Observability

MONITORING AUS SYSTEMSICHT?!

Wie bei vielen Hype-Wörtern ist auch „Observability“ zunächst nicht klar definiert – verschiedene Akteure verbinden damit offenbar unterschiedliche Dinge. Ziel des vorliegenden Beitrags ist es, den Begriff und die damit zusammenhängenden Möglichkeiten und Anwendungen fundiert zu ergründen und in den Kontext der Informationssicherheit einzuordnen.

Der Begriff Observability geistert seit einiger Zeit durch die Informationssicherheits-Landschaft – wie viele „Hype-Wörter“ als neues Kleid einer bekannten Technik oder Sicherheitsmethode, in diesem Fall als „neues Monitoring“ oder Prozess im Kontext des Betriebs eines Security-Information-and-Event-Managements (SIEM). Mit der Umsetzung oder Anwendung von Observability werden viele Vorteile propagiert, die mit dem einen oder anderen Produkt oder gar einer Technologieentwicklung verbunden werden. Ein „tieferer“ Einblick wird aber nicht vermittelt – daher bleibt auch unklar, was Observability denn nun eigentlich ist oder sein soll: eine Haltung, eine Aufgabe oder vielleicht eine Geschäfts- oder Sicherheitsmethode?! So fehlt letztlich nicht nur die Darstellung von Grundlagen und Wissen, sondern auch die Möglichkeit zur Einsicht in Aufgaben und Maßnahmen, die zur Verwirklichung etwaiger Vorteile erforderlich wären.

Definitionen

Gartner deklariert im Artikel „Die Monetarisierung beobachtbarer Daten wird Gewinner von Verlierern trennen“ [1] die „Applied Observability“ als Trendtechnologie: Diejenigen, die bis zum Jahr 2026 Observability erfolgreich einsetzen, werden mit einem Wettbewerbsvorteil durch kürzere Entscheidungsfindungen belohnt. Erforderlich hierfür sei, dass „verwertbare Daten aus verschiedenen Quellen angemessen verbunden, optimiert und kontextbezogen erweitert werden“. Für Gartner ist Applied Observability die „Nutzung von beobachtbaren Daten in einem hochgradig orchestrierten und integrierten Ansatz über Geschäftsfunktionen, Anwendungen sowie Infrastruktur- und Betriebsteams hinweg“.

Während Gartner die Observability also als Datenmanagement auf der Organisationsebene verortet, erfolgt durch Hersteller und Anbieter von Sicherheitslösungen eine Verknüpfung mit der Performance-Verbesserung beim Betrieb von IT-Systemen. So definiert etwa Splunk in [2] Observability als Mittel zur Verbesserung der Kontrolle über komplexe Systeme: Verstanden wird Observability als „Fähigkeit, die internen Zustände eines Systems zu messen, indem man seine Ausgabewerte untersucht“. Mithilfe detaillierter Einblicke durch umfangreiche Erfassung von Telemetriedaten (Metriken, Logs und Traces) stellt Splunk Observability als Möglichkeit zur Unterstützung eines breiten Spektrums von Problemen vor. Richtigerweise merkt das Unternehmen

an, dass Observability „gar nicht so neu ist und bereits vor Jahrzehnten in der Systemsteuerungstheorie geprägt wurde“.
Die englischsprachige Wikipedia [3] schließlich beschreibt Observability als „Measure of how well internal states of a system can be inferred from knowledge of its external outputs“ (einen deutschsprachigen Wikipedia- Eintrag gibt es derzeit noch nicht). Observability soll demnach die Möglichkeit eröffnen, das Verhalten eines Gesamtsystems aus den System-Outputs zu bestimmen. Geht es also darum, Zustände einer „Blackbox“ aus der Beobachtung, Erfassung und Interpretation des Outputs herzuleiten? Dies entspricht der ursprünglichen Definition der System(steuerungs)theorie.
Diese drei Ansätze machen deutlich, dass es sehr unterschiedliche Ausprägungen der Begriffsverwendung gibt: Die Spanne reicht von einem datenzentrierten Ausgangspunkt (Gartner), bei dem ein Datenmanagement zum Geschäftserfolg beiträgt, bis hin zu einem Optimierungsansatz für Betriebs- und auch Sicherheitsprozesse. Der Begriffsursprung deutet schließlich auf eine Fragestellung zur Steuerungstheorie, welche Assoziationen zur Verknüpfung zwischen Beobachtung/Erfassung und gegebenenfalls auch (System-) Steuerung aufwirft – also eine Einflussnahme auf fehlerhafte, nicht intendierte Systemzustände. Doch Vorsicht: Die Aussage „What gets measured, gets managed“ ist simplifiziert und in ihrer Anwendung oft missverstanden, wenn nicht falsch (vgl. etwa [4]): Zwischen Erfassung (Measurement) und Steuerung/ Beherrschung liegen bisweilen Welten!
Insofern ist es lohnend – ausgehend von der Ursprungsdefinition und der Herleitung des Begriffs – grundlegende Eigenschaften, Prinzipien und methodische Ansätze zu erfassen. Dieses Grundwissen eröffnet dann Möglichkeiten zu einer zweck- und zielorientierten Transformation auf das Anwendungsfeld Informationssicherheit in Geschäftssystemen. Hierbei können Methoden der Systemtheorie und des Security-Engineering hilfreich sein.

