WHITEPAPER

Darum ist Cyberresilienz das Fundament von Unternehmensresilienz

Fünf entscheidende Kriterien für CISOs, CIOs und CTOs

splunk>
turn data into doing

Jedes Unternehmen hat in der Pandemie massive Veränderungen durchgemacht und musste im Nachgang von Covid-19 zusehen, wie es sich neu ausrichten und überleben konnte. Angesichts der Unwägbarkeiten der heutigen volatilen Märkte ist der Zeitpunkt optimal, sich damit zu beschäftigen, wie sich die Unternehmensresilienz verbessern ließe, damit das eigene Geschäft inmitten all der Ungewissheit gedeihen kann.

Mit der Digitalisierung der Wirtschaft entstehen durch die komplexen Business- und Technologie-Ökosysteme neue Risiken für betriebliche Abläufe und die Rentabilität. Wenn sie überleben und wachsen wollen, dann müssen Unternehmen **Resilienz in den Betriebsabläufen verankern.**

Heutzutage setzen Unternehmen – zu Recht – auf das Konzept von Resilienz. Sie müssen die Geschäftsfortführung sicherstellen, eine flexibel einsetzbare Belegschaft aufbauen und eine Technologie einsetzen, die mitwächst und hilft, die jeweils aktuellen Herausforderungen zu bewältigen.

Durch die rasante Digitalisierung sämtlicher Bereiche – von der Customer Experience bis zum Backoffice – sind die resilienzrelevanten Systeme heute digitale Systeme. Cyberresilienz ist daher wichtiger denn je. Cyberresilienz wird am besten als die Fähigkeit verstanden, Ereignisse zu antizipieren, darauf zu reagieren und sie zu überstehen – Ereignisse, die Services unterbrechen könnten, den Unternehmenszugriff auf kritische Technologien verhindern oder entscheidende Geschäftsprozesse abbrechen. Cyberresilienz ist nicht mehr die alleinige Domäne der Sicherheitsteams, sie umfasst längst auch die IT- und DevOps-Teams. Schließlich stehen Sicherheit, Performance und Zuverlässigkeit der gesamten digitalen Ressourcen des Unternehmens auf dem Spiel.

In diesem Whitepaper geht es um die Trends der Digitalisierung, um die Komplexitäten moderner Architekturen und um die kaum vorhersehbaren Entwicklungen der Bedrohungslandschaft, mit denen CISOs (Chief Information Security Officers) konfrontiert sind. Dort, wo sich Technologie und Risiko überschneiden, müssen aber auch CIOs (Chief Information Officers) und CTOs (Chief Technology Officers) Verantwortung übernehmen – es ist ihre gemeinsame Aufgabe, ein genuin resilientes Unternehmen zu schaffen, das in den heutigen Umgebungen reaktionsschnell, agil und innovativ agieren kann.

Die Tatsachen der Gegenwart

Unternehmen, die heute erfolgreich sein wollen, sollten sich vor Augen halten, wie sehr sich die Welt in den vergangenen fünf Jahren verändert hat. „Business as usual" gibt es nicht mehr. „Alles ist anders" ist eher das Motto im Geschäftsleben der Gegenwart. Niemand hätte geahnt, mit welchem Tempo die Digitalisierung alle Aspekte des Geschäfts übernommen hat, von der Belegschaft im Homeoffice und Hybrid Work über die Lieferketten bis hin zur Interaktion mit der Kundschaft. Und wer hätte die rasche Akzeptanz von Hybrid-Cloud-Modellen vorhergesehen, die zu komplexen Architekturen geführt haben, bei denen die Workloads zwischen der Cloud und den Servern on premises hin- und herwandern? Es scheint fast so, als sei das einzig Beständige in der Gegenwart die andauernde Ungewissheit.

Digitale Datensilos

Das Thema Unternehmensresilienz ist mittlerweile digital bestimmt. Neue Anforderungen haben die Technologielandschaft radikal verändert: flexible Arbeitsumgebungen, Omnichannel im Einzelhandel und im Finanzwesen, innovative digitale Plattformen, Telemedizin, E-Learning etc. Parallel dazu ist nahezu alles Papier auf den Schreibtischen in den Bürohäusern zu digitalen Prozessen geworden; Speicher, Lösungen, Services und Anwendungen finden dabei meist in der Cloud statt.

Die Digitalisierung hat im gesamten Unternehmen zu einer Fülle von Daten geführt – aber auch zu Datensilos. Was die IT-Abteilung erfasst, ist für die Sicherheitsabteilung meist gar nicht sichtbar, was die effektive Arbeit beider Teams behindert. Dieser Mangel an Transparenz ergibt tote Winkel und Technologiestaus, sodass Schadakteure eindringen können, deren Treiben dann über Tage, Wochen oder sogar Monate hinweg unentdeckt bleibt. Ein Beispiel dafür ist die Log4j-Schwachstelle, die monatelang und millionenfach von Hackern ausgenutzt wurde, bevor sie im Dezember 2021 bekannt wurde.

