Artikel

12 Fragen für jede Führungskraft, die zeigen, ob ihre Daten tatsächlich wiederherstellbar sind

Ransomware, Gefahren durch Insider und Betriebsstörungen sind keine seltenen Ereignisse mehr. Sie sind zur dauerhaften Realität geworden. Dennoch können die meisten Unternehmen immer noch nicht mit Sicherheit sagen, dass sie ihre Daten wiederherstellen können, wenn es darauf ankommt.

Diese Diskrepanz hat einen einfachen Grund: Backups und Snapshots sind Inputs – die Wiederherstellbarkeit ist ein Ergebnis.

Kontinuierliche Datensicherung, regelmäßige Backups, Snapshots und Sicherheitskontrollen sind notwendig. Allerdings garantieren sie nicht, dass die Systeme in realen Drucksituationen schnell, reibungslos und in der richtigen Reihenfolge wieder online gehen. Viele Unternehmen entdecken den Unterschied erst, wenn sie während eines Ernstfalls versuchen, ihre Systeme wiederherzustellen – und dann ist es zu spät, um gegenzusteuern.

Wiederherstellbarkeit ist der wirkliche Maßstab für Ausfallsicherheit. Und Führungskräfte können und sollten Drucktests durchführen, bevor ein Angriff, ein Hardware-Ausfall oder menschliches Versagen das Problem ans Licht bringen.

Die folgende kurze Checkliste für Führungskräfte enthält Fragen, bei denen es nicht um Tools oder Architektur geht. Sie sollen Lücken frühzeitig aufdecken, solange noch die Möglichkeit besteht, sie zu schließen. Wenn Sie diese Fragen klar beantworten können, sind Sie auf dem besten Weg zu einer Recovery-First-Strategie, die den modernen Bedrohungen und der Realität in hybriden Umgebungen gerecht wird.

Was „wiederherstellbar“ tatsächlich bedeutet

Bevor wir uns den Fragen zuwenden, ist es hilfreich, Klarheit über den Standard zu schaffen.

Wiederherstellbar bedeutet, die folgenden Aspekte bei der Wiederherstellung erreichen zu können:

- **Wiederherstellung zu einem Zeitpunkt ohne Kompromittierung**, der den Geschäftserwartungen (RPO) entspricht
- **Wiederherstellung mit hinreichender Geschwindigkeit, um den Geschäftsbetrieb aufrechtzuerhalten** (RTO) – also nicht nur auf Daten, sondern auch priorisierte Dienste bezogen
- **Wiederherstellung in eine Umgebung, die nicht unmittelbar erneut infiziert wird**, mit angemessener Isolation und Validierung

Wenn einer dieser Aspekte nicht erreicht wird, bleibt Ausfallsicherheit auf eine Behauptung beschränkt und bietet keine Kontrollmöglichkeit.

Wie Sie diese Checkliste verwenden

Sie brauchen nicht gleich am ersten Tag perfekte Antworten. Ziel ist die frühzeitige Erkennung von Lücken – solange es noch Handlungsmöglichkeiten gibt.

Nutzen Sie die Fragen für eine kurze Selbsteinschätzung:

— **Grün:** dokumentiert, getestet und gemessen

— **Gelb:** teilweise umgesetzt oder nicht getestet

— **Rot:** angenommen, unbekannt oder „vermutlich"

Achten Sie besonders auf die roten Antworten. Dort verstecken sich oft Verzögerungen und Risiken.

Sicherungsfrequenz (hier beginnt die Wiederherstellbarkeit)

Das Vertrauen in die Wiederherstellung beginnt mit dem Verständnis, wie viel Datenverlust Ihr Unternehmen tatsächlich verkraften kann – und ob Ihre Schutzmaßnahmen dazu passen.

1. **Welchen RPO-Wert müssen wir bei unseren Tier-0- und Tier-1-Services erreichen – und können wir diesen Wert in der Praxis und nicht nur in der Theorie einhalten?**
   Viele Teams können aus dem Stand einen RPO-Wert nennen. Nur wenige haben nachgewiesen, dass ihr aktuelles Sicherungsmodell ihn auch unter Druck erfüllen kann.

2. **Sind unsere Wiederherstellungspunkte fein genug definiert, um den wenige Sekunden vor dem Datenverlust herrschenden Zustand wiederherzustellen, oder begnügen wir uns mit dem letzten planmäßigen Backup?**
   Wenn Angriffe oder Datenkorruption sich über einen längeren Zeitraum erstrecken, können weit verteilte Wiederherstellungspunkte direkt zu inakzeptablem Datenverlust führen.

3. **Haben wir eine einheitliche Frequenz für Wiederherstellungspunkte in den unterschiedlichen On-Premises-, Cloud- und SaaS-Plattformen – und wie wirken sich Abweichungen in der Frequenz auf unsere Wiederherstellungsstrategie aus?**
   In hybriden Umgebungen wird Uneinheitlichkeit häufig übersehen. Sicherungslücken entstehen häufig dort, wo die Richtlinien voneinander abweichen.

Warnsignale:

„Wir kennen unseren RPO für Tier-0 nicht."

„Wir haben für alles eine Standard-Backup-Richtlinie."

„Cloud-Workloads werden anders gehandhabt – nicht einheitlich."

Unveränderlichkeit und Isolation (nicht verhandelbare Eigenschaften im Zeitalter der Ransomware)

Die Unveränderlichkeit verhindert zwar das Löschen und Verschlüsseln von Wiederherstellungskopien, ist aber allein nicht ausreichend. Isolation und betriebliche Disziplin entscheiden darüber, ob unveränderliche Kopien einen realen Angriff tatsächlich überstehen. In den meisten Umgebungen wird beides benötigt.

