COHESITY

WHITEPAPER

Aufbau von Cyber-Resilienz in einer Zeit destruktiver Cyberangriffe

Bewerten Sie Ihr Unternehmen mit dem Cohesity Destructive Cyberattack Resilience Maturity Model.

INHALTSVERZEICHNIS

Zusammenfassung

Daten sind für Unternehmen und gemeinnützige Organisationen lebenswichtig. Sie sind ein wesentlicher Bestandteil von Prozessen und Arbeitsabläufen. Diese sind so sehr von Informationstechnologie abhängig geworden, dass jeder Versuch, zu manuellen papiergestützten Prozessen zurückzukehren, zu Betriebsstörungen führt. Diese können wiederum die Fähigkeit einer Organisation, ihre Produkte oder Dienstleistungen anzubieten, erheblich beeinträchtigen.

In der Vergangenheit fielen diese Betriebsstörungen in den Bereich „Betriebskontinuität und Notfallwiederherstellung“ (engl. Business Continuity und Disaster Recovery, BC/DR) und betrafen nur eine kleine Anzahl genau definierter Szenarien wie Überschwemmung, Brand, Stromausfall, Fehlkonfiguration und Geräteausfall. Zurzeit sind Betriebsstörungen am häufigsten auf destruktive Cyberangriffe zurückzuführen.

In diesem Whitepaper gehen wir der Frage nach, warum die traditionellen Ansätze, die IT-Betriebsteams auf Szenarien wie die Betriebskontinuitäts- und Notfallwiederherstellung angewendet haben, nicht mehr ausreichen, um dieser neuen Bedrohung zu begegnen. Wir erörtern ferner, warum die bisher von Sicherheitsteams bei nicht destruktiven Cyberangriffen genutzten Prozesse unzureichend sind.

Abschließend zeigen wir pragmatische Schritte auf, die Organisationen ergreifen können, um ihre Widerstandsfähigkeit mit dem Cohesity Destructive Cyberattack Resilience Maturity Model gegenüber destruktiven Cyberangriffen zu stärken. Anhand dieses Modells können Unternehmen ihre aktuelle Resilienz bewerten und eine Roadmap zu deren Verbesserung entwickeln.

Die neue Bedrohung und warum traditionelle Ansätze versagen

Ransomware geht zwar auf den 1989 veröffentlichten „AIDS-Trojaner“ zurück, aber erst als 20 Jahre später Kryptowährungen aufkamen, konnte man mit solchen Attacken leicht Geld verdienen, was die heutige Angriffsflut auslöste.

Eine weitere Art von destruktiven Attacken tauchte 2012 auf, als die Flame- und die Shamoon-Wiper-Malware entdeckt wurden. Diese zielten erfolgreich auf die Vernichtung der Daten von iranischen bzw. saudi-arabischen Ölfirmen ab. Im Gegensatz zu Ransomware-Attacken, die von Kriminellen zur Geldbeschaffung genutzt werden, sind diese Wiper-Attacken das Werk staatlicher Akteure oder deren Handlanger mit dem Ziel, den Interessen oder der Wirtschaft eines anderen Staates Schaden zuzufügen. In Anbetracht der aktuellen geopolitischen Lage hat die Welt in letzter Zeit eine deutliche Zunahme von Wiper-Angriffen erlebt.

Von der Pionierzeit der Informationssicherheit bis hin zum Aufkommen von destruktiven Ransomware-Attacken wurden Unternehmen in diesem Bereich vor allem mit Datendiebstahl konfrontiert. Anders als bei Betrug oder dem Diebstahl physischer Güter verfügt das Unternehmen bei Datendiebstahl noch immer über eine Kopie seiner Daten und kann diese nutzen, um den Kunden weiterhin seine Produkte und Dienstleistungen anzubieten. Die Folgen dieser Angriffe sind daher die sekundären Verluste in Form von Rufschädigung, potenziellen Rechtsstreitigkeiten mit Partnern oder betroffenen Personen, deren Daten gestohlen wurden, sowie Geldstrafen.

Heute, im Zeitalter destruktiver Cyberangriffe wie Ransomware und Wiper-Attacken, kommt zu diesen sekundären Verlusten noch ein primärer Verlust hinzu: die Unfähigkeit des Unternehmens, seine Produkte und Dienstleistungen bereitzustellen. Ein Großteil der sekundären Verluste entsteht bereits vor einem Vorfall, da schlichtweg die geeigneten Verhinderungsmechanismen fehlen. Im Hinblick auf die primären Verluste zählt hingegen jede Sekunde, die nicht für Reaktions- und Wiederherstellungsaktivitäten aufgewendet werden muss. Bei Ausspähangriffen auf Unternehmensdaten konnte man sich den Luxus leisten, ineffiziente und ineffektive Reaktions- und Wiederherstellungsprozesse zu tolerieren. Bei Angriffen auf die Integrität bzw. die Verfügbarkeit von Daten, die für ein Unternehmen betriebskritisch sind, ist dies nicht mehr möglich.

Die jüngsten Entwicklungen im Bereich Ransomware as

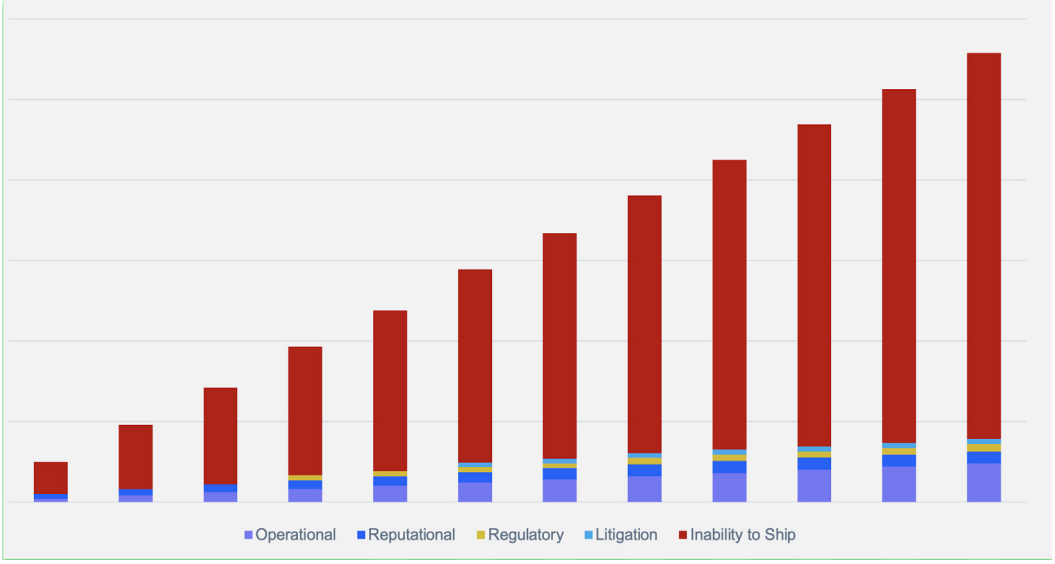

Abbildung 1: *Kennzeichnende Auswirkungen verschiedener Arten von Verlusten im Zeitverlauf*

a Service (RaaS) erschweren die Abwehr immer mehr. In der Vergangenheit hatten wir es insgesamt mit ein paar Dutzend Ransomware-Akteuren zu tun, die eine eigene Infrastruktur betrieben und Angriffe durchführten. Die Zahl der Angriffe wurde dadurch begrenzt, dass die Akteure die für den Betrieb ihrer Infrastruktur erforderlichen technischen Kompetenzen zusammenbringen mussten.

