arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Warum die Einbindung des CEO für die Cyber-Resilienz entscheidend ist

Von Sven Richter, Marketing Manager DACH bei Arcserve

Überall auf der Welt werden Unternehmen jeder Art und Größe von Cyberangreifern bedroht und täglich machen neue Angriffe Schlagzeilen. Dennoch gehen viele CEOs immer noch nicht aktiv an dieses Problem heran. Eine kürzlich von Arcserve durchgeführte weltweite Studie zeigt, dass es bei Geschäftsführern eine erhebliche Wissenslücke gibt, wenn es um die Absicherung ihrer Unternehmen geht: nur 34 Prozent der CEOs kennen den Disaster-Recovery-Plan ihres Unternehmens, und nur 11 Prozent haben Kenntnisse über die Einzelheiten dieses Plans.

Diese Erkenntnisse sind angesichts der zunehmenden Verbreitung von Cyberbedrohungen wie Ransomware besonders erschreckend. Da die Angriffe immer ausgefeilter durchgeführt werden und häufiger auftreten, ist es notwendig, dass Führungskräfte eine zentrale Rolle bei der Ransomware-Resilienz übernehmen. Ohne die Mitwirkung der Führungsetage besteht ein erhöhtes Risiko, dass lediglich ein reaktiver Ansatz beim Schutz und der damit eng verbundenen Daten- und Systemwiederherstellung im Notfall verfolgt wird. Dies kann für Unternehmen im Falle eines Cyberangriffs zu längeren Ausfallzeiten, Datenverlusten und möglichen finanziellen Rückschläge führen.

Doch warum besteht diese Wissenslücke? In der Vergangenheit haben es viele CEOs vorgezogen, sich bei technischen Aspekten ihrer Geschäftsabläufe herauszuhalten. Und sie haben die Notfallwiederherstellung als Aufgabe der IT-Abteilung, und nicht als eine für das Überleben ihres Unternehmens zentrale Säule betrachtet. Doch Disaster Recovery zu

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

vernachlässigen ist heute keine Option mehr. CEOs müssen jetzt aktiv in die Planung und Ausführung einbezogen werden.

Warum die Teilnahme von CEOs entscheidend ist

Die Beteiligung des CEOs ist aus mehreren Gründen wichtig. Erstens geben CEOs die Prioritäten und Werte ihres Unternehmens vor. Durch ihre aktive Teilnahme an Diskussionen und Entscheidungen im Zusammenhang mit dem Datenschutz und der Datensicherheit senden sie eine klare Botschaft an das gesamte Unternehmen, wie wichtig der Schutz sensibler Informationen ist. Diese Führungsrolle fördert eine Kultur der Verantwortung und Rechenschaftspflicht im gesamten Unternehmen.

Zweitens ist die Unterstützung durch den CEO auch für die Sicherung der notwendigen Ressourcen von entscheidender Bedeutung. Initiativen zum Schutz von Daten und zur Wiederherstellung von Daten im Katastrophenfall erfordern oft erhebliche Investitionen in Technologien, Mitarbeiterschulungen und in die Infrastruktur. Wenn der CEO diese Maßnahmen aktiv unterstützt, signalisiert er dem Rest der Organisation, dass diese Investitionen Priorität haben.

Drittens besitzen Führungskräfte auch Kenntnisse über die Kernfunktionen des Unternehmens, kritische Daten und wichtige Interessengruppen. Dieses Wissen ist für die Identifizierung potenzieller Risiken und Schwachstellen unerlässlich und kann für die Erstellung eines robusten Notfallplans entscheidend sein. Durch die Einbeziehung des CEOs wird sichergestellt, dass der Plan mit den Gesamtzielen des Unternehmens übereinstimmt und zudem an sich verändernde Geschäftsanforderungen kontinuierlich angepasst werden kann.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Ein weiterer wichtiger Aspekt ist die Einhaltung von Vorschriften. In Europa unterliegen alle Unternehmen den strengen Datenschutzvorschriften, wie der Allgemeinen Datenschutzverordnung (DSGVO). Hinzu kommen branchenbezogene oder international Vorschriften wie dem Datenschutz für KRITIS-Unternehmen oder dem Health Insurance Portability and Accountability Act (HIPAA) der USA. Diese Richtlinien schreiben spezifische Maßnahmen zum Schutz sensibler Daten vor und bei Nichteinhaltung drohen schwere Strafen. Durch die aktive Beteiligung an der Entwicklung und dem Testen von Notfallwiederherstellungsplänen können Führungskräfte sicherstellen, dass ihre Organisationen alle für sie geltenden Vorschriften einhalten.

