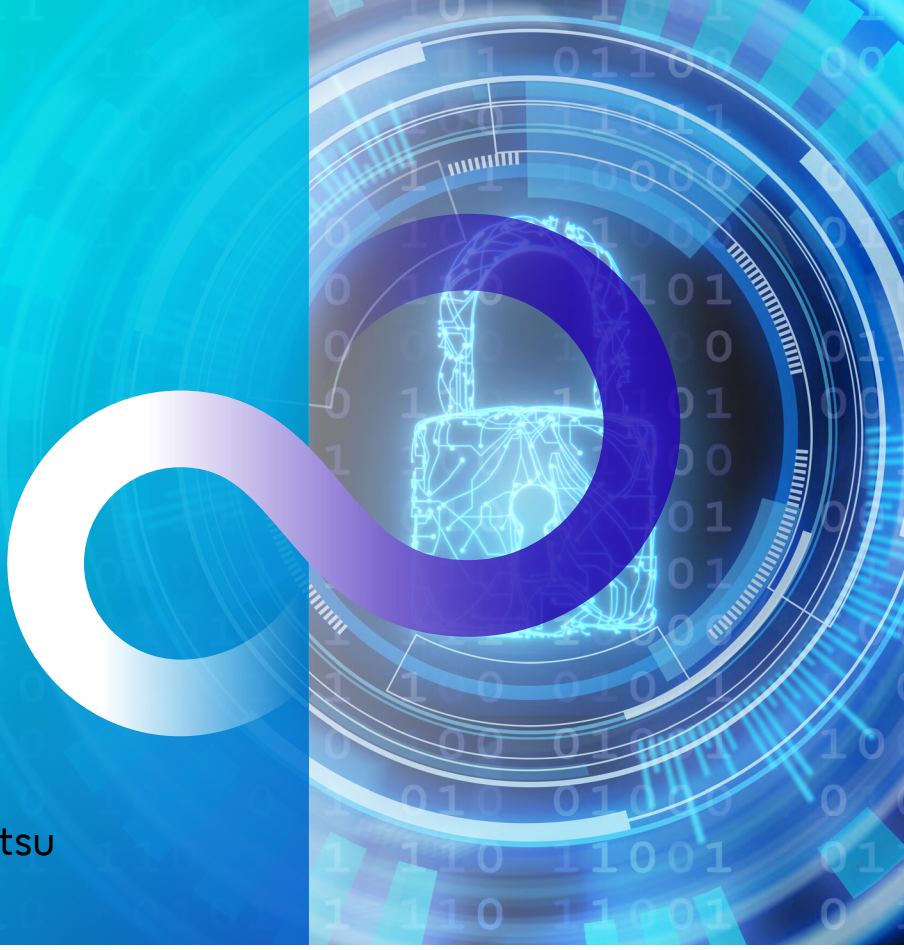
FUJITSU

Vorbeugen ist besser als bezahlen



Die datengesteuerte Ransomware-Strategie von Fujitsu

Cyberattacken, insbesondere durch Ransomware, bedrohen zunehmend den Erfolg der digitalen Transformation in vielen Unternehmen. Der wirtschaftliche Schaden durch Ransomware nimmt von Jahr zu Jahr zu. Alle 11 Sekunden wird ein Unternehmen Opfer eines Ransomware-Angriffs. Experten gehen davon aus, dass es im Jahr 2031 etwa alle 2 Sekunden eine Ransomware-Attacke geben wird und der jährliche Schaden von heute etwa 20 Milliarden Dollar auf 250 Milliarden Dollar ansteigt.

Daten sind die Basis intelligenter Unternehmen. Daher hängt die erfolgreiche digitale Transformation immer mehr von der Fähigkeit ab, eine einheitliche Architektur für Datenmanagement und Datensicherung in modernen Multi-Cloud-Infrastrukturen zu entwickeln. Aber wie kann Ihr Unternehmen cybersicher werden?

Dazu muss die Cybersicherheit zunächst als wesentlicher Aspekt Ihrer Unternehmensziele betrachtet werden. Als digitales Unternehmen müssen Sie auch die Sicherheit Ihrer Systeme und Prozesse priorisieren und digitale Wertschöpfungsketten schaffen, die die Daten Ihrer Kunden und Partner zuverlässig schützen. Ein sicheres und komfortables Nutzererlebnis sollte dabei oberste Priorität haben.

Diese Herausforderung wird jedoch zunehmend komplexer, da Cyberkriminelle jetzt sogar Backups – die letzte Verteidigungslinie gegen Ransomware – ins Visier nehmen. Erhält ein Angreifer Zugriff auf Ihre Backups, hat Ihr Unternehmen kaum eine Chance, die Zahlung von Lösegeld zu vermeiden.