Am Anfang stand die Regelungstechnik

Der Begriff Observability wurde ursprünglich 1960 durch Rudolf E. Kálmán in seinem Aufsatz „On the general theory of control systems“ definiert [5]. Control-Systems sind in diesem Zusammenhang Regelungssysteme mit der Eigenschaft, gewünschte Ausgangsgrößen in vorgegebener Art und Weise auf definierte Werte zu halten. Dies lässt sich etwa durch einen Heizungsthermostat veranschaulichen, der die Zimmertemperatur auf einen festgelegten Wert „regelt“. Aufgabe des „Controlling“ ist es, Änderungen der Eingangsgrößen und äußere Einwirkungen möglichst zuverlässig und schnell ausgleichen. Das System ist insofern dynamisch, dass nicht nur Eingangsgrößen und Einwirkungen Änderungen unterliegen, sondern auch die Änderung der Ausgangsgrößen nicht linear und zeitlich direkt erfolgt: Denn die Ausgangsgrößen „folgen“ den Vorgaben des Controllers unter Umständen mit zeitlich und physisch bedingten verzögerten Reaktionen.
Kálmán betrachtete die Regelungsvorgänge rein mathematisch mit einer (theoretisch) unendlichen Menge von Ausgangs- und Eingangsgrößen und stellte sich die Frage, ob der interne Zustand des „Control-Systems“, das heißt die aktuellen Werte der Eingangs- und Steuerungsgrößen, ausschließlich

durch Erfassung der Ausgangsgrößen bestimmt werden kann. Diese Form der Bestimmbarkeit, also den Rückschluss auf interne Systemzustände durch Beobachtung der Ausgangsgrößen, bezeichnete er als Observability.
Mit dieser Ursprungsdefinition des Begriffs für Control-Systems sind allgemeine Eigenschaften und Charakteristika verbunden, die als Grundlage für die Übertragung und Anwendung in andere Systeme dienen können. Hierbei ist wesentlich, dass Ausgangsgrößen als Informationen zu Systemzuständen interpretiert werden beziehungsweise dieser Interpretationsvorgang an sich im Fokus der Bestimmung steht.

Anforderungen an „observierbare“ Systeme

Observability im Sinne Kálmáns stellt eine Systemeigenschaft dar: Das System kann observiert werden – um einmal einen eingedeutschten Begriff zu verwenden. Dies bedingt, dass die vom System ausgegeben Ausgangsgrößen und -daten quantitativ und qualitativ erfassbar sind. Mit dieser „Qualität“ ist verbunden, dass Ausgangsgrößen (Ausgangsdaten) voneinander unabhängig sind, also unterschiedliche Informationen repräsentieren: Sind zwei Ausgangsgrößen miteinander gekoppelt, sodass etwa in gleichartiger Weise auf eine oder mehrere Eingangsgrößen reagiert wird, liegt unter Umständen eine Redundanz vor, wodurch der Informationsgehalt der Ausgangsgrößen reduziert ist.

- Das betrachtete System muss unterschiedliche interne Zustände einnehmen (können), die sich in Ausgangsgrößen widerspiegeln. Fasst man Einfluss- und Eingangsgrößen des Systems gesamtheitlich auf, müssen die internen Zustände mit Änderungen dieser Größen variieren.
- Das System muss eine ausreichende Zahl von Ausgangsgrößen ausgeben. Sowohl die Ausgangsgrößen an sich als auch die Verknüpfung verschiedener Ausgangsgrößen stellen Informationen dar, durch die man auf interne Zustände des Systems schließen kann – je größer ihre Anzahl, umso mehr Informationen lassen sich bilden.
- Das Control-System muss eine ausreichende Anzahl an Steuerungsoptionen haben. In der Kybernetik – quasi das Theoriegebäudes zu Steuerungsprozessen – ist das sogenannte Gesetz der Varietät von Ashby bekannt: Dieses wird so interpretiert, dass ein Steuerungssystem umso mehr Systemeinflüsse ausgleichen kann, je mehr Steuerungsoptionen gegeben sind. Im Idealfall existieren mehr Optionen als mögliche Einflussgrößen, sodass das System immer „beherrscht“ wird.