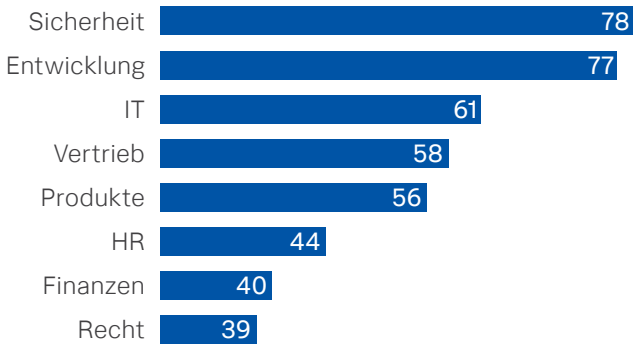
Hinzu kommt eine Unmenge neuer Anwendungen – laut IDC werden allein 2023 bis 2025 ganze 750 Millionen hinzukommen. Sowohl Dev-Teams als auch Fachbereichsentwickler und Operations-Teams müssen sich bei ihren Innovationen aber an Effizienz- und Governance-Kriterien orientieren können. Insgesamt wirft der Umstieg in digitale Welten eine immer größere Menge von Risiken auf, die jedes Unternehmen in den Griff bekommen muss.

Komplexe Architekturen

Je mehr die Cloud-Migration Fahrt aufnimmt, desto mehr zeichnet sich als Ziel eine Hybrid-Cloud ab, bei der manche Workloads on premises bleiben, während Cloud-Daten, -Services und -Apps auf diverse Anbieter verteilt sind. Stand 2022 sind 60 % der Unternehmensdaten in Clouds gespeichert. Gartner schätzt allerdings, dass 2025 bis zu 95 % der Cloud-Sicherheitsausfälle darauf zurückzuführen sein werden, dass die Kundschaft ihre Cloud-Risiken nicht angemessen handhabt.

Einer der Hauptgründe für die Cloud-Einführung ist, dass SaaS (Software as a Service) so bequem zu nutzen ist. Früher waren Anwendungen Sache der Sicherheits-, Entwicklungs- und IT-Abteilungen; heute werden über 56 % aller Unternehmensanwendungen von den Geschäftsbereichen verantwortet.

Security, Entwicklung und IT haben die meisten Apps



Durchschnittliche Anzahl der verwendeten Apps, nach Abteilung

Quelle: CIO Dive, September 2021

Diese „Appifizierung" und Automatisierung von Workloads und Workflows hat dazu geführt, dass die Menge der Speicher, Services und Anwendungen in den meisten Unternehmen kaum mehr überschaubar ist; gleichwohl sind all diese digitalen Ressourcen für den Tagesbetrieb unerlässlich. Telearbeit und ein vernetztes Ökosystem von Supply-Chain-Partnern mit unterschiedlichem Digitalisierungsstand kommen erschwerend hinzu und machen die Architektur insgesamt noch komplexer. 2022 waren 19 % aller Cybersicherheitsvorfälle auf die Kompromittierung eines Geschäftspartners zurückzuführen. Und 5G, das neue Möglichkeiten für IIoT (Industrial Internet of Things) und Edge eröffnet, bringt noch mehr Anwendungen und Endpunkte in die Infrastruktur der Unternehmen.

Der Vorstoß in die Cloud hat aber seinen Preis: eine zunehmend größere Angriffsfläche – das war bei SolarWinds, Log4j und den jüngsten Atlassian-Hacks schmerzhaft zu spüren. Jeder neue API-Endpunkt, jeder Cloud-Datenspeicher, jede GitHub-Änderung und SaaS-Anwendung wird zu einem potenziellen Einfallstor für Angreifer. Die Abbildung und das Monitoring der kritischen Ressourcen erfordert erhebliche Resilienz-Investitionen in Menschen, Prozesse und Produkte.

Es ist derzeit nur eine Frage, wann, nicht ob ein Unternehmen Opfer eines Cyberangriffs wird. Etwa die Hälfte der Firmen gab bei einer jüngeren Umfrage zu Protokoll, dass sie in den letzten zwölf Monaten kompromittiert worden sei; 46 % hatten in den letzten 24 Monaten mindestens einen Ransomware-Angriff zu verzeichnen. Die durchschnittlichen Kosten einer solchen Attacke belaufen sich derzeit auf $ 4,54 Millionen, wobei 83 % der Befragten mehrfach betroffen waren.

Unvorhersehbarkeit

Zum Jahresanfang 2020 war kaum ein Unternehmen auf eine Pandemie, eine Inflation oder einen Krieg in Europa gefasst. Heute wissen wir, dass es in einem herausfordernden geopolitischen Umfeld darauf ankommt, mit allem zu rechnen. Die Vorbereitung in Ungewissheit ist ein entscheidender Bestandteil der lang- und kurzfristigen Planung eines jeden Unternehmens geworden.

Die bestehenden Systeme sind bereits bis zur Belastungsgrenze ausgereizt. Dennoch muss das Unternehmen flexibel und agil bleiben – von den Beschäftigten im Homeoffice über die VPNs bis zu den Cloud-Infrastrukturen –, damit es mit Schwankungen in allen Geschäftsbereichen umgehen kann, ob mit Engpässen der Lieferkette oder überraschender Nachfrage.

