eBOOK

Leitfaden zur Cyber-Bereitschaft und Recovery-Fähigkeit

ERFAHREN SIE, WIE IHR UNTERNEHMEN RESILIENT WIRD UND BLEIBT

Commvault®

INHALT

Die Sicherheits-, IT- und Operations-Teams vieler Unternehmen unterscheiden nicht zwischen Cyber Recovery und Disaster Recovery. Während des Cyber Recovery-Prozesses nach aktuellen Vorfällen haben sich jedoch im Vergleich zu einer herkömmlichen Disaster Recovery einige spezielle Schwierigkeiten ergeben. Die unterschiedlichen Taktiken, Techniken und Vorgehensweisen der Angreifer haben gezeigt, dass bei Cyber Recovery-Plänen folgendes berücksichtigt werden muss:

- **Unvorhersehbarkeit und sich ständig weiterentwickelnde Bedrohungen:** Im Gegensatz zu Naturkatastrophen sind Cyberangriffe arglistig und Angreifer bemühen sich sehr, ihre Handlungen und Bewegungen zu verschleiern. Aus diesem Grund kann es schwierig sein, festzustellen, wann genau der Angriff begonnen hat, welche Systeme betroffen sind oder wie hoch der Schaden ist..
- **Sekundäre Angriffe:** In einigen Fällen haben Angreifer während des Wiederherstellungsprozesses Codes zum Starten sekundärer Angriffe oder zum Erstellen dauerhafter Backdoors eingeschleust, die bei einer Wiederherstellungsaktion automatisch geöffnet werden.
- **Kompromittierte Backups:** Oft haben es Angreifer gezielt auf Backups abgesehen, um sicherzustellen, dass Wiederherstellungsversuche wirkungslos bleiben. Das steigert die Notwendigkeit, ein Lösegeld zu zahlen, um Betriebsdaten wiederherzustellen.
- **Zeitdruck:** Unternehmen stehen oft unter einem enormen Druck, nach einem Cyberangriff schnell wieder online zu gehen. Ausfallzeiten kosten ein Unternehmen nachweislich bis zu $14 056 pro Minute. Und zu allem Übel kann eine rasche Wiederherstellung dazu führen, dass bereits kompromittierte Systeme wiederhergestellt werden und den Schaden noch verstärken.
- **Ressourcenabfluss:** Cyber Recovery kann ein ressourcenintensiver Prozess sein, der die Expertise von IT-, Sicherheits- sowie Rechtsabteilungen und manchmal sogar der Strafverfolgungsbehörden erfordert. Dies kann ohnehin knappe Ressourcen in einem Unternehmen belasten und Sicherheits- und Operations-Teams von anderen möglichen Cyberbedrohungen ablenken.

Indem Unternehmen ein Verständnis für diese Herausforderungen entwickeln, können sie einige grundlegende Elemente der Disaster Recovery nutzen, um einen Cyber Recovery-Plan zu erstellen, der diese Schwierigkeiten antizipiert und ihnen hilft, nach einem Angriff schneller wieder auf die Beine zu kommen.

Dieser Leitfaden hilft Ihnen dabei, die Basis dafür zu legen, Ihr Unternehmen cyber-resilient zu machen. Wir geben Ihnen, unter Berücksichtigung einiger der gängigsten Richtlinien, Konzepte, Ideen und Prozesse an die Hand, die Sie für die Entwicklung Ihres eigenen Plans benötigen.

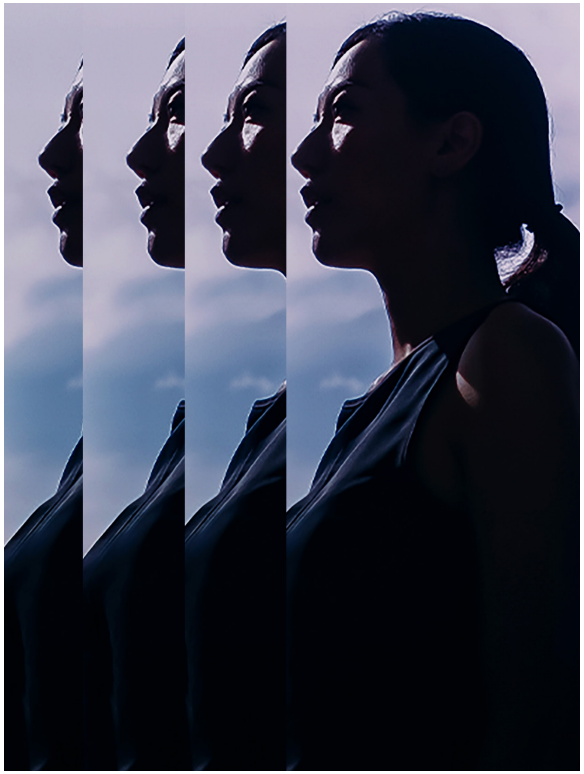
[1] Enterprise Management Associates, "IT outages: 2024 costs and containment," Valerie O'Connell, Research Director, April 2024.