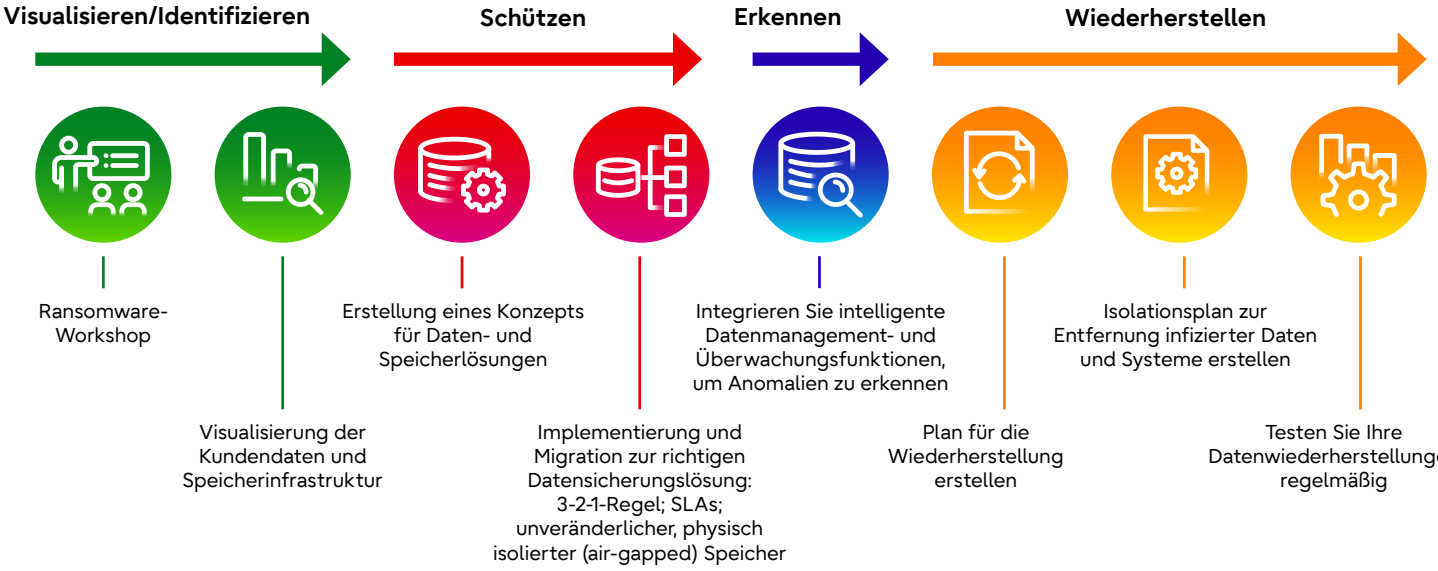
Sie können diesen Bedrohungen mit einem mehrstufigen Ansatz für die Datensicherung begegnen. Das erfordert umfassende Kenntnisse und regelmäßige Schulungen, damit Sie sich auf Cyber-Attacken vorbereiten können. Daher sollten Sie mit einem erfahrenen und vertrauenswürdigen Partner wie uns zusammenarbeiten. Wir begleiten Sie auf dem Weg zu einer cybersicheren IT-Infrastruktur und sorgen dafür, dass Ihr Unternehmen alle Vorteile neuer Sicherheitsverfahren und Technologien nutzt.

Was ist Ransomware?

Ransomware ist Schadsoftware, die Ihr Unternehmen über das Netzwerk angreift und vor allem auf aktive Server, aber auch auf Backup-Daten abzielt. Die Software verschlüsselt wichtige Dateien und macht sie unzugänglich, bis das geforderte Lösegeld gezahlt wird. Ransomware führt zu Systemausfällen und Datenverlust und somit zu wirtschaftlichen Verlusten. Weitere Folgen: Ein Image-Schaden für das Unternehmen und Vertrauensverlust bei Kunden und Partnern.

Der Schutz vor Cyberkriminalität ist für Unternehmen unerlässlich

Nutzen Sie unsere datengesteuerte Strategie gegen Ransomware. Damit können Sie sich gegen Ransomware-Attacken verteidigen und die Sicherheit Ihrer Daten verbessern – lokal und in der Cloud. Wir unterstützen Sie auch bei der Implementierung von Daten- und Speicherlösungen, die ihren Schutz gegen Cyberkriminalität und Ransomware-Angriffe verbessern. Zunächst beginnen wir mit einer gründlichen Evaluierung Ihrer geschäftlichen Anforderungen und vorhandener Sicherheitslücken. Wir arbeiten dabei mit Partnern zusammen, um Ihnen beim Aufbau einer sicheren und modernen Infrastruktur zu helfen. In den weiteren Schritten zeigen wir Ihnen, wie Sie Ihre IT gegen Hacker schützen können, die es auf Ihre Daten abgesehen haben.



Das Potenzial bewährter Verfahren und Lösungen ausschöpfen

Schutz Ihrer Daten mit 3-2-1-Ansatz
(3 Datenkopien auf 2 verschiedenen Medien, davon 1 Kopie an einem separaten Standort). So stellen Sie sicher, dass mindestens eine Kopie funktionsfähig bleibt, selbst wenn die beiden anderen verloren gehen, zerstört oder durch einen Ransomware-Angriff verschlüsselt werden.

Sichern Ihrer Daten mit unveränderlichem Speicher.
Erreicht Ransomware die vorderste Verteidigungslinie Ihres Unternehmens, sind Daten, die in einem unveränderlichen, vom Netzwerk getrennten Speicherpool liegen, gegen Verschlüsselung oder Löschung geschützt und stehen somit für eine Wiederherstellung zur Verfügung.

Nutzen Sie Offline-Backups und physisch getrennten Speicher.
Offline-Kopien verringeren als Teil des Datensicherungsplans das Risiko eines Malware-Angriffs. Das Air-Gapping (die physische Isolierung) Ihrer Daten mit Bandspeichern ist die kostengünstigste Variante, um Ihre Daten zu schützen und nach einem Ransomware-Angriff wiederherzustellen.

Auf Nummer sicher

Verhindern Sie kriminelle Cyberangriffe mit unserer Ransomware-Strategie. Unser umfangreiches Datenschutz-Ökosystem umfasst Lösungen für Identifizierung, Schutz, Lokalisierung und Wiederherstellung Ihrer Daten zu jedem Zeitpunkt im Daten-Lebenszyklus. Auf **www.fujitsu.com/de/data-protection** finden Sie weitere Informationen.

Kontakt bei Rückfragen: Telefon: 00800 372 100 00*
E-Mail: CIC@ts.fujitsu.com

* kostenfrei aus allen Netzen in Deutschland, Österreich und der Schweiz