Die aufgeführten Eigenschaften fokussieren gemäß der ursprünglichen Definition der Observability darauf, aus Ausgangsgrößen auf interne Zustände zu schließen – diese Blickrichtung soll hier als „Inside-out- Sicht“ bezeichnet werden. Aus Sicht der Systemtheorie stellt dies jedoch nur eine Hälfte des Mechanismus dar: Wie angedeutet sind zur „Erfassung“ der internen Zustände die Ausgangsgrößen isoliert oder durch Verknüpfungen in „passende“ Informationen zu überführen, mit denen man nicht nur ein Verständnis der internen Vorgänge erlangt, sondern im Weiteren wirksame

Aktionen zur Steuerung des Systems herleitet. Mögliche Aktionen erfordern jedoch die Einnahme der umgekehrten Perspektive, das heißt die Betrachtung von Voraussetzungen, Mechanismen und Modellen, die überhaupt erst einen Handlungsspielraum eröffnen. Diese umgekehrte Perspektive kann als „Outside-in-Sicht“ bezeichnet werden – sie repräsentiert die Erkenntnisprozesse des Beobachters, zu denen sich ebenfalls grundlegende Eigenschaften und Voraussetzungen darstellen lassen.

Modellierung

Schlüsse auf die internen Zustände eines Systems basieren auf einer Vorstellung von der Struktur und Funktionsweise des Systems. Die Grundlage des Beobachters ist somit ein Systemmodell: Darunter sollen hier die Abbildung der Systemanteile in Form von Komponenten und Funktionen, deren Zusammenhänge sowie die Prozesse und Akteure zur Darstellung der Vorgänge verstanden werden, die zur Erreichung spezifischer Ziele erforderlich oder gegeben sind. Ein Systemmodell der Informationssicherheit umfasst beispielsweise alle isolierten beziehungsweise integrierten Systemanteile und -funktionen, die in Gänze die Sicherheitsanforderungen der Geschäfts-/Unternehmensprozesse gewährleisten sollen.
Grundlegend lassen sich für Modelle folgende Klassifikationen erwägen, die hier mit dem Fokus auf Anwendungen der Informationssicherheit bewertet werden:

- Es existiert noch kein Systemmodell, das heißt, das Modell wird/muss im Sinne eines Black-Box-Ansatzes erst ermittelt werden. Dieser metaphysische Ansatz wird hier nicht weiter betrachtet.
- Es existiert ein Modell des Gesamtsystems, von dem die interne Struktur und die Funktionszusammenhänge zwischen Systemkomponenten bekannt sind. Der Erkenntnisprozess kann somit zur Ermittlung des „Normal- Verhaltens“ beziehungsweise der Erfassung von Abweichungen zum normalen Systemverhalten dienen.
- Es existieren mehrere Modelle beziehungsweise Teilmodelle und der Erkenntnisprozess dient der Verifikation, welches Modell vorliegt, oder der Bildung eines neuen (abgeleiteten) Modells. Der Modellbegriff ist hier auf einzelne Funktionsabläufe – wie die Verifikation der Aktivitäten von Schadsoftware –reduziert.

Diese drei dargestellten Klassen bilden unterschiedliche Erkennungsebenen ab: von grundlegend zu fallspezifisch/praktisch. Dies führt dazu, dass mit dem Erkenntnisprozess verschiedene Ziele und Zwecke verfolgt werden (können): Ein und dieselben Ausgangsgrößen können je nach Blickrichtung anders interpretiert und verwendet werden – die Daten können somit auch einen unterschiedlichen Informationsgehalt haben.
Die Interpretation der Ausgangsgrößen lässt sich als Auswahl- und/oder Verifizierungsprozess verstehen: Durch Prüfung von Korrelationen zwischen gegebenen Größen und „erwartetem Modellverhalten“ erfolgt ein systematisches Bestätigen oder Verwerfen der Modelleigenschaften. Zur

Korrelation können die Ausgangsgrößen entweder direkt/nativ Informationen darstellen oder es kann notwendig sein, unterschiedliche Ausgangsgrößen in einer Vorstufe geeignet zu einer Information zu verknüpfen. Dies determiniert auch die erforderlichen Ressourcen zur Durchführung einer unter Umständen zeitkritischen Bewertung.
Schließlich ist festzuhalten, dass je nach Zielen und Zwecken Erkenntnisprozesse automatisiert durchgeführt oder zumindest unterstützt werden können. Gerade bei einer personellen Bewertung erscheint es sinnvoll (und erforderlich?), hierzu mehrere Instanzen einzubinden, um unterschiedliche Denk-Verzerrungen (Biases) zu minimieren.

