MEDIALINE

Cyber Recovery as a Service by Medialine (CRaaS)

Ermöglicht schnelle Wieder-herstellung und Nutzung Ihrer IT-Infrastruktur nach einem erfolgreichen Ransomware-Angriff

MEDIALINE GROUP

1. Einführung

In einer zunehmend digitalen Welt sind Unternehmen mehr denn je auf ihre IT-Infrastruktur angewiesen. Doch mit der Digitalisierung wächst auch die Bedrohung durch Cyberkriminalität. Ransomware-Angriffe sind heute eine der größten Gefahren für die Geschäftskontinuität. Diese Angriffe können innerhalb von Minuten ganze Unternehmen lahmlegen, indem sie kritische IT-Systeme verschlüsseln und den Zugang zu wichtigen Daten und Anwendungen verhindern. In solchen Momenten zählt jede Minute – es geht nicht nur um den Schutz von Daten, sondern um die Existenz des gesamten Unternehmens.

Viele Unternehmen verlassen sich auf herkömmliche Backup- und Recovery-Lösungen, die in die Cloud ausgelagert sind. Diese Lösungen sind jedoch stark von einer stabilen Internetverbindung abhängig, was in Krisensituationen zu erheblichen Verzögerungen führen kann, wenn diese Verbindung gestört ist. Darüber hinaus kann die Wiederinbetriebnahme in der Cloud kompliziert sein, insbesondere wenn die lokale IT-Infrastruktur beschädigt ist. Es besteht das Risiko, dass auch Cloud-Backups durch Cyberangriffe kompromittiert werden. Ohne eine zuverlässige, sofort einsatzbereite Hardware vor Ort ist ein lokaler Betriebsstillstand so gut wie unausweichlich.

In Krisenzeiten, in denen Emotionen hochkochen und der Druck enorm ist, ist es riskant, auf die kurzfristige Beschaffung und Einrichtung von Hardware zu setzen. Der Aufbau eines Notbetriebs, der effektiv und sinnvoll ist, lässt sich nicht innerhalb weniger Tage improvisieren. An diesem Punkt sind die CIOs und die Geschäftsführung gleichermaßen gefordert. Es ist ihre gemeinsame Verantwortung, sicherzustellen, dass das Unternehmen auf solche Krisenszenarien vorbereitet ist, um handlungsfähig zu bleiben.

Cyber Recovery as a Service (CRaaS) bietet die Lösung, die Unternehmen benötigen, um in solchen extremen Situationen zu bestehen. CRaaS stellt sicher, dass Ihre IT-Infrastruktur innerhalb kürzester Zeit wieder voll funktionsfähig ist, selbst wenn Ihre primären Systeme durch Ransomware-Angriffe kompromittiert wurden. Mit CRaaS sind Sie nicht nur vorbereitet – Sie sind geschützt.

2. Cyber Recovery as a Service by Medialine im Detail

Vorbereitung auf den Ernstfall

Ein erfolgreicher Wiederherstellungsprozess im Falle eines Ransomware-Angriffs beginnt lange vor dem eigentlichen Vorfall. Der Schlüssel liegt in der sorgfältigen Planung und Vorbereitung. CRaaS ist kein reaktiver Ansatz, sondern ein proaktiver Service, der darauf abzielt, jede mögliche Variable zu berücksichtigen, bevor ein Angriff überhaupt stattfindet.

Sizing und Implementierung

Der Erfolg von CRaaS hängt maßgeblich von einer genauen Planung und Implementierung ab. Vor der eigentlichen Implementierung des Services führen wir gemeinsam mit Ihnen einen Basis-Workshop durch, um die Größe und Anforderungen Ihrer Backup-Lösung sowie der Notfall-Hardware festzulegen.

Workshop zur Bedarfsanalyse und Sizing

In diesem Workshop analysieren wir gemeinsam mit Ihnen die spezifischen Anforderungen Ihres Unternehmens. Dazu gehören die Datenmenge, die Rechenleistung und die Speicherkapazität, die im Ernstfall benötigt werden. Basierend auf diesen Informationen entwickeln wir eine maßgeschneiderte Notfall-Hardware-Plattform, die genau auf die Bedürfnisse und die Größe Ihres Unternehmens abgestimmt ist.

