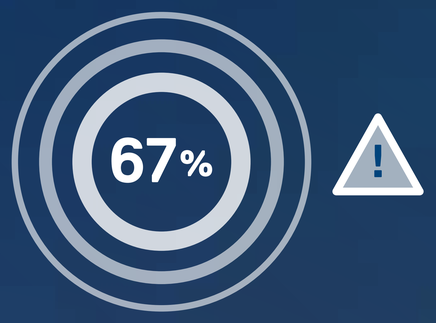
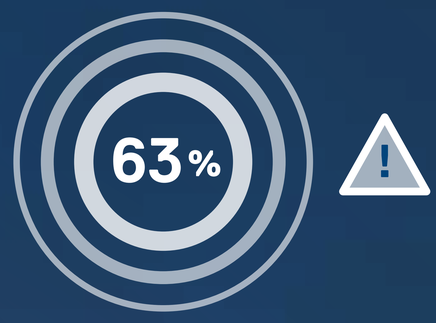
Fünf Tipps für mehr **Cyber-Resilienz** im Unternehmen

Einen hundertprozentigen Schutz vor Cyber-Attacken gibt es nicht. Unternehmen müssen sich daher auf den Ernstfall vorbereiten und in der Lage sein, die Auswirkungen erfolgreicher Attacken zu minimieren und den Geschäftsbetrieb schnellstmöglich wiederaufzunehmen. Doch wie lässt sich solche Cyber-Resilienz erreichen?



67 Prozent der Unternehmen fürchten, ihre Data Protection sei nicht ausreichend, um mit der Bedrohung durch Ransomware und andere Malware fertigzuwerden.



63 Prozent der Unternehmen sind nicht überzeugt, alle geschäftskritischen Daten nach einer schwerwiegenden Attacke wiederherstellen zu können.

Dell Global Data Protection Index 2022

1. Zero Trust umsetzen: Das Sicherheitskonzept Zero Trust sieht ein restriktive Rechtevergabe und konsequente Verifizierung aller Zugriffe vor. Damit schränkt es den Handlungsspielraum von Cyberkriminellen erheblich ein. Selbst mit einem gekaperten Account können sie sich nicht innerhalb der Infrastruktur bewegen und auf andere Systeme zugreifen.

2. IT-Sicherheit automatisieren: Moderne Security-Tools bieten einen hohen Automatisierungsgrad. Sie führen nicht nur Integritätschecks durch, um Manipulationen an Dateien und Systemen zu erkennen, sondern nutzen KI, um ungewöhnliches Benutzerverhalten aufzuspüren. Sobald sie eine Bedrohung entdecken, können sie automatisch Gegenmaßnahmen einleiten.

5. Data Protection konsolidieren: Eine Vielzahl spezialisierter Data-Protection-Lösungen von verschiedenen Anbietern macht nicht nur den IT-Teams viel Arbeit, sondern kann im Ernstfall auch die Wiederherstellung verzögern oder verhindern. Die Ausfallzeiten und Kosten steigen. Durch eine Konsolidierung lässt sich das verhindern und das Schutzniveau anheben.

3. Silos vermeiden: Systeme und Anwendungen, die offene Schnittstellen und Standards unterstützen, erleichtern die Migration von Daten und Workloads. Damit stellen sie sicher, dass sich der Geschäftsbetrieb im Ernstfall schnell fortsetzen lässt. Ohne diese Offenheit stecken Daten oft in Silos fest und können nicht zuverlässig gesichert oder wiederhergestellt werden.

4. Datentresore nutzen: Da Cyberkriminelle inzwischen gezielt Backups unbrauchbar machen, gehört eine Kopie der wertvollsten Daten in einen Cyber Recovery Vault. Diese Datentresore sind durch ein betriebliches Air Gap vom Rest der Infrastruktur getrennt. Werden die Originaldaten kompromittiert, lassen sie sich aus dem Vault garantiert wiederherstellen.

DELL Technologies