Wie können Organisationen die Führungsetage einbeziehen?
Organisationen haben diverse Möglichkeiten, CEOs und leitende Angestellte angemessen in die Aufrechterhaltung der Cyber-Resilienz einzubeziehen. Dazu gehören beispielsweise die Schärfung des Bewusstseins für Datenschutz, sowie regelmäßige Schulungen, in denen die Führungskräfte über die sich entwickelnde Landschaft der Cyberbedrohungen und die Bedeutung der Disaster-Recovery-Planung informiert werden. Diese Schulungen sollten die potenziellen Auswirkungen von Cyber-Bedrohungen auf den Geschäftsbetrieb und die entscheidende Rolle der Notfallwiederherstellung bei der Abschwächung solcher Risiken hervorheben. Sie können den Führungskräften das entscheidende Wissen vermitteln, damit sie fundierte Entscheidungen treffen können.

Darüber hinaus können spezielle Ausschüsse oder Arbeitsgruppen für Cybersicherheit unter Leitung der Unternehmensführung die aktive Beteiligung und die laufende Entwicklung von Richtlinien erleichtern. Diese Gruppen stellen sicher, dass Cybersicherheitsmaßnahmen in die Unternehmensagenda integriert werden und mit den allgemeinen

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Geschäftszielen übereinstimmen. Darüber hinaus wird durch die Einbeziehung von Überlegungen zur Notfallwiederherstellung und Cybersicherheit in strategischen Planungssitzungen und regelmäßigen Vorstandssitzungen die Bedeutung dieser Themen auf höchster Entscheidungsebene betont.

Die Zusammenarbeit mit externen Experten und die Teilnahme an Branchenforen können der Führungsebene ebenfalls wertvolle Einblicke und Anhaltspunkte liefern. Die Einbeziehung externer Perspektiven hilft Führungskräften, über neue Bedrohungen und bewährte Verfahren zur Risikominimierung informiert zu bleiben. Regelmäßige Übungen und Simulationen ermöglichen es den Führungskräften außerdem, die Reaktionsmechanismen der Organisation aktiv zu testen und verbesserungswürdige Bereiche zu ermitteln.

Fazit

Die aktive Beteiligung der Führungskräfte an der Planung der Notfallwiederherstellung fördert eine Kultur der Resilienz. Indem sie die Bedeutung der Datensicherheit und die Bereitschaft, diese bestmöglich zu fördern betonen, können die Führungskräfte letztlich den Erfolg des Unternehmens in jeder potenziellen Krise sicherstellen.

Folgen Sie Arcserve auf LinkedIn oder X und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve Blog.

###

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Über Arcserve
Arcserve gehört weltweit zu den Top-5-Herstellern von Datensicherungslösungen und bietet als Anbieter von Unified Data Resilience Lösungen eine einheitliche Plattform für die Ausfallsicherheit von Daten an. Das Unternehmen stellt das breiteste Spektrum an Best-in-Class-Lösungen für die Verwaltung, den Schutz und die Wiederherstellung aller Datenumgebungen zur Verfügung. Die Lösungen von Arcserve eignen sich für KMUs und Großunternehmen, unabhängig von deren Standort und der Komplexität der Infrastruktur. Sie beseitigen die Komplexität und bieten gleichzeitig erstklassigen, kosteneffizienten, flexiblen und massiv skalierbaren Datenschutz und Sicherheit für alle Datenumgebungen. Dazu gehören On-Prem-, Off-Prem- (einschließlich DRaaS, BaaS und Cloud-to-Cloud), hyperkonvergente und Edge-Infrastrukturen. Dank der vier Jahrzehnte langen Erfahrung des Unternehmens mit preisgekrönten IP-Lösungen und der kontinuierlichen Konzentration auf Innovation können Partner und Kunden, darunter MSPs, VARs, LARs und Endbenutzer, sicher sein, dass sie den schnellsten Weg zu Daten-Workloads und -Infrastrukturen der nächsten Generation finden. Arcserve ist ein zu 100 Prozent channelorientiertes Unternehmen, das in über 150 Ländern vertreten ist und mit 19.000 Vertriebspartnern die kritischen Datenbestände von 235.000 Kunden schützt. Erfahren Sie mehr unter arcserve.com und folgen Sie Arcserve auf X oder LinkedIn.

Unternehmenskontakt
Jock Breitwieser
Arcserve
+1 408.800.5625
jock.breitwieser@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
arcserve@tc-communications.de