Zwischenfazit

Observability hat zwei Sichten, die sowohl die Systemeigenschaft (Inside-out-Sicht) als auch die Erkenntniseigenschaft (Outside-in-Sicht) repräsentieren. Beide Eigenschaften bedingen einander wechselseitig: Das Schließen von Erkenntnissen bedingt, dass einerseits Daten vorliegen – und andererseits erfolgt das Schließen dadurch, dass zu den Daten ein „Modell“ der inneren Zustände des Systems gebildet, verifiziert oder auf andere Weise modifiziert/aktualisiert wird. Je nach gegebener Klassifikationsebene des Modells ist hiermit auch eine (eigen-)kritische Haltung verbunden, frei nach George Box: „Im Prinzip sind alle Modelle falsch, aber manche sind nützlich.

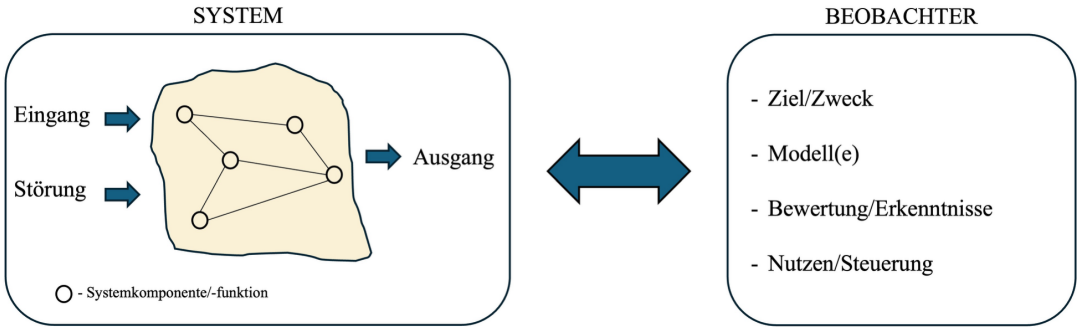

Abbildung 1: Observability und Eigenschaften

Zur Anwendung und Nutzung der „Observability“ in unterschiedlichem Kontext können die dargestellten Eigenschaften und Charakteristika zugrunde gelegt und ausgeprägt werden (Abb. 1). Damit die durch die Observability gewonnenen Erkenntnisse zu einem effektiven Gesamtnutzen beitragen, ist der Fokus auch auf originäre Management-Prozesse zu erweitern.

Security-Kontext

Zur vollständigen Übertragung und Anwendung der Observability-Eigenschaften in den Kontext „Informationssicherheit“ ist es zunächst sinnvoll, den Betrachtungsgegenstand, also das Objekt der „Observation“ zu definieren. Im Folgenden wird hierzu der Begriff des Security- Systems als zusammenhängende und gesamtheitlich gesteuerte funktionale Struktur bestehend aus Sicherheitskomponenten und -funktionen aufgefasst. Komponenten und Funktionen sind als die zu

Security-Measures/-Controls implementierten Sicherheitsmaßnahmen zu sehen, die entweder in Geschäftssysteme und -anwendungen integriert oder als dedizierte Ergänzungen identifizierbar sind. Das Security-System ist grundlegend als eine Betriebsschicht oberhalb der Geschäftssysteme und -anwendungen zu verstehen, welche die sicherheitsorientierte Funktionsfähigkeit der Geschäftsprozesse und -daten gewährleisten soll. Alle Komponenten und Funktionen von Security-Systemen werden durch deren Sicherheitsanforderungen vorgegeben.

Zur Transformation der Erkenntnisse zur Observability stellt sich die grundlegende Frage, welche Ziele und Erkenntnisse verfolgt werden (sollen): Grundlegende Zielsetzung ist das Sicherstellen eines störungsfreien Geschäftsbetriebs ohne den Verlust von Nutzbarkeit und Kontrollierbarkeit der Geschäfts-Prozessabläufe, -Objekte und -Assets inklusive Daten und Ressourcen. Mit dem Verständnis, dass Störungen im weiten Sinne als Abweichungen vom Normalzustand definiert sind, gilt es, die Vorgänge und Zustände festzulegen, die im besonderen Fokus stehen.

Da das Security-System initial durch Struktur und Funktionen bekannt ist, entfällt die Inside-out-Sicht. Im Kontext der Informationssicherheit ist somit die Outside-in-Sicht maßgeblich, der Fokus liegt also im Erkenntnisprozess der Vorgänge innerhalb des Security-Systems. Als Übertragung der hierzu oben genannten Eigenschaften und Charakteristika kann als erste Arbeitshypothese zu dieser Sicht die Security-Observability wie folgt beschrieben werden:

Security-Observability ist ein System- und Betriebskonzept, welches durch umfassende Erfassung, Ausund Bewertung von Daten des Security-Systems (bzw. seiner Komponenten und – Funktionen) eine frühzeitige Erkennung, eine effektive Verhinderung sowie im Ereignisfall eine ursachenorientierte Behebung von Systemstörungen ermöglicht. Das wesentliche Element der Security-Observability ist ein – möglichst automatisierter – Erkenntnisprozess, der Daten in relative und absolute Informationen zum Systemzustand transformiert.

