Werkzeuge für das Schwachstellen-management

Das Angebot an Werkzeugen für das Schwachstellenmanagement ist in den letzten Jahren stark gewachsen. Unsere Marktübersicht versucht, jenseits von Buzzwords und Vertriebsversprechen Orientierung zu geben und zu erklären, warum nicht jeder Weg für jeden ans gewünschte Ziel führt.

Von Leonard Frank und Mirko Casper

Bei der Suche nach einem Produkt, mit dem sich die im vorherigen Artikel „Schwachstellenmanagement: mehr als Scannen und Finden" ab Seite 50 beschriebenen Anforderungen in die Praxis umzusetzen lassen, stößt man auf eine Vielzahl von Herstellern, die alle „irgendwas mit Schwachstellenmanagement" bieten. Neben etablierten Playern ergänzen besonders in den letzten Jahren auch Hersteller aus anderen Bereichen, etwa der klassischen Endpoint Protection, ihre Produkte um Schwachstellenmanagement-Features.

Nach einem Blick unter die Haube folgt allerdings oft die Ernüchterung: Viele dieser Features können Schwachstellen zwar identifizieren, lassen einen aber mit der Behandlung, also dem eigentlichen „Management", allein. Manche können Schwachstellen nur auf Windows-Systemen erkennen, aber nicht auf Linux-Systemen. Wieder andere prüfen nur auf Software-, aber nicht auf Konfigurationsschwachstellen.

Vielfältige IT-Landschaften benötigen vielfältige Ansätze

Die Vielfalt zeigt sich besonders im Bereich der Identifikation, denn IT-Landschaften bestehen heute typischerweise nicht mehr nur aus Clients, Servern und ein paar Netzwerkgeräten. Viele Unternehmen nutzen gleich mehrere Cloud-Plattformen und Containerplattformen wie Docker oder Kubernetes. Nicht nur die dort betriebenen Systeme und Anwendungen können Schwachstellen enthalten, sondern auch die Plattformen selbst. Für die Erfassung solcher Schwachstellen sind meist spezialisierte Produkte nötig.

Ähnlich sieht es im Bereich der Produktionstechnik, also Operational Technology (OT), aus. Generische Schwachstellenscanner wissen meist nicht mit den spezifischen Bedrohungen für OT-Geräte umzugehen und können, schlimmer noch, mit ihren Scans Fehler oder gar Abstürze verursachen und so komplette Produktionsstraßen zum Stillstand bringen. Spezialwerkzeuge für diesen Bereich unterscheiden sich in ihrem Ansatz, diese Probleme zu umschiffen.

Ein weiterer Sonderfall ist der zentrale Verzeichnisdienst des Unternehmens – typischerweise Microsofts Active Directory oder Entra ID (vormals Azure AD). Denn auch hier gibt es Potenzial für Konfigurationsschwachstellen, die von generischen Scannern kaum abgedeckt werden. Aufgrund ihrer gravierenden Folgen kann es aber trotzdem sinnvoll sein, sie im Rahmen des Schwachstellenmanagements zu erfassen.

Dass wesentliche Teilbereiche unserer heutigen heterogenen Asset-Landschaften von klassischen Schwachstellenscannern nicht oder nur eingeschränkt abgedeckt werden können, haben auch die Hersteller verstanden und zumindest die etablierten unter ihnen haben Spezialösungen dafür im Angebot.

Verschiedene Architekturen

Um hier nicht die Übersicht zu verlieren und am Ende aufs falsche Pferd zu setzen, empfiehlt es sich, die grundlegenden Architekturoptionen zu betrachten. Es lassen sich hier zwei Paradigmen identifizieren, die massiven Einfluss auf die technische Umsetzung haben: Ökosysteme und Aggregatoren.

iX-TRACT

- Schwachstellenmanagement-Produkte oder -Features gibt es zahlreiche, sowohl von etablierten Herstellern als auch von Produktanbietern aus anderen Bereichen. Letztere unterstützen Nutzer aber oft nicht beim eigentlichen Management.
- Heutige IT-Landschaften umfassen mehr als das klassische Dreigespann Client, Server, Netzwerkgeräte. Für Cloud- oder Containerplattformen sind generische Schwachstellenscanner jedoch nur begrenzt geeignet, Spezialwerkzeug ist hier gefragt.
- Neben dem Erfassen und Behandeln von Schwachstellen sollte man bei den Werkzeugen Schnittstellen zu den anderen operativen IT-Prozessen nicht übersehen.

