サイバーセキュリティー特集

新ガイドラインへ対応

国内企業へのサイバー攻撃が猛威を振るい、金融界も被害にさらされている。5月には、金融機関から業務を受託する情報会社でランサムウエア（身代金ウイルス）感染が発生。後に、34機関の情報流出が明らかになった。金融庁は金融機能の安定確保や預金者の保護を目的に10月4日に新たなガイドラインを公開。経営層へサイバーセキュリティー規程や業務プロセスを年に1回以上、見直す指針を示した。金融機関の業務がデジタル化へ移行するなか、セキュリティー対策を強化する3社を紹介する。

APIの脆弱性を克服

マクニカソリューションズ（横浜市）は、アカマイテクノロジーのサービスを提供し、API（データ連携の接続仕様）のセキュリティー対策を万全にする。アカマイ社の調査では、攻撃者がAPIを狙う割合はウェブ攻撃の約4分の1を占め、金融機関にも影響が及ぶという。同社のサービスは、自社のAPIを全て探索し、一覧表を作成するほか、使われていないものも探索できる。また、150以上の自動セキュリティーテストを開発に組み込める。機械学習を利用することで、データ改ざんや漏えいなどの脆弱性や攻撃を特定することも可能だ。マクニカソリューションズは「これまで対応しきれなかったAPI特有の脆弱性に対し、包括的なソリューションを提供できる」としている。国内の複数行が関心を示し、商談中だ。

金融機関の業務はデジタルテクノロジーを活用しており、より一層のセキュリティー対策が求められる

多層防御で対策を強化

金融機関のシステム運用の安全確保をサポートするのはエンカレッジ・テクノロジ（東京都）。同社は特権ID管理に必要な機能を網羅した「ESS AdminONE」を提供している。同サービスは多要素認証やパスワード管理などによる多層防御で攻撃対策を強化するもの。管理者が作業者に代わってログインすることで、厳重にパスワードを管理し、アクセスを制御する。パスを非表示にし、覗えいを防ぐ。アクセス許可は誰がどの特権IDを利用可能か設定し、不正アクセスを防止する。ログイン失敗時の履歴収集にも対応。パスワード払当たり攻撃の際に、ログイン失敗時の履歴を定期的に収集し、兆候を察知できることも特徴だ。同社の製品は2000以上の金融機関で導入が進んでいる。

仮想パッチで環境保護

トレンドマイクロ（東京都）は正規のセキュリティーパッチをすぐ導入できない環境へ、暫定的なセキュリティーを担保する「仮想パッチ」で金融機関の脆弱性対策を強化する。閉域環境や、サポートが終了したOSに有効だ。

金融機関で導入が進むのは「TippingPoint」と「Deep Discovery Inspector」。TippingPointはレガシーシステムや勘定系システムに有効で、広範囲で不正なアクセスや異常を検知する。同社の脅威インテリジェンスを活用し、怪しい通信をブロック可能。運用負担が少なく、正規のパッチが提供される90日以上前から保護できる。Deep Discovery Inspectorは内部の通信をすべて監視し、異常を検知できる。北国銀行で導入されており、金融庁の新ガイドライン2項、サイバーセキュリティー管理体制の要件を満たすため、金融機関からの問い合わせが急増中だ。

◇

紹介したサービスの詳細資料は、QRコードからダウンロードできます。