infopulse

Ultimative BCP-Checkliste

Sind Ihre Backups sicher?_

01

Besteht die Gefahr, dass ein Cyberangriff Ihre Vermögenswerte auslöscht oder beschädigt? Wenn ja, sollten Sie für die **Sicherheit Ihrer Backup-Speicher sorgen:**

Sicherer Aufbewahrungsort:

Finden Sie einen Platz außerhalb der Reichweite von Cyberkriminellen, welche Ihre Schwachstellen ausnutzen und Ihre Daten ohne entsprechende Erlaubnis einfach löschen oder entfernen können.

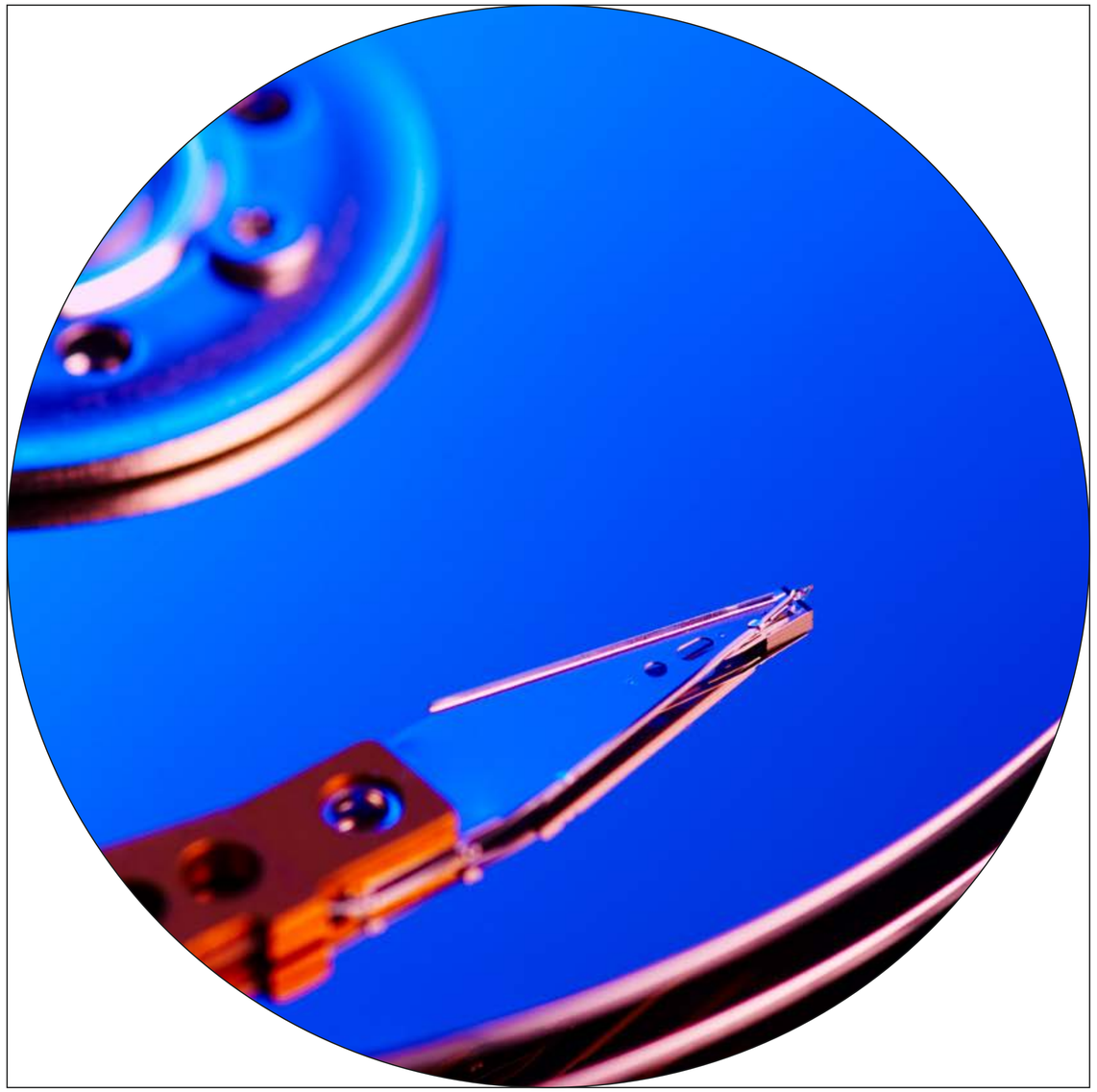
Sichere Netzwerke:

Isolieren Sie Ihre Netzwerke, auf denen Backup-Systeme arbeiten und Backups gespeichert sind.

Sichere Konten:

Es empfiehlt sich, getrennte Konten für die Verwaltung von Backup-Systemen zu verwenden, diese aber nicht täglich aufzudecken.

Sie müssen Ihre Backup-Systeme und -Prozesse regelmäßig einer Sicherheitsüberprüfung unterziehen.