Die Beurteilung der Systemzustände ist grundsätzlich von den Zielsetzungen abhängig. Aus umgekehrter Sicht bedeutet dies, dass mit den Zielsetzungen gleichzeitig der Detaillierungsgrad der Beobachtungen und Erkenntnisse definiert wird. In der Folge bestimmt der Detaillierungsgrad in einem weiteren Schritt die technischen, manuellen und prozeduralen Aufwände zur Erreichung der Zielsetzungen. Allen voran sind diese durch die verwendbaren Daten und Datenquellen definiert.

Datenquellen

Veröffentlichungen und Produkt-Werbungen benennen häufig drei bis fünf Datenquellen als Grundlage zur Durchführung der Kernaufgaben (siehe beispielsweise [6,7]). Diese werden teilweise als Telemetriedaten oder als „Pillars“ (Säulen der Observability) bezeichnet. Umfasst sind mindestens Logdaten, Traces und Metriken der Systemkomponenten – diese müssen zur Umsetzung der genannten Prozeduren um externe Daten wie Indikatoren, technische Standards und Modelle erweitert werden. Die Datenarten korrespondieren einerseits mit der beschriebenen Abstufung der

Erkenntnisprozesse; andererseits sind hiermit mindestens folgende – für die Aufwandsabschätzung relevanten – Aspekte verbunden:

- Der Umfang der Logdaten und damit der potenzielle Informationsgehalt für die Erkenntnisprozesse ist sowohl von Systemdesign und -funktionen als auch von der Konfiguration der Systeme abhängig. Je nach System werden in Logdaten Systemvorgänge über alle sieben Verarbeitungsschichten des ISO/OSI-Referenzmodells protokolliert. Darüber hinaus können Logdaten neben Systemvorgängen auch Ausgaben zu Systemleistungsdaten (Capabilities) wie CPU-Auslastungsdaten, Speicherkapazitäten, Warteschlangenzustände et cetera umfassen.
- Traces sind auf der Ebene technischer Abläufe Aufzeichnungen und Logdaten-Auswertungen gegenüber technischen Standards. Im Rahmen von Incident-Bearbeitungen erfolgen Auswertungen auch mithilfe von parametergesteuerten Suchen nach Abläufen (z. B. eine chronologische Auflistung aller Aktivitäten einer Account-Kennzeichnung). Darüber hinaus lassen sich mit Traces auch Informationen im Sinne eines Störoder Angriffsprofils zusammentragen.
- Metriken werden in der Regel durch Daten-Verknüpfungen und Vergleiche zu standardisierten oder definierten Systemeigenschaften gebildet, wobei sich Vergleiche dynamisch auf vorherige Beobachtungszeiträume oder statisch auf festgelegte Schwellwerte beziehen können. Die Besonderheit von Indikatoren (z. B. Indicators of Compromise, IoCs) ist, dass diese einer kurzlebigen („ephemeralen“) Dynamik unterliegen und somit zur Prüfung der Betroffenheit automatisiert erfasst, genutzt und auch wieder aus Prüfroutinen gelöscht werden müssen.

Log- und Tracedaten sind umfänglich und inhaltlich so zu konfigurieren, dass die für die Sicherheit der Geschäftsprozesse relevanten Daten zur Verfügung stehen. Im Kontext der Informationssicherheit erfolgt hierzu eine Risikoabwägung auf kritische oder hoch-relevante Daten. Dies verdeutlicht gleichzeitig, dass auch Observability ein risikoorientierter Ansatz ist. Vorgaben zu kritischen/hoch-relevanten Daten können eine hohe Bandbreite umfassen und reichen etwa von Daten zu rechtlichen, vertraglichen und zertifizierungsorientierten Nachweisprozeduren bis hin zu Prozessen des Exposure-Managements.
Selbstredend zeigt sich hierbei ein Wechselspiel zwischen Daten und Informationen beziehungsweise Erkenntnissen zu Systemzuständen: Neben der Dynamik der Nutzbarkeit von Indikatoren, Metriken sowie Stör- oder Angriffsprofilen sind auch regelmäßige Prüfungen und Anpassungen aufgrund technologischer und geschäftlicher Entwicklungen vorzunehmen.