DAS NIST CYBER SECURITY FRAMEWORK ALS WEGWEISER

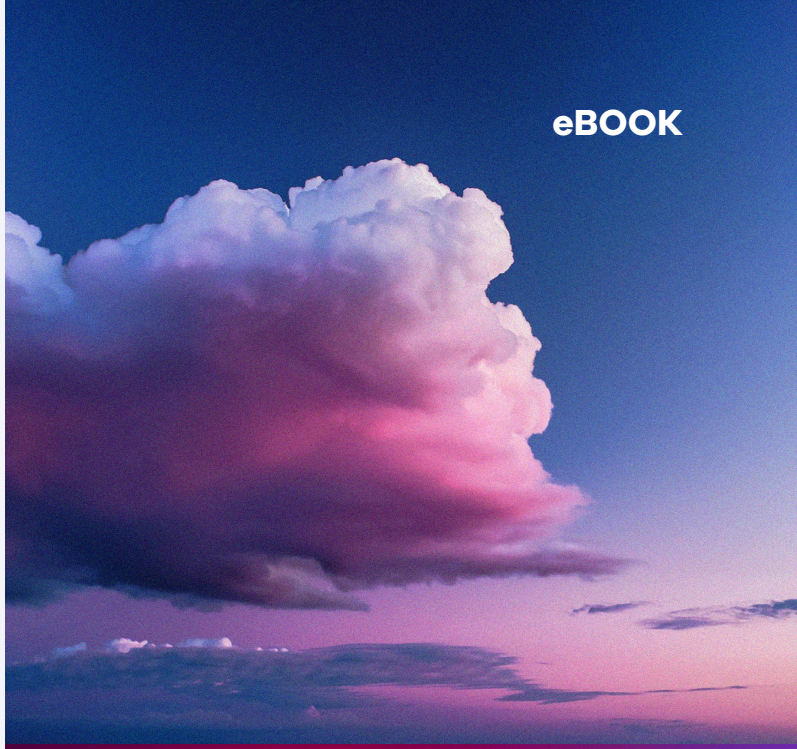
Das Cyber Security Framework des National Institute of Standards and Technology (NIST CSF) ist seit langem ein Wegweiser für Sicherheitsteams zur Entwicklung und Ausrichtung ihrer Sicherheitsprogramme und zum Schutz vor neuen und sich weiterentwickelnden Cyberbedrohungen

Anhand der Kategorien Identifizieren, Erkennen, Schützen, Reagieren und Wiederherstellen, wird erklärt, wie man jeden Bereich für eine erfolgreiche Cyber Recovery weiter ausbaut.

1. **Identifizieren.** Analysieren Sie Ihre Daten, auch sensible/kritische Daten, und finden Sie heraus, wo sie sich befinden und wer dafür verantwortlich ist.
2. **Erkennen.** Nutzen Sie Sicherheitsfunktionen und -technologien, um zu überwachen, was mit Ihrer Umgebung und Ihren Daten geschieht.
3. **Schützen.** Implementieren Sie Mechanismen, um Ihre sensiblen oder kritischen Daten zu sichern und sie für die Wiederherstellung vorzubereiten.
4. **Reagieren.** Entfernen Sie den Angreifer aus Ihrer Umgebung, und entfernen oder schützen Sie den Angriffsvektor, über den Ihr Unternehmen infiltriert wurde. Wenn sich das nicht schnell erledigen lässt, bereiten Sie eine neue, intakte und nicht kompromittierte Arbeitsumgebung für die Wiederherstellung vor, die zur Fortsetzung des Geschäftsbetriebs verwendet werden kann.
5. **Recover.** Erstellen Sie eine nicht kompromittierte Version Ihrer gesamten Umgebung, einschließlich aller Daten, Anwendungen und der Infrastruktur.



VORBEREITUNG AUF DAS UNVORSEHBARE



Cyber-Vorfälle sind naturgemäß oft versteckte Angriffe, die Tage oder Wochen hinter den Kulissen vorbereitet werden, bevor es zu verheerenden Schäden kommt.

> ## 194 Tage, oder mehr als sechs Monate beträgt
>
> **die durchschnittliche Verweildauer–die Zeit, die ein Angreifer während eines Angriffs tatsächlich innerhalb eines Unternehmens verbringt**[1]

Unternehmen führen seit langem Penetrationstests durch, um Bereiche mit schwacher Abwehr zu identifizieren sowie Tabletop-Übungen, um die Disaster Recovery-Fähigkeit zu testen. Doch angesichts der Vielfalt an Cyberangriffen, ist in der Praxis zu berücksichtigen, dass in einem echten Cyber Recovery-Szenario nahezu nichts als vertrauenswürdig gilt.

Backups müssen auf permanente Malware gescannt werden. Die Infrastruktur muss bereinigt werden, um sicherzustellen, dass nur autorisierte Benutzer anwesend sind. Und Anwendungen und Daten müssen auf Backdoors überprüft und in einen Zustand vor dem Angriff (oder vor der Infiltration) versetzt werden.

