The bridge to possible

シスコの金融業界向けソートリーダーシップ

金融機関のレジリエンスを確保

金融機関のレジリエンスを確保

金融業界のインフラがレジリエンス（回復力）を備えていることは、世界経済が機能するうえで非常に重要です。金融業界のインフラに影響を与える外的要因と内的要因の規模が拡大しスピードが増すにつれて、リスク管理は今までになく重要になっています。金融業界はこの 20 年間、重大な信用リスク、市場リスク、事業運営リスクを引き起こした前例のない予測不可能な出来事を乗り越えてきました。

今日の金融機関は、大規模なリスクを軽減し、予測不可能な変化の中でビジネスを保護する機能を備えた、回復力の高い運用モデルを必要としています。そのためには、金融サービスのデジタル化の推進、従業員のより一層の分散化、クラウドの利用による競争力の確保が必要であり、これに伴う新たなサイバーリスクに対処しなければなりません。

規制環境の変化

サイバーリスクは、金融業界において規模とスピードの点で最も増加している事業運営リスクです。サイバー犯罪者に最も狙われやすい業界の 1 つが金融業界なのです。データ侵害が発生すると多大な影響が生じるため、金融業界は、サイバーセキュリティの習熟度や保護、各種基準との整合性を高いレベルで保証しています。たとえば IT リスクに関する国際標準化機構(ISO) 27000 シリーズや米国国立標準技術研究所（NIST）のサイバーセキュリティ フレームワークなどの基準です。

規制当局は最近、増加するサイバーリスクに対応するために金融機関や監査人向けのガイダンスを更新しました。米国当局動向情報 連邦金融機関検査協議会（FFIEC）は、米国の銀行向けの情報技術検定ハンドブック『Architecture, Infrastructure, and Operations』の更新版と、金融機関のサービスおよびシステムへの認証とアクセスに関するガイダンスを発行しました。これらの更新は、アクセスや認証、クラウドコンピューティング、サードパーティ提供のサービスなどデジタル金融サービス機能に関連するリスクが増大している状況に対処することを目的としたものです。英国では金融行為規制機構（FCA）が、将来の規制監査に先立って、テレワークまたはハイブリッドワークを検討している金融機関向けの最初のガイダンスを発行しました。世界中で、規制当局や中央銀行による同様の措置が講じられています。

FFIEC

FFIEC は、米国政府の正式な省庁間機関であり、金融機関の連邦審査に関する統一原則、基準、および報告書様式を規定する権限を与えられています。FFIEC が作成したサイバーセキュリティ評価ツールは、金融機関のサイバーセキュリティ体制を評価するために広く使用されています。

FFIEC の評価ツールの概要を説明するシスコのブログ記事をご紹介します。

- FFIEC の規制に関する基本情報
- FFIEC サイバーセキュリティ成熟度評価ツール
- FFIEC のハンドブック『Architecture, Infrastructure, and Operations』の紹介

サイバー犯罪者はゼロデイ脆弱性に目を付けているため、金融サービス情報共有分析センター (FS-ISAC) はサイバー脅威の活動が増加すると予想しています。FS-ISAC は、7,000 の金融機関で構成される業界コンソーシアムです。

ソーシャルエンジニアリング、マルウェア、分散型サービス拒否(DDoS) 攻撃は、業界全体で最も一般的な持続的脅威です。2022 年以降の FS-ISAC の予測は、以下のような、金融機関にとって厳しいサイバーリスク環境を反映したものです。

- 地政学的緊張が国家によるサイバー攻撃に反映される
- 国家が金融業界のサプライチェーンに影響を与える
- ランサムウェアグループが今後も専門化し続ける
- サードパーティのリスクが今後も金融機関を脅かす
- ゼロデイ脆弱性が増加する
- 規制当局が管理を厳格化する
- インシデント対応が高度化する

デジタル化と複雑化

デジタル化が促進されたことで、それに伴う急速な IT 環境の変化と複雑さの増大に対する認識が高まりました。デロイト金融サービスセンターと FS-ISAC によると、これは金融機関にとってサイバーセキュリティの最大の課題です。新しい製品やサービスの開発におけるクラウド、データ分析、AI/ML の利用拡大、テレワーク環境とハイブリッドワーク環境に対するサポートの必要性により、保護すべき対象の範囲と規模が拡大しています。

IT リーダーや事業運営リスク担当のリーダーは、この増大する保護対象を管理し、多種多様なセキュリティソリューション間でセキュリティをオーケストレーションする際の複雑さを軽減するために、セキュリティを企画・設計段階から確保するための方策である「Security by Design」のアプローチに注目しています。セキュリティの専門家は、組織全体で拡張することのできる、包括的で管理しやすい統合ソリューションを提供する機能を必要としています。その目的は、セキュリティの可視性を高め、次に何が起こるかを予測し、適切な行動を取り、組織全体のサイバーレジリエンスへの投資を強化することです。

急速なデジタル化と普及促進により複雑さが増大

金融機関向けのセキュリティ対策

Cisco® Secure のポートフォリオでは、クラウドエッジからネットワーク、アプリケーション、ワークロード、エンドユーザーやデバイスまで、あらゆるものを保護する業界トップクラスのセキュリティを提供しています。

- Cisco Secure XDR は、Extended Detection and Response (XDR) 機能により可視性と実用的なインサイトを提供するものです。セキュリティチームが脅威を追跡、調査、修復しやすくなります。
- Cisco Secure の接続ソリューション は、セキュアアクセス サービスエッジ (SASE) の機能を提供し、ネットワーキング機能とセキュリティ機能をクラウドで集約して、ユーザーがどこにいてもシームレスかつ安全にアプリケーションにアクセスできるようにします。
- シスコのゼロトラストは、ユーザーやデバイス、場所を問わず、すべてのアプリケーションと環境へのあらゆるアクセスを保護する包括的なソリューションです。
- Cisco Secure Firewall は、お客様の計画策定、優先順位付け、ギャップの解消、災害からの復旧をさらに強力にサポートします。現在は、従業員、データ、支店やオフィスが世界中に分散しています。このような状況では、ファイアウォールは万全を期す必要があります。

パートナーになる

サイバーリスクをめぐっては今後も課題が生じることが予想されますが、同業他社や規制当局、シスコのようなセキュリティソリューション プロバイダーと連携することで、金融機関のサイバーリスク管理体制が整います。

詳細情報

金融機関向けのサービスとテクノロジーの詳細は、シスコ ファイナンス サービス ソリューションに掲載しています。サイバーレジリエンスの詳細については、サイバーレジリエンスのページをご覧ください。

C11-3578322-00 04/23