> Agilität bedeutet letztlich die Erkenntnis, dass immer noch eine neue Welle der Ungewissheit aufschlagen wird. Und dass in dieser Situation eine anpassungsfähige Infrastruktur entscheidend ist, mit der Unternehmen im Handumdrehen gegenhalten, umsteuern oder aufstocken können.

Jedes Unternehmen muss sich die Frage stellen, wie gut es auf diese Unvorhersehbarkeit und Ungewissheit eingerichtet ist. Angesichts hoher Inflation, turbulenter Märkte und unerwarteter Verknappung (ob bei Mikro-

chips oder Babynahrung) sollte jedes Unternehmen in der Lage sein, Herausforderungen als Möglichkeiten und Ungewissheit als Chance zu nehmen.

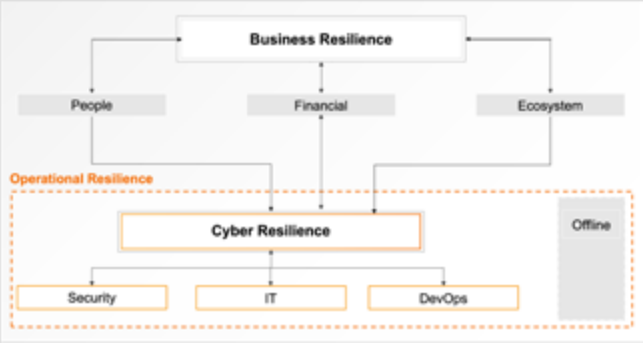
Nicht nur Cyberangriffe haben erhebliche Auswirkungen auf den Geschäftserfolg und können die Existenz des Unternehmens gefährden, sondern auch sonstige Ausfälle, Fehler und Downtime-Phasen. Der Anteil der Ausfälle, die Kosten von über als $ 100.000 verursachen, ist in den letzten Jahren sprunghaft angestiegen: 60 % der Ausfälle führen zu Verlusten von mindestens $ 100.000, ein Anstieg um 39 Prozentpunkte gegenüber 2019. Bei den Fortune-1000-Firmen kosten Ausfälle kritischer Ressourcen im Durchschnitt über $ 1 Million pro Stunde.

Cyberresilienz neu definiert

Im Dezember 2021 veröffentlichte das National Institute of Standards and Technology (NIST) ein wegweisendes Paper mit dem Titel „Developing Cyber-Resilient Systems“ (‚Entwicklung cyberresilienter Systeme‘). Damit wurde aufgezeigt, wie wichtig resiliente digitale Netzwerke für den Erfolg von Unternehmen und Organisationen in dieser „neuen Normalität“ sind.

> Cyberresilienz ist die Fähigkeit, widrige Bedingungen, Belastungen, Angriffe oder Kompromittierungen von Systemen, die auf Cyberressourcen angewiesen sind, zu antizipieren, zu verkraften, sich wieder zu fangen und neu aufzustellen. Cyberressourcen sind Ressourcen, die Informationen in elektronischer Form erstellen, speichern, verarbeiten, verwalten, übertragen oder entsorgen und auf die über ein Netzwerk zugegriffen werden kann.

„Aus Risikomanagement-Perspektive soll Cyberresilienz dazu beitragen, das mit der Abhängigkeit von Cyberressourcen verbundene Risiko für Mission, Betrieb, Organisation, Unternehmen oder Branche zu reduzieren“, erklärt NIST. Normalerweise stellen sich Unternehmen Cyberressourcen als Netzwerke, Firewalls und Sicherheitskomponenten wie E-Mail-Schutz oder Identitäts- und Zugriffsmanagement (IAM) vor. Im heutigen digitalen Zeitalter sind jedoch alle im Unternehmen auf Cyberressourcen angewiesen, vom Hybrid-Cloud-Stack, mit dem ein Finanzdienstleister seine Banking-App betreibt, über die elektronischen Entwürfe eines neuen Kampfflugzeugs bis hin zu den digitalen Komponenten der Lieferketten großer Lebensmittelhändler.



Das Unternehmensresilienz-Framework zeigt, dass Cyberresilienz von grundlegender Bedeutung ist

Das NIST-Konzept führt die getrennten Gruppen aus Sicherheit, IT und DevOps, die alle gemeinsam für Cyberressourcen verantwortlich sind, zusammen. Diese Gruppen müssen gemeinsam die Grundlagen des Geschäfts sicherstellen: dass der Zugang zu erfolgskritischen Technologien gewährleistet bleibt, dass Geschäftsprozesse ausgeführt werden können und Services verfügbar bleiben. Einfach ausgedrückt: „Wer nicht einloggen kann, kann gar nichts machen.“

> *„Wer nicht einloggen kann, kann gar nichts machen.“*

Angesichts steigender Erwartungen vonseiten der Kundschaft und zunehmend komplexer Umgebungen können getrennte Security, IT und DevOps keine Resilienz mehr gewährleisten. Die Fachleute von Gartner sind der Ansicht, dass die CISOs sich gegenüber dem Rest der Führungsebene neu positionieren müssen: als Risikomanagement-Partner (statt als die Instanz, die Einbrüche verhindert). CISOs müssen mit CIOs und CTOs zusammenarbeiten und gemeinsam eine durchgängige Cyberresilienz-Strategie entwickeln, die als tragende Grundlage der Unternehmensresilienz dienen kann.