Viele dieser Akteure haben jedoch festgestellt, dass es für sie profitabler ist, ihre Ransomware-Plattformen und Toolkits „Partnern" zugänglich zu machen, die keinerlei technische Kenntnisse benötigen, sondern nur die personellen Ressourcen für den Angriff bereitstellen. Im Gegenzug behalten die Partner in der Regel 80 % der eingenommenen Lösegelder, während der Plattformbetreiber 20 % einstreicht. RaaS hat es den Plattformbetreibern zudem ermöglicht, sich stärker auf die Innovation der Angriffstools ihrer Plattform zu konzentrieren, um sich von anderen Akteuren abzuheben. Daraus resultiert die Abkehr vom Phishing als primärem Angriffsvektor hin zu anderen Techniken mit höheren Erfolgsquoten, wie z. B. die Ausnutzung von Schwachstellen in der mit dem Internet verbundenen Infrastruktur. Dies kann innerhalb weniger Tage geschehen, lange bevor Unternehmen die Angriffsfläche durch Patches absichern können. Ein weiterer deutlicher Trend ist die Verwendung von Anmeldedaten, die bei früheren Angriffen gestohlen wurden.

Obwohl wir zunehmend mit Angriffen und ihren immer schwerwiegenderen Folgen konfrontiert werden, strömten die Investitionen in Cybersicherheit traditionell in den Datenschutz und die Angriffserkennung, da der Schwerpunkt früher auf Datenausspähung lag. Die Ausgaben für Prävention und Erkennung sind zwar von entscheidender Bedeutung, um zu verhindern, dass das Unternehmen aufgrund der Flut der fast täglich auftretenden Einbruchsversuche untergeht. Sie reichen aber nicht aus, um dem Umfang und der Raffinesse der heutigen destruktiven Cyberangriffe gerecht zu werden. Ein kurzer Blick auf die Schlagzeilen der letzten 12 Monate zeigt, dass viele Unternehmen mit Cybersicherheitsbudgets in zweistelliger Millionenhöhe durch Ransomware erheblich in ihren Betriebsabläufen gestört wurden. Es genügt also nicht, in Schutz und Erkennung zu investieren. Wir ziehen unsere Gräben immer breiter und unsere Mauern immer höher, aber die Gegner bauen daraufhin einfach bessere Boote und höhere Leitern, oder sie bahnen sich mittels Social Engineering den Weg durch die Tore unserer Festung.

Fast alle aktuellen Regelwerke für Cybersicherheit wie das **NIST Cybersecurity Framework 2.0** und Vorschriften wie die **EU-Richtlinie über Netzwerk- und Informationssicherheit 2.0 (NIS2)** oder der **EU Digital Operational Resiliency Act (DORA)** konzentrieren sich auf den Aufbau von Resilienz. Der Fokus liegt dabei nicht nur auf der Fähigkeit, Angriffe zu verhindern und zu erkennen, sondern auch darauf, Cyberangriffe durch Reaktion und Wiederherstellung zu überwinden – zwei Funktionen, in die bislang zu wenig investiert wurde.

In einem durchschnittlichen Unternehmen sind über 130 verschiedene Cybersecurity-Tools installiert, von denen die allermeisten nicht ausreichend integriert und operationalisiert sind, um zu verhindern, dass Unternehmen Opfer eines Cyberangriffs werden. Jede weitere Investition in Vorbeugung und Erkennung wird wahrscheinlich nur einen Bruchteil des Cyber-Risikos verringern und zugleich zu mehr Konflikten mit den Anwendern, weniger Flexibilität für das Unternehmen, mehr Alarmmüdigkeit, höheren Lizenzkosten und zu noch mehr zu verwaltender Sicherheitsinfrastruktur führen. Ausgaben für Reaktion und Wiederherstellung hingegen ermöglichen die Cyber-Resilienz, die diese neuesten Regelwerke und Vorschriften fordern und die aufgrund der heutigen Bedrohungen durch Cyberangriffe unerlässlich sind.

Die fünf Hindernisse beim Erreichen von Cyber-Resilienz

Traditionelle BC/DR-Wiederherstellungsansätze sind bei Cyberangriffen ungeeignet

Eines der größten Hindernisse auf dem Weg von der Cybersicherheit zur Cyber-Resilienz besteht darin, dass in vielen Unternehmen Teams für die Reaktionen auf Angriffe verantwortlich sind, die dem Chief Information Security Officer (CISO) unterstehen. Die Wiederherstellung hingegen liegt in den Händen von Teams, die dem Chief Information Officer (CIO) unterstehen. Diese beiden Abteilungen haben die entsprechenden Kompetenzen meist weitgehend unabhängig voneinander aufgebaut, da sie ursprünglich für die Bewältigung unterschiedlicher Bedrohungen verantwortlich sein sollten. In der Vergangenheit bekämpften die CISOs Datendiebstähle, während sich die CIOs mit der Geschäftskontinuität und Notfallwiederherstellung (Business Continuity und Disaster Recovery, BC/DR) befassten. Die BC/DR-Strategien bezogen sich auf eine begrenzte Anzahl leicht nachvollziehbarer Bedrohungsszenarien wie Überschwemmung, Feuer, Erdbeben, Stromausfall, Geräteausfall und Konfigurationsfehler.

Unternehmen mit riesigen Cybersicherheitsbudgets und gut etablierten BC/DR-Programmen geraten als Opfer von Ransomware in die Schlagzeilen, weil sie es versäumt haben, diese beiden Aspekte an destruktive Cyberangriffe anzupassen. Enorme Kosten und massive Beeinträchtigungen der Kunden sind die Folge.

Die BC/DR-Pläne des CIO sind darauf ausgelegt, eine kleine Anzahl genau definierter Grundursachen zu behandeln. Automatisierung und Orchestrierung können bei der Wiederherstellung eine große Rolle spielen, und der letzte Snapshot eines Systems ist in der Regel derjenige, der wiederhergestellt wird.

Im Gegensatz dazu zielen Angreifer bei destruktiven Cyberattacken aktiv auf die Backups ab, um diese unzugänglich zu machen und so ihre Erfolgschancen zu erhöhen. Diese Angreifer können jede beliebige Kombination der wenigen hundert MITRE-ATT&CK-Techniken iterativ in beliebiger Reihenfolge einsetzen, um durch Ausnutzung von Schwachstellen in das Unternehmensnetzwerk einzudringen. Einmal eingedrungen, erweitern sie ihre Privilegien, die auch nach der Wiederherstellung von einem Backup bestehen bleiben. Sie bewegen sich lateral im Unternehmensnetz, stehlen Daten und löschen oder verschlüsseln diese schließlich.

Die höchsten Kosten nach einem destruktiven Cyberangriff entstehen den Unternehmen, deren Backups vom Angreifer unbrauchbar gemacht werden oder bei denen angegriffene Systeme ohne geeignete Abhilfemaßnahmen zur Beseitigung der Bedrohungen und Schwachstellen wiederhergestellt werden. Dies hat zur Folge, dass dieselben Systeme innerhalb von Sekunden oder Minuten erneut infiziert sind.