Notfall-Hardware-Plattform

Diese Plattform ist das Herzstück unseres Services und besteht aus folgenden, sorgfältig ausgewählten Komponenten:

Mobiles Rack: Ein robustes, transportables Rack, das alle notwendigen Hardware-Komponenten enthält. Es ermöglicht die schnelle Lieferung und Inbetriebnahme der Notfall-Hardware an Ihrem Standort, auch unter schwierigen Bedingungen.

Firewall und Router: Diese Komponenten schützen Ihre Netzwerke während der Wiederherstellung und stellen die notwendige Konnektivität sicher. Die Notfall-Hardware wird in einer strikt getrennten Netzwerkumgebung betrieben, um den Zugriff durch potenzielle Angreifer zu verhindern.

Top of the Rack Switches und Managementswitch: Diese Netzwerkkomponenten optimieren den Datenverkehr und die Verwaltung Ihrer Ressourcen. Der Netzwerkverkehr der Notfall-Hardware wird vollständig isoliert, um unerlaubte Zugriffe und weitere Angriffe zu verhindern.

Virtualisierungshosts: Diese ermöglichen die schnelle Bereitstellung und Wiederherstellung Ihrer virtuellen Maschinen. Wir unterstützen eine Vielzahl von Virtualisierungsplattformen, darunter VMware, Red Hat und Microsoft, um sicherzustellen, dass Ihre IT-Umgebung flexibel und kompatibel bleibt.

All Flash Storage System: Ein Hochleistungs-Speichersystem für maximale Zuverlässigkeit und Geschwindigkeit. Es stellt sicher, dass Ihre Daten verfügbar sind und keine Verzögerungen entstehen.

Backup Server und Backup Target: Diese sorgen für die kontinuierliche Sicherung und Wiederherstellung Ihrer Daten, die regelmäßig die regelmäßig an einen sicheren Ort repliziert werden. Ihre Daten werden schreibgeschützt aufbewahrt und durch eine Air Gap-Technologie zusätzlich gesichert, die den Zugriff nur zu festgelegten Zeiten erlaubt und so das Risiko eines Angriffs minimiert.

USV (Unterbrechungsfreie Stromversorgung): Eine USV stellt sicher, dass Ihre Notfall-Hardware auch bei einem Stromausfall weiter betrieben wird, um die Wiederherstellung nicht zu gefährden.

Implementierung der Backup-Infrastruktur

Nach dem Sizing implementieren wir die Backup-Infrastruktur in Ihrem Unternehmen. Diese umfasst sowohl die Hardware als auch die Software, die für die kontinuierliche Sicherung und Replikation Ihrer Daten notwendig ist. Die Daten werden täglich an einen sicheren Ort repliziert. Diese Replikation erfolgt in einem schreibgeschützten Zustand, sodass die Daten vor Veränderungen oder Manipulationen geschützt sind. Dank der Air GapTechnologie besteht keine permanente Verbindung zwischen Ihrem Unternehmen und dem sicheren Speicherort. Diese Technologie stellt sicher, dass die Replikation zu festgelegten Zeiten erfolgt und die Daten während der restlichen Zeit vor unbefugtem Zugriff sicher sind.

Erste Inbetriebnahme und Probelauf

Nach der ersten vollständigen Replikation Ihrer Daten wird die Theorie in der Praxis überprüft. Hierbei wird ein Ernstfall simuliert, um sicherzustellen, dass die erarbeiteten Konzepte und Prozesse reibungslos funktionieren. Die gesicherten Backups werden auf die Notfall-Hardware wiederhergestellt, um die Umgebung für den Einsatz beim Kunden vorzubereiten.

