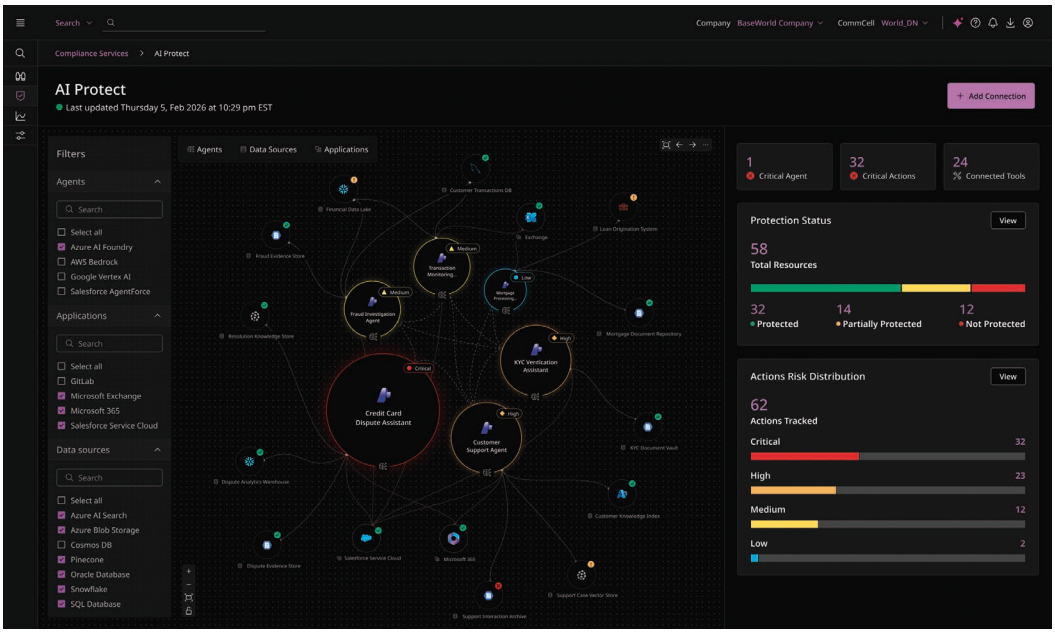
Drei Säulen der Cyberresilienz in Zeiten der agentischen KI



Künstliche Intelligenz kann Schwachstellen der eigenen Backups erkennen helfen.

KI gibt jedem Amateur mächtige Werkzeuge in die Hand, um Unternehmensnetze und Backups zu attackieren. Sie nehmen so den Opfern jegliche Chance, ihre Daten nach der Attacke wiederherzustellen. Diese neuen Risiken erfordern einen neuen Ansatz für Resilienz, der selbst KI als Gegenmittel einsetzt.

Generative KI erhöht Gefahr

Generative KI hat sich zu einem Kraftmultiplikator für Cyberkriminelle entwickelt. Die Einstiegshürden sind wesentlich gesunken und selbst unerfahrene Angreifer können schneller und skalierter Schaden anrichten. Laut den Sicherheitsforschern von Unit 42 brauchen KI-gestützte Angriffe nur 25 Minuten, um in ein Netz einzudringen und Daten zu stehlen. Menschliche Angreifer bräuchten hierfür mindestens zwei Tage.

Die Lage wird durch agentische KI weiter eingetrübt. Solche Agenten können ihr Vorgehen und ihre Strategien in Echtzeit anpassen, aus Abwehrmaßnahmen lernen und Angriffe schneller weiterentwickeln, als Menschen zurückschlagen können. Zum ersten Mal seit langer Zeit hat man den Eindruck, dass die Angreifer den Verteidigern ein Stück weit voraus sind. Keine Organisation, ganz gleich in welcher Branche, kann nun ausschließen, dass sie erfolgreich angegriffen wird.

Kernidee echter Cyberresilienz

Manche Verantwortliche für IT-Sicherheit oder für IT-Betrieb sind schlecht auf die neuen Gefahren vorbereitet und stützen ihre Cybersicherheitsstrategien weiter auf der Annahme, Angriffe verhindern zu können. Wichtiger wird sein, sich von einer rein präventiven Denkweise zu emanzipieren und sich darauf zu fokussieren, wie man die Folgen einer erfolgreichen Attacke eindämmen und schnell wieder zum Urzustand zurückkommen kann – die Kernidee echter Cyberresilienz.

1. Vom Backup zum Wiederaufbau

Hier geht es um den Weg vom Backup zum vollständigen Wiederaufbau der gesamten Anwendungsumgebung. Bisher war die Kalkulation recht einfach: Backup = Ein Restore ist möglich. Allein schon wegen Ransomware und Modellen wie Mythos geht diese Gleichung nicht mehr auf. Die KI-gestützten Modelle wie Mythos haben offenbart, dass Angreifern wohl bald Wege offenstehen, selbst gezielt und hochskalierbar nach Software-Schwächen zu suchen, um unbemerkt in Firmennetze einzudringen. Dort können sie dann die gefährliche Fracht platzieren, seien es Ransomware-Codes oder Fake-Accounts in Active Directories, von wo aus sie hunderte von Tagen im Netz spionieren und weitere Backdoors installieren können.