Erfolgspfade zu Cyberresilienz

Unternehmen, die Resilienz aufbauen wollen, müssen ganz bestimmte Fähigkeiten entwickeln – Fähigkeiten, mit denen sie einerseits Worst-Case-Szenarien überstehen, mit denen sie andererseits das Geschäft unter veränderlichen Bedingungen weiterentwickeln können.

Doch wo beginnen? Welche Teile des Netzwerks sind wirklich vom Monitoring erfasst? Haben die Beschäftigten die passenden Skillsets? Wie schnell können sie Probleme und Incidents erkennen, wie schnell

können sie reagieren? Wenn Sie diese Fragen ehrlich beantworten und dann die Lücken zwischen Ist- und Soll-Zustand schließen, sind Sie auf dem besten Weg Richtung Cyberresilienz. Im Folgenden zeigen wir die fünf wichtigsten Erfolgspfade auf und definieren außerdem, wie Resilienz mit hohem Reifegrad aussehen sollte.

Fünf Fähigkeiten zum Aufbau von Cyberresilienz

Transparenz

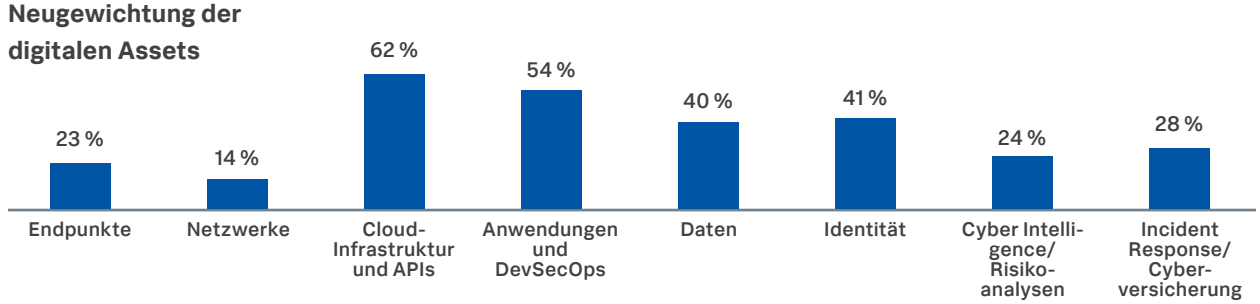
Angesichts von Datensilos und komplexen Architekturen neigen Unternehmen dazu, um einzelne Teams, Produkte oder Tools herum „Resilienz-Taschen" zu bilden. So hat z. B. die IT-Abteilung eine Liste von Endgeräten, die sie an die Belegschaft ausgibt. Diese Informationen werden aber nicht an das Sicherheitsteam weitergegeben, das den Bestand mühsam selbst erfassen muss – statt einfach auf einen gemeinsamen, kontrollierten Datenbestand zuzugreifen. So etwas kann katastrophale Folgen haben – z. B. wenn eine kritische Schwachstelle nicht gepatcht wird und Angreifer über das übersehene Gerät ins Firmennetz gelangen.

Wenn Verantwortliche zulassen, dass sich Resilienz nur in solchen Taschen entwickelt, wird es unmöglich, Risiken über die Systeme hinweg zu messen und zu verwalten. Das hat Gartner zufolge bittere Konsequenzen: „Die meisten Unternehmen unterscheiden nicht zwischen (strategischer) Unternehmensresilienz und operativer (taktischer) Resilienz. Sie beschränken sich bei beiden Anstrengungen auf IT-Projekte und einige wenige Geschäftsfunktionen. Das Unternehmen läuft daher Gefahr, seine Geschäftsziele zu verfehlen."

Früher, als es noch ein Rechenzentrum vor Ort und einen abgezählten Satz von Anwendungen gab, kontrollierten die Sicherheitsteams „das Netzwerk". Heute ist „das Netzwerk" etwas, dessen unklare Grenzen durch die Endpunkte der Remote-Beschäftigten, durch (Hybrid-) Clouds und durch die Software bestimmt werden, die in den Abteilungen ohne Kenntnis der IT installiert wird.

Security-, IT- und DevOps-Teams wissen, dass sie nur diejenigen digitalen Ressourcen warten und schützen können, die sie im Blickfeld haben. Observability bedeutet genau diese Transparenz in der gesamten Umgebung, von Telefon und Laptop bis zu den Public, Multi- und Hybrid-Clouds. Observability ist eine unerlässliche Resilienz-Voraussetzung. Jede digitale Ressource, die genutzt wird und deren Leistung optimiert werden soll – ob UX, Datenbanken, Endpunkte oder Cloud-Apps –, muss abgebildet und ins Monitoring einbezogen sein. Ein Full-Stack-Monitoring kann z. B. schnell Ort und Einzelheiten eines Events ausgeben, egal ob ein Angriff im Gange ist oder eine Datenbank schwächelt. Die Teams können dann schneller und effektiver reagieren.

