for NSIC Management Zone from the remote NSIC's administrator should be decrypted there. No encrypted traffic should cross the NSIC Perimeter. Otherwise, any malicious code encrypted by attackers can cross it inside the encrypted tunnel. A sandbox solution [11] is used for this purpose as a highly controlled environment for detecting and blocking any malicious activity (such as Advanced Persistent Threats (APTs), advanced malware, and 0-day attacks) at the pre-infection stage before intruders will use some evasion techniques. In particular, it should be able to detect malware in data files before it is fully deployed, by watching the activity at the processor instruction level during the exploit phase, when the attack is trying to obtain unlawful execution privileges from the operating system;
3) *Trusted Zone* with the controlled environment after the internal back-end FW for NSIC's internal-exposed systems (like internal load balancing/performance optimization, device testing, and troubleshooting platforms, application services and management, services with limited access to NSIC's staff only, etc.);
4) *Restricted Zone* for NSIC's high risk and/or mission-critical systems (critical services and servers, NSIC's Data Center with a knowledge base and another DBs with sensitive data, etc.);
5) *Management Zone* for all NSIC's assets such as infrastructure services, network devices, and traffic telemetry, storage, and Data Center with computational power and applications necessary to support NSIC's centralized functioning and accommodate its big data, virtualization, configuration, changes, patch, backups and IS management systems, including IS centralized real-time logging, monitoring and reporting, Security Information and Event Management (SIEM) system, Security Orchestration and Automatic Response (SOAR) [12] system, analytical tools, regulatory compliance, security scanners, etc.

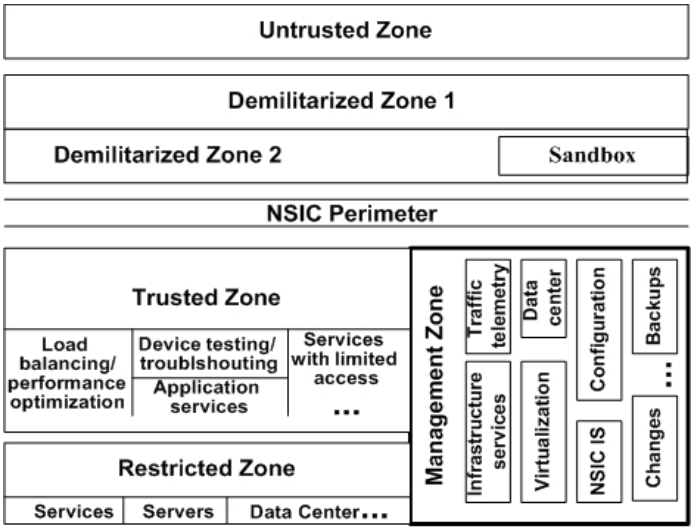

Figure 2. Detailed NSIC's security zone infrastructure.

We propose to design several subzones within trusted and restricted security zones that enable special cases, listed above under the description of their functional components and additional subzone boundary control.

4. Recommended NPTs for use in the NSIC's zones

For the developed NSIC's secure zone architecture, applicable measures and tools of ensuring its IS are determined. They are designed to protect its network infrastructure, device functions, information resources and data, user management, etc. The main subsystems providing "defense-in-depth" [13] for NSIC are as follows:

- protection of the network level (appropriate setting of network equipment, FWs, crypto routers, etc.), including, for example, registration of interaction processes between various information systems in normal modes and a case of IS violations;
- protection against unauthorized access (for example, unauthorized review and copying of electronic documents, data changes, and violation of software integrity) for all NSIC's elements, including built-in NPTs;
- protection of the application level;
- cryptographic protection of information to protect data and documents during transmission and at rest (in storage);
- protection of the telecommunications network, including, for example, control over the functioning of all intranet's elements;
- technological protection of information (protection at the level of technological information processing processes).