Produkte für klassische IT-Systeme

Hersteller	Produkt	Betrieb		Abdeckung			Technik		
		on Premises	Cloud	Windows	Linux	Netzwerkgeräte	nicht authentifiziert	authentifiziert	agentenbasiert
Greenbone	Greenbone Enterprise	✓	✓	✓	✓	✓	✓	✓	–
Holm Security	VMP	✓	✓	✓	✓	✓	✓	✓	✓
Microsoft	Defender Vulnerability Management	–	✓	✓	✓	✓	✓	(✓)	✓
Outpost 24	Outscan NX	✓	✓	✓	✓	✓	✓	✓	✓
Qualys	Qualys VM	✓	✓	✓	✓	✓	✓	✓	✓
Rapid7	InsightVM	✓	–	✓	✓	✓	✓	✓	✓
Tenable	Security Center / Vulnerability Management	✓	✓	✓	✓	✓	✓	✓	✓
WithSecure	Elements Vulnerability Management	✓	–	✓	✓	✓	✓	✓	✓

✓ vorhanden / trifft zu; (✓) teilweise vorhanden / trifft teilweise zu; – nicht vorhanden / trifft nicht zu

Die herkömmlichen Lösungen sind Vertreter der ersten Variante, der Ökosysteme. Hierunter fallen eine Menge von Tools, teils von verschiedenen Anbietern, die miteinander funktionieren, um möglichst alle Arten von Assets abzudecken. Idealerweise auch vollintegriert und über eine zentrale Plattform zugänglich. Die Kehrseite: Diese Ökosysteme sind Walled Gardens (geschlossene Plattformen), mit ihnen lassen sich nur die mit den Komponenten des Ökosystems gefundenen Schwachstellen verwalten. Eine Anbindung weiterer Spezialprodukte ist nicht oder nur sehr hakelig möglich.

Dafür sind sie typischerweise ausgestattet mit vielen Features, einem proprietären Score inklusive Threat Intelligence, Tracking der Behandlung und vorgefertigten Analyse-Dashboards. Diese geben allerdings oft einen klaren Weg vor, von dem sich nur schwer abweichen lässt. So lässt sich beispielsweise nicht tiefer gehend in die Berechnung des Scores eingreifen, der Behandlungsprozess ist nur begrenzt auf die eigenen Bedürfnisse anpassbar und das Datenmodell lässt sich nicht erweitern, um etwa unternehmensspezifische Informationen zu Assets anzuzeigen.

Mit Ökosystemen kann man vergleichsweise schnell zu einem produktiv nutzbaren Schwachstellenmanagement kommen. Ändern sich jedoch die Anforderungen, beispielsweise weil neue Assetklassen dazukommen oder unternehmensspezifische Faktoren in die Priorisierung oder den Behandlungsprozess einbezogen werden sollen, stoßen Ökosysteme häufig an ihre Grenzen.

Identifikation und Verarbeitung trennen

Als Alternativentwurf sind in den letzten Jahren diverse Hersteller auf den Markt gekommen, die hier unter dem Begriff Aggregatoren zusammengefasst werden sollen. Sie sind darauf spezialisiert, Daten aus vielen verschiedenen IT-Lösungen zusammenzuführen und einen einheitlichen Blick darauf zu ermöglichen. Viele dieser Produkte kommen aus den Bereichen Asset-Management und Continuous Controls Monitoring, ein paar Hersteller haben sich auch Schwachstellenmanagement auf die Fahne geschrieben. Als Beispiele wären hier Brinqa (siehe Abbildung 1) und Noetic zu nennen.

Im Gegensatz zu Ökosystemen konzentrieren sich Aggregatoren nur auf das Handling von Daten, das bedeutet, sie identifizieren selbst keine Schwachstellen, sondern sind dafür auf andere Produkte angewiesen. Das klingt zunächst nach unnötigen zusätzlichen Investitionen, aber viele Unternehmen verfügen bereits über entsprechende Produkte, oft ohne sich dessen bewusst zu sein. Denn auch die Hersteller von Endpoint Protection und Endpoint Detection and Response (EDR) haben den Trend erkannt und arbeiten daran, dass ihre Agents in Zukunft auch Schwachstellen identifizieren können.

Manche davon ermöglichen es sogar, die Endpoints selbst als einfachen Scanner zu verwenden, um auch Geräte ohne

Ein Aggregator wie Brinqa kann einen einheitlichen Blick auf Daten aus verschiedenen Lösungen liefern und so einen zentralen Überblick über das Gesamtrisiko ermöglichen (Abb. 1).