Resilienz setzt also voraus, dass alle Teams wissen, wo ihre Sachen sind – ganz gleich, ob diese „Sachen" nagelneue Hybrid-Clouds sind oder ein Messenger mit Verschlüsselung auf den Privattelefonen der Beschäftigten. Bei der Bestandsaufnahme und Katalogisierung der digitalen Assets im Unternehmen müssen die Ver-



Quelle: Forgepoint CISO Security Priorities Model

antwortlichen festlegen, was in puncto Cyberresilienz Priorität haben soll. Angesichts zunehmend vernetzter und voneinander abhängiger Systeme müssen Unternehmen nicht nur prüfen, welche Ressourcen am wichtigsten sind, sondern auch, wie sich Änderungen in einem Bereich auf nachgelagerte Prozesse auswirken. In einem Softwareunternehmen z. B. wird End-to-End-Netzwerksicherheit wichtig sein, und es dürfte Wert darauf gelegt werden, dass eine Warnung ergeht, sobald eine neue API oder App ins Spiel kommt. Entsprechend müssen die Verantwortlichen grundlegende Transparenz schaffen und den gesamten Digitalbestand ihrer Geschäftsprozesse von Anfang bis Ende abbilden.

Erkennung

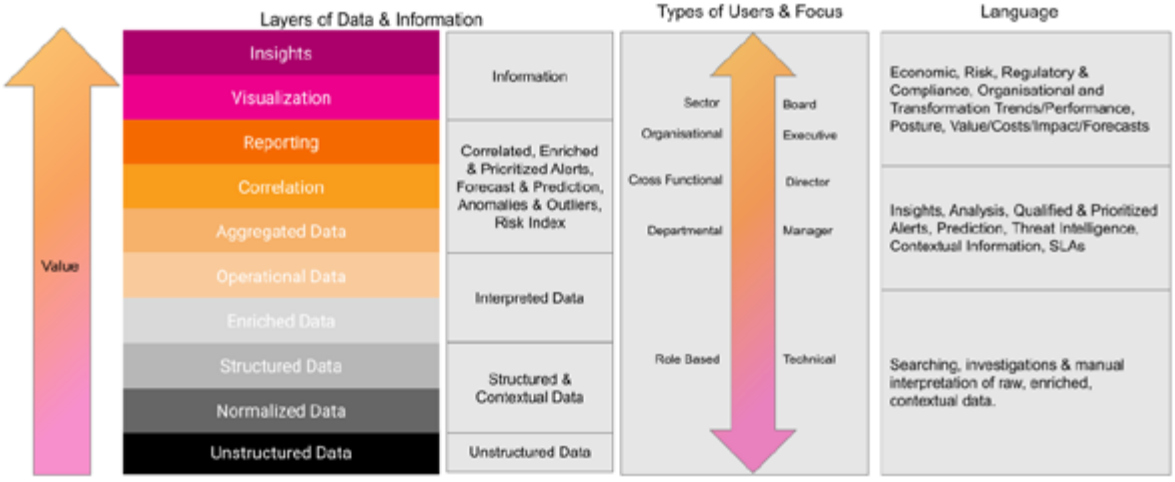
Wenn IT-, DevOps- und Sicherheitsteams alles im Blick behalten, was im Unternehmen vor sich geht, dann müssen sie auch in der Lage sein, Probleme bereits in der Entstehung aufzuspüren und zu identifizieren, statt Minuten, Stunden oder sogar Tage verstreichen zu lassen. In der Frühphase eines Problems verlieren sie unter Umständen sogar noch mehr Zeit, wenn sie mangels Kontext und gemeinsamer Datengrundlage nicht erkennen können, ob das Problem auf einen harmlosen Ausfall oder auf einen Angriff zurückzuführen ist.

Erste Voraussetzung von Erkennung ist eine vollständige Abdeckung. Mit anderen Worten: Die Teams müssen sichergehen, dass sie kontinuierlich alles überwachen, was wichtig ist. Die Verantwortlichen können zwar bestimmte Systeme oder Fachleute als kritische Ressourcen einstufen und das Monitoring hier schärfer einstellen, während für selten genutzte Systeme oder Endpunkte weniger strenge Anforderungen gelten, aber letztlich muss alles ins Monitoring einbezogen sein. Das Monitoring muss rund um die Uhr funktionieren und sofort Alarm schlagen, wenn ein System irgendwie ausfällt. Eine winzige Störung, das bloße Aufflackern einer Warnung, könnte ein Indikator dafür sein, dass ein Hacker gerade ins Netzwerk eindringt – oder dass es in einem schlecht getesteten Code-Release knirscht. Ohne vollständige Abdeckung und die Möglichkeit des Datenaustauschs zwischen den Teams besteht immer die Gefahr, dass etwas durch die Maschen schlüpft.

> 82 % der CISOs stehen unter Druck, weil sie ihre Datenanalysen verstärken sollen, und 85 % der Unternehmen sagen, dass Analysen für die Cybersicherheit jetzt eine größere Rolle spielen.