[1] Cost of a Data Breach Report 2024, IBM.

MINIMALE FUNKTIONS-FÄHIGKEIT: DER ERSTE SCHRITT ZUR WIEDERHERSTELLUNG NACH EINEM CYBERANGRIFF

Sobald Ihr Unternehmen von einem Cyberangriff getroffen wurde, ist der Druck enorm hoch, so schnell wie möglich wieder zum normalen Betrieb zurückzukehren. Der beste Weg, um die Geschäftstätigkeit schnell wieder aufzunehmen? Stellen Sie zumindest die minimale Funktionsfähigkeit wieder her – die kritischsten Anlagen, die Sie benötigen, um den kontinuierlichen Betrieb aufrechtzuerhalten. Auf diese Weise können Sie die wichtigsten Tätigkeiten Ihres Unternehmens weiterführen, während eine vollständige Wiederherstellung durchgeführt wird.

Sobald Sie Ihre kritischsten Systeme, Prozesse und Daten identifiziert haben, die es Ihnen ermöglichen, die minimale Funktionsfähigkeit wiederherzustellen, müssen Sie einen Plan erstellen, wie Sie diese im Falle eines Vorfalls wiederherstellen werden. Sie müssen den Ausfall von Downtime verstehen und Ihren Plan regelmäßig testen und aktualisieren.

Lesen Sie Das ultimative Handbuch zur minimalen Funktionsfähigkeit um mehr über die Schritte zur Wiederherstellung Ihrer Geschäftstätigkeiten und unsere empfohlenen Praktiken zu erfahren.

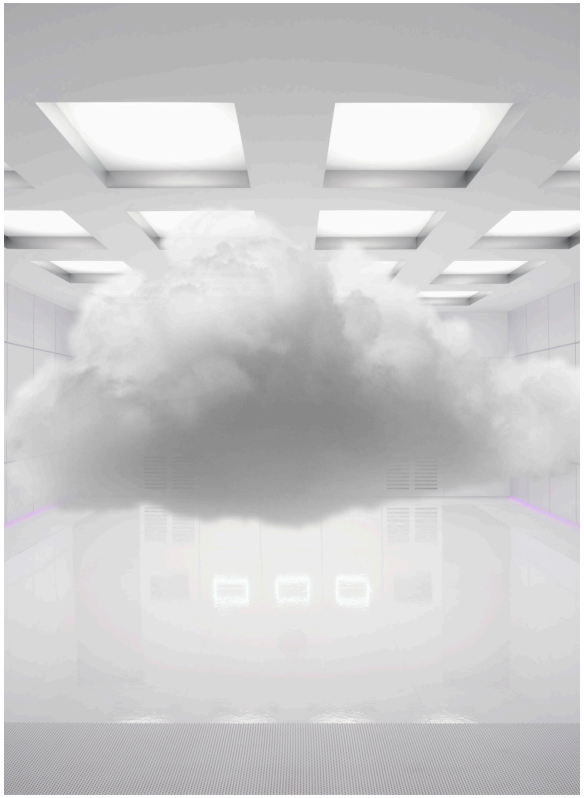
DIE SCHNELLSTE UND VOLLSTÄNDIGSTE WIEDERHERSTELLUNG NACH EINEM CYBERANGRIFF

Commvault bietet Lösungen, um Ihre Daten, Anwendungen und Workloads zu schützen, zu testen und wiederherzustellen – und bietet so eine umfassende Wiederherstellung und echte Cybersicherheit.

Commvault® Cloud Cleanroom™ Recovery ermöglicht es Ihnen, in einer sicheren, on-demand, cloudbasierten Umgebung zu testen und wiederherzustellen. Sie können Anwendungen und Daten einfach wiederherstellen und die Forensik nach einem Vorfall durchführen. Sie verfügen über eine isolierte Wiederherstellungsumgebung für die Geschäftskontinuität im Falle eines Angriffs.

Commvault Cloud Rewind™ ermöglicht eine nahezu sofortige Wiederherstellung und schreibt automatisch Codes, um Daten wiederherzustellen und Anwendungen neu aufzubauen, sodass Sie innerhalb von Minuten nach einem Ausfall wieder im Geschäft sind – alles ohne manuelle Eingriffe.

Commvault Cloud for Active Directory Enterprise Edition bietet eine schnelle Wiederherstellung für AD- und Entra ID-Umgebungen. Es hilft bei der Automatisierung und Orchestrierung der Wiederherstellung von AD-Umgebungen nach einem Vorfall, sodass Sie schnell wieder die minimale Funktionsfähigkeit erreichen können.



eBOOK

Eine Gewissheit in Sachen Cybersicherheit: Böswillige Akteure werden weiterhin versuchen, Schwachstellen zu finden. Bleiben Sie ihnen einen Schritt voraus mit einem gut durchdachten Wiederherstellungsplan und einer Strategie, **um Ihre Daten zu schützen und den kontinuierlichen Betrieb trotz Bedrohungen aufrechtzuerhalten.**

Learn more: **www.commvault.com/de/minimum-viability**

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®