Die Angreifer verschlüsseln dann nicht nur Daten oder sabotieren Systeme, sie beschädigen auch die notwendigen Recovery-Funktionen. Dazu gehören das Deaktivieren oder Löschen von Snapshots. Kriminelle manipulieren auch Richtlinien zum Vorhalten von Backups oder kompromittieren die Ebenen der Orchestration. Selbst der sogenannte unveränderliche Speicher ist oft nicht immun. Angreifer können die Ebene der Backup-Administration und der Backup-Richtlinien kompromittieren, bevor Snapshots aktiviert werden. Zudem nutzen sie Konfigurationsfehler aus.

Golden Copies

Resilienz verlangt nicht nur die Fähigkeit, solche Angriffe abzuwehren, sondern auch die Tools, um eine gesamte IT in ihrer Struktur wiederherzustellen, beispielsweise durch das Zurücksetzen von Daten, Applikationen, Netzwerken, Identitätsframeworks und deren Cloud-Abhängigkeiten.

Die IT-Datensicherheit scannt die dafür notwendigen Artefakte kontinuierlich und legt sie als vertrauenswürdige, sogenannte „Golden Copies“ für saubere Point-in-Time-Wiederherstellungen ab. Golden Copies sind umfassend auf Malware, Fehlkonfigurationen und Sicherheitslücken gescannte Point-in-Time-Images. Sie bieten validierte und saubere Datenpunkte. Dabei handelt es sich aber nicht nur um reine Kopien einzelner Dateien, sondern um verifizierte, saubere Snapshots ganzer Stacks von Applikationen.

Autor:
Christian Kubik
Director Sales Engineering DACH
Commvault
www.commvault.com

Point-in-Time-Recovery

Für die Point-in-Time-Recovery der gesamten IT erfasst eine Sicherheitsplattform umfassende Point-in-Time-Snapshots der Infrastrukturkomponenten, darunter Netzwerkkonfigurationen, Rechenressourcen, Softwareimages und deren gegenseitige Abhängigkeiten. Nur so lässt sich auch der Infrastrukturkontext für einen funktionsfähigen Betrieb wiederherstellen.

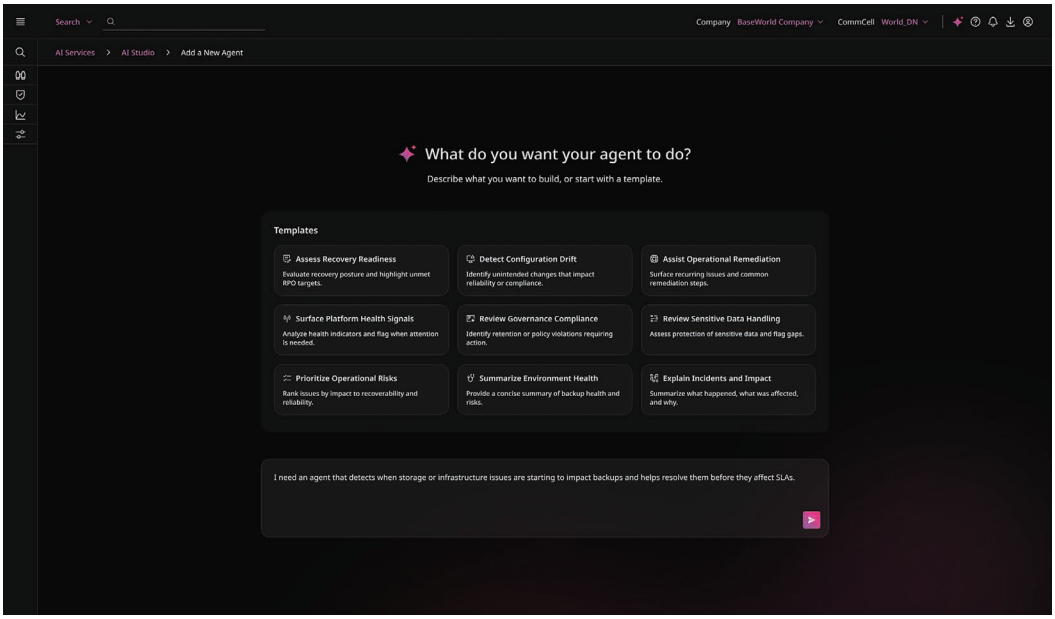
2. Regelmäßige Ernstfalltests

Von seltenen Disaster-Recovery-Manövern zu regelmäßigen Ernstfalltests: Disaster-Recovery-Tests sind selten. Vielleicht findet einmal im Jahr eine Tabletop-Simulation statt. Das meist aber nur, um Vorgaben der Compliance zu erfüllen. IT-Resilienz erfordert jedoch, aus dem Ausnahmezustand des „Recovery" eine vorab durchdachte und durchgespielte Unternehmensroutine zu machen.