Produkte für die Cloud

Hersteller	Produkt	Plattformen			Abdeckung		
		AWS	Azure	GCP	CSPM	VMs und Dienste	Container
Aqua	Cloud Native Security Platform	✓	✓	✓	✓	✓	✓
CheckPoint	CloudGuard	✓	✓	✓	✓	✓	✓
CrowdStrike	Falcon Cloud Security	✓	✓	✓	✓	✓	✓
Fortinet	FortiCNP	✓	✓	✓	✓	✓	✓
Microsoft	Defender for Cloud	✓	✓	✓	✓	✓	✓
Netskope	Public Cloud Security	✓	✓	✓	✓	✓	–
Qualys	TotalCloud	✓	✓	✓	✓	✓	✓
Rapid7	InsightCloudSec	✓	✓	✓	✓	✓	✓
Tenable	Cloud Security	✓	✓	✓	✓	✓	✓
Wiz	Wiz	✓	✓	✓	✓	✓	✓
Zscaler	Posture Control	✓	✓	✓	✓	✓	✓

✓ vorhanden / trifft zu; – nicht vorhanden / trifft nicht zu; CSPM – Cloud Security Posture Management

Agent, etwa Netzwerkhardware, zu erfassen. Aber selbst wenn zusätzlich ein Scanner beschafft werden muss, ist die Anzahl der abzudeckenden Systeme deutlich geringer, wodurch die Lizenzkosten entsprechend niedriger ausfallen.

Ein weiterer Vorteil ist, dass die Auswahl der Identifizierungsprodukte nicht an ein Ökosystem gebunden ist. Dadurch können beliebige Kombinationen von Speziallösungen eingesetzt werden, was eine Best-of-Breed-Strategie erlaubt. Für die Anbindung bieten Aggregatoren nicht nur von Haus aus viele Integrationen, sondern ermöglichen es zudem, weitere Tools mit geringem Aufwand anzubinden. Einige der Hersteller versprechen sogar, zusätzlich benötigte Integrationen kostenfrei zu implementieren.

An eigene Bedürfnisse anpassbar

Wie im vorherigen Artikel ab Seite 50 beschrieben sind besonders Priorisierung und Behandlung entscheidend für ein effektives Schwachstellenmanagement, und gerade hier glänzen die Aggregatoren. Denn durch ihre Flexibilität lässt sich hier vom Datenmodell über die Priorisierung bis hin zum Prozessdesign alles feingranular auf das eigene Unternehmen anpassen. Mehrstufige Freigabe-Flows, maßgeschneiderte Priorisierung, basierend auf unternehmensspezifischen Merkmalen oder bereits existierenden Threat-Intelligence-Lösungen – all das ist mit einem Aggregator möglich.

Eine solche Flexibilität und Anpassbarkeit hat auch ihren Preis. Ein Schwachstellenmanagement auf einem Aggregator aufzubauen erfordert deutlich höhere Initialaufwände. Die Hersteller versuchen zwar, einen möglichst hohen Nutzen out of the box bereitzustellen, aber letztlich braucht es immer eine gewisse Zeit, bis alles angebunden und eingespielt ist. Das alles erhöht auch die Gesamtkomplexität im Vergleich zu Ökosystemen deutlich, denn statt alle Teilbereiche des Schwachstellenmanagements über einen Hersteller zu beziehen, besteht das Konzept hier aus vielen Komponenten, die ineinandergreifen müssen. Dafür ermöglicht es ein Aggregator, wirklich alle Potenziale auszuschöpfen und das Schwachstellenmanagement so zukunftsfähig wie möglich zu gestalten.

Ökosysteme und Aggregatoren sind nicht die einzigen Möglichkeiten. Es kann durchaus eine Option sein, zunächst auf verschiedene Insellösungen zu setzen, ohne diese in einer zentralen Plattform zusammenzuführen. Ein solches Konzept kann bei Bedarf zu einem späteren Zeitpunkt immer noch um eine zentrale Aggregation ergänzt werden.

Welcher Ansatz am Ende für das eigene Unternehmen der richtige ist, lässt sich erst sagen, wenn man die eigenen Gegebenheiten und Anforderungen kennt – sowohl im Hinblick auf die aktuelle Situation als auch auf mögliche künftige Entwicklungen.