Informationsebenen und Verwendungszwecke

Jede Ebene baut auf der darunterliegenden auf



Die Datenstufen der Unternehmensresilienz

Zur Cyberresilienz beitragen können sämtliche Daten, die im Unternehmen erfasst werden. Logs, Metriken, Traces und andere unstrukturierte Daten können eine Fülle von Rohinformationen liefern. Doch erst wenn diese Daten normalisiert und angereichert sind, werden sie für das Unternehmen wirklich wertvoll. Manche Unternehmen verwenden zwar immer noch unstrukturierte Daten für Sicherheits- oder Observability-Aufgaben, aber der Trend geht heutzutage eindeutig in Richtung Automatisierung, die angereicherte Daten ergibt und Security-Abläufe dadurch effizienter macht.

Als Nächstes müssen Unternehmen aus ihren Monitoring-Daten auch effektiven Nutzen ziehen können, etwa indem sie Suchläufe einrichten oder ausgewählte Daten einer systematischen Analyse unterziehen. Korrelierte und aggregierte Daten können die Grundlage von Warnmeldungen mit abgestufter Priorisierung sein, von praktisch verwertbaren Bedrohungsinformationen oder von analytischen Erkenntnissen zu Trendentwicklungen von Security und Geschäft.

Der Wert dieser Daten lässt sich durch Automatisierung noch steigern. Eine robuste Plattform, die Daten aus allen Tools und Services zusammenführt und bei Überschreitung definierter Schwellenwerte Warnmeldungen auslöst, kann inkrementelle Risiken identifizieren, die einer Punktlösung verborgen blieben. Automatisierte Tools zur Verhaltensanalyse in Kombination mit maschinellem Lernen können verdächtige Muster in scheinbar unzusammenhängenden Aktionen erkennen und sie Fachleuten zur weiteren Untersuchung zuweisen.

Und schließlich dienen die gesammelten Daten auch dazu, auf Basis vergangener Ereignisse und aktueller Trends Incidents im Voraus zu erkennen. Analysen, die mit normalisierten, korrelierten und angereicherten Daten aus dem gesamten Unternehmen arbeiten, können tote Winkel ausleuchten und gehaltvollere Warnmeldungen ausgeben, die auf tatsächliche Probleme oder Bedrohungen hinweisen. Die besten Security-, IT- und DevOps-Teams nutzen heute leistungsfähige fortschrittliche Analysen zur Erkennung von Bedrohungen und zur Erstellung zuverlässiger Warnmeldungen.

Untersuchung

Wenn eine Warnmeldung beim Team eingeht, besteht der erste Schritt in einer Soforteinschätzung, ob es sich um einen Fall handelt, der sofortige Aufmerksamkeit erfordert. Zu diesem Schritt gehört unter Umständen die Anreicherung mit Kontext von IP-Adressen, Tags, Hosts, Netzwerk- und CPU-Daten etc. Analysten greifen dabei häufig auch auf externe Dienste zurück, die aktuelle Bedrohungsinformationen liefern, sodass anhand von Kompromittierungsindikatoren geprüft werden kann, ob eine Datei oder Domain ein Risiko darstellt.

Dieser Prozess erfordert von Hand jedoch einiges an Zeit. Analysten verbringen manchmal Stunden mit einer einfachen Sichtung und müssen auch bei der übrigen Fehler-Ursachen-Analyse Daten aus unterschiedlichen Tools und Dashboards einzeln abfragen und Rohdaten-Logs durchforsten. Darüber hinaus müssen sie Beweise und Artefakte mühsam zusammentragen, mitunter in so schlichten Tools wie Notepad.

Im Vorteil sind dagegen Unternehmen mit soliden Funktionen zur schnellen Untersuchung, die sämtliche Daten, die sie benötigen, auf einer zentralen Konsole versammelt finden, sie durchsuchen und darauf zugreifen können, egal wo die Daten letztlich liegen.

Reaktion

Eine schnelle Reaktion auf Events ist entscheidend für die Geschäftsfortführung. Die Teams müssen Bedrohungen innerhalb von Minuten untersuchen und entschärfen können – und nicht erst nach Stunden oder gar Tagen. Das bedeutet, dass manuelle Systeme und einfache Playbooks durch automatisierte Reaktionen ersetzt werden müssen, die bereits Entscheidungen über erste Abhilfemaßnahmen treffen können. Durch die Orchestrierung der Tool-Inputs und -Outputs zur Koordinierung der Reaktionsmaßnahmen in der gesamten Infrastruktur lassen sich die Reaktionszeiten verkürzen, und den Teams bleibt mehr Zeit für die proaktive Suche nach Bedrohungen, für Red-Team-Blue-Team-Trainings und für andere Sicherheitsoptimierungen.

Allerdings finden die ohnehin überlasteten Teams kaum die nötige Zeit, Prozesse und manuelle Playbooks zu analysieren und Aufgaben zu automatisieren. Diese Arbeit ist jedoch eine notwendige Cyberresilienz-Bedingung. Je mehr sich die Infrastruktur ausdehnt und je mehr Tools Verwendung finden, desto weniger können manuelle Prozesse Schritt halten. Erst durch Automatisierung der ersten Incident-Analysen und -Reaktionen können die Teams Situationen schnell genug bearbeiten und sich trotzdem strategischen Aufgaben widmen.