Untersuchung und Schadensbegrenzung laufen unabhängig voneinander

Bei der Wiederherstellung nach destruktiven Cyberangriffen ist das IT-Betriebsteam auf das Sicherheitsteam angewiesen, um zu verstehen, welche Schritte zur Verhinderung einer erneuten Infektion oder eines erneuten Angriffs unternommen werden müssen. Die Untersuchungen des Sicherheitsteams umfassen die folgenden Punkte:

- Vom Angreifer ausgenutzte Schwachstellen, damit das IT-Betriebsteam diese patchen kann, bevor die Systeme wieder in Betrieb genommen werden
- Bösartige Konten und Authentifizierungsanbieter, die aus den Systemen entfernt werden müssen
- E-Mails, die in den Posteingängen der Nutzer liegen und darauf warten, wieder angeklickt zu werden
- Persistenzmechanismen in geänderten Konfigurationsdateien, die entfernt werden müssen
- Binärdateien oder Bibliotheken, die vom Angreifer durch bösartige Versionen ersetzt wurden
- Änderungen an Registrierungseinträgen oder Domänenstrukturen

- Kontrollen, die den Angriff nicht verhindern oder erkennen konnten, um diese zu verstärken und ihr erneutes Versagen zu verhindern
- Alle sonstigen Artefakte des Angriffs, die aus dem wiederhergestellten System entfernt werden müssen

Bei den immer häufiger auftretenden LOL („Living off the land")-Angriffen werden genau die Instrumente, die eigentlich zur Verwaltung der Umgebung dienen, gegen diese eingesetzt. Wie wirkt es sich auf die Wiederherstellung aus, wenn PowerShell oder SSH nicht verfügbar sind?

Wenn der CIO isoliert handelt, kann er ein Recovery Time Objective in Aussicht stellen, das allein von der Festplattengeschwindigkeit, der Pipe und der Wiederherstellungssoftware abhängt, unabhängig von der Zeit, die die Eindämmungs-, Untersuchungs- und Beseitigungsschritte der Reaktionsphase in Anspruch nehmen. Erst wenn es zu einem Vorfall kommt, macht das Unternehmen die bittere Erfahrung, dass die für die Reaktion eingeplante Zeit bei Weitem nicht ausreicht. Oder es verzichtet darauf und ist so gezwungen, mehrere Wiederherstellungsschritte zu unternehmen, von denen jeder die RTO-Zeit verlängert. Andernfalls ist eine sofortige Neuinfektion unvermeidbar. Der CIO und der CISO müssen zusammenarbeiten, um mit dem Vorstand und den Abteilungsleitern realistische Zielvorgaben für RTOs festzulegen, die sowohl die Reaktionszeit als auch die Wiederherstellungsdauer berücksichtigen.

Sicherheitskontrollen sind vielleicht nicht verfügbar

Der CISO hat ihre Funktionen möglicherweise vorwiegend auf Datendiebstahl ausgerichtet. Das Unternehmen geht vielleicht von der Verfügbarkeit von Kernfunktionen in den Bereichen IT, Sicherheit und Gebäuden aus, die nach einer Attacke wahrscheinlich nicht mehr funktionieren. In einem konkreten Fall wurden die Zugangskontrollsysteme gelöscht, sodass der physische Zugang zu Gebäuden und Räumen verhindert wurde, die für die Einleitung der Gegenmaßnahmen erforderlich waren. Auch die Voice-, IP- und E-Mail-Systeme waren betroffen, wodurch die Kommunikation mit Versicherungen, Geschäftspartnern, Aufsichtsbehörden, der Justiz und der Presse nicht mehr möglich war. (Die Presse musste Mitarbeiter des Unternehmens über LinkedIn kontaktieren, um herauszufinden, was los war. Dabei stellte sich heraus, dass die Mitarbeiter selbst nicht wussten, was vorgefallen war, da auch niemand mit ihnen kommunizieren konnte. Negative Presseberichte waren die Folge.)

BC/DR-Prioritäten konzentrieren sich oft zuerst auf kritische Unternehmensanwendungen, da sie vom IT-Betriebsteam in Zusammenarbeit mit den jeweiligen Abteilungen festgelegt werden, ohne das Sicherheitsteam einzubeziehen. Es ist jedoch von entscheidender Bedeutung, eine vertrauenswürdige Mindestreaktionsfähigkeit (Minimum Viable Response Capability, MVRC) wiederherzustellen, damit IT-Team und Sicherheitsabteilung mit internen und externen Partnern zusammenarbeiten können, um den Vorfall in den Griff zu bekommen.

Nach einem destruktiven Cyberangriff können Sicherheitskontrollen ausfallen

In fast jedem Regelwerk für die Reaktion auf Cybervorfälle, sei es der **SANS Institute Six Step Incident Response Lifecycle** oder der **NIST SP800-61r2 Computer Security Incident Handling Guide**, stellt die Eindämmungsphase einen entscheidenden Schritt dar, um die Ausbreitung von Angriffen, beispielsweise mit Ransomware oder Wiper-Malware, zu verhindern. Die Schwierigkeit liegt darin, dass wir für die Untersuchung, Beseitigung und Wiederherstellung auf den Zugang zum Endpoint angewiesen sind. Remote-Forensik-Imaging und Endpoint-Sicherheitskontrollen wie **End Point Detection and Response (EDR)** bzw. **eXtended Detection and Response (XDR)** gehören heutzutage zum festen Bestandteil jedes Sicherheitsarsenals.

Abbildung 2: *Eindämmung gehört zu den Best Practices bei der Reaktion auf Vorfälle, kann aber die Verwendung von Sicherheitstools behindern*

Sicherheitskontrollen sind unter Umständen nicht vertrauenswürdig

Das MITRE ATT&CK Framework, der De-facto-Standard für die Analyse des Verhaltens von Angreifern bei einem Cyberangriff, umfasst 14 Taktiken, die die einzelnen Schritte von Angreifern beschreiben. Die Taktik „Defense Evasion“ beschreibt die Möglichkeiten, mit denen Angreifer Sicherheitskontrollen umgehen können. ***Beachten Sie, dass diese spezielle Taktik 42 Techniken umfasst, mehr als jede andere***. Wenn Sie Ihre Backups nicht schützen und sich vollständig auf erkennungstechnische Sicherheitskontrollen auf Endpunkten verlassen, sind sie anfällig für Kompromittierungen. Das kann wiederum dazu führen, dass Unternehmen laufende Ransomware- und Wiper-Angriffe nicht erkennen und keine Wiederherstellung mehr durchführen können.

Zusammenfassend lässt sich sagen, dass viele Unternehmen als Reaktion auf einen destruktiven Cyberangriff den Einsatz des CIO-Teams mit traditionellen BC/DR-Prozessen und -Technologien planen, sofern das Backup selbst nicht angegriffen wurde. Das CIO-Team kann erst dann zur Wiederherstellung übergehen, wenn das CISO-Team den Vorfall untersucht und die erforderlichen Abhilfemaßnahmen bzw. das Risiko einer erneuten Infektion identifiziert hat. Dabei wird vom CISO-Team möglicherweise nicht bedacht, wie sich ein solcher Angriff auf seine Reaktionsfähigkeit auswirkt. In diesem Fall könnte es dann auf das CIO-Team angewiesen sein, um diese wiederherzustellen.