4. **Bewahren wir mindestens eine Wiederherstellungskopie auf, die sowohl unveränderlich als auch von der Produktionsumgebung und den Netzwerken isoliert ist?**
   Wenn Angreifer über dieselben Wege, über die sie in Ihre Produktionsumgebung gelangen, auch auf Ihre Wiederherstellungsdaten zugreifen können, reicht die Unveränderlichkeit allein möglicherweise nicht aus.

5. **Ist die Unveränderlichkeit auf technischer Ebene verankert – oder können die Aufbewahrungs- oder Löschschutzmaßnahmen mit einer kompromittierten Admin-ID geändert werden?**
   In vielen Fällen sind die Zugangsdaten – und keine Malware – die Ursache der Probleme. Die Wiederherstellungskontrollen müssen dieser Tatsache Rechnung tragen.

6. **Was hindert Angreifer, wenn sie als erstes die Wiederherstellungsdaten ins Visier nehmen, daran, unseren Wiederherstellungspfad zu entdecken, zu verschlüsseln oder zu sabotieren?**
   Diese Frage legt offen, ob mit der Annahme „Sicherheit durch Unbekanntheit" operiert wird, die modernen Bedrohungstaktiken nicht standhält.

Ein hilfreiches Mindset

Wenn Ihr Wiederherstellungskonzept davon ausgeht, dass Angreifer Ihre Umgebung nicht verstehen, ist es bereits veraltet.

Disziplinierte Tests (Wiederherstellung gibt es nur, wenn sie getestet ist)

Unerprobte Notfallpläne scheitern nicht unbemerkt – sie scheitern in den stressigsten Momenten, denen ein Unternehmen ausgesetzt sein kann.

7. **Wann haben wir zuletzt einen Wiederherstellungstest von Tier-0-Anwendungen in realistischem Umfang durchgeführt – und haben wir die Wiederherstellungszeit gemessen?**
   Kleine, unvollständige Tests können die Komplexität realer Wiederherstellungsszenarien nicht abbilden.

8. **Überprüfen wir routinemäßig die Integrität unserer Backups und Wiederherstellungsressourcen, bevor wir sie benötigen?**
   Wenn Sie beschädigte Datensicherungen erst während eines Zwischenfalls zu erkennen, wird aus einem technischen Problem eine Geschäftskrise.

9. **Können wir die Wiederherstellung zur forensischen Validierung in einer isolierten Umgebung durchführen, bevor wir erneut die Verbindung mit der Produktionsumgebung herstellen?**
   Eine schnelle Wiederherstellung ist wichtig. Eine saubere Wiederherstellung ist unerlässlich.

Die bittere Wahrheit

Ohne Übung wird die Wiederherstellung zur Improvisation.

Identitätskontrollen und Wiederherstellungsprioritäten (weil die Geschwindigkeit davon abhängt)

Bei der Wiederherstellungsgeschwindigkeit geht es nicht nur um Speicherplatz oder Infrastruktur. Oft wird sie durch Identitätssysteme, Zugriffskontrollen und unklare Prioritäten eingeschränkt.

10. **Sind die Datensicherungs- und Wiederherstellungskontrollen durch MFA, ein System mit minimalen Berechtigungen und getrennte Rollen geschützt – und haben diese Kontrollen auch dann Bestand, wenn AD oder IAM kompromittiert wurden?**
    Wenn Identitätssysteme ausfallen, geht oft auch die Berechtigung für Wiederherstellungen verloren.

11. **Gibt es eine dokumentierte Wiederherstellungsreihenfolge für Tier-0-Services – und wurde diese getestet?**
    Identität, Netzwerk, DNS, Kernplattformen und Daten werden standardmäßig nicht gleichzeitig wieder online gebracht. Die Reihenfolge ist wichtig.

12. **Wie schnell können wir die wichtigsten Anwendungen aus einer unveränderlichen Kopie wiederherstellen – und welche Abhängigkeiten verlangsamen die Time-to-Service, jenseits der Time-to-Data?**
    Führungskräfte erleben Ausfälle als Verlust von Funktionen, nicht als Verlust von Dateien. Die Wiederherstellungspläne sollten diese Tatsache berücksichtigen.

Von der Checkliste zur Umsetzung

Bei dieser Bestandsaufnahme geht es nicht darum, dass Sie sich selbst bewerten. Es geht um die Bündelung von Anstrengungen an Stellen, an denen sich Risiken am schnellsten verringern lassen.

Praktische nächste Schritte:

— Identifizieren Sie die **drei wichtigsten roten Antworten** und weisen Sie ihnen eindeutige Verantwortliche zu.

— Legen Sie einen **Rhythmus für Wiederherstellungstests** fest und machen Sie die Ergebnisse bekannt – und nicht nur Versprechungen.

— Legen Sie die Wiederherstellung für die **ungünstigsten Bedingungen** aus, unter der Annahme, dass Angreifer Ihre Umgebung durchschauen.

Der Nachweis der Wiederherstellbarkeit lässt sich nicht mit dem Kauf eines weiteren Tools oder dem Ankreuzen eines weiteren Kästchens bewerkstelligen. Er ergibt sich aus wiederholten Wiederherstellungen der wesentlichen Elemente auf einen bekannten, sauberen Zustand innerhalb festgelegter Zeitvorgaben für die Wiederherstellung.

Weitere Informationen unter

HPE.com/data

HPE.com besuchen

Jetzt chatten

a00155955DEE

HEWLETT PACKARD ENTERPRISE

hpe.com