Denken Sie daran, dass die Automatisierung im Laufe der Zeit skaliert werden muss, damit sie dem wachsenden Umfang und der Komplexität des Unternehmens gerecht wird. Skalierbar muss auch die Orchestrierung sein. Wenn ein Tool nicht so skaliert, dass es mit den Inputs und Outputs der anderen Tools mithalten kann, dann treten die Daten auf der Stelle und die Teams vergeuden wertvolle Zeit damit, diese Tools irgendwie zur Zusammenarbeit zu bewegen. Die Verantwortlichen im Unternehmen müssen also einen realistischen Blick auf die Probleme, ihre Tools, ihre Teams und die Notwendigkeiten der Cyberresilienz werfen und sich dann auf die Bereiche konzentrieren, in denen sie mit Orchestrierung etwas erreichen können.

Zusammenarbeit

Cyberresilienz ist nicht nur eine Frage der Technologie, sondern auch von Menschen und Prozessen. In den Unternehmen steht ein Kulturwandel an, denn Cyberresilienz betrifft auch die Zusammenarbeit der Teams von Sicherheit, IT und DevOps.

Die Entwicklungsteams können heute keine Anwendungen mehr bauen, ohne den Aspekt Sicherheit zu berücksichtigen. Diese Integration ist eines der wichtigsten DevSecOps-Prinzipien: die durchgängige Berücksichtigung von Security-Aspekten bei der Erstellung neuer Anwendungen bzw. der Erweiterung bestehender Systeme. Sicherheit ist nicht mehr die Aufgabe eines Teams, sondern die Aufgabe aller.

Seitdem SRE (Site Reliability Engineering) in den Unternehmen Einzug hält, liegt der Fokus stärker auf Resilienz im Sinne von Hochverfügbarkeit, von erfüllten Kundenerwartungen und von digitalen Systemen, die SLAs (Service Level Agreements) und SLOs (Service Level Objectives) einhalten müssen. SRE-Modelle müssen nun als oberste Ziele nicht nur Zuverlässigkeit und Wiederherstellung, sondern auch Resilienz umfassen. Dazu ist erforderlich, dass sowohl die SRE- als auch die Sicherheitsteams stärker zusammenarbeiten und automatisieren, damit sie ihre Daten gemeinsam nutzen und ihre jeweiligen Aufgaben optimal erledigen können.

Cyberresilienz wird so zu etwas werden, das für alle gilt, vom IT-Management über das SRE-Personal bis zu DevSecOps- und Datenfachleuten. Diese Ausweitung umfasst Prozessautomatisierung, Ziele und Metriken für SLAs und SLOs ebenso wie Retrospektiven, in denen Incidents genauer unter die Lupe genommen werden, damit sich daraus lernen lässt.

Da die Grenzen zwischen IT, DevOps, DevSecOps und Security verschwimmen, ist es zur Zusammenarbeit erforderlich, dass die Teams Daten gemeinsam nutzen. Sie können und sollten Systeme und Prozesse einrichten, die Transparenz schaffen und Telemetriedaten gemeinsam nutzen und damit ein vollständiges Bild der Ressourcen, Abhängigkeiten und potenziellen Probleme des Unternehmens ergeben. Dann können die Teams bei schweren Störungen oder heftigen Angriffen besser mit unerwarteten Downtimes umgehen und die Krisenkommunikation sowohl zeitnah als auch dateninformiert bewältigen. Je mehr die Teams zusammenarbeiten und je mehr Tools und Daten sie gemeinsam nutzen können, desto größer ist die Cyberresilienz des Unternehmens.

Aussagekräftige Metriken

Die Arbeit nimmt kein Ende – darin sind sich IT- und Sicherheitsfachleute einig. Die Cybersecurity-Teams sind, wie alle anderen Teams, ständig dabei, ihre Tools und Verfahren zu optimieren. Incident-Revision, aktualisierte Reaktionsmaßnahmen und Red-Team-Blue-Team-Übungen dienen effektiv der Cyberresilienz. Dasselbe gilt für die Optimierung zweier Schlüsselmetriken: der Mean Time to Detection (MTTD) und der Mean Time to Respond (MTTR).

60 % der Unternehmen sagen, dass die Transparenz von Anwendungen und Datenbeständen ihre Cyberresilienz verbessert hat. 57 % dieser Unternehmen nutzen zur Resilienzoptimierung eine Kombination aus Automatisierung, KI und maschinellem Lernen.

Diese beiden Metriken können eine erste Antwort auf die Frage geben, wie lange es dauert, Incidents zu finden und zu beheben. Die MTTD kann allerdings variieren, je nachdem, ob es sich um einen einmaligen Vorfall handelt oder um einen Angreifer, der sich langsam über mehrere Vektoren anschleicht. Ein niedriger MTTR-Wert ist natürlich gut, aber es wird immer komplexe Incidents geben, deren Behebung viel Zeit in Anspruch nimmt, was sich wiederum auf die gesamte Metrik auswirkt.

Es gibt noch weitere nützliche Metriken, die mit Blick auf die Cyberresilienz von Interesse sind. Die Kombination von Service Level Indicators (SLIs) und Service Level Objectives (SLOs) etwa zeigt, wie gut ein Service funktioniert und ob dieser Wert der anvisierten Verfügbarkeit entspricht. Wenn ein Service z. B. seine SLOs beständig verfehlt, ist klar, dass eine Untersuchung fällig ist. Es kann sein, dass der Service kompromittiert ist oder dass er einfach regelmäßig überlastet ist und mehr Ressourcen benötigt.