Cloud-Plattformen machen die dafür notwendige Testfrequenz praktikabel und kostengünstig. Datensicherheitsverantwortliche können ganz einfach Sandboxes als digitalen Manöverraum einrichten und diesen nach erfolgtem Test wieder löschen, ohne im Voraus Rechen- und Speicherkapazitäten reservieren zu müssen. Diese Flexibilität beseitigt die traditionellen Hindernisse, um eine Cyber Recovery vorab durchzuspielen und ermöglicht häufigere, gründlichere sowie aussagekräftigere Tests.

Chaos-Tests

Darüber hinaus können Unternehmen durch den Einsatz von Chaos-Tests in einem geklonten isolierten digitalen Raum überprüfen, wie sich Systeme in der realen Drucksituation verhalten. Hier simulieren die Teams die Ausfälle von Netzwerk, Authentifizierung oder beschädigte Abhängigkeiten. Im Gegensatz zu Standardtests, die oft nur vorhersehbare Szenarien durchspielen, basieren Chaos-Tests auf Unvorhersehbarkeit, hinterfragen kontinuierlich für selbstverständlich gehaltene Annahmen und decken Schwachstellen in der Applikations- und Infrastruktur-Resilienz auf.



Eigene Recovery-Agenten beschleunigen die Wiederherstellung.

Minimum Viability Framework

Eine weitere nützliche Strategie ist ein Minimum Viability Framework. Hier liegt der Schwerpunkt darauf, geschäftskritische Dienste wie Identitätssysteme oder branchenspezifisch Auftragswesen, Check-out oder Patientenversorgungsplattformen wiederherzustellen. Wer seine Abläufe in geschäftskritische, unternehmenskritische und nicht kritische Kategorien unterteilt, kann Wiederherstellungstests praktikabel und strategisch auf eine optimale Geschäftskontinuität abstimmen.

3. Funktionsübergreifender Recovery-as-Code

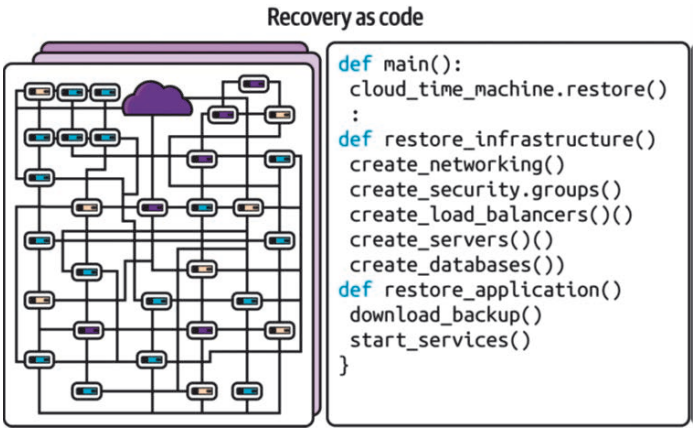
Von isolierten Playbooks zu funktionsübergreifender Recovery-as-Code (RaC): Alle im Ernstfall an der Recovery beteiligten Akteure arbeiten im Vorfeld zu oft weitgehend isoliert voneinander. Die Bereiche Sicherheit, IT-Betrieb, Applikationen und Geschäftskontinuität führen jeweils ihre eigenen Runbooks. Diese sind über Word-Dokumente, Ticketingsysteme und PowerPoint-Präsentationen verstreut gespeichert. Anwendungsabhängigkeiten, Cloud-Konfigurationen und Identitätssysteme sind so oft nicht dokumentiert und nicht ganzheitlich getestet – bis es zu spät ist.

Eine effektive Möglichkeit, diesem Problem zu begegnen, ist Recovery-as-Code (RaC), die fragmentierte, statische Playbooks in automatisch generierte, versionskontrollierte Pipelines umwandelt. RaC strukturiert die Recovery als ausführbaren Code, den die Verantwortlichen testen und im Laufe der Zeit weiterentwickeln können. So verfügen alle Teams über eine Single Source of Truth. Außerdem aktualisieren die Beteiligten den automatisierten RaC mit jedem Testdurchlauf.

Die Unternehmens-IT gewinnt dadurch sowohl an Tempo als auch an Sicherheit. Ereignisse, die früher tagelange Ausfallzeiten verursachten, lassen sich nun innerhalb weniger Stunden beheben, da die Teams nicht mehr genötigt sind, unklare Dokumentationen zu interpretieren. Der ausführbare Code lässt sich zudem konsistent über verschiedene Umgebungen hinweg skalieren und passt sich modernen DevOps-Praktiken an.

Fazit

Der Aufstieg agentischer KI bedeutet, dass Cyberangriffe letztlich unvermeidlich geworden sind und sich schneller, intelligenter und folgenschwerer auswirken. Ein zentrales Mittel dagegen ist auch eine verbesserte Cyberresilienz. Eine vollumfassende Recovery, regelmäßige automatisierte Tests und RaC ersetzen eine fragile Prävention durch aktive Resilienz. Nicht unwichtig ist auch der Einsatz von KI-Agenten unter eigener Recovery-Flagge. ◄



Die Kombination von Point-in-Time-Recovery und Recovery-as-Code vereint alle Schritte für die Wiederherstellung in ausführbare und automatisierte Pipelines.