arcserve®
Protect what's priceless.

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

Wenn die Cyberresilienz hinkt, sind meist drei Fehler schuld

Von René Claus, EMEA MSP Sales Director bei Arcserve

Die Folgen eines Cyberangriffs können verheerend sein. Sie reichen von finanziellen Verlusten über Rufschädigung bis hin zu rechtlichen Auswirkungen. Und das Risiko steigt. Neueste Studien bestätigen, dass es den Ransomware-Angreifern in 71 Prozent der Attacken gelingt, die Daten zu verschlüsseln und dass sich die Kosten für die Wiederherstellung bei der Bezahlung eines Lösegelds insgesamt verdoppeln. Zudem werden in Deutschland bei 30 Prozent der Ransomware-Angriffe auch Daten gestohlen. Die gute Nachricht: Unternehmen können sich davor schützen, indem sie die fünf Säulen der Cyberresilienz berücksichtigen: identifizieren, schützen, erkennen, reagieren und wiederherstellen. Allerdings passieren bei der Umsetzung der Cyberresilienz immer wieder Fehler, welche in Folge eine vermeintliche Sicherheit implizieren – genau so lange, bis die Cyberkriminellen eine Lücke im scheinbar sicheren Schutzwall finden und großen Schaden anrichten. Die Erfahrung der Spezialisten für Datensicherheit und Wiederherstellung von Arcserve zeigt, dass es sich in den betroffenen Unternehmen meist um drei Fehler handelt, die zu einem hohen Risiko führen und in Folge zu Schäden durch Cyberattacken beitragen.

Der Wert der digitalen Daten wird unterschätzt

Einer der folgenreichsten Fehler bei den Bemühungen um Cyberresilienz besteht darin, dass Unternehmen die Bedeutung und den Wert ihrer Daten falsch einschätzen. Um die Strategie der Cyberresilienz in der Cybersecurity zu realisieren, ist es von essenzieller Bedeutung, den genauen Wert der Daten, einschließlich geistigem Eigentum, Kundendaten und geschützten Informationen, vollständig zu erfassen. Erst dann wird den Verantwortlichen die Bedeutung der Daten für das Unternehmen klar und welche Ressourcen,

arcserve®
Protect what's priceless.

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

Budgets und Lösungen nötig sind, um diese zu schützen. Oft führt ein nicht ausreichendes Bewusstsein zu unzureichenden Schutzmaßnahmen, etwa zu schwachen Passwörtern, veralteter Software und unzureichenden Zugangskontrollen und dazu, dass das Unternehmen Cyberbedrohungen überhaupt erst ausgesetzt wird.

Fakt ist, dass mit der zunehmenden Abhängigkeit von Digitaltechnologien und datengesteuerten Entscheidungsprozessen die digitalen Werte wertvoller sind denn je. Gleichwohl sind die Cyberkriminellen auf der Jagd nach exakt diesen Daten, denn neben der Verschlüsselung, der Betriebsunterbrechung und der Lösegeldforderung lassen sich diese im Untergrund zu horrenden Preisen verkaufen. Unternehmen sollten daher eine gründliche Risikobewertung durchführen, um ihre wichtigsten Werte zu identifizieren, potenzielle Achillesfersen besser zu verstehen und um robuste Sicherheitsanweisungen zum Schutz der Daten zu implementieren. Zu diesen Maßnahmen sollten die kontinuierliche Überwachung, das Patchen und Aktualisieren von Systemen und Software sowie die Implementierung starker Authentifizierungsmechanismen und Verschlüsselungsprotokolle gehören.

Ein besonderes Augenmerk sollten Unternehmen zudem auf der Prüfung potenziell veralteter Betriebssysteme und Anwendungen legen. Denn diese können ein erhebliches Problem und eine beträchtliche Lücke in der Strategie zur Datensicherheit darstellen – beispielsweise, wenn ein Backup-Anbieter die veralteten Betriebssysteme nicht unterstützen kann. Es ist wichtig zu prüfen, wie viele Legacy-Anwendungen auf älteren Betriebssystemen betrieben werden und ob diese gesichert werden können. Wenn ein Unternehmen – eventuell gezwungenermaßen – noch Altanwendungen einsetzt und diese nicht gesichert werden können, muss dieses Problem unbedingt gelöst werden, um Datenschutz und -sicherheit zu gewährleisten.

arcserve®
Protect what's priceless.

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

Das ineffektive Management von Risiken durch Dritte

Viele Unternehmen verlassen sich bei der Unterstützung ihrer Geschäftsabläufe zunehmend auf Drittanbieter, Lieferanten und Dienstleister. Diese externen Partner haben oft Zugang zu wichtigen Systemen, Daten und Netzwerken. Doch nicht alle Drittanbieter verfügen über eine solide Cybersicherheitsstruktur und können damit zu einer kritischen Schwachstelle beziehungsweise zum Einfallstor für Cyberangriffe werden.