Nach dieser Wiederherstellung wird die Notfall-Hardware an Ihren Standort geliefert und dort final in Betrieb genommen. Während dieses Prozesses ergeben sich häufig wertvolle Erkenntnisse, die in den Workshops theoretisch vielleicht übersehen wurden. Diese Erkenntnisse fließen direkt in die Erstellung und kontinuierliche Anpassung des Notfallhandbuchs ein, welches als essenzieller Leitfaden im Ernstfall dient. Dieses Notfallhandbuch ist der zentrale Guide sowohl für die Mitarbeiter Ihres Unternehmens als auch für das Team der Medialine. Es stellt sicher, dass alle Beteiligten genau wissen, welche Schritte im Ernstfall zu unternehmen sind, und dass keine wichtigen Details übersehen werden.

Regelmäßige Workshops und Tests

Vorbereitung ist der Schlüssel zu einer erfolgreichen Krisenbewältigung. Deshalb ist ein zentraler Bestandteil von CRaaS die regelmäßige Durchführung von Workshops und Testläufen, die sicherstellen, dass alle Prozesse im Ernstfall reibungslos funktionieren.

Halbjährliche Test-Recovery

Alle sechs Monate führen wir ein umfassendes Test-Recovery durch, bei dem wir die Notfall-Hardware in Betrieb nehmen und die Wiederherstellung Ihrer IT-Umgebung simulieren. Dieser Test ist mehr als nur eine Übung; er dient dazu, die spezifischen technischen Anforderungen Ihres Unternehmens zu berücksichtigen und sicherzustellen, dass Ihre IT-Mitarbeiter genau wissen, wie sie im Ernstfall vorgehen müssen.

Die Test-Recovery verfolgt mehrere Ziele:

- Sicherstellung der Handlungsfähigkeit im Ernstfall: Durch die regelmäßigen Übungen sind Ihre Mitarbeiter bestens auf den Ernstfall vorbereitet. Sie lernen, wie sie die Notfall-Hardware effektiv einsetzen und die notwendigen Schritte zur Wiederherstellung Ihrer IT-Infrastruktur unternehmen. Diese Übungen minimieren die Wahrscheinlichkeit von Fehlern und sorgen dafür, dass Ihr Unternehmen auch in einer Krise schnell wieder funktionsfähig ist.
- Überprüfung und Anpassung des Notfallhandbuchs: Während der Workshops und Tests überprüfen wir gemeinsam mit Ihnen das Notfallhandbuch, das als Leitfaden im Ernstfall dient. Dieses Dokument wird kontinuierlich aktualisiert und an neue Erkenntnisse sowie veränderte Bedingungen angepasst. Ein präzises und aktuelles Notfallhandbuch ist von unschätzbarem Wert, da es sicherstellt, dass alle Beteiligten wissen, was zu tun ist, und dass keine wichtigen Details übersehen werden.
- Identifizierung von Schwachstellen: Durch die Testläufe können wir potenzielle Schwachstellen in Ihrer Notfallstrategie identifizieren und entsprechende Gegenmaßnahmen ergreifen. Dies umfasst sowohl technische als auch prozessuale Aspekte, sodass wir sicherstellen können, dass Ihre IT-Infrastruktur im Ernstfall optimal geschützt ist.

Im Ernstfall: Schnelle Reaktion und Sicherung

Sollte es zu einem tatsächlichen Ransomware-Angriff kommen, ist eine schnelle Reaktion entscheidend. Unser CRaaS-Service bietet Ihnen die Sicherheit, dass wir sofort Maßnahmen ergreifen können, um den Schaden zu minimieren und den Geschäftsbetrieb schnell wiederherzustellen.

Bereitstellung und Inbetriebnahme der Notfall-Hardware

Im Ernstfall greifen wir auf die vorbereitete Hardware-Plattform zurück, die schnellstmöglich an Ihren Standort geliefert wird. Diese Hardware ist bereits auf die spezifischen Anforderungen Ihres Unternehmens zugeschnitten und wird vollständig vorinstalliert geliefert. Alle Systeme sind bereits vorkonfiguriert, und die Wiederherstellung Ihrer Daten aus dem Backup ist bereits abgeschlossen. Bei der Ankunft vor Ort müssen die Systeme nur noch final in Betrieb genommen werden, was den Wiederherstellungsprozess erheblich beschleunigt.

