KIRAS Erfolgsgeschichten

Projekt : CIIS – Cyber Incident Information Sharing
Informationsverteilung bei sicherheitsrelevanten Cyber-Zwischenfällen
Kurzbeschreibung

Ziel des Projektes CIIS *war die Entwicklung von Mechanismen zur effizienten Analyse von System-Logdaten über Aktivitäten und Angriffe in IKT-Netzen kritischer Infrastrukturen (Informationskorrelation, Aggregation, Fingerprinting, Visualisierung), und auch die Entwicklung von Methoden und Technologien für den Organisations-übergreifenden Austausch von Informationen über Cyber-Incidents zur besseren Abwehr von Cyberangriffen und zur effizienteren Bewertung der aktuellen Bedrohungslage. Dadurch sollte die Widerstandsfähigkeit von Systemen gegenüber Cyberangriffen in sensiblen Bereichen (z.B. Betreiber von kritischen Infrastrukturen) erhöht werden, der Informationsaustausch in diesen sensiblen Themen sowohl zwischen Unternehmen als auch zwischen Organisationseinheiten in großen Organisationen verbessert und insgesamt die operative Sicherheit im Betrieb kritischer Infrastrukturen gesteigert werden.*

Technologische Auswirkungen

Die derzeitige Implementierung der AIT AECID Technologie basiert auf einer Logdatenanalyse. Die Logdatenanalyse zur Erkennung von Sicherheitsvorfällen hat in einigen Bereichen klare Vorteile gegenüber der Nutzung von Netzwerkdaten:

- Es sind keine Analysebibliotheken für alle am Netzwerk gesprochenen Protokolle notwendig, stattdessen werden die Logdaten der involvierten Programme genutzt.
- Eine aufwändige und risikobehaftete Entschlüsselung von verschlüsselten Netzwerkprotokollen ist nicht notwendig.
- AECID ermöglicht eine kostengünstigere Analyse bei Alt/Legacysystemen, bei denen sich aufgrund der geringen Zahl bzw. nicht mehr vorhandener Dokumentation die Implementierung spezifischer Bibliotheken zur binären Netzwerkdatenanalyse nicht mehr rentieren.
- AECID ermöglicht eine rechenzeitgünstigere Analyse, da in Logdaten üblicherweise besonders wichtige Ereignisse und Informationen protokolliert werden, man auf der Netzwerkebene aber den gesamten Datenstrom zerlegen und diese Elemente erst extrahieren muss.
- Die Logdatenanalyse berücksichtigt nicht nur kommunizierte Daten, sondern auch den internen Zustand der beteiligten Systeme. So kann z.B. am Netzwerk nur erkannt werden, dass ein Server einen Loginversuch abgelehnt hat, aus den Logs wäre aber auch gleichzeitig der Grund erkennbar. Ein falsch eingetipptes Passwort als Grund könnte erwartbar und normal sein, ein gesperrter oder gelöschter Account oder sonstige Fehlerursachen nicht. So kann die Wahrscheinlichkeit des Passwortvertippens unterschiedlicher Nutzer ermittelt werden. Da der Nutzer „backup“ sich automatisiert anmeldet und sich daher nie vertippt, würde schon ein einziger Fehlversuch eine signifikante Abweichung darstellen.
- AECID erlaubt eine Anpassung der Regeln an das jeweilige Betriebsumfeld. So kann z.B. erkannt werden, dass die erfolgreiche Anmeldung eines Nutzers immer nur von

gewissen Rechnern aus erfolgt. Zugriffe von anderen Maschinen sind daher potentiell verdächtig.

Eine Besonderheit der modernen AIT AECID Technologie ist die einfache Einbindung in vorhandene IT-Infrastrukturen und entsprechende Betriebsprozesse. Da eine Musteranalyse erfolgt, ist keine detaillierte Kenntnis über die konkreten IT-Systeme für die Konfiguration notwendig. Vorteile sind damit:

- Integrationsmöglichkeit in bereits bestehende Sicherheitsinfrastrukturen: AECID agiert als weiterer Sensor und meldet erkannte Abweichungen an die bereits etablierten Systeme, also z.B. SIEM-Lösungen (Security information and event management). Damit können auch die bereits etablierten Incident-Handling-Prozesse beibehalten werden.
- Nutzung der in Produktionsfeldern häufigen zentralen Logdatenaggregation als einfach anzuzapfende Quelle von Logdaten. Dadurch kann meist eine aufwändigere verteilte Installation vermieden werden.
- Automatisierte Erkennung der Logdatenstruktur zur Extraktion der analyserelevanten Daten aus den Logeinträgen zur Reduktion des menschlichen Aufwands beim Einbinden neuer Quellen.
- Spezielle Implementierungen mit geringsten Leistungsanforderungen an das Zielsystem sind z.B. zur internen Überwachung von Embedded-Devices möglich.