Wie steht es um Ihre Haupt-Webseite und deren Backups?_

02

Auch wenn Sie Ihre Haupt-Webseite gesichert haben, können Angreifer später eine Sicherheitslücke finden und Backups aufspüren. Deshalb müssen Sie bei der Arbeit zum Schutz Ihrer Webseite sicherstellen, dass Ihre sekundäre(n) Webseite(n) über dieselbe Sicherheitsstufe wie die Haupt-Webseite verfügen.

Sind Ihre Umgebungsparameter synchronisiert?_

03

Richtlinien und Sicherheitsregeln enthalten in der Regel fest kodierte Werte. Differenzen in den Umgebungsparametern können dazu führen, dass das Sicherheitsniveau sinkt, Sicherheitsrichtlinien falsch funktionieren und Raum für schädliche Angriffe geschaffen wird. Der Ausweg aus einem möglichen Malheur ist die Automatisierung: Verwenden Sie Vorlagen, dynamische Objektnamen oder Skripte. Setzen Sie mithilfe genauer Planung und Tests konsistente Sicherheitsrichtlinien sowohl an primären als auch an sekundären (Backup-)Standorten ein.

Wichtige Schritte:

Implementieren und testen Sie bestehende Richtlinien, um mögliche Unterschiede und Unstimmigkeiten bei den Assets festzustellen.

Prüfen Sie bestehende Zugriffslisten und Berechtigungseinstellungen.

Testen Sie den Ausfall der Haupt-Webseite und versuchen Sie, die volle Funktionalität mit einem Backup wiederherzustellen.

Führen Sie Sicherheitsprüfungen für die Haupt- und Nebenwebseiten durch

Können Ihre primären Kommunikationskanäle einem Chaos standhalten?_

04

Ein Angreifer kann Ihre wichtigsten Kommunikationskanäle lahmlegen, wodurch Sie kaum eine Chance haben, proaktiv zu reagieren. Auf diese Weise bekommen die Eindringlinge mehr Zeit, um auf Systemressourcen zuzugreifen und die bestehenden Kontrollen zu übernehmen. Allerdings können Sie Backup-Kommunikationskanäle (oder sekundäre Kommunikationskanäle) für Ihre Mitarbeiter einrichten: einen Mechanismus für die Kommunikation mit den verantwortlichen Personen, den Sie im Falle eines Ausfalls der Infrastruktur, eines Verstoßes oder einer Beeinträchtigung nutzen können. Idealerweise sollte dieser Mechanismus außerhalb der Infrastruktur liegen und nicht von Ihren Unternehmenskonten, der Infrastruktur oder sogar den Arbeitsplätzen des Unternehmens abhängen. Achten Sie darauf, dass alle Teams kommunizieren können, falls der Hauptkommunikationskanal nicht zur Verfügung stehen sollte.

Optimieren Sie die Sicherheit Ihres Ökosystems, indem Sie diese Fragen stellen_

05

1. Wie gewährleistet Ihre Infrastruktur die hohe Verfügbarkeit der Dienste?
2. Wie führen Sie den Backup-Prozess durch? Was ist Ihr Backup-Plan? Wie stellen Sie die Kohärenz sicher? Wie lange können die Daten verloren gehen? Erfüllt Ihr Backup-Plan die Anforderungen?
3. Wie können Sie Backups zeitnah kontrollieren und sicherstellen, dass sie nicht ausfallen?
4. Wie betreiben Sie Ihre Backup-/Sekundärstandorte?
5. Gibt es Unterschiede bei den Lösungen, der Leistung oder den Modellen?
6. Wie verteilen Sie die Konfigurationen zwischen den Standorten?
7. Wie testen Sie die Sicherheit der gleichen Services an verschiedenen Standorten?
8. Ist Ihr Sicherheitsteam in der Lage, den Haupt- und den Neben-/Backup-Aufbewahrungsort mit demselben Maß an Transparenz zu überwachen?
9. Decken Ihre Erkennungssysteme alle Standorte ab? Werden Bedrohungen für die sekundäre Website/das Backup erkannt?
10. Wie schützen/isolieren Sie Ihr(e) Backup-System/Lösung?
11. Wie können Sie Ihre Management-Pläne von den Hauptnetzen isolieren?

Über Infopulse

Infopulse, Teil des führenden nordischen Unternehmens für digitale Dienstleistungen Tietoevry, ist ein internationaler Anbieter von Dienstleistungen in den Bereichen Softwareentwicklung, Anwendungsmanagement, Cloud und IT-Betrieb sowie Cybersicherheit für kleine und mittelständische Unternehmen und Fortune-100-Unternehmen in aller Welt. Das 1991 gegründete Unternehmen hat ein Team von über 2.300 Fachleuten und ist in 7 Ländern in Europa und Nord- und Südamerika vertreten.

Zahlreiche etablierte Marken vertrauen auf Infopulse, darunter BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Offshore Norge, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group und andere.

Weitere Informationen finden Sie unter **www.infopulse.com**

Kontakt

PL +48 (606) 291-154

DE +49 (69) 505-060-4719

US +1 (888) 339-75-56

UK +44 (8455) 280-080

UA +38 (044) 585-25-00

BG +359 (876) 92-30-90

BR +55 (21) 99298-3389

info@infopulse.com