Protected Server

Nativ integrierte Cyber Protection für Server und VMs

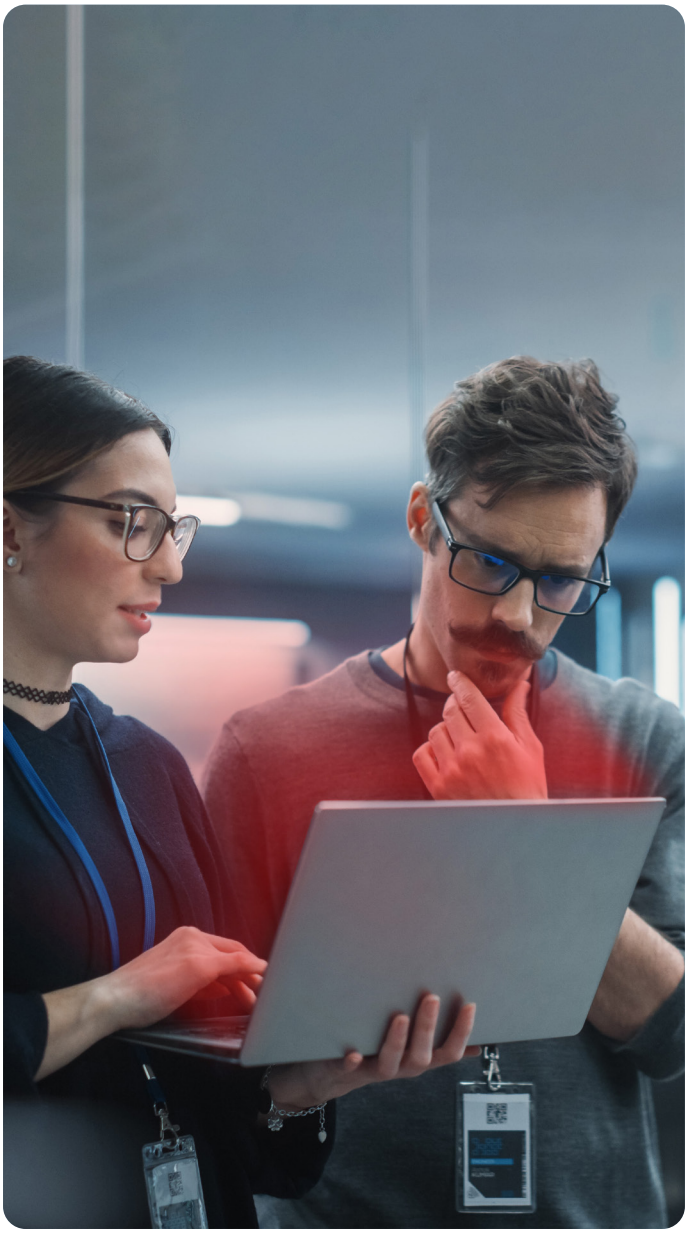
Cyber-Resilienz geht über die herkömmliche Cybersicherheit hinaus. Es geht nicht nur darum, Angriffe zu verhindern, sondern auch darum, dass Ihr Unternehmen im Falle eines Angriffs weiterarbeiten kann. Das National Institute of Standards and Technology (NIST) definiert Cyber-Resilienz wie folgt: „Cyber-Resilienz ist die Fähigkeit, auf ungünstige Bedingungen, Belastungen, Angriffe oder Kompromittierungen von Systemen vorbereitet zu sein, diesen standzuhalten, sich von ihnen zu erholen und sich entsprechend anzupassen."

Wie schnell kann sich Ihr Unternehmen im Ernstfall wieder erholen? Ohne klare Playbooks für die Reaktion auf Zwischenfälle, ohne geeignete Tools sowie ohne definierte RTOs (Recovery Time Objectives) und RPOs (Recovery Point Objectives) birgt jede Störung das Risiko von Umsatzverlusten, dem Verlust von Kundenvertrauen und dauerhaften Imageschäden.

Herausforderungen bei der Cyber-Resilienz

Unternehmen jeder Größe stellen fest, dass Ausfallzeiten weitaus kostspieligere Folgen haben als nur den Verlust von Daten. Zudem stehen sie unter zunehmendem Druck, Vorschriften einzuhalten, und unterliegen einer verstärkten regulatorischen Aufsicht. Jede Lücke in der Vorbereitung kann Bußgelder, Sanktionen und einen Reputationsverlust nach sich ziehen.