Isolierung und Schutz der neuen Umgebung

Ein wichtiger Aspekt unseres Ansatzes ist die Isolierung der Notfall-Hardware von Ihrem bestehenden Netzwerk. Da zum Zeitpunkt eines Angriffs oft nicht bekannt ist, woher die Bedrohung ursprünglich kam und ob der Angreifer noch aktiv ist, betreiben wir die Notfall-Hardware in einer vollständig getrennten Netzwerkumgebung. Dies schützt die wiederhergestellten Systeme vor weiteren Angriffen und stellt sicher, dass der Wiederherstellungsprozess nicht gefährdet wird.

Kritische Abwehr: Wenn alles auf dem Spiel steht – Wir überlassen nichts dem Zufall

Solange die Notfall-Hardware das letzte Bollwerk ist, das Ihren Betrieb vor einem vollständigen Stillstand bewahrt, wird sie durch unser Managed SOC (Security Operations Center) umfassend abgesichert. Diese kontinuierliche Überwachung ist entscheidend, um sicherzustellen, dass keine weiteren Bedrohungen die Wiederherstellung und den fortlaufenden Betrieb gefährden können. Das SOC erkennt potenzielle Bedrohungen in Echtzeit und ergreift sofortige Gegenmaßnahmen, um die Integrität und Verfügbarkeit Ihrer wiederhergestellten IT-Infrastruktur zu gewährleisten. Solange die Notfall-Hardware den Betrieb aufrechterhält, sorgt das Managed SOC für den notwendigen Schutz gegen alle potenziellen Angriffe.

Erweiterte Sicherheitsfunktionen: KI-gestützte Bedrohungserkennung

In der kritischen Phase nach einem Ransomware-Angriff ist es von größter Bedeutung, dass die bereitgestellte Notfall-Hardware-Plattform vor weiteren Angriffen geschützt wird. Unser Managed SOC setzt hierfür auf eine leistungsstarke Kombination aus menschlicher Expertise und Künstlicher Intelligenz (KI), um potenzielle Bedrohungen proaktiv zu erkennen und abzuwehren.

KI-basierte Systeme überwachen kontinuierlich alle Aktivitäten auf der Notfall-Hardware und analysieren in Echtzeit das Verhalten, um ungewöhnliche Muster zu identifizieren, die auf Sicherheitsvorfälle hindeuten könnten. Diese fortschrittliche Technologie ermöglicht eine schnelle Erkennung und Reaktion auf Bedrohungen. Doch die Effektivität dieser Systeme wird durch die Erfahrung und das Urteilsvermögen unserer Sicherheitsexperten ergänzt.

Die KI identifiziert verdächtige Aktivitäten und leitet diese sofort an unsere erfahrenen Analysten weiter, die die Situation beurteilen und die erforderlichen Maßnahmen einleiten. Diese Kombination aus menschlicher Intuition und maschineller Präzision stellt sicher, dass Bedrohungen nicht nur schneller erkannt, sondern auch sofort neutralisiert werden, bevor sie Schaden anrichten können. Durch die Implementierung dieser hybriden Überwachungslösung in unser Managed SOC können wir die Sicherheit des zur Verfügung gestellten Stacks erheblich verstärken und somit das Risiko weiterer Schäden in einer ohnehin schon kritischen Situation minimieren.

Threat Hunting zur Wiedererlangung der Kontrolle über die kompromittierte Umgebung

Neben der Absicherung des zur Verfügung gestellten Stacks bieten wir Ihnen ein spezialisiertes Threat Hunting-Team, das parallel zur Wiederherstellung Ihrer IT-Infrastruktur arbeitet. Dieses Team von erfahrenen Sicherheitsexperten ist darauf spezialisiert, aktive Bedrohungen in Ihrer kompromittierten Umgebung zu identifizieren und zu neutralisieren.

Während unser CRaaS-Service den Wiederherstellungsstack absichert, arbeitet das Threat Hunting-Team daran, die verbleibenden Bedrohungen in Ihrer bestehenden IT-Umgebung aufzuspüren. Das Team analysiert in Echtzeit alle Aktivitäten in der kompromittierten Umgebung, identifiziert Anomalien und verfolgt verdächtiges Verhalten, um die Quelle der Bedrohung zu isolieren und zu eliminieren.