Erkenntnisse

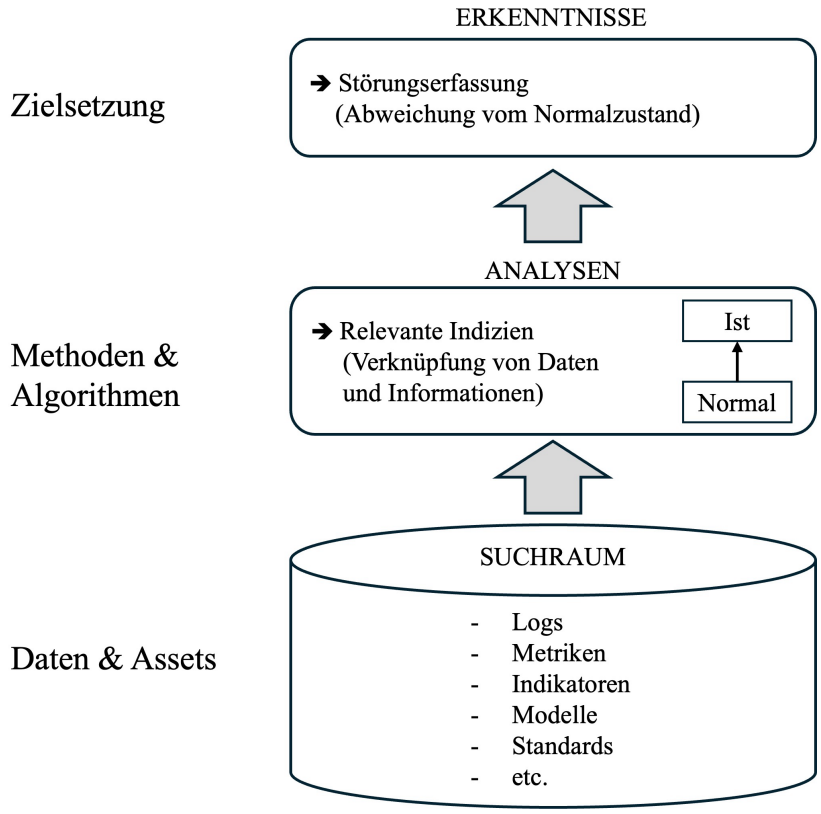

Abbildung 2: Erkenntnisprozess zur Security-Observability

Als wesentliches Element der Security-Observability wurde der Erkenntnisprozess zur Erfassung und Bewertung des Systemzustands angegeben, wobei hier faktische oder potenzielle Störungen erfasst werden sollen (siehe Abb. 2).

Erkenntnisse und Informationen können dabei allgemeinen Betriebsaufgaben im Kontext Performance- und Kapazitätsmanagement oder auch Aufgaben in Bezug auf SLA-, Qualitäts- und Verfügbarkeitsnachweisen dienen. Als Kernaufgaben gemäß der genannten Arbeitshypothese wären jedoch folgende Aspekte hervorzuheben:

- Security-Observability dient dem Security-Event-Management, das Zustandsmeldungen (Protokoll-/Log-Daten) der Security-Komponenten und -Funktionen erfasst. Zustandsmeldungen können sowohl von Herstellern vorgegebene Ausgaben (Fehlermeldungen) als auch konfigurierte Metriken und Schwellwerte zu System-

/Funktionsauslastungen sein. Dies kann als passiver Erkenntnisgewinn bezeichnet werden, da die Ursachen zu Zustandsmeldungen in der Regel unmittelbar ableitbar sind.

- Durch die Verknüpfung von Daten lassen sich als aktiver Erkenntnisgewinn Informationen über Betriebszustände ableiten. Verknüpfungen können hierbei manuell oder automatisiert erfolgen und können sich an chronologischen, technischen oder prozessualen Aktivitäten orientieren. Chronologisch orientierte Erkenntnisse basieren beispielsweise auf Auslastungen von Übertragungskapazitäten, CPU-Auslastungen oder Ähnlichem zu definierten Beobachtungsperioden, die etwa durch Performance-Parameter repräsentiert werden. Durch Vergleiche der Parameter lassen sich gegebenenfalls ungewöhnliche Aktivitäten erfassen (Anomalien). Technische Aktivitäten sind Standard-Protokollabläufe (Traces), wie sie beispielsweise für Anmeldeprozeduren mit CHAP/PAP oder beim Aufbau einer TCP/IP-Verbindung verzeichnet werden. Prozessuale Aktivitäten sind hingegen solche, die mit bekannten (typisierten) Abläufen böswilliger Eingriffe in die Geschäftsprozesse verbunden werden. Bei diesen sogenannten Kill-Chains erfolgt etwa eine Prüfung beziehungsweise ein Vergleich mit den im MITRE-ATT&CK-Framework strukturierten Angriffsmethoden. Aber auch simple Zugangsversuche können prozessualen Aktivitäten zugeordnet werden. Die Erkennung eines anormalen Verhaltens bedingt hier jedoch eine Verknüpfung und Interpretation mit Metadaten des Zugangsversuchs wie Zugangszeiten, Quell-Lokationen oder Häufigkeiten von Anmeldeversuchen.
- Eine weitere Erkenntnisstufe kann durch Vergleich von Betriebsvorgängen mit Daten und Abläufen aus externen Quellen erfolgen und als induzierter Erkenntnisgewinn bezeichnet werden. Derartige Erkenntnisse konzentrieren sich dann im Allgemeinen nur noch auf ungewollte negative Betriebseinflüsse, indem etwa nach Kommunikationsparametern wie aktuellen Indicators of Compromise (IoCs) gesucht wird.
- Während die vorigen drei Punkte die Prüfung aktiver, realer Vorgänge des Security-Systems umfassen, können Erkenntnisse schließlich auch für potenzielle Vorgänge generiert werden (etwa durch Penetrationstests oder Simulationen). Diese Aktivitäten stellen – ähnlich wie Systemscans auf bekannte Schwachstellen – die Sicht- und Betrachtungsgrenze der Security-Observability dar.

