Cortex Xpanse_WP_Perimeter Exposure-JP

ネットワーク境界の脆弱性に対する戦術的ガイド

ホワイト ペーパー

よくある境界
脆弱性とその対策

特定のタイプの攻撃は、手口が単純で把握が容易です。たとえば、電子メール フィッシングはユーザーを騙してリンクを開かせたり、認証情報を入力させます。分散型サービス拒否攻撃 (DDoS) は Web サイトに大量のトラフィックを送信して、本来の通信を妨害するものです。

その一方で、把握が難しいネットワーク攻撃も存在します。そうした攻撃の容易さや影響の性質は、脆弱性の内容に大きく左右される可能性があります。このホワイト ペーパーでは、最も一般的な境界脆弱性を 5 つ取り上げ、その対策を解説します。

複雑なネットワーク境界の脆弱性に対する備えを

企業の間で急速に普及しているクラウドは、生産性と業務効率を高める反面、セキュリティ リスクをもたらす可能性があります。たとえば、クレジット カードとメール アドレスさえあれば、従業員はセキュリティ チームの許可や補助を受けることなく、クラウド　ベースの製品やサービスを簡単に導入できます。しかも、その事実がセキュリティ　チームに通知されない場合さえあるのです。こうした事例は、企業のクラウド上の攻撃対象領域が拡大し、気づかない間に未知の資産が増える原因のひとつです。
このホワイト　ペーパーでは、従来のソリューションがクラウドでは機能しない理由と、そうした弱点を克服する方法を解説します。また、クラウド移行プロジェクトで発生する重大な問題を監視・解決する方法についても解説します。