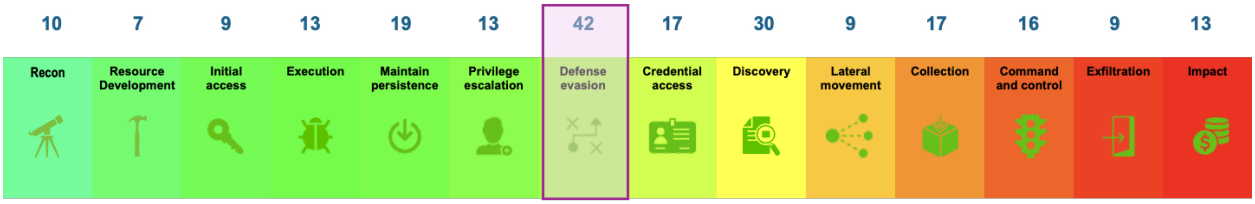

Abbildung 3: *Defence Evasion hat von allen 14 Taktiken die höchste Anzahl an ATTa-CK-Techniken*

Der Weg von der Cybersicherheit zur Cyber-Resilienz

Fast alle beauftragten Sicherheitsunternehmen, die täglich mit dieser Art von Vorfällen zu tun haben, wissen, dass der Schlüssel zur Minimierung des erreichbaren RTO bei destruktiven Cyberangriffen in der Einrichtung isolierter Reaktions- und Wiederherstellungsumgebungen liegt. Diese Unternehmen müssen im Chaos nach dem Vorfall mit dem Kunden zusammenarbeiten, um solche Umgebungen einzurichten. Sie sind unerlässlich, um die Systeme wieder zum Laufen zu bringen und die Erfolgschancen für einen erneuten Angriff zu minimieren.

Aufgrund ihrer Erfahrung mit traditionellen BC/DR-Szenarien bieten einige Datenmanagementanbieter isolierte Umgebungen an, die nur auf die Wiederherstellungsbedürfnisse des IT-Betriebsteams ausgerichtet sind. Sie vergessen dabei jedoch die eigentliche Beziehung zwischen Reaktion und Wiederherstellung, die für die Gewährleistung der Cyber-Resilienz erforderlich ist.

Wenn die Ursachen des Vorfalls nicht behoben werden, kann es zu erheblichen Verzögerungen bei der Wiederaufnahme der Produktion kommen, da die Systeme nach einem erneuten Angriff mehrfach wiederhergestellt werden müssen. Diese wiederholten Wiederherstellungen, die jeweils die dem Unternehmen versprochene RTO-Zeit in Anspruch nehmen, führen zu langwierigen Ausfällen, die weit über das hinausgehen, was beim Erstellen der Wiederherstellungspläne als tolerierbar erachtet wurde.

Cohesity ist der Ansicht, dass die Reaktionsanforderungen des Sicherheitsteams und des IT-Betriebsteams für die Minimierung der Auswirkungen gleich wichtig sind. Bei Ansätzen, die sich auf die schnelle Wiederherstellung von Systemen konzentrieren, ohne die Art des Angriffs zu ermitteln, werden weder die Angriffsfläche noch die Artefakte des Angriffs entfernt. Laufende Angriffe infizieren die wiederhergestellten Systeme innerhalb von Minuten erneut. Ransomware-Banden arbeiten zunehmend mit „Double Tap"-Angriffen, bei denen sie Unternehmen in einem „Doppelschlag" erneut angreifen, wenn sie sich weigern, Lösegeld zu zahlen. Diese Angreifer nutzen dabei dieselben Schwachstellen wie beim ersten Mal aus, um sich Zugang zu verschaffen, sofern diese nicht beseitigt wurden.

Cohesity hat eine zentrale Plattform mit Funktionen entwickelt, die beide Teams nutzen können, um die Effektivität und Effizienz der Reaktionen und Wiederherstellungsaufgaben zu verbessern.

Betreten Sie den Reinraum

Es gibt viele Definitionen für einen Reinraum (engl. Clean Room). Bei Cohesity definieren wir einen Reinraum als eine isolierte Umgebung, in der das Sicherheitsteam die notwendigen Untersuchungsschritte durchführen kann, um zu klären, wie es zu dem betreffenden Angriff kam. Die Definition eines zeitlichen Ablaufs für den Vorfall ermöglicht es, ein Manifest mit Gegenmaßnahmen für die Wiederherstellungsphase zu erarbeiten, um die Bedrohung zu beseitigen und einen erneuten Vorfall zu verhindern.

Der Reinraum unterliegt in der Regel der Verantwortung des Sicherheitsteams. In dieser Phase der Untersuchung werden die Systeme noch nicht wiederhergestellt. Sie werden isoliert untersucht, sodass Abhängigkeitsbeziehungen weitestgehend irrelevant sind. Die Isolation gewährleistet, dass als einwandfrei bekannte Sicherheitstools verwendet werden, um die bereits erwähnte Verteidigungsumgehung zu vermeiden. Dies verhindert, dass der Angreifer die Reaktionsmaßnahmen beobachten oder stören kann, und es besteht nicht mehr die Gefahr, dass bereits wiederhergestellte Rechner von Systemen innerhalb des Reinraums erneut infiziert werden.

Der Reinraum ist Teil einer Mindestreaktionsfähigkeit (Minimum Viable Response Capability, MVRC), die Cohesity innerhalb von Minuten einrichten kann, und von dieser abhängig. Der Aufbau einer vertrauenswürdigen, als einwandfrei bekannten Infrastruktur unterstützt die Zusammenarbeit, die Kommunikation und andere Arbeitsabläufe während des Reaktions- und Wiederherstellungsprozesses. Die Wiederherstellung von Sicherheitstools auf einen als einwandfrei bekannten Zustand in einer isolierten Umgebung hilft dem Unternehmen, den vielfältigen Umgehungstechniken der Angreifer auszuweichen.

Cohesity bietet darüber hinaus eine Reihe nativer Funktionen zur Unterstützung der Anforderungen des Sicherheitsteams im Reinraum an. Dank der Bedrohungssuche in **Cohesity DataHawk** können die Angriffsbekämpfer auf einen kuratierten Feed mit über 170.000 Gefährdungsindikatoren (Indicators of Compromise, IoCs) zugreifen, die von Ransomware-Akteuren im MITRE ATT&CK Framework verwendet werden. Dies hilft Unternehmen, die Techniken zu identifizieren, mit denen die Angreifer im Verlauf des Angriffs arbeiten.

Der kuratierte Feed kann durch eigene Threat Intelligence-Feeds des Kunden oder von Dritten bereitgestelltes Material ergänzt werden. Artefakte, die das Sicherheitsteam des Kunden während der forensischen Phase in den Systemen findet, können in Cohesity eingespeist werden, um nach weiteren betroffenen Systemen zu suchen. Diese Systeme können dann ebenfalls in die Untersuchung einbezogen werden.