Das beginnt in der Regel mit der Frage, welche Assetklassen überhaupt abgedeckt werden sollen. Sollen beispielsweise zusätzlich zur Standard-IT auch Cloud-Ressourcen und das Active Directory miterfasst werden, schränkt das die Auswahl auf Ökosysteme ein, die entsprechende Spezialfunktionen bereitstellen. Im Folgenden stellen wir ein paar typische Produkte kurz vor und vermitteln einige Einblicke in die Schwachstellenidentifizierung für die häufigsten Assetklassen. Dazu gehören neben klassischen IT-Systemen wie Clients, Servern, Netzwerkhardware und Appliances auch Cloud-Plattformen und -Ressour-

Produkte für Operational Technology (OT)

Hersteller	Produkt	Betrieb		Technik	
		on Premises	Cloud	aktive Scans	Analyse des Netzwerkverkehrs
Claroty	Continuous Threat Detection (CTD)	✓	✓	✓	✓
Dragos	Platform	✓	✓	–	✓
Microsoft	Defender for IoT	✓	✓	✓	✓
Nozomi	Guardian	✓	✓	✓	✓
Qualys	VMDR OT	–	✓	✓	✓
Rapid7	InsighVM	✓	(✓)	✓	–
SCADAfence	Platform	✓	✓	✓	✓
Tenable	OT Security	✓	✓	✓	✓
Verve	Security Center	✓	✓	–	✓

✓ vorhanden / trifft zu; (✓) teilweise vorhanden / trifft teilweise zu; – nicht vorhanden / trifft nicht zu

Produkte für das Active Directory

Hersteller	Produkt	Betrieb		Abdeckung		Kernfunktionen	sonstige Funktionen		
		on Premises	Cloud	lokales AD	Entra ID (vorm. Azure AD)	Vulnerability-Scan	Angriffserkennung	Recovery	IoC-Scanning
Microsoft	Defender for Identity	–	✓	✓	✓	✓	✓	–	–
Netwrix	StealthAUDIT	✓	–	✓	✓	✓	–	–	–
Ping Castle	PingCastle	✓	–	✓	✓	✓	–	–	✓
SentinelOne	Singularity RangerAD	✓	✓	✓	✓	✓	✓	✓	✓
Semperis	Purple Knight	✓	–	✓	✓	✓	–	–	✓
Semperis	Directory Service Protector	–	✓	✓	✓	✓	✓	✓	✓
SpecterOps	BloodHound Enterprise	–	✓	✓	✓	✓	–	–	–
Tenable	Identity Exposure	✓	✓	✓	✓	✓	✓	–	✓

✓ vorhanden / trifft zu; – nicht vorhanden / trifft nicht zu; IoC – Indicators of Compromise (Anzeichen einer Kompromittierung)

cen, Produktionstechnik und das Active Directory.

Die klassischen IT-Systeme

Das Erfassen von Schwachstellen bei klassischen IT-Systemen ist im Regelfall die einfachste Aufgabe. Hier gibt es besonders viel Auswahl, denn neben dedizierten Lösungen für das Schwachstellenmanagement liefern auch immer mehr Produkte, zum Beispiel aus dem Bereich Endpoint Protection, die gewünschten Informationen. Man muss also nicht zwingend etwas Neues kaufen, um Schwachstellen zu finden. Es sollten allerdings neben Software- auch Konfigurationsschwachstellen erfasst werden – daran mangelt es jedoch nicht nur bei einigen Endpoint-Produkten, sondern auch bei manchen etablierten Playern im Bereich Schwachstellenmanagement. Da so das Ziel einer möglichst umfassenden Schwachstellenidentifizierung nicht erreicht werden kann, sind diese Produkte hier nicht berücksichtigt. Eine Übersicht liefert die Tabelle „Produkte für klassische IT-Systeme".

Die Platzhirsche in dieser Kategorie sind die „großen Drei": Qualys, Rapid7 und Tenable. Diese Hersteller sind seit Langem am Markt vertreten und bieten ein ausgereiftes Produktportfolio, das sie in den letzten Jahren stetig erweitert haben. Ein gewisser Sonderfall ist Greenbone, das neben der kostenpflichtigen Enterprise-Version mit mehr Funktionen und offiziellem Support auch eine – auf der Webseite ein wenig versteckte – kostenfreie Community-Edition als Open-Source-Software anbietet.