Mögliche Auswertungen durch die AECID Technologie (Abbildung 1) umfassen:

- Network Interaction Graph Analyse: welche Maschinen kommunizieren miteinander.
- Authentication Interaction Graph: wer meldet sich von welcher Maschine wo an, mit welchen Credentials/Key Fingerprints.
- Syscall Audit Anomalieerkennung: Erkennen von atypischen Abläufen wie z.B. Admin-Fehlverhalten, Software-Fehlfunktion, Angriffen, aber auch von unsicheren Software- & Fehlkonfigurationen.

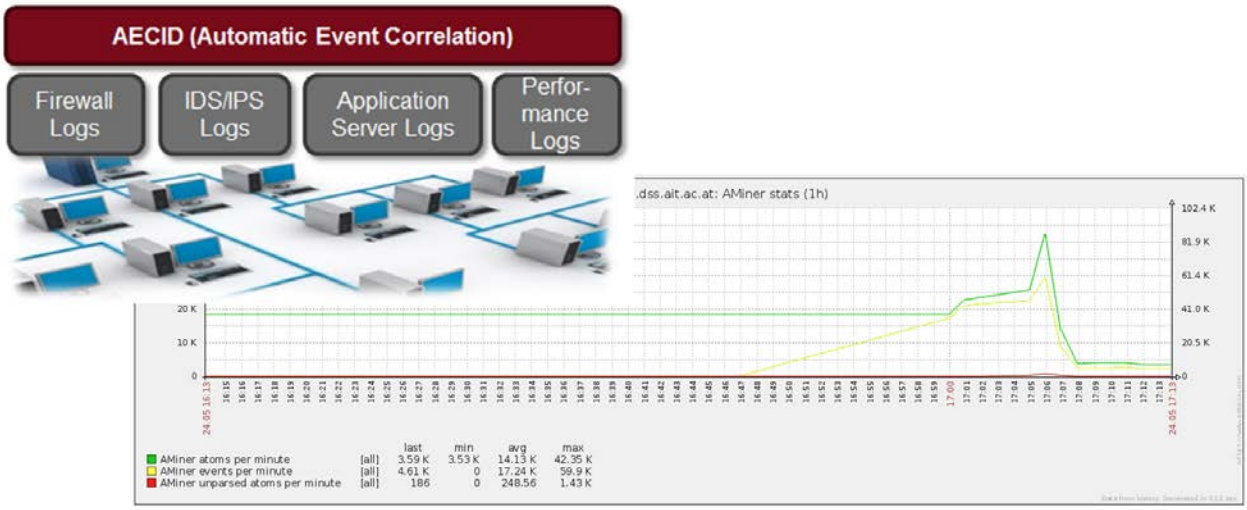

Abbildung 1: AECID erkennt Abweichungen vom Normalzustand in Logdatenströmen und versucht diese zu klassifizieren

Technische Leistungsmerkmale in einem exemplarischen Piloten

In einem Pilotversuch ist AECID seit Anfang 2016 (zum Zeitpunkt des Verfassens dieses Artikels 18 Monate) auf einem zentralen Remote-Syslog-Server im Einsatz. Dabei wird folgende Infrastruktur beobachtet und laufend analysiert:

- 4 Zonen: DMZ, interne Services, 2 Entwicklungszonen;
- getrennt durch Firewalls
- 25 Server
- 25 Firewalls, je 1 auf 1 Server
- Analysierte Log-Zeilen: 4Mio/Tag
- Apache-Systeme (6 Stück) mit etwa 20.000 Zugriffen/Tag
- Netzwerktransfers mit ~20GB/Tag
- ~20 Entwicklersysteme

Leistungsbedarf des Systems

- RAM-Bedarf zur Verarbeitung 15MB
- Disk 350kB
- CPU-Bedarf 1-2% bei 2.5GHz CPU

Wirtschaftliche Auswirkungen

Das Verwertungsmodell von AECID ist in Abbildung 2 überblicksmäßig dargestellt.

