VERITAS

リカバリの確実な実施

明確なリカバリ計画の策定

ダウンタイムやデータ盗難に繋がる障害を回避するために、ベリタスのサイバーリカバリチェックリストを活用して、耐障害性の強化に向けて今すぐ備えましょう。

フェーズ 1

フェーズ 1 ¦ 30 日

基盤の確立

ビジネスを保護するために以下の点について検討しましょう。

- すべてのワークロードの保護ポリシーと保持ポリシーを作成します。
- 改ざん不可能なストレージを使用します。
- 3-2-1 ルールに沿ったバックアップ戦略を策定します。3 つのコピーを 2 つの形式で作成し、1 つは仮想エアギャップや物理エアギャップなどを活用したオフサイトに保管します。また、SaaS のテナント分離が不可欠です。
- セキュリティ制御 (MFA、MPA、ネットワークのセグメント化、RBAC、暗号化など) を適用します。
- 専用アプライアンスを強化します。
- AI を活用した異常検出を導入します。
- マルウェアの検出とデータ保持ルールを実装します。
- 常に最新のソフトウェアとセキュリティパッチを利用します。

フェーズ 2

フェーズ 2 ¦ 60 日

リスクをプロアクティブに管理

人、プロセス、テクノロジに重点を置きます。

- 「保護されていない」重要な資産を特定します。
- ダークデータ評価を実施します。
- 機密データを見つけて分類します。
- リスクの高いエンドユーザーの行動を特定して監視します。
- 分離型リカバリ環境 (IRE またはクリーンルーム) を構築します。
- リカバリ用のランブックを作成し、業務に優先順位を付けます。
- SecOps チームと連携し、インシデント対応用のプレイブック (SIEM / SOAR / XDR 統合など) を作成します。

フェーズ 3

フェーズ 3 ¦ 90 日

改善、リハーサル、適用

- SLA に従い、バックアップ成功率 100% を目指して、データ保護ポリシーを調整します。
- AI を活用した異常検出を微調整します (誤検出 / 検出漏れの排除)。
- 業務を中断しないリカバリリハーサルなどの机上演習を実行します。
- リカバリのリハーサルを行い、結果を検証します。

サイバーリカバリチェックリストの詳細を確認する ›

VERITAS

1 (866) 837-4827 • www.veritas.com/ja/jp