Es existieren weit mehr als die hier genannten Produkte – wobei die nicht erwähnten keinesfalls automatisch schlechter sind als die erwähnten. Vielmehr basieren die Produkttabellen in diesem Artikel hauptsächlich auf der Präsenz der Hersteller am deutschen Markt sowie der langjährigen Erfahrung der Autoren aus realen Schwachstellenmanagement-Projekten in Unternehmen unterschiedlicher Größe. Die Einschätzung deckt sich dabei weitgehend mit den Meinungen renommierter Fachexperten des FIRST und Analysten wie Gartner.

Schwachstellen in der Cloud

Der Cloud-Bereich ist schon etwas spezieller. Neben einfachen virtuellen Maschinen, die wie klassische IT-Assets erfasst werden können, stößt man hier auch auf etwas speziellere Assetklassen wie Serverless Functions oder Container. Außerdem sind die eingesetzten Technologien vielfältig und ständig im Wandel. Da sich Cloud-Ressourcen oft deutlich von klassischen IT-Assets unterscheiden, sind hier spezialisierte Produkte für das Identifizieren von Schwachstellen nötig. Die wichtigsten Kandidaten listet die Tabelle „Produkte für die Cloud" auf.

Aber auch die Cloud-Plattformen selbst können empfindliche Konfigurationsschwachstellen aufweisen. Produkte, die sich auf die Erfassung solcher Schwachstellen konzentrieren, tragen meist die Bezeichnung Cloud Security Posture Management (CSPM), während Produkte, die sich auf Schwachstellen in Cloud-Ressourcen konzentrieren, unter der Bezeichnung Cloud Workload Protection (Platform; CWP/CWPP) erhältlich sind. Tools, die beides in sich vereinen, werden häufig als Cloud-Native Application Protection Platform (CNAPP) bezeichnet.

Schwachstellenmanagement im Containerbetrieb ist ein separates Thema. Hier können sich Schwachstellen nicht nur in laufenden Containern und Containerplattformen wie Docker oder Kubernetes verbergen, sondern auch in den zugrunde liegenden Container-Images. Die Produkte und ihre Funktionen sind hier so vielfältig wie die Containerplattformen selbst. Die im Folgenden genannten

Kriterien für Ökosysteme und Aggregation

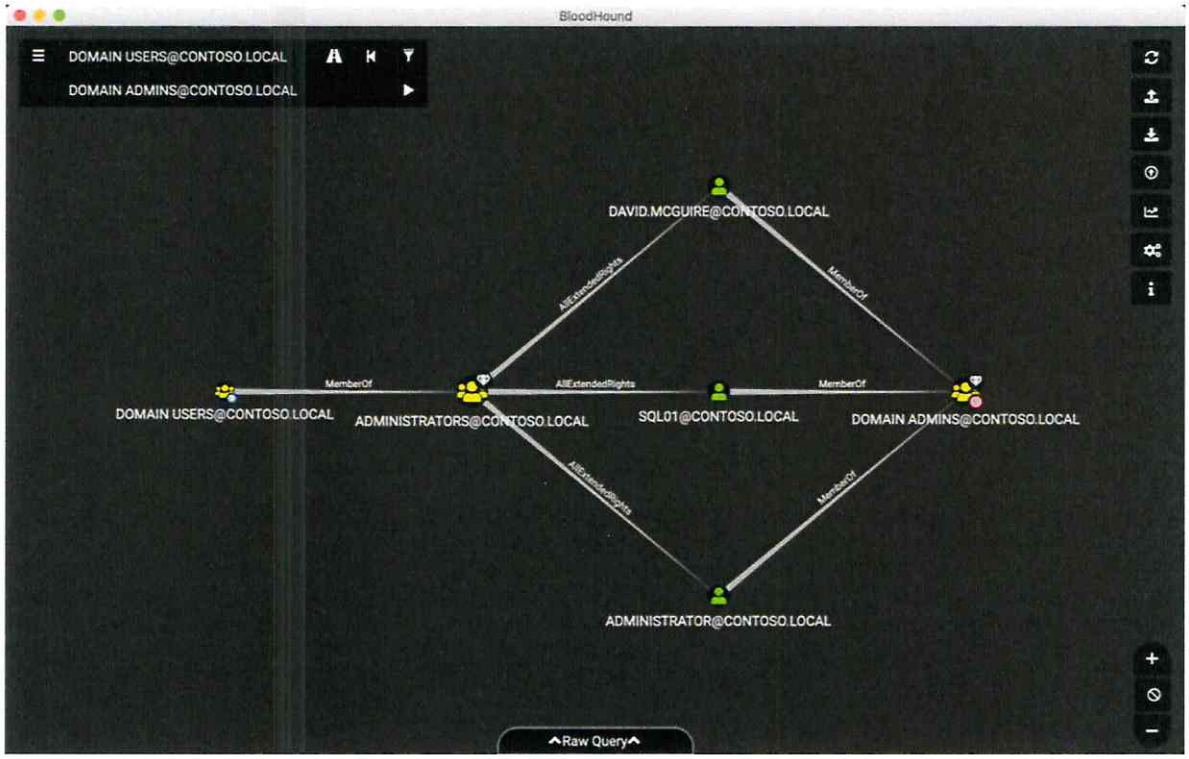
Ökosysteme können die richtige Wahl sein, wenn …