Da die Bedrohungssuche mit Cohesity nicht von einem Endpoint-Agenten abhängt, ist sie nicht anfällig für Abwehrumgehungstechniken, die gegen XDR- und EDR-Systeme eingesetzt werden. Dieser Prozess erfolgt außerdem völlig passiv und kann von den Angreifern weder bemerkt noch gestört werden. Da die Bedrohungssuche mit Cohesity zudem durch das Backup unterstützt wird, funktioniert sie auch dann noch, wenn Unternehmen Hosts und Netzwerke zur Eindämmung isolieren. Außerdem ist die Aufbewahrungsfrist für Backups in vielen Unternehmen in der Regel länger als der Protokollierungszeitraum von Sicherheitslösungen. Das verschafft Unternehmen die Möglichkeit, Aktivitäten staatlicher Akteure aufzuspüren, die langsame Angriffe durchführen, wie z. B. vorbereitete Wiper-Attacken mit langer Verweilzeit.

In der Digitalforensik mussten sich die Ermittler bisher auf ein einzelnes, nach dem Vorfall aufgenommenes forensisches Bild stützen und Hypothesen darüber aufstellen, wie ein System in den jeweiligen Endzustand gelangt ist. Mit **Cohesity DataProtect** können forensische Ermittler jetzt eine Zeitreise durch den gesamten Vorfall unternehmen und in Sekundenschnelle Abbilder des Dateisystemstatus laden. Heutzutage können Ermittler mit ihren Tools Dateisysteme vergleichen, um schnell Abweichungen in Konfigurationen zu erkennen und Persistenzmechanismen und bösartige Benutzerkonten aufzuspüren. Außerdem können sie Binärdateien extrahieren, die in Sandboxen zur Detonation gebracht werden und so weitere IoCs erzeugen, die in die Bedrohungssuche von DataHawk eingespeist werden können.

Obwohl viele Unternehmen die rechtlichen Auswirkungen von Daten in ihren strukturierten Datenspeichern (z. B. Datenbanken) gut im Griff haben, verfügen die meisten über eine Fülle unstrukturierter Daten, zu denen auch regulierte und andere sensible Daten gehören. Es ist

bekanntermaßen schwierig, diese Daten zu überblicken, da sie unternehmensweit verstreut sein können und im Falle eines destruktiven Cyberangriffs womöglich verschlüsselt oder gelöscht werden. Die Datenklassifizierungsfunktion von Cohesity DataHawk nutzt fortschrittliche KI/ML-basierte Erkennungsverfahren, um diese verstreuten regulierten Daten direkt in den Backups zu lokalisieren und zu klassifizieren. Dies erleichtert die Einhaltung gesetzlicher Vorschriften zur Benachrichtigung der Aufsichtsbehörde und der betroffenen Personen über jede Kompromittierung vertraulicher Daten.

Cohesity hat die **Data Security Alliance** gegründet, um den Kontext der Daten eines Unternehmens in die bestehenden Tools des Sicherheitsteams zu integrieren. Im Zeitalter von Clouds, Containern und Hypervisoren – in denen sich Infrastrukturen in Sekundenschnelle instanziieren lassen – sind es die Daten, die nicht so leicht ersetzt werden können. Es sind auch die Daten, für die Compliance-Vorschriften gelten, und die der Angreifer letztendlich stehlen, verschlüsseln oder löschen möchte. Cohesity baut kontinuierlich Beziehungen zu führenden Sicherheitsanbietern wie Palo Alto Networks, Cisco, CrowdStrike, ServiceNow, Tenable, Qualys, BigID, Okta, Securonix, CyberArk und Zscaler sowie zu Unternehmen mit Erfahrung in der Erbringung sicherheitsbezogener Profesional Services wie Mandiant und TCS auf. Dadurch ist Cohesity führend bei der Entwicklung von Innovationen, die die Reaktion auf Cyberangriffe und die Wiederherstellung von Daten durch den Datenkontext revolutionieren, und hilft Unternehmen, ihre bestehenden Ausgaben für Cybersicherheit besser einzusetzen.

Die Bedeutung von Staging

Ein Staging Room ist eine Wiederherstellungsumgebung, für die in der Regel das IT-Betriebsteam verantwortlich ist. Darin werden Systeme entweder schnell aus als einwandfrei bekannten Quellen neu aufgebaut oder aber wiederhergestellt und bereinigt. Dort werden auch die vom Sicherheitsteam vorgegebenen Schritte zur Bedrohungsabwehr durchgeführt. Außerdem werden im Staging Room die Abhängigkeitsbeziehungen zwischen den einzelnen Hosts berücksichtigt, bevor die wiederherzustellenden Funktionen getestet werden. So wird gewährleistet, dass die Maßnahmen zur Wiederherstellung und Schadensbegrenzung keine Probleme in der Produktionsumgebung verursachen. Von den reparierten Systemen werden dann ein letztes Mal Backups angefertigt, um eine Ausgangsbasis für den Fall zu schaffen, dass etwas übersehen wurde, und nicht wieder bei Null anfangen zu müssen.

Cohesity SmartFiles bietet die Möglichkeit, als einwandfrei bekannte Installationen auf unveränderlichen Medien zu speichern, um sicherzustellen, dass sie für Angreifer unzugänglich sind. Diese können dann schnell auf Windows- und Linux-Systemen gemountet werden, sodass IT-Orchestrierungs- oder Skripting-Tools die Systeme wiederherstellen können. Golden-Master-Kopien von Systemen lassen sich mit Cohesity DataProtect sichern und klonen. Auf diese Weise können Konfigurationen und Daten aus Snapshots entsprechend der Untersuchungsergebnisse des Sicherheitsteams über die gesamte Zeitachse hinweg wiederhergestellt werden.

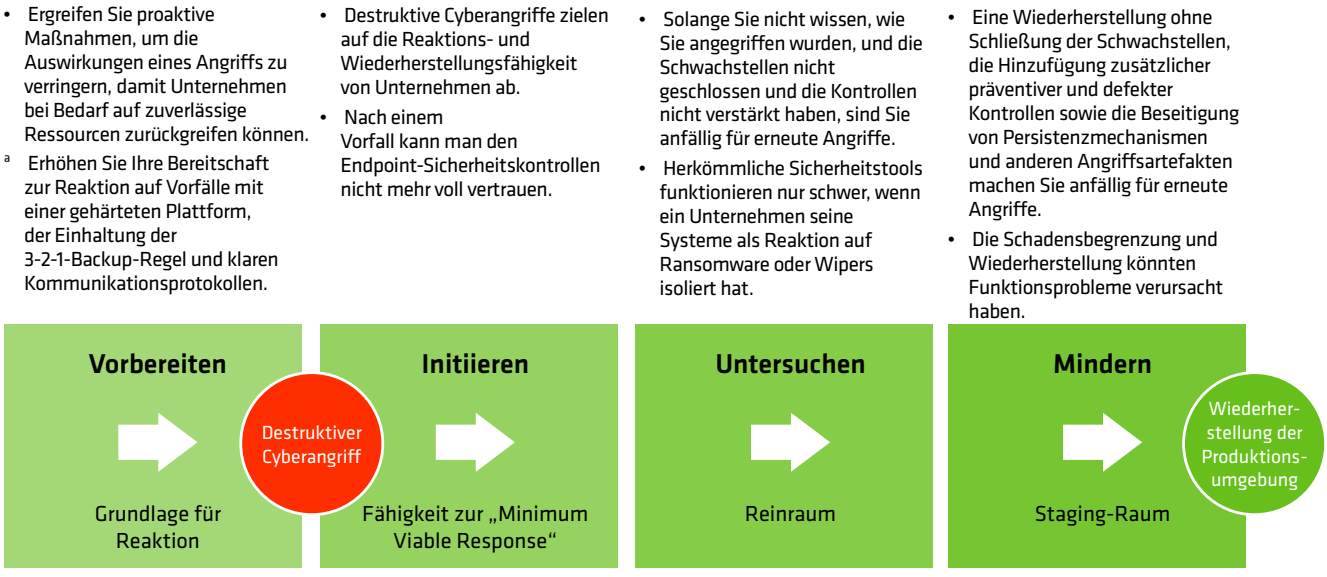

Abbildung 4: *Zeitachse des Vorfalls, die den Verlauf vom Angriff bis zur Wiederherstellung zeigt*