The following set of measures and NPTs necessary and sufficient for the functioning of the NSIC and its self-defense are proposed:

- Identity and Access Management (IAM) systems: password, two or more factor authentication, biometric authentication for special zones and subzones, including special databases, server access control lists, etc.;
- tools for capturing data flow and individual packets – tools for Network Traffic Analysis [14];
- anti-virus software and malware protection;
- Intrusion Detection System/Intrusion Prevention System (IDS/IPS) with Deep Packet Inspection (DPI) and sensors on all critical (especially important) communication channels of the NSIC;

- security and access control gateways, including FWs (Next-Generation FWs (NGFW), etc.) at the boundaries of zones and subzones, to manage their perimeters and study each packet passing through the boundaries for each session at a speed in "hard" real-time;
- tools for monitoring the integrity of file systems, separate files, software, etc.;
- Data Loss Prevention (DLP) system, sandbox, and content monitoring tools;
- tools for web and URLs filtering based on a FW for web applications (WAF);
- tools for protecting applications, specialized clouds, wireless access, and virtualization, as needed;
- tools for cryptographic information protection (CIP) with support for public key infrastructure (PKI), electronic signatures, and VPN, especially when working with IS-related data analytics;
- tools for continuous logging and log management;
- tools for protecting NSIC's endpoints, device testing, and troubleshooting;
- tools for generating alerts about danger in real-time using SIEM and Security Orchestration and Automatic Response (SOAR) systems;
- tools for managing configuration settings and installing security updates;
- tools for managing eliminating vulnerabilities and installing security updates, including security scanners and systems for static and dynamic testing of application security;
- load balancers and backup proxy servers;
- backup tools;
- tools for assessing IS risks;
- tools for collecting digital evidence for investigating IS incidents, etc.

Realizing that with an integrated approach to ensuring NSIC's IS it is very difficult to separate clearly the listed NPTs into security zones, since many of them must operate at the same time in several zones at once, and IDS/IPS sensors by their nature are necessarily installed in all zones with a central console at the control level, let us indicate their possible approximate location as follows:

- DMZ for intranet's users and developers, NSIC's personnel and contract workers: IAM system (password authentication), anti-virus software, IDS/IPS, VPN, NGFW, CPI tools, log management system, DLP system, sandbox, static and dynamic application security testing systems;
- Trusted zone (low or medium IS risks) for NSIC's developers, personnel, and contract workers: IAM system (password authentication), anti-virus software, IDS/IPS, VPN, NGFW, at the border, WAF, log management system, CIP system, integrity control tools, load balancing tools, endpoint protection tools, device testing and troubleshooting, systems for static and dynamic application security testing;
- Restricted zone (high IS risks) for a limited number of NSIC's users (IS analysts, etc.): IAM system (two or more factor authentication, biometric authentication for special subzones), anti-virus software, IDS/IPS, VPN, NGFW at the border, log management system, CIP tools, integrity control tools, endpoint protection tools, IS risk assessment tools;
- Management zone (high IS risks) for privileged network administrators and IS administrators and NSIC's auditors: IAM system (two or more factor authentication, biometric authentication), anti-virus software, VPN, NGFW at the border, log management system, CIP tools, integrity control tools, endpoint protection tools, backup tools, tools for capturing data flow and individual packets, security scanners, systems for static and dynamic application security testing, tools for managing configuration settings and installing security updates, SIEM and SOAR systems, tools for collecting digital evidence of IS incidents.

5. Conclusion

In addition to the list of NPTs, in the conclusion, several significant comments regarding IS controls in NSICs are given.

An important idea for this level is the separation of management data and data characterizing the intranet's IS. It will ensure that the second group of data does not interfere with the NSIC's management and the freedom to manage the entire NSIC from affecting the data of the second group, as well as management of the levels of platforms and software in the mode real-time and protection against computer attacks.

In the NSIC's secure zone architecture, if necessary, virtual local area networks (VLANs) should be used, which is consistent with the support of data centers with big and fast IS-related data and interaction with virtual devices and hosts that implement virtual switches. It is important that the separate NSIC's virtual servers, intended for big data management, are protected under all applicable standards and organization's documents, for example, unnecessary services (for example, FTP) that are used for hacking by cybersecurity intruders should be removed for them.

It is also necessary to organize a timely process for managing software and operating system patches, backup services, and encryption of necessary data and documents.