Cyberresilienz macht agil

Zusammengenommen bilden die genannten Kriterien eine solide Grundlage für Unternehmensresilienz. Auf dieser Grundlage können CISOs, CIOs und CTOs ihr Unternehmen nicht nur durch disruptive Zeiten bringen, sondern es letztlich sicher durch Landschaften steuern, die sich laufend verändern.

Agile Unternehmen sind in der Lage, Technologie als Vorteil im Wettbewerb zu nutzen. Resiliente Unternehmen können flexibel skalieren und neue Funktionen einführen, ohne den Service zu unterbrechen. Agilität bedeutet: Das Unternehmen kann mit Unerwartetem schnell und routiniert umgehen, sodass das Geschäft weiterläuft, als wäre nichts geschehen.

Cyberresilienz in der Zukunft

In den nächsten drei bis fünf Jahren wird sich das Konzept von Cyberresilienz weiterentwickeln, damit es weiterhin das leistet, was Unternehmen in stürmischen Zeiten benötigen. Das gilt auch angesichts des Umstands, dass sich geschäftliche Anforderungen und betriebliche Parameter ebenfalls ändern.

Cybersecurity Mesh Architecture

Mit der zunehmenden Arbeitslast der Sicherheitsteams ist auch die Menge der verwendeten Tools gewachsen. Viele CISOs sind bemüht, dieses Sammelsurium hinter sich zu lassen und einen einheitlichen Security-Ansatz zu entwickeln. Seit 2015, als Gartner den Begriff „Security Orchestration, Automation and Response“ (SOAR) prägte, geht die Entwicklung der Unternehmen in Richtung einer orchestrierten Vorfallreaktion; dadurch ist die Effizienz gestiegen, und die Reaktionszeit hat sich verkürzt. Doch obwohl SOAR den Sicherheitsteams die richtige Richtung weist, ist es so, dass viele Unternehmen ihre SOAR-Plattform parallel zu älteren Bestandstools betreiben, dass sie sich mit Datensilos herumschlagen und zur Koordination der einzelnen Tools immer noch Handarbeit nötig ist.

Diese Unternehmen stellen fest, dass es mehr braucht als SOAR, wenn „alles überall und in Echtzeit“ abgedeckt werden soll. Und genau hier setzt das Konzept der Cybersecurity Mesh Architecture (CSMA) an. CSMA strebt ein vollständig integriertes System von Sicherheitstools und -daten an, das sämtliche Ressourcen abdeckt, von der Cloud über Laptops und Datenbanken bis zu den E-Mails, mit zentralisierten Dashboards, Warnmeldungen und Berichten sowie einem Identitätsmanagement für sämtliche User, Geräte und Services. Kurzum: CSMA erleichtert die automatisierte Interoperabilität der Sicherheitstools und konsolidiert die Verwaltung von Richtlinien und Daten für all diese Tools.

Nach jahrzehntelangen Bemühungen mit Einzeltools und im Bestreben, sämtliche Daten auf einer einzigen zentralen Plattform zusammenzuführen, haben Unternehmen noch immer mit den Problemen von umfassender Abdeckung und schneller Erkennung und Reaktion zu kämpfen. CSMA zeichnet ihnen einen Pfad, auf dem sie in mehreren Phasen zu einer einheitlichen Plattform übergehen können, sodass sie nicht mit einem einzigen Satz von den bestehenden Systemen auf die einheitliche Plattform springen müssen.

In der vernetzten Welt von heute ist der Schutz von Informationen und Technologien ein wesentliches Element der Unternehmensresilienz. Wo das Cyberresilienz-Programm auf den Grundprinzipien Transparenz, Erkennung und Untersuchung, Reaktion, Zusammenarbeit und Agilität basiert, ist das Geschäft sicher. Und wenn sich die Verantwortlichen nicht ständig um Sicherheit oder Performance sorgen müssen, können sich die Unternehmen auf Innovation und Wachstum konzentrieren. Ein Unternehmen, das sicher und zuverlässig online ist, zeigt seiner Kundschaft und seinen Partnern, dass es vertrauenswürdig ist, dass es auf alle Herausforderungen und Chancen der Zukunft gefasst ist. Cyberresiliente Unternehmen sind in der Lage, inmitten der Unwägbarkeiten unserer sich ständig verändernden Welt zu florieren.

Resilienz erfordert Transparenz. Mit Splunk sehen Sie alles, sodass Sie schnell handeln und sich jeder Situation anpassen können. Mehr erfahren.

splunk>

Mehr erfahren: www.splunk.com/asksales

www.splunk.de

Splunk, Splunk> und Turn Data Into Doing sind Marken und eingetragene Marken von Splunk Inc. in den Vereinigten Staaten und anderen Ländern. Alle anderen Markennamen, Produktnamen oder Marken gehören den entsprechenden Inhabern. © 2023 Splunk Inc. Alle Rechte vorbehalten.

22-26214-Splunk-WhyCyberResilienceistheFoundationforBusinessResilience-WP-102_GER_V2