Zusammenführung von IT und Sicherheit für mehr Cyber-Resilienz

Die Zusammenführung der vom Sicherheits- und IT-Betriebsteam verwendeten Reaktions- bzw. Recovery-Prozesse, Teams und Technologien ist der Schlüssel zur Stärkung der Cyber-Resilienz. Eine isolierte Betrachtung dieser Funktionen führt nur zu größeren Schäden, wenn es zu einem Cybervorfall kommt.

Der Ansatz von Cohesity, eine zentrale Plattform für beide Teams zur Verfügung zu stellen, beschleunigt die Reaktionsmaßnahmen des Sicherheitsteams bei gleichzeitiger Integration mit bestehenden Sicherheitstools. Dies steigert die Effizienz und Effektivität sowohl der Reaktion als auch der Wiederherstellung, stärkt die Resilienz und reduziert die Auswirkungen.

So nutzen Sie einen Clean Room für die Vorfallsreaktion

Zahlreiche Unternehmen verfügen nicht über die geeignete Umgebung, um Vorfälle schnell zu untersuchen und sicherzustellen, dass die Systeme bei der Wiederherstellung ihrer Daten nicht erneut infiziert werden.

Sehen Sie sich unser On-Demand-Webinar an und erhalten Sie praktische Details für die Entwicklung einer Strategie zur Vorfallsreaktion, um die Bereitschaft und Reaktionsfähigkeit Ihres Unternehmens zu stärken, ohne weitere Risiken einzugehen.

Webinar ansehen

Das Cohesity Destructive Cyberattack Resilience Maturity Model

In diesem Whitepaper werden mehrere bewährte Konzepte zur Verbesserung der Cyber-Resilienz behandelt. Der nächste logische Schritt besteht darin, die eigene Resilienz zu bewerten und herauszufinden, wie (und wo) Sie sich verbessern können.

Zu diesem Zweck stellen wir Ihnen das **Cohesity Destructive Cyberattack Resilience Maturity Model** vor.

Dieses Reifegradmodell soll Unternehmen dabei helfen, ihre Widerstandsfähigkeit gegenüber destruktiven Cyberangriffen wie Ransomware- und Wiper-Angriffen zu verbessern. Das Modell setzt klare Maßstäbe und bietet eine strukturierte Roadmap, die Unternehmen beim Erreichen effektiver und effizienter Abläufe unterstützt, die gegen Cyberangriffe gewappnet sind.

Das Cohesity-Modell ist auf die gängigsten Frameworks zur Cybersecurity-Reaktion und -Wiederherstellung abgestimmt, z. B. den SANS Institute 6 Step Incident Response Process, das RE&CT Framework, MITRE D3FEND und den NIST SP800-61 Computer Security Incident Handling Guide. So können Unternehmen branchenweite Best Practices übernehmen.

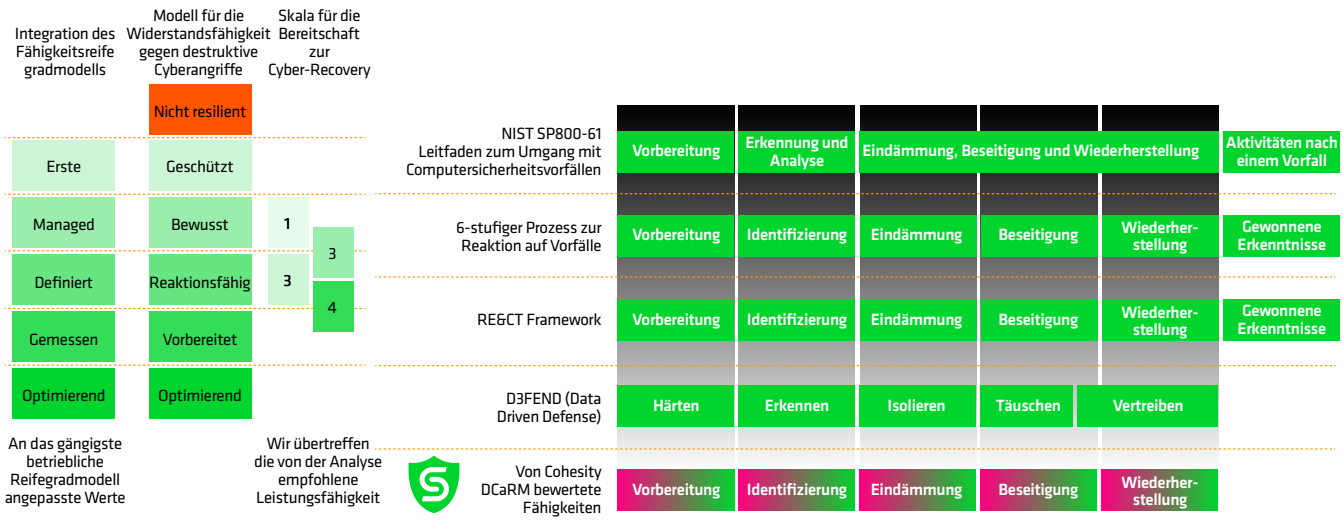

Abbildung 5: *Anhaltspunkte für die Anpassung des Cohesity Destructive Cyberattack Resilience Maturity Model an gängige Reaktions- und Wiederherstellungs-Frameworks*

Das Reifegradmodell ermöglicht es Unternehmen, ihre operativen Fähigkeiten in den fünf Stufen zu bewerten, die für die Cyber-Resilienz erforderlich sind:

1. Vorbereitung auf einen Vorfall
2. Identifizierung und Untersuchung des Angriffs
3. Eindämmung der Verbreitung des Angriffs
4. Beseitigung von Bedrohungen und Verringerung der Angriffsfläche, um künftige Angriffe zu verhindern
5. Wiederherstellung eines sicheren Systemzustands

Die Reifegrade des Modells sind in der nachstehenden Tabelle dargestellt:

Reifegrad	Beschreibung
Nicht resilient	Das Unternehmen verfügt über keine ausreichende Resilienz, um einem destruktiven Cyberangriff standzuhalten, ohne dass die Bereitstellung seiner Produkte und Services wesentlich beeinträchtigt wird.
Wiederherstellbar	Das Unternehmen hat Disaster-Recovery- und Business-Continuity-Funktionen aufgebaut, die jedoch möglicherweise von Angreifern attackiert werden; es fehlen angemessene Untersuchungs- und Bereinigungsphasen, um eine erneute Infektion oder einen erneuten Angriff zu verhindern.
Verstärkt	Das Unternehmen hat seine Fähigkeiten gestärkt, eine Wiederherstellung nach Angriffen durchzuführen.
Bewusst	Das Unternehmen ist in der Lage, die frühen Stufen eines destruktiven Cyberangriffs aufzudecken, der nicht vermieden werden kann und von der Eindämmungsphase der Vorfallsreaktion nicht betroffen ist. Es wurde ein Modell der geteilten Verantwortung zwischen dem IT- und Sicherheitsteam entwickelt, um mit Vorfällen umzugehen.
Reaktionsfähig	Das Unternehmen ist in der Lage, die Tools wiederherzustellen, die für die Vorfallsreaktion und die Kommunikation mit Stakeholdern erforderlich sind; es verfügt über isolierte Umgebungen, die die Untersuchung von Vorfällen, die Beseitigung von Bedrohungen und die Durchführung von Systemtests vor der Wiederherstellung in der Produktionsumgebung ermöglichen. Das Unternehmen treibt kontinuierliche Verbesserungen voran, indem es End-to-End-Übungen für verschiedene Angriffssituationen durchführt, das Reaktionsvermögen der Mitarbeiter für künftige Vorfälle schult, Prozesse optimiert und nach Möglichkeiten zur Automatisierung sucht, um Effektivität und Effizienz zu steigern. Des Weiteren ist das Unternehmen im Falle eines Angriffs in der Lage, die Infrastruktur und Ressourcen, die für die Handhabung und Reaktion auf den Vorfall erforderlich sind, schnell wiederherzustellen.
Optimierend	Das Unternehmen verfügt über Kennzahlen und Telemetrie, um die kontinuierliche Optimierung von Prozessen, Mitarbeitern und Technologie voranzutreiben. Die proaktive Erkennung und Klassifizierung von Daten gewährleistet eine End-to-End-Governance und die regulatorische Compliance. Das Unternehmen verfügt über die Fähigkeit, nicht nur Systeme wiederherzustellen, sondern auch die Infrastruktur schnell wieder in einen vertrauenswürdigen Zustand zu versetzen. Die Untersuchung von Vorfällen, der Wiederaufbau der Infrastruktur und die Datenwiederherstellung sind optimiert, sodass diese Aufgaben parallel durchgeführt werden können.

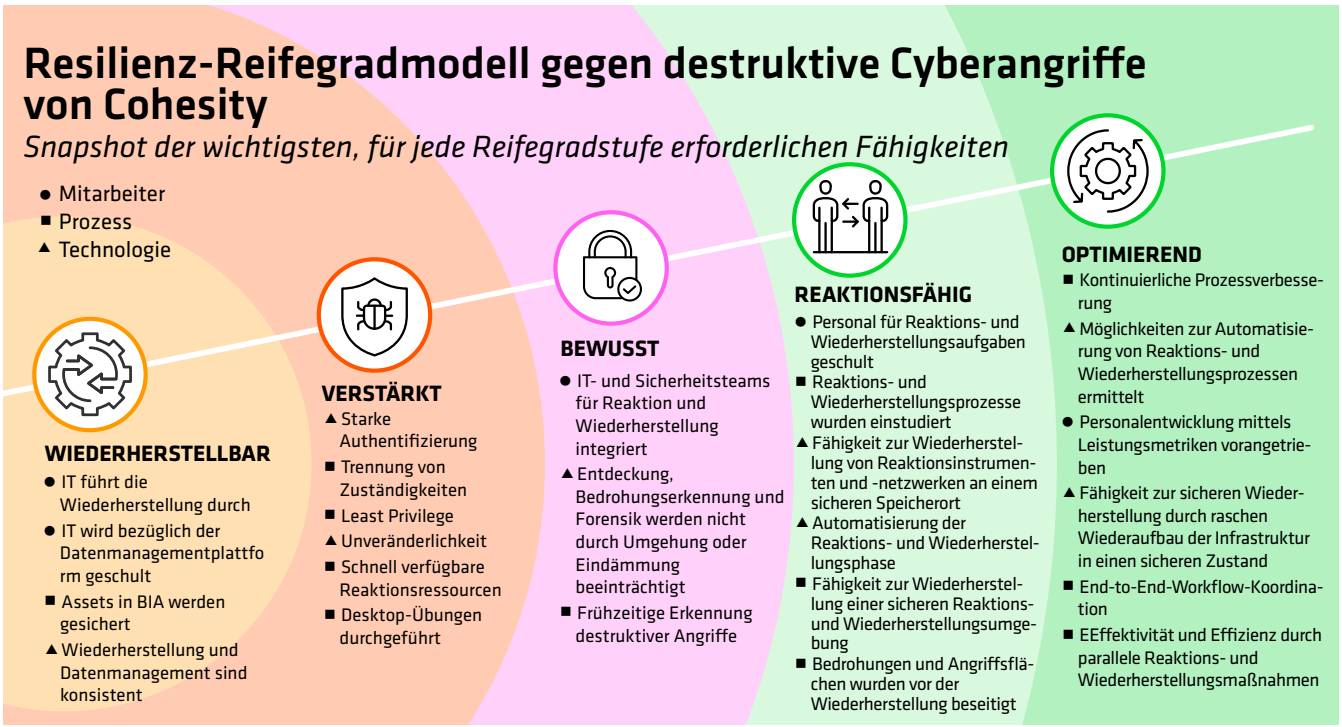

Abbildung 6: *Snapshot der wichtigsten Fähigkeiten für die jeweilige Reifegradstufe des Cohesity Destructive Cyberattack Resilience Maturity Model*

Das Cohesity Destructive Cyberattack Resilience Maturity Model bietet eine herstellerunabhängige Roadmap. Dieser Ansatz ermöglicht es seinen Anwendern, sich an einem Best-Practice-Framework für Reaktionen und Wiederherstellungen zu orientieren, dabei Cyber-Resilienz zu erreichen sowie Governance, Mitarbeiter und Prozesse auf angemessenem Niveau zu entwickeln. Die Roadmap sorgt dafür, dass die Technologie die Betriebsergebnisse unterstützt und optimiert, anstatt sie zu steuern.