To ensure the synchronization of all events in the intranet and the accuracy of log recording, it is important to correctly set the computer clock (timer) (for example, according to the universal global (Greenwich Mean Time), local daylight saving time or "summer" time). Log management tools and the data contained in them should be adequately protected from possible unauthorized access and operational problems, including the impossibility of shutdown, the invariability of the types of registered events, the prohibition of editing or deleting, as well as registration of the complete log recording and cases of the impossibility of recording events due to failures, or cases of overwriting new data over old ones. Data from the intranet's sources should immediately upon registration go to the NSIC's data lake.

The activities of the NSIC's administrator, operators, and analysts should be monitored by an IDS/IPS managed outside their area of authority and should be recorded in a separate log.

This list of recommendations can be expanded, but this is the topic of the next research.

Acknowledgements

This work was supported by the MEPhI Academic Excellence Project (agreement with the Ministry of Education and Science of the Russian Federation of August 27, 2013, project no. 02.a03.21.0005).

References

[1] Cost of a Data Breach Report 2019 (2019). URL: https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf (accessed by 04.03.2021).

[2] 2018 Insider Threat Report (2018). URL: https://crowdresearchpartners.com/insider-threat-report/ (accessed by 04.03.2021).

[3] 2019 Insider Threat Report: Executive Summary (2019). URL: https://enterprise.verizon.com/resources/ executivebriefs/insider-threat-report-executive-summary.pdf (accessed by 04.03.2021).

[4] Verizon. Data breach report highlights how unsecured cloud storage opens door to attacks (2020). URL: https://www.zdnet.com/article/verizons-data-breach-report-highlights-how-unsecured-cloud-storage-opens-door-to-attacks/ (accessed by 04.03.2021).

[5] Website hacking statistics of 2020 (2020). URL: https://www.webarxsecurity.com/website-hacking-statistics-2018-february/ (accessed by 04.03.2021).

[6] Miloslavskaya, Natalia, Tolstoy, Alexander, and Migalin, Anton. «Network Security Intelligence» Educational and Research Center. In: Bishop M., Futcher L., Miloslavskaya N., Theocharidou M. (eds) Information Security Education for a Global Digital Society. WISE 2017. Advances in Information and Communication Technology. Springer, 2017. Vol. 503. Pp. 157-168. DOI: 10.1007/978-3-319-58553-6_14.

[7] Miloslavskaya N. Network Security Intelligence Center as a combination of SIC and NOC. Postproceedings of the 9th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2018 (Ninth Annual Meeting of the BICA Society). Procedia Computer Science. 2018. Vol. 145, pp. 354-358. DOI: 10.1016/j.procs.2018.11.084.

[8] Miloslavskaya N. Developing a Network Security Intelligence Center. Postproceedings of the 9th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2018 (Ninth Annual Meeting of the BICA Society). Procedia Computer Science. 2018. Vol. 145, pp. 359-364. DOI: 10.1016/j.procs.2018.11.085.

[9] Miloslavskaya, Natalia. Security Zone Infrastructure for Network Security Intelligence Centers. In: Samsonovich A., Klimov V. (eds) Postproceedings of the 10th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2019. Procedia Computer Science. 2020. Pp. 51-56. DOI: 10.1016/j.procs.2020.02.113.

[10] Litkevich, Ben. DMZ (networking) (2019). URL: http://searchsecurity.techtarget.com/definition/DMZ (accessed by 04.03.2021).

[11] Exposing the Unkown: How Sandboxing Technology Fights Modern Threats. White Paper. CheckPoint Software Technologies Ltd (2015). URL: http://www.checkpoint.com (accessed by 04.03.2021).

[12] Security Orchestration, Automation And Response (SOAR) (2017). URL: https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar (accessed by 04.03.2021).

[13] Defense in Depth and How it Applies to Web Applications Retrieved March 12, 2019, from DZone: https://dzone.com/articles/defence-in-depth-and-how-it-applies-to-web-applica.
[14] 2019 Gartner Market Guide for Network Traffic Analysis (2019). URL: https://www.gartner.com/en/documents/3902353/market-guide-for-network-traffic-analysis (accessed by 04.03.2021).