Durch den Einsatz fortschrittlicher Analysetechniken und Tools stellt das Threat Hunting-Team sicher, dass keine versteckten Angreifer oder Schadsoftware in Ihrem Netzwerk verbleiben, die Ihre wiederhergestellte Umgebung erneut gefährden könnten. Diese parallelen Maßnahmen sind entscheidend, um die Kontrolle über Ihre gesamte IT-Infrastruktur schnell und effektiv zurückzugewinnen und den Wiederherstellungsprozess zu sichern.

Mit der Unterstützung des Threat Hunting-Teams können Sie sicher sein, dass nicht nur Ihre neue Notfall-Hardware geschützt ist, sondern auch Ihre bestehende, kompromittierte Umgebung gründlich gesäubert und stabilisiert wird, sodass Sie den Normalbetrieb ohne weitere Unterbrechungen wieder aufnehmen können.

Rückführung der Dienste auf die wiederhergestellte Infrastruktur nach Behebung der Gefahr

Nachdem die Notfall-Hardware über mehrere Wochen ihren Dienst getan hat und die Betriebsunterbrechung erfolgreich abgewehrt werden konnte, steht der nächste entscheidende Schritt an: die Rückführung der Dienste auf die ursprüngliche, wiederhergestellte Infrastruktur. Sobald die ursprüngliche Hardware, die durch den Angriff kompromittiert wurde, von Forensikern freigegeben und für den Gebrauch als sicher eingestuft wird, unterstützen wir Sie bei den erforderlichen Maßnahmen.

In dieser Phase unterstützen wir bei eventuellen Neuinstallationen der Systeme und sorgen für eine reibungslose Migration von der Notfall-Hardware zurück auf Ihre eigene Plattform. Ziel ist es, den Normalzustand Ihrer IT-Infrastruktur wiederherzustellen, ohne den laufenden Betrieb zu unterbrechen.

Nach einer sorgfältig überwachten Übergangsphase, in der sichergestellt wird, dass alle Dienste stabil laufen und keine Sicherheitslücken bestehen, beginnen wir mit dem Abbau der Notfall-Hardware. Gleichzeitig wird die Backup-Replikation in den Normalbetrieb überführt, sodass Ihre Systeme erneut in der bewährten Umgebung gesichert und geschützt sind.

3. Zusammenfassung

Cyber Recovery as a Service (CRaaS) bietet Ihnen eine umfassende, maßgeschneiderte Lösung, die weit über traditionelle Backup- und Wiederherstellungsansätze hinausgeht. Unser Service gewährleistet nicht nur eine schnelle und effektive Wiederherstellung Ihrer IT-Infrastruktur nach einem Ransomware-Angriff, sondern bietet auch ein Höchstmaß an Sicherheit und Schutz für Ihre letzten verbleibenden Ressourcen. Mit CRaaS sind Sie bestens gerüstet, um auch in den kritischsten Situationen handlungsfähig zu bleiben und Ihre Geschäftsprozesse ohne größere Unterbrechungen fortzusetzen.

Durch die Kombination aus präziser Planung, regelmäßigen Tests, spezialisierter Hardware, fortschrittlichem Sicherheitsmanagement, parallelem Threat Hunting und einer sicheren Datenreplikation bieten wir Ihnen die Sicherheit, dass Ihre IT-Infrastruktur in besten Händen ist – selbst im Ernstfall. Mit **CRaaS** können Sie sich darauf verlassen, dass Sie jederzeit auf eine Krise vorbereitet sind und schnell wieder zum normalen Geschäftsbetrieb zurückkehren können.

Haben wir Ihr Interesse geweckt?
Vereinbaren Sie jetzt einen Termin und wir beraten Sie gerne über die Möglichkeiten von Cyber Recovery as a Service by Medialine in Ihrem Unternehmen.

Kontaktieren Sie uns unter:
+43316 225029 oder **sales.at@medialine.com**