Erfolgreiche Pilotversuche wurden im Zuge des Projekts 2013 - 2016 sowohl in der AIT-eigenen Infrastruktur durchgeführt, sowie bei speziellen Anwendern mit überdurchschnittlich hohen Sicherheitsansprüchen.

Weiters wurden 2015 und 2016 durch die Analyse von Syscall Audit Logs mittels AECID in AIT-internen Pilotversuchen zahlreiche Schwachstellen in der weit verbreiteten Linux Virtualisierungs-Lösung LXC gefunden, dokumentiert und an die Entwickler zur Berichtigung weitergeleitet (CVE-2015-1331[1], CVE-2015-1334[2], CVE-2015-1335[3], CVE-2016-8649[4]).

2013 und 2016 wurde AECID mehrfach patentiert. Neben dem damit verbundenen Werbeeffekt sieht die weitere Strategie vor diese Patente[5,6] im Zuge von Lizenzierungsmodellen auch wirtschaftlich zu nutzen.

Um den Verwertungsprozess zu unterstützen ist es essentiell Reputation und Vertrauen in die von AIT entwickelte Lösung AECID aufzubauen. Dies ist insbesondere mit Hilfe der teilweisen Veröffentlichung von AECID-Komponenten als Open Source gelungen. Dabei erfolgte die Veröffentlichung unter der GPLv3 durch die einschlägigen Community Prozesse, die es erlauben, AECID als Teil etablierter Linux-Distributionen (Ubuntu[7] und Debian[8]) auszurol-

[1] http://www.securityfocus.com/bid/75999
[2] http://www.securityfocus.com/bid/75998
[3] http://www.securityfocus.com/bid/76894
[4] http://www.securityfocus.com/bid/94498
[5] Skopik F., Fiedler R. (2013): A50292/2013 (AT 514.215) - Verfahren zur Feststellung von Abweichungen von einem vorgegebenen Normalzustand, April 2013.
[6] Skopik F., Fiedler R. (2016): EP 1416597.2-1853 - Method for detecting deviations from a given standard state, Juni 2016.
[7] http://manpages.ubuntu.com/manpages/zesty/man1/AMiner.1.html

len. Der damit verbundene Qualitätssicherungsprozess und die erzielte Sichtbarkeit, sollten einen hinreichenden Werbeeffekt generieren, der einen direkten Zugang zu Endanwendern (Systemintegratoren, Lösungsanbietern) unterstützt. Dabei war die Strategie, nur die Kernkomponente „AMiner“ mit eingeschränkter Funktionalität 2016 zu veröffentlichen, welche als „Teaser“ diente – d.h., einerseits potentiellen Endanwendern die Fähigkeit von AECID zu demonstrieren, und andererseits Feedback von der technischen Community einzuholen. Letzteres erlaubte auch die breite Validierung des Systems durch die Community, weil v.a. im Zuge des Inklusionsprozesses in Debian wertvolles Feedback zur Erhöhung der Codequalität erfolgte. Die Verwertung komplexer Add-On Module, welche v.a. die geschützten Algorithmen enthalten, als auch spezifische Anpassungen für Bedarfsträger und damit auch deren Feedback, erfolgen im Zuge gesonderter Projekte. Weiters besteht die Möglichkeit den Open Source Teil unter der GPLv3 mittels Dual Licensing später kommerziell zu verwerten.

Die erfolgreiche Inklusion in die beiden Linux-Distributionen Ubuntu und Debian demonstriert auch die dafür erforderliche hohe Code-Qualität und rechtfertigen den Einsatz von AECID auch in Produktivumgebungen.