Unternehmen versäumen es oft, die Cybersicherheit ihrer Drittanbieter gründlich zu bewerten und sicherzustellen, dass diese mindestens die gleichen Sicherheitsstandards einhalten wie sie selbst. Durch eine schlechte Cyberresilienz bei Dritten können Schwachstellen in der Cybersicherheitskette entstehen. Damit haben Cyberkriminelle die Möglichkeit, Schwachstellen in den Systemen von Drittanbietern auszunutzen und sich über die digitale Kette (Supply Chain) unbefugten Zugang zu den Daten oder Systemen eines Unternehmens verschaffen. Eine umfassende Due-Diligence-Prüfung von Fremdherstellern sorgt für Abhilfe. Damit wird deren Cybersicherheitsfähigkeit bewertet, was gleichzeitig zu soliden Verträgen und Vereinbarungen führt, in denen die Sicherheitserwartungen und Verantwortlichkeiten klar definiert sind. Selbstverständlich gilt dieser einmalige Status Quo nicht für die Ewigkeit. Eine regelmäßige Prüfung der Drittanbieter stellt sicher, dass diese in ihren Security-Bestrebungen nicht nachlassen, sondern ihre Security hinsichtlich der stetig veränderlichen Bedrohungslandschaft anpassen und weiterentwickeln. Übrigens sind derartige Prüfungen gleichzeitig die Grundlage für die Einhaltung von Datenschutzvorschriften.

Das Cyberrisiko im Zusammenhang mit Dritten ist für Unternehmen, die in einer hybriden Cloud-Umgebung arbeiten, besonders akut. Denn die Unterstützung unterschiedlicher Cloud-Plattformen und die Sicherstellung,

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

dass diese gut miteinander funktionieren, kann komplex sein und Sicherheitslücken zur Folge haben. Die Lösung: Unternehmen sollten eine angemessene Datenschutz- und Wiederherstellungsstrategie für ihre hybride Cloud-Umgebung entwickeln. Dazu gehört die Wahl einer Cloud-Speicherlösung, die kontinuierliche Snapshots, mehrere Wiederherstellungspunkte und Sicherheitskontrollen für private, öffentliche und SaaS-Umgebungen bietet.

Notfallpläne ohne Tests sind im Notfall selten gut

Unternehmen investieren beträchtliche Ressourcen und Budgets in die Entwicklung von Notfallplänen. Ziel ist es, im Notfall die Auswirkungen von Cyberangriffen auszuhebeln oder zumindest abzumildern. Allerdings verschwinden derartige Pläne oft ohne weitere Prüfung oder kontinuierliche Anpassung in der Schublade, bis sie eines Tages gebraucht werden. Dann ist es allerdings oft zu spät, denn keiner weiß, ob der Plan auch wirklich funktioniert, da weder das Zusammenspiel von Mitarbeitern und Technologie getestet und geübt wurde und da sich seit der Erstellung des Plans zu viele Rahmenbedingungen maßgeblich geändert haben. Die Erfahrung zeigt: Strategien und Pläne zur Reaktion auf Vorfälle sind nur dann wirksam, wenn sie regelmäßig getestet, verfeinert und auf der Grundlage der sich entwickelnden Cyberbedrohungen und der sich ändernden Geschäftsanforderungen aktualisiert werden.

Um dieses Problem zu beseitigen und um die Wirksamkeit der Notfallpläne festzustellen, sollten Unternehmen regelmäßig Übungen beziehungsweise simulierte Cyberangriffsszenarien durchführen. Diese Übungen helfen, Lücken und Schwachstellen in den Plänen zu erkennen und notwendige Anpassungen vorzunehmen. Dazu gehört auch eine detaillierte Bewertung der Tests, um die Wirksamkeit der Reaktion und das Optimierungspotenzial zu ermitteln. Diese kontinuierliche Feedback-Schleife ist entscheidend für die

arcserve®
Protect what's priceless.

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

Verbesserung der Reaktionsfähigkeit eines Unternehmens sowie für die Wirksamkeit und Relevanz der Pläne.

Mit Sicherheit sicher

Eines ist klar: während sich die Bedrohungslandschaft weiterentwickelt, müssen Unternehmen Fehler bei ihren Bemühungen um Cyberresilienz vermeiden. Das Verständnis über den Wert der Daten, das effektive Management von Risiken durch Dritte und das aktive, regelmäßige Testen von Notfallplänen sind die Grundlage für eine funktionierende und robuste Cyberresilienz.

Erfahren Sie mehr unter arcserve.com und folgen Sie Arcserve auf Twitter 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