Werfen wir einen genaueren Blick auf die Reifegrade:

- **Wiederherstellbar**: Ein Unternehmen, das sich auf dieser Stufe befindet, verfügt über ein ausgereiftes Niveau der Notfallwiederherstellung und Business Continuity. Es hat angemessene Business-Impact-Bewertungen durchgeführt, um kritische Dienste und deren unterstützende Infrastruktur zu ermitteln, und Recovery Point Objectives und Recovery Time Objectives (RPO/RTO) festgelegt. Dem Unternehmen fehlen allerdings die erforderlichen Schutzmaßnahmen auf seiner Datenmanagementplattform, um sie vor Angreifern zu schützen. Es behandelt destruktive Cybervorfälle in der Regel wie herkömmliche Disaster-Recovery- und Business-Continuity-Szenarien, ohne die komplizierenden Faktoren von Cyberangriffen zu berücksichtigen. Bei diesem Reifegrad mangelt es außerdem an einer engen Zusammenarbeit zwischen IT und Sicherheit zur Bewältigung von Cybervorfällen.
- **Verstärkt**: Bei diesem Reifegrad hat das Unternehmen anerkannt, dass es früher oder später angegriffen wird. Es hat Schutzmaßnahmen ergriffen, um die unvermeidlichen Auswirkungen zu mildern. Des Weiteren hat es beispielsweise folgende Sicherheitsprinzipien implementiert: Least Privilege Access, Unveränderlichkeit (um das böswillige Ändern oder Löschen von Backups zu verhindern), Aufgabentrennung (um zu verhindern, dass ein abtrünniger oder kompromittierter Administrator schädliche Änderungen vornimmt) und Vaulting (um die Fähigkeit zur Wiederherstellung außerhalb der Reichweite des Angreifers zu stellen). Vaulting hilft dem Unternehmen auch bei der Einhaltung von sicheren Backup-Konventionen wie dem 3-2-1-Prinzip.
- **Bewusst**: Ein Unternehmen auf dieser Stufe hat ein klar definiertes Modell der geteilten Verantwortung von IT und SecOps eingeführt. Es ist in der Lage, Bedrohungen aufzudecken und digitale Forensik durchzuführen, selbst wenn Angreifer die Sicherheitssysteme der Endgeräte umgehen. Außerdem kann das Unternehmen die Bedrohungssuche während der Eindämmung fortsetzen, wenn Hosts und Netzwerke isoliert sind. Es werden zwar Threat Feeds verwendet, aber sie sind oft veraltet und enthalten keine regelmäßigen Updates, um die neuesten bestätigten Bedrohungen durch Ransomware-as-a-Service-Plattformen und Schwachstellen zu berücksichtigen. Darüber hinaus fehlt dem Unternehmen

ein Defence-in-Depth-Modell, mit dem es die frühen Phasen eines Angriffs aufdecken kann, bevor die Systeme beeinträchtigt werden.

- **Reaktionsfähig**: Bei diesem Reifegrad ergreifen Unternehmen die notwendigen Schritte zur Untersuchung von Vorfällen und zur Beseitigung von Bedrohungen, bevor sie die Systeme wieder in Betrieb nehmen, um eine erneute Attacke oder eine Neuinfektion durch denselben Angreifer zu verhindern. Isolierte Umgebungen für die Untersuchung und Problembehebung sind vorhanden, um die Eindämmungsanforderungen zu erfüllen. Außerdem werden bei diesem Reifegrad kontinuierliche Verbesserungen und Übungen eingeführt, damit die Prozesse, Mitarbeiter und Technologien, die für die Reaktion und sichere Wiederherstellung nach einem Vorfall erforderlich sind, für den Ernstfall einsatzbereit sind. (Ihre SOC-Analysten, Incident-Responder und leitenden Angestellten dürfen nicht zum ersten Mal einen Ransomware- oder Wiper-Angriff erleben, bei dem Ihre Daten von Ransomware verschlüsselt werden oder alle Systeme im Unternehmen gelöscht werden. Tabletop-Übungen sind nützlich, aber sie testen nicht die End-to-End-Workflows, -Fähigkeiten und -Technologien, die in einem realen Szenario erforderlich sind).

Das Unternehmen führt auch realistische Angriffsszenarien durch, die alle für die Cyber-Resilienz erforderlichen Komponenten vorbereiten. Kein Vorfall gleicht dem anderen, wodurch ein Unternehmen mit variierenden Übungsaspekten besser in der Lage ist, Prozesse zu optimieren. Das Unternehmen sucht regelmäßig nach Möglichkeiten zur Automatisierung und trainiert das Reaktionsvermögen der Mitarbeitenden.

Schließlich können Unternehmen in dieser Phase schnell das Vertrauen in ihre Netzwerke und Sicherheitstools wiederherstellen und haben innerhalb weniger Minuten weitere Ressourcen zur Verfügung, um mit ihren Reaktionsmaßnahmen zu beginnen. Sie haben zuverlässige Methoden für die Reaktion, Kommunikation und Untersuchung im Rahmen eines Angriffs in einem Worst-Case-Szenario. Anders ausgedrückt: Sie sind auf Szenarien vorbereitet, in denen Sicherheitskontrollen umgangen werden, Türzugangssysteme ausfallen und es keine CMDB, Ticketingsysteme, E-Mail oder Voice-over-IP gibt, um mit Strafverfolgungsbehörden, Cyber-Versicherern, der Presse, Aufsichtsbehörden oder betroffenen Personen zu sprechen.

- **Optimierend**: Diese Stufe ist die Spitze der Cyber-Resilienz. Das Unternehmen hat proaktive Maßnahmen für die Erkennung und Klassifizierung ergriffen. Somit ist es in der Lage, seine Daten wiederherzustellen und es hat während ihres gesamten Lebenszyklus angemessene Maßnahmen zum Risikomanagement getroffen. Die Workflows werden so optimiert, dass sie mit den gesetzlichen Vorschriften und den Benachrichtigungsverpflichtungen an betroffene Personen übereinstimmen. Dadurch werden Bußgelder vermieden und das Unternehmen hält die Vorschriften von DORA, NIS 2, HIPAA, der Prudential Regulatory Authority und der Security and Exchange Commission ein. Während beim Reifegrad „Reaktionsfähig“ noch nach Möglichkeiten zur Automatisierung von Workflows gesucht wird, geht es beim Grad „Optimierend“ um die übergreifende Steuerung, Orchestrierung und Verwaltung des gesamten End-to-End-Prozesses für Reaktionen und Wiederherstellungen. Dieser Reifegrad gibt leitenden Angestellten, Vorständen und externen Stakeholdern die Gewissheit, dass das Unternehmen in Sachen Cyber-Resilienz an vorderster Front steht.

Die Vorbereitung auf Cyberangriffe und deren Handhabung haben dafür gesorgt, dass solch ein Modell betriebskritisch ist. Diese Angriffe stellen heute die größte Bedrohung für die Bereitstellung von Produkten und Services durch Unternehmen dar. Experten und in der Praxis tätige Fachleute für Cybersicherheit mit jahrzehntelanger Erfahrung in der Reaktion auf Cybervorfälle und der Wiederherstellung von Daten haben dieses Modell entwickelt. Damit kann ein Unternehmen wie Ihres seine aktuellen Fähigkeiten verstehen, seinen Reifegrad mit dem anderer Unternehmen in der Branche oder Ihrer Region vergleichen und eine messbare Roadmap für künftige Verbesserungen erstellen.

Über den Autor

James Blake verfügt über mehr als drei Jahrzehnte operativer Erfahrung in der Abwehr von Cybervorfällen und hat End-to-End-Sicherheitsfunktionen für mehr als 30 Fortune-/FTSE 100-Unternehmen aufgebaut. Er war auch an der Aufarbeitung der Folgen hunderter großer Vorfälle beteiligt, darunter mehrere staatliche Wiper-Attacken und Dutzende von Ransomware-Angriffen. Er ist Head of Global Cyber Resiliency Strategy bei Cohesity.

Erfahren Sie mehr auf Cohesity.com

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000059-002 DE 4-2025