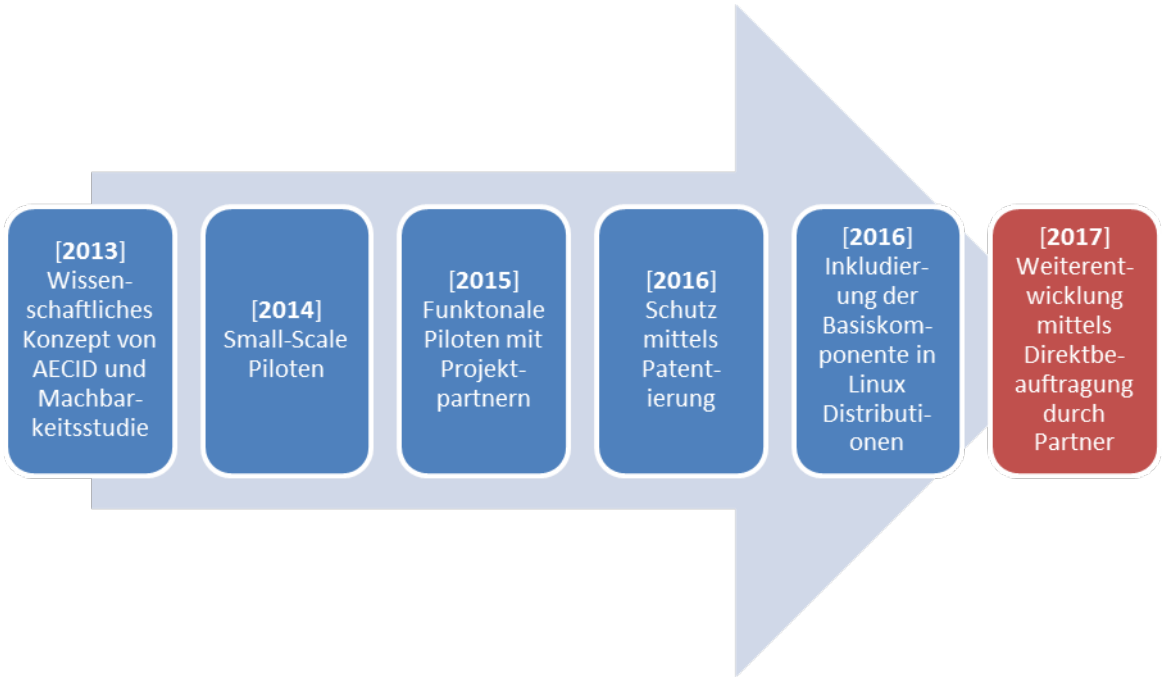

Abbildung 2: AECID Verwertungsmodell

Die Weiterentwicklung bzw. Anpassung der intelligenten Lernkomponente wurde für 2017 bereits von Partnern beauftragt.

Ausblick

Die zukünftige Entwicklung sieht insbesondere den Einsatz von AECID in der Industrieautomatisierung mit besonderem Fokus auf den Schutz kritischer Infrastrukturen vor. Dies ist gerade deswegen ein vielversprechendes Gebiet, weil einerseits mit Bestrebungen in den Bereichen Intelligente Stromnetze und Industrie 4.0 die Vernetzung von Industriesteueranlagen massiv zunimmt, andererseits, die Sicherheitsanforderungen in diesen Bereichen be-

[8] https://packages.debian.org/stretch/logdata-anomaly-miner (Debian stretch, stable branch, Juni 2017)

sonders hoch, jedoch effiziente Lösungen am Markt noch rar sind. AECID kann hier einen wesentlichen Beitrag leisten. Wichtige Untersuchungen hierzu erfolgen seit Beginn 2017 im Projekt synERGY[9].

Links

- AIT Austrian Institute of Technology GmbH, Center for Digital Safety & Security (Ko-ordinator) -- https://www.ait.ac.at
- Energie AG Oberösterreich Data GmbH -- https://www.energieag.at
- T-Systems Austria -- https://www.t-systems.com/at/de
- VRVis Forschungs GmbH -- http://www.vrvis.at/
- Bundesministerium für Inneres (BM.I) -- http://www.bmi.gv.at
- Bundesministerium für Landesverteidigung und Sport (BMLVS) -- www.bmlvs.gv.at/
- Institut für Rechts- und Kriminalsoziologie -- http://www.irks.at/
- Netelligenz e.U. -- http://www.netelligenz.at/

[9] IKT der Zukunft, Ausschreibung 2016; Fördernummer 855457; https://synergy.ait.ac.at/