Die Verwaltung von Vorfällen mithilfe fragmentierter Tools führt ebenfalls zu unnötiger Komplexität. Ohne eine einheitliche Strategie geraten IT-Teams schnell in ein operatives Chaos. Das liegt daran, dass sie Schwierigkeiten haben, Erkennung, Reaktion und Wiederherstellung über mehrere Konsolen und Agenten hinweg zu koordinieren. Diese Ineffizienzen erhöhen die Kosten, verlangsamen die Reaktionszeiten und vergrößern das Haftungsrisiko. Besorgniserregend sind auch die steigenden Prämien für Cyberversicherungen. Eine schlechte Resilienz kann sogar dazu führen, dass der Versicherungsschutz komplett verweigert wird.



Technologische Hindernisse für Resilienz

Unternehmen beschleunigen die digitale Transformation. Dadurch wird es jedoch schwieriger, Resilienz zu erreichen. Hybride IT-Umgebungen, die sich über lokale Systeme, Cloud-Plattformen und Remote-Endpunkte erstrecken, bieten eine ständig wachsende Angriffsfläche. Dies führt zu mehr Abhängigkeiten und einzelnen Fehlerpunkten. Gleichzeitig werden die Bedrohungen immer ausgefeilter. Ransomware, Lieferketten-Angriffe und Insider-Risiken nutzen die Sicherheitslücken aus, die durch Einzellösungen entstehen. Einzellösungen können zwar spezifische Risiken reduzieren, schaffen aber auch blinde Flecken, manuelle Prozesse und Schwachstellen, die Cyberkriminelle schnell ausnutzen können.

Wie erreicht man Cyber-Resilienz?

Für echte Cyber-Resilienz ist mehr erforderlich als nur eine starke Abwehr. Es geht darum, die Kontinuität zu gewährleisten – unabhängig davon, welche Störung auftritt. Unternehmen können Resilienz erreichen, indem sie einen strukturierten Ansatz verfolgen. Dieser beginnt mit der **Vorbereitung** auf Risiken durch Asset-Mapping, Schwachstellenbewertung und Patch-Management. Um Bedrohungen **standhalten** zu können, müssen Unternehmen diese in Echtzeit erkennen und eindämmen können. Dafür sind fortschrittliche Funktionen wie KI-gestützter Endpunktschutz und ML-basierte Überwachung erforderlich. Diese proaktiven Maßnahmen sind jedoch nur dann effektiv, wenn sie mit einer zuverlässigen Wiederherstellungsstrategie kombiniert werden.

Die Wiederherstellung ist der nächste wichtige Schritt. Durch eine schnelle, zuverlässige und malwarefreie Wiederherstellung von Daten und Systemen wird die Ausfallzeit auf ein Minimum reduziert. Bei einem schwerwiegenden Ausfall hat die Sicherstellung der Geschäftskontinuität höchste Priorität. Mit Acronis Cloud Disaster Recovery können Unternehmen sofort ein Failover ihrer Workloads in die Acronis Cloud oder zu Microsoft Azure durchführen. Das sofortige Failover gewährleistet die Kontinuität selbst bei schwerwiegenden Ausfällen und dient als sichere Fallback-Umgebung, bis die vollständige Wiederherstellung der primären Systeme abgeschlossen ist.

Da Resilienz kein statischer Zustand ist, müssen Unternehmen sich **anpassen**. Sie müssen aus Vorfällen lernen, ihre Teams schulen und ihre Abwehrmaßnahmen im Laufe der Zeit verfeinern.

Das Spektrum von Disaster Recovery (DR)

Bei diesen Strategien geht es letztlich nicht nur um die Wiederherstellung nach einer Krise, sondern auch darum, wichtige Geschäftsfunktionen unter widrigen Umständen aufrechterhalten zu können, um die operative Resilienz zu gewährleisten. Von entscheidender Bedeutung ist dabei die Fähigkeit, Services innerhalb von Minuten statt Tagen wiederherzustellen, um finanzielle Verluste zu minimieren und das Kundenvertrauen zu wahren.