Die genannten Aspekte verdeutlichen, dass der Erkenntnisgewinn in zunehmend aufwendigeren Stufen erfolgt: Verknüpfungen und Interpretationen der Daten setzen beim induzierten Erkenntnisgewinn eine Suche und Verifikation entweder mit extern heranzuziehenden, teilweise hoch dynamischen Daten voraus – beim aktiven Erkenntnisgewinn sind zumindest komplexe Informationsketten aus den Daten zu bilden, die dann wiederum mit externen Datenquellen abzugleichen sind. Klar wird, dass hiermit automatisierte Methoden und Prozeduren/ Algorithmen verbunden sind, die entsprechend implementiert werden müssen. Dies und die Tatsache, dass sich

nicht alle Daten/Informationen automatisiert gewinnen lassen, verdeutlicht, dass die Erkenntnisprozesse auch von den Kenntnissen, Skills und Denkmethoden der für diese Security-Aufgaben verantwortlichen Mitarbeiter* abhängig sind.

Risikofaktoren

Die bereits angesprochene Risikoorientiertheit der Observability erhält mit den Erkenntnisprozessen zusätzliche Aspekte: Neben der offensichtlichen Abhängigkeit von Skills der Security-Mitarbeiter ist nochmals darauf hinzuweisen, dass die Erkenntnisse als potenzielle oder tatsächliche Systemstörungen in weitere Betriebsprozesse einfließen. Als Risikokomponente sind hierbei die unzweifelhaft auftretenden False-Positive- Meldungen zu werten, die zu einer (vermeidbaren?) Bindung von Ressourcen für ihre Bearbeitung führen. Anzustreben – und damit als permanente Aufgabe gegeben – ist zumindest eine Minimierung solcher Meldungen. Risikorelevant ist dabei, dass eine Reduzierung der Fehlschlüsse entweder eine Vergrößerung der Datenbasis oder eine Optimierung der Datenverknüpfungen nach sich zieht – beides führt zu komplizierteren und unter Umständen komplexeren Verfahren und Algorithmen.

Eine weitere Risikorelevanz ergibt sich daraus, dass Systemstörungen als Abweichungen vom „Normalzustand“ definiert sind, dieser Normalzustand an sich aber schon ein dynamischer Zustand ist. Somit ist die Interpretation, wann ein Ereignis eine – im Wortsinne – „bemerkenswerte“ Anomalie darstellt, einer permanenten potenziellen Fehlinterpretation unterworfen.

Abschließend spielen unter Risikoaspekten die noch gravierenderen False-Negative-Ereignisse ebenfalls eine Rolle: Bei aller Optimierung der Mechanismen und Algorithmen ist zu verinnerlichen, dass gravierende Ereignisse auch einmal schlicht übersehen werden können. Die gerade noch rechtzeitig entdeckte Hintertür in den XZ-Utils für Linux kann hierfür als aktuelles Beispiel dienen. Abseits der Betrachtung, dass diese Bedrohung offensichtlich als „Vulnerability by Design“ implementiert wurde, ist hier der Erkennungsvorgang von Interesse: Die Entdeckung beruhte auf der Beobachtung und Bewertung von Performanceinformationen (Benchmark-Daten) einer Anmeldeprozedur (SSH-Login). Eine nur systemtechnisch merkbare Abweichung von normalen Anmeldezeiten hat hier einen Aufmerksamkeitsreiz (psychologisch: Salienz) bewirkt – das berühmte „Moment mal, da stimmt etwas nicht!“ Weitere Analysen haben dann zur Aufdeckung des Nachladens von Schadcode geführt. Die Verknüpfung einer Anmeldeprozedur mit dem Laden von Software ist an sich nichts Besonderes – bemerkenswert war, dass das Laden der Software nicht durch den angemeldeten Benutzer initiiert wurde. Methodisch war also gerade das Fehlen eines Aktionsschritts in diesem Kontext das Sicherheitsereignis.

