CyberMonoLog

Cyber Security MONITORING and LOGGING Best Practice Guidance

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS F&E-Dienstleistungen 2020	**Status**	abgeschlossen
Projektstart	01.01.2022	**Projektende**	30.06.2023
Zeitraum	2022 - 2023	**Projektlaufzeit**	18 Monate
Keywords	Cyber Security, Logging, Monitoring, Guidelines		

Projektbeschreibung

Schwerwiegende Cyber-Angriffe auf Unternehmen und kritische Infrastrukturen beherrschen die wöchentliche Berichterstattung. Viele Vorfälle der jüngeren Vergangenheit, wie etwa der Tod einer deutschen Patientin aufgrund eines Ransomware-Angriffs auf eine Uni-Klinik im September 2020, oder die großflächige Unterwanderung von Infrastrukturen wie im Falle der SolarWinds-Hacks 2020, unterstreichen die brisante Lage. Neben diesen beispielhaften Berichten, verdeutlicht auch der Cybercrime Bericht 2019 des Bundeskriminalamts mit einem Anzeigenanstieg von 69,7% (widerrechtlicher Zugriff auf ein Computersystem), sowie 291,3% (Datenverarbeitungsmissbrauch) gegenüber dem Vorjahr, die wenig erfreuliche Security-Statistik.

Während jahrzehntelang der Fokus der Cyber Security Domäne auf Prävention und Perimeter-Sicherheit lag, hat sich die Ausrichtung in den letzten Jahren in Richtung aktiver Reaktion gewandelt. Es gilt als allgemein anerkannt, dass eine komplexe Infrastruktur auf Dauer nicht erfolgreich vor Angriffen geschützt werden kann. Daher ist es wichtig, das Zeitfenster der Angreifer – vom initialen Eindringen bis zu deren Entdeckung und dem Ergreifen von ersten Gegenmaßnahmen – auf die kürzest mögliche Zeitspanne zu reduzieren. Damit verringern sich auch die Möglichkeiten der Angreifer, schon das initiale Eindringen in ein Netz für einen erfolgreichen Angriff zu nutzen (d.h. das Erreichen der eigentlichen Ziele sicherzustellen, wie das Exfiltrieren von Daten oder das Lahmlegen einer Infrastruktur). Das Erkennen von Angriffen und die rasche Reaktion darauf sind daher essentielle Fähigkeiten für Organisationen – nicht nur für die Großindustrie, sondern insbesondere für kritische Infrastrukturanbieter (KI), als auch für den in Österreich so wichtigen KMU Sektor. Gerade diese agieren jedoch oft unter enormen Kostendruck, was den üblicherweise Ressourcenaufwändigen Einsatz komplexer Cyber Security Lösungen entgegensteht. Zudem sind Betreiber wesentlicher Dienste nach dem NISG auch dazu verpflichtet Cyber Security Lösungen nach dem Stand der Technik zum Einsatz zu bringen.

Ziel des Projekts ist daher die Erarbeitung von Best Practices für Cyber Security Monitoring und Logging (CyberMonoLog) basierend auf den bekannten Angriffstechniken und unter besonderer Berücksichtigung jener, welche nicht durch allgemein angewandte Best Practices/Standards bereits effektiv unterbunden werden. Angriffstechniken, welche aus wirtschaftlicher oder technischer Sicht typischerweise reaktiv behandelt werden, müssen durch Monitoring aufgedeckt werden. Letztendlich liegt dem Projekt somit ein Optimierungsproblem zugrunde: Es ist für eine Organisation unmöglich alle bekannten Angriffstechniken mit ökonomischen Mitteln zu erkennen. Die Forschungsfrage ist daher, welche Datenquellen (bzw. davon

emittierten Ereignisse) mit welchen Methoden analysiert werden müssen (Ranking), um mit vorab festgelegtem Ressourceneinsatz die meisten relevanten Angriffstechniken zu erkennen.
Die Ergebnisse des Projekts sollen möglichst praxisnahe Best Practice Guidelines zur Umsetzung einer Monitoring-Strategie für KMUs und KIs sein. Die Ausführungen werden sich auf den bekannten Stand der Technik stützen und die Anwendbarkeit der E-gebnisse durch eine Cross-Validierung mit externen Stakeholdern sowie Bedarfsträgern und Behörden und Experten von CERT.at sichergestellt. Rechtliche Aspekte (Datenschutz, arbeits-/dienstrechtliche Belange) werden berücksichtigt.

Abstract

Severe cyber attacks on companies and critical infrastructures dominate the weekly press reports. Many recent incidents, such as the death of a German patient as a result of a ransomware attack on a university clinic in September 2020, or the extensive infiltration of infrastructures, as in the case of the SolarWinds hacks 2020, underline the serious situation. In addition to these exemplary reports, the Cybercrime Report 2019 by the Federal Criminal Police Office (Bundeskriminalamt) also illustrates the unpleasant security statistics with an increase of complaints of 69.7% (illegal access to a computer system) and 291.3% (data processing abuse) compared to the previous year.
While the focus of the cyber security domain has been on prevention and perimeter security for decades, the focus has changed in the past few years towards active reaction. It is generally accepted that a complex infrastructure cannot be successfully protected against attacks in the long term. It is therefore important to reduce the attacker's time window - from the initial intrusion to their discovery and the taking of the first countermeasures - to the shortest possible time span. This also reduces the attacker's ability to use the initial intrusion into a network for a successful attack (i.e. to ensure that the actual goals are achieved, such as exfiltrating data or paralyzing an infrastructure). Detecting attacks and reacting quickly to them are therefore essential skills for organizations - not only for large-scale industry, but especially for critical infrastructure providers (CI) as well as for the SME sector, which is so important in Austria. However, in particular these often operate under enormous cost pressure, which is contrary to the usually resource-intensive use of complex cyber security solutions. In addition, operators of essential services are also obliged to use state-of-the-art cyber security solutions according to the NISG.
The aim of the project is therefore to develop best practices for cyber security monito-ing and logging (CyberMonoLog) based on the known attack techniques and with sp-cial consideration of those that are not already effectively prevented by generally applied best practices / standards. Attack techniques, which are typically treated reactively from an economic or technical point of view, must be uncovered through monitoring. Ultimately, the project is based on an optimization problem: It is impossible for an organization to identify all known attack techniques with economic means. The research question is therefore which data sources (or the events emitted by them) have to be analyzed with which methods (ranking) in order to identify most of the relevant attack techniques with a predefined use of resources.
The results of the project should be readily applicable best practice guidelines for the implementation of a monitoring strategy for SMEs and CIs. These guidelines will be based on the known state of the art and the applicability of the results is ensured by cross-validation with external stakeholders as well as authorities and experts from CERT.at. Legal aspects (data protection, labor law issues) are taken into account

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- SBA Research gemeinnützige GmbH
- Bundesministerium für Inneres
- Technische Universität Wien
- Bundeskanzleramt
- nic.at GmbH