- man nur klassische IT-Systeme abdecken will;
- die Anzahl der Assets überschaubar ist;
- die gleichen Personen über die Behandlung von Schwachstellen entscheiden, die sie auch umsetzen;
- sonstige IT-Prozesse nicht strikt definiert sind oder eine Integration in sie optional ist;
- man möglichst schnell ans Ziel kommen muss.

Es kann sich hingegen lohnen, auf Aggregation zu setzen, wenn …

- man besonders viele Systeme erfassen muss;
- viele verschiedene Assetklassen abgedeckt werden sollen;
- man seine Ziele mit herkömmlichen Ansätzen bisher nicht erreichen konnte;
- das Vorgehen bei der Behandlung zwischen mehreren Stakeholdern abgestimmt werden muss;
- damit zusammenhängende (adjazente) operative IT-Prozesse angebunden werden sollen;
- die Anforderungen an das Schwachstellenmanagement einen hohen Anpassungsgrad erfordern;
- man bereit ist, mehr Zeit zu investieren, um am Ende ein besseres Ergebnis zu erhalten.

Die Kriterien sind bewusst nicht als Ausschlusskriterien gedacht. Wenn sie zutreffen, kann dies ein Indiz für einen der Wege darstellen.



Mit BloodHound können Analysten Schwachstellen im Active Directory aufspüren, etwa Nutzer, die über mehrere Umwege Zugriff auf Domain-Admin-Privilegien erlangen können (Abb. 2).

Werkzeuge sind eher Generalisten, die möglichst weite Teile der Cloud-Landschaft abdecken sollen. In Unternehmen, die stark auf Container setzen, kann es aber durchaus sinnvoll sein, darauf spezialisierte Produkte einzusetzen.

Viele der genannten Produkte bieten weit mehr als nur Schwachstellenidentifikation. So verfügen manche beispielsweise auch über verschiedene Funktionen aus den Bereichen Malwareschutz, Data Loss Prevention (DLP) oder Absicherung von APIs. Bei der Auswahl sollte man solche zusätzlichen Funktionen berücksichtigen. Es kann auch gut sein, dass im Unternehmen bereits aus anderen Gründen eine Investition im Bereich Cloud-Sicherheit ansteht. In diesem Fall kann es sinnvoll sein, auch das Identifizieren von Schwachstellen mit auf die Anforderungsliste zu schreiben.

OT-Sicherheit nicht vernachlässigen

Ein sehr spezielles Thema ist die Produktionstechnik, auch Operational Technology (OT) genannt. Selbst wenn sich die Definitionen streng genommen unterscheiden, stößt man hier häufig auf die synonym verwendeten Bezeichnungen Supervisory Control and Data Acquisition (SCADA) und Industrial Control Systems (ICS).

Geräte, Systemarchitekturen und Protokolle, die man in diesem Bereich findet, unterscheiden sich deutlich von typischen IT-Technologien. Auch wenn man bei Schlagwörtern wie Industrie 4.0 vermuten könnte, dass sich IT und OT immer weiter annähern, ist das keineswegs immer der Fall. Denn im Gegensatz zur IT sind etwa Systeme mit 16 MByte RAM und Windows NT als Betriebssystem in der OT keine Ausnahme. Und anders als in der IT können bereits massive Schäden entstehen, wenn ein OT-System nur für wenige Sekunden nicht antwortet. Viele der Technologien, auf denen moderne Schutzkonzepte der IT aufbauen, etwa EDR, sind im OT-Bereich so gut wie nie zu finden. Umso wichtiger ist es, die Schwachstellen der eigenen OT-Infrastruktur zu kennen.