False-Negative-Meldungen, also die Nicht-Erkennung/- Meldung vorliegender Anomalien ist ein permanentes Risiko aller Observability-Aktivitäten. Allein die Existenz derartiger Ereignisse, die nur mit tiefgreifenden Analysen zu fassen sind, kann und sollte vielleicht den Aufwand zur Aufdeckung von Anomalien relativieren.

Abgrenzung

Nachdem die bisherigen Ausführungen Observability im Allgemeinen und im Security-Kontext dargestellt haben, soll abschließend auf das Verhältnis zwischen Observability und Monitoring eingegangen werden. Auch hierzu wurde seitens des Autors keine Literatur gefunden, welche die Unterschiede und/oder Gemeinsamkeiten aus allgemeiner Systemsicht detailliert behandelt.
Der Autor interpretiert dies so, dass eine kontinuierliche Entwicklung des Monitoring-Verständnisses und der Monitoring-Aktivitäten stattgefunden hat. Im Kontext der derzeitigen Sicherheitslagen, äußeren Einwirkungen und der Komplexität erforderlicher Maßnahmen zur Systemsicherheit wird mit dem Begriff „Observability“ primär ein Wandel in der Grundhaltung zur Bewertung der Systemsicherheit verbunden. Neben passiven Erkenntnissen, die auf direkte Systemprobleme hinweisen, werden Informationen zu Systemvorgängen eben auch zur Erkennung von „anormalen“ Vorgängen herangezogen. Die Gestaltung der Erkenntnisprozesse folgt dabei der Vielfalt möglicher negativer beziehungsweise potenziell schädlicher Beeinflussungsmöglichkeiten.
Grundlegende Voraussetzungen für eine effektive Nutzung der Daten/Informationen sind mindestens die Definitionen der Erkenntniszielsetzungen im Lichte formaler und geschäftlicher Anforderungen, die Bereitstellung/ Nutzung aller Systemdaten im Sinne eines gemeinsamen Datentopfes („Single Pane of Glass“) sowie die Bereitstellung/Vorhaltung technischer und personeller Ressourcen. Damit wird auch klar, dass der wesentliche Aufwand einer „Observability-Lösung“ nicht in der Bereitstellung von Sicherheits-Tools im Sinne von Hard- und Software liegt.

Fazit

Observability ist ein neuer Begriff in der Informationssicherheit. Mit dem Wissen um seinen Ursprung und die Anwendung im „ursprünglichen Sinne“ ist eine vielfältige Bereicherung der Informations-/Cyber-Sicherheit möglich. Neben der Systematisierung und Zustandsbewertung eines Security-Systems kann und sollte Observability darüber hinaus als systemtechnischer Monitoring-Management-Prozess verstanden werden. So gelingt es, die Lücke zwischen Begriffen, Produkten und ihren Versprechungen, Notwendigkeiten und Entscheidungen auf ein solides (neutrales) Fundament zu heben.

Literatur

[1] Lori Perri, Die Monetarisierung beobachtbarer Daten wird Gewinner von Verlierern trennen, Gartner Insights, November 2022, www.gartner.de/de/artikel/monetarisierung-beobachtbarer-daten-wird-gewinnervon-verlierern-trennen

[2] Splunk, Was ist Observability?, Data Insider, Mai 2023, www.splunk.com/de_de/data-insider/what-is-observability.html
[3] Wikipedia, Observability, Mai 2024, https://en.wikipedia.org/wiki/Observability
[4] Simon Caulkin S., The rule is simple: be careful what you measure, The Guardian, Februar 2008, www.theguardian.com/business/2008/feb/10/businesscomment1
[5] Rudolf Emil Kálmán, On the general theory of control systems, in: IFAC Proceedings Volumes, Volume 1, Issue 1, August 1960, S. 491, online verfügbar über https://doi.org/10.1016/S1474-6670(17)70094-8
[6] Arfan Sharif, The Three Pillars Of Observability: Logs, Metrics, And Traces, Crowdstrike Cybersecurity 101, Oktober 2023, www.crowdstrike.com/cybersecurity-101/observability/three-pillars-of-observability/
[7] Fabian Dietz, Was ist Observability: Von Telemetriedaten bis Einsatz und Software-Tools, Objektkultur Blog, September 2023, https://blog.objektkultur.de/was-ist-observability-von-telemetriedaten-bis-einsatzund-software-tools/