In der Regel werden DR-Strategien anhand der RPOs und RTOs, die sie erreichen können, kategorisiert.
Zwei der am häufigsten verwendeten Strategien sind:

Warm DR

Dieser Ansatz zeichnet sich durch ein ausgewogenes Verhältnis zwischen Kosten und Wiederherstellungsgeschwindigkeit aus. Er nutzt vorkonfigurierte Systeme, die schnell online geschaltet werden können. Damit wird das „Wiederherstellen"-Ziel erreicht, Ausfallzeiten zu minimieren und gleichzeitig definierte RPO- und RTO-Werte einzuhalten.

Cold DR

Beim Cold DR steht die Wiederherstellung von Systemen und Daten im Mittelpunkt. Dieser Ansatz basiert auf einer vollständigen Wiederherstellung aus Backups. Das führt zwar zu längeren Wiederherstellungszeiten, aber zu geringeren laufenden Kosten.

Die Integration von Erkennung, Schutz und Wiederherstellung verschafft Unternehmen einen entscheidenden Vorteil: Sie können nicht nur Krisen überstehen, sondern auch gestärkt aus ihnen hervorgehen. Mit Acronis Cloud Disaster Recovery können sie für jeden Workload das richtige Maß an Resilienz festlegen. Die Failover-Optionen reichen dabei von Warm DR und Cold DR, bei denen Dienste nach einem Ausfall wiederhergestellt werden, bis hin zu nahezu sofortiger Kontinuität mit integriertem Hot DR. Diese Flexibilität stärkt die Abwehr in jeder Phase der Cyber-Resilienz.

Die Acronis Protected Server Lösung

Die Acronis Protected Server Lösung vereint Backup, Disaster Recovery, Endpoint-Sicherheit, Risikobewertung und Data Loss Prevention in einer einzigen, nativ integrierten Cyber-Protection-Plattform. Dieser Ansatz ersetzt Einzellösungen, verringert die Anzahl der Tools und gewährleistet Resilienz, ohne zusätzliche Komplexität zu erzeugen. Die Plattform deckt alle Phasen ab, die für Resilienz notwendig sind: Vorbereiten, Standhalten, Wiederherstellen und Anpassen. Mit nur einer Plattform, einem einzigen Agenten und einer einzigen Konsole können Unternehmen Bedrohungen schneller erkennen, den Betrieb ohne Unterbrechungen wiederherstellen und sich kontinuierlich an neue Risiken anpassen.

VORBEREITEN	STANDHALTEN	WIEDERHERSTELLEN	ANPASSEN
• Geräte-Erkennung • Data-Protection-Karte • Inventarisierung von Assets • Schwachstellen-bewertung • Patch-Management	• Bedrohungserkennung in Echtzeit • KI-gestützte Endpoint Detection and Response (EDR) • ML-basierte Überwachung • Schnelle Eindämmung aktiver Bedrohungen	• Sichere und automatisierte Datenwiederherstellung • Cloud Disaster Recovery (CDR) • Unveränderliche Backups • Hypervisor-Mobilität • Wiederherstellung von malwarefreien Punkten	• Überwachung und Verwaltung von Endpunkten • Security Awareness Training (SAT) • Templates für die Reaktion auf Zwischenfälle mit Hinweisen

Warum sich Unternehmen für Acronis entscheiden

Heutzutage sind Cyberangriffe unvermeidbar. Abhilfe schafft die Cyber-Resilienz-Lösung von Acronis. Sie vereint KI-gestützten Schutz vor Bedrohungen und cloudbasiertes Disaster Recovery in einer einzigen Plattform. Anders als bei fragmentierten, ausschließlich auf Prävention ausgerichteten Ansätzen gewährleistet Acronis, dass kritische Daten durch unveränderliche Backups, eine KI-basierte Ransomware-Erkennung und einen sicheren, malwarefreien Recovery-Prozess geschützt und wiederherstellbar sind.

Dank vollständig cloudgemanagtem Disaster Recovery, sofortigem Failover in die Acronis Cloud, nutzungsbasierter Abrechnung und kundenkontrollierter Tests und Ausführungen liefert die Acronis Protected Server Lösung Cyber Protection auf Enterprise-Niveau, jedoch ohne die Kosten und Komplexität klassischer Legacy-Infrastrukturen. Das Ergebnis sind schnellere Wiederherstellungen, geringere Betriebsrisiken und eine zuverlässige Geschäftskontinuität, wenn es darauf ankommt.

Kontaktieren Sie uns

InovaTech GmbH
https://www.inovatech.at
office@inovatech.com
00435029299