Generische Schwachstellenscanner wissen in der Regel wenig von den spezifischen Bedrohungen und Anforderungen der OT-Welt. Dazu kommt, dass OT-Geräte extrem sensibel sein können. So können schon Ping-Pakete manche OT-Geräte zum Absturz bringen. Aus diesem Grund funktioniert das Identifizieren hier meist etwas anders. Der erste Ansatz ist, Schwachstellen über das alleinige Mitschneiden und Analysieren des Netzwerkverkehrs ohne Eingriff in die Kommunikation zu erkennen. Zusätzlich setzen manche Hersteller auf ein strikt beschränktes Set „sicherer" Abfragen, um weitere Informationen über die Geräte zu erlangen.

Als Sonderfall der in den in der OT-Tabelle aufgeführten Produkte ist hier der Hersteller Rapid7 zu nennen, der neben einer Integration seines SCADAfence in den eigenen Schwachstellenscanner InsightVM auch ein besonders zurückhaltendes Scanprofil anbietet, das einen Scan von OT-Geräten ermöglichen soll. Einige Hersteller von OT-Security-Produkten haben Funktionen wie Anomalieerkennung, die Analyse von PCAP-Dateien oder den Abgleich mit OT-spezifischen Threat-Intelligence-Feeds als zusätzliche Features in ihre Produkte integriert.

Active Directory und Entra ID

Da das Active Directory (AD) in der Regel zu den kritischsten Infrastrukturen eines Unternehmens gehört, ist es sinnvoll, es in ein Schwachstellenmanagement einzubeziehen. Denn neben den typischen

Softwareschwachstellen, die alle Anwendungen betreffen können und bereits mit generischen Scannern abgedeckt sind, gibt es hier eine ganze Fülle AD-spezifischer Konfigurationsschwachstellen.

Was die Auswahl hier erschwert, ist, dass Schwachstellenmanagement typischerweise nicht die Kernfunktion von Anwendungen für AD-Security ist. Der Fokus liegt häufig eher auf konstanter Überwachung und Anomalieerkennung oder gezieltem Threat Hunting [1]. Manche Produkte wie Netwrix StealthAUDIT decken weit mehr Anwendungen als nur das Active Directory ab. Daher ist es hier, wie schon bei den Cloud-Produkten, sinnvoll, eine solche Lösung nicht nur aus Sicht des Schwachstellenmanagements zu bewerten.

Dafür gibt es in diesem Bereich gleich drei kostenlose Tools. Mit Purple Knight von Semperis können Anwender nicht nur Schwachstellen aufdecken, sondern das Active Directory gezielt nach Anzeichen einer bereits erfolgten Kompromittierung durchsuchen. Auch das von Vincent Le Toux entwickelte PingCastle kann für eine Überprüfung der eigenen Domäne kostenlos genutzt werden und ist darüber hinaus quelloffen. Als weiteres Open-Source-Produkt ist das bei Red und Blue Teams beliebte BloodHound Community zu nennen (siehe Abbildung 2). Hierbei handelt es sich um eine kostenfreie Variante von BloodHound Enterprise mit geringerem Funktionsumfang, die auf die manuelle Anwendung durch Analysten ausgerichtet ist.

Was in der AD-Produkttabelle auffällt, ist, dass nur zwei der Ökosysteme vertreten sind: Microsofts Defender for Identity und Tenables Identity Exposure. Wer sich für keines der beiden entscheiden möchte, das AD aber dennoch in ein zentrales Schwachstellenmanagement einbinden will, wird hier zu einer Aggregationslösung greifen müssen.

Weitere relevante Punkte

Ob Ökosystem, Aggregationskonzept oder Sammlung von Insellösungen – mit dem Identifizieren von Schwachstellen ist nur der erste Schritt getan. Für welchen Ansatz man sich auch entscheidet, bei der Produktauswahl spielen noch weitere Aspekte eine Rolle.

Die Priorisierung ist dabei ein entscheidender Faktor, denn hier trennt sich die Spreu vom Weizen. Besonders wer auf eine zentrale Aggregation verzichtet, sollte sicherstellen, dass sich unternehmensspezifische Asset-Informationen, insbesondere eine Kritikalitätsbewertung, in das Produkt importieren lassen und in die Priorisierung einfließen. Im Idealfall über eine Integration in ein bestehendes Asset-Management oder alternativ über eine API oder den Import von CSV-Dateien. Bonuspunkte gibt es, wenn weitere Aspekte in die Priorisierung einbezogen werden können, etwa ob ein System aus dem Internet erreichbar ist oder ob es personenbezogene Daten enthält.

