デジタル 資産 セキュリティ チェックリスト

デジタル 資産 ベンダー管理

- ☐ お客様は、ドメイン、ドメインネームシステム(DNS)、セキュアソケットレイヤ(SSL)のプロバイダーを把握していますか。
- ☐ お客様の全てのデジタル資産プロバイダーが、企業レベルのサポートを24時間365日ご提供していますか。
- ☐ お客様の全てのデジタル資産プロバイダーは、ISO27001認証のデータセンター、SOC 2®コンプライアント、第三者の侵入、SQLインジェクションおよびXSSなどを含む脆弱性テストやセキュリティテストなどのシステム保護に重点を置いた投資を行ってきていますか。
- ☐ お客様の全てのデジタル資産プロバイダーは、スタッフトレーニングにしっかりと投資をしてきていますか。(例:定期的なフィッシング詐欺の電子メールテスト、外部ネットワーク(リモート)へアクセス時の二要素認証を含むセキュリティトレーニング、フィッシングへの意識向上)、
- ☐ お客様の全てのデジタル資産プロバイダーは、お客の保護にしっかりと投資をしてきていますか。(例:IPバリデーション、二要素認証、権限コンタクトポリシー、オーダーやリクエストは電話ではなく必ず書面で行う、フェデレーテッドアイデンティティ)
- ☐ どのプロバイダーも、フィッシング詐欺、ソーシャルエンジニアリング、DNSハッキング、もしくは分散サービス妨害 (DDoS) 攻撃に屈した記録はありませんか。
- ☐ お客様の全てのデジタル資産プロバイダーは、単に第三者の認定を利用するのではなく、彼ら自身が認定を受けたプロバイダーですか。例:レジストリから直接認定を受けそれを活用するドメインプロバイダー、認定局 (CA) から認定を受けた証明書プロバイダー。

ドメイン 管理

- ☐ お客様は全てのドメインネームのポートフォリオを把握していますか。
- ☐ 信頼のおけるプロバイダーと決まった場所での自動更新ポリシーを結んでいますか。
- ☐ 全ての社員は新規ドメイン登録時の一元化処理の訓練を受けており、順守していますか。
- ☐ WHOISテンプレートや、登録した時点で提供されなければならないユーザ定義フィールドに明確なガイドラインが示されていますか。
- ☐ 会社の一元化ポリシーから外れるような会社登録を特定する手続きを行っていますか。

DNS 管理

- ☐ お客様は全DNSプロバイダーのポートフォリオを把握していますか。
- ☐ 信頼できる100%アップタイム保証がある企業レベルでないDNSのドメインを特定する手続きを行っていますか。
- ☐ 全ての社員は全ての新しいバイタルドメインを企業レベルのDNS上に設定する訓練を受け、それを順守していますか。

SSL 管理

- ☐ お客様は全てのSSLプロバイダーを把握していますか。
- ☐ 全ての社員が、新しい証明書の購入や、古い証明書の交換時の一元化処理の訓練を受けており、順守していますか。
- ☐ 会社の一元化ポリシーから外れるSSL証明書を特定する手続きを行っていますか。

バイタル(ビジネス上重要な)ドメイン 管理

- ☐ 全てのバイタルドメインを迅速に特定し、それらが安全であると実証できますか。
- ☐ お客様のバイタルドメインの全DNSプロバイダーは、信頼性のある100%アップタイムを保証し、そのしっかりした記録がありますか。
- ☐ 全てのバイタルドメインは、適格な企業レベルのSSL証明書を使用していますか。
- ☐ 全てのバイタルドメインは、DNSキャッシュポイズニングを防ぐため、ドメインネームのシステムセキュリティ拡張を利用していますか。
- ☐ 全てのバイタルドメインは、DNSハイジャックを防ぐため、マルチロックを採用していますか。
- ☐ 全ての必須ドメインは、電子メール認証サービスを採用していますか。

スレッドミティゲーション(脅威緩和) 続き

- ☐ DNS以外の他のサーバーを保護するために、追加DDos緩和サービスを使用していますか。
- ☐ フィッシング攻撃からの脅威を最小限に抑えるため、フィッシングの監視や削除サービスと合わせて、電子メール認証サービスを利用していますか。

日本語対応可 +852 2345 7555 cscdigitalbrand.services/jp