Aus Prozessperspektive ergeben sich weitere Anforderungen. Gibt das Produkt einen Prozess für die Schwachstellenbehebung vor, sollte man prüfen, ob er auch zur Praxis im eigenen Betrieb passt oder sich zumindest daran anpassen lässt. Wichtige Eckpunkte, die ein Werkzeug erfüllen sollte, sind die lückenlose Dokumentation von Behandlungsentscheidungen und die Möglichkeit einer Risikoakzeptanz mit regelmäßiger Reevaluation.

Alternativ ermöglichen manche Produkte auch, den kompletten Prozess mit einem externen Ticketsystem abzuwickeln. Das hat den Vorteil, dass bereits bestehende und gewohnte Tools dafür genutzt werden können, mit denen sich der Prozess meist flexibel gestalten lässt. Allerdings geht dies zulasten der Analysemöglichkeiten, denn nützliche Metriken wie die Rate erfolgloser Behandlungsversuche lassen sich so nur schwer oder gar nicht auswerten.

Darüber hinaus sollte man auch Schnittstellen zu anderen Prozessen und den zugehörigen Tools beachten. Typische Kandidaten sind Asset-, Change- und Patch-Management. Gerade Unternehmen, die auf komplexe Freigabeprozesse mit mehreren Stakeholdern angewiesen sind, sollten hier genau hinschauen.

Aber nicht nur, was ein Produkt prinzipiell kann, ist wichtig. Mindestens genauso wichtig ist, was es an Anpassungsmöglichkeiten mitbringt, um den gewünschten Funktionsumfang zu bekommen. Wer das Schwachstellenmanagement schnell produktiv nutzen will, kommt mit einem Ökosystem meist schneller zum Ziel, kann dafür aber langfristig an Grenzen stoßen. Der Einsatz einer Aggregationslösung bietet hier zwar deutlich mehr Zukunftssicherheit, aber je nach Umfang des Konzepts können für die Implementierung einige Monate ins Land gehen. Wer sich für diesen Weg entscheidet, muss Geduld mitbringen.

Fazit

Was ist jetzt das passende Produkt für wen? Wie so häufig in der IT-Sicherheit ist die Antwort ein entschiedenes „Es kommt darauf an“. Was letztendlich am sinnvollsten ist, hängt von den Anforderungen, Wünschen und Vorstellungen des jeweiligen Unternehmens ab. Dabei spielt die Unternehmensgröße genauso eine Rolle wie die aktuell und zukünftig eingesetzten Technologien und gelebten Prozesse. Eine allgemeingültige Empfehlung kann es also nicht geben. Die Kriterien für Ökosysteme und Aggregation im gleichnamigen Kasten können aber vielleicht eine Hilfestellung bei der Entscheidung bieten. Sie sind dabei bewusst nicht als Ausschlusskriterien gedacht. Wenn sie aber zutreffen, kann dies ein Indiz für einen der Wege darstellen.

Welche Produkte man am Ende einsetzt, ob Ökosystem, Aggregation oder Insellösungen – nur wer sich mit seinem Schwachstellenmanagement auseinandersetzt und es den eigenen Zielen entsprechend gestaltet, wird damit langfristig glücklich werden. Und das ist bitter nötig, denn die Zahl der neuen Schwachstellen steigt immer schneller, moderne Software besteht aus immer mehr Bestandteilen und unsere IT-Infrastrukturen werden immer komplexer. Eines lässt sich mit Sicherheit sagen: Log4Shell wird nicht die letzte Schwachstelle dieser Größenordnung sein. Wer nicht betroffen sein will, sollte bis dahin besser ein schlagkräftiges Schwachstellenmanagement haben. (ur@ix.de)

Quellen

[1] Tabea Nordieker, Threat Hunting; Angriffe auf Microsoft 365 aufspüren; iX 11/2023; S. 82

LEONARD FRANK

ist Seniorberater bei der Firma cirosec. Er berät Kunden in Konzeptfragen der Defensive, unter anderem Schwachstellenmanagement, und hilft ihnen als Incident Responder beim Umgang mit Cyberangriffen.

MIRKO CASPER

ist Seniorberater bei der Firma cirosec. Er führt Penetrationstests auf Netzwerkebene durch und berät Kunden zu ISMS-Themen, insbesondere zu Schwachstellenmanagement.