サイバーセキュリティ最前線

DXを推進する中小企業こそ「セキュリティの穴」の発見が急務!!

昨今、スタートアップ企業や中小企業によるDX（デジタルトランスフォーメーション）が全国各地で加速している。そこで、あらためてDXをすすめる際のセキュリティ上の注意点やセキュリティ対策について紹介したい。

2024年上半期のセキュリティインシデント

2024年上半期にセキュリティインシデント（情報セキュリティに関連する事件・事故）に遭った企業（公表事例）を編集部で調べたところ、当事者側の過失（紛失や誤設定）を除いて134件が確認された。そのうち約3分の1にあたる45件はウェブサイトへの攻撃で、さらにその15件はオンラインショップに関連するものだった。警察庁によると、2023年のランサムウェア（身代金要求型ウイルス）の被害件数は197件、不正アクセス禁止法違反の検挙数は521件となっているため、実際にはまだまだ多くの被害があるはずだ。

ウェブサイトへの攻撃では、積水ハウスやKADOKAWAなどの有名企業だけでなく、中小企業などの被害事例も目立った。とくにオンラインショップについては特定分野に特化した専門的な小規模サイトなどが被害を受けていた。

こうした被害の背景にはDX（デジタルトランスフォーメーション）の急速な進展があるかもしれない。長年にわたってITセキュリティに取り組む㈱ブロード（東京都千代田区）は「本来はDXと並行してセキュリティ対策をすすめなければならないが、全体的にセキュリティ侵害をきちんと想定していないケースが多く、『セキュリティの穴』が存在してしまっている」と指摘する。

とくに注意が必要なのが中小企業のウェブサイトやオンラインショップだ。「自分たちのサイトは攻撃対象になるような規模ではない」といった考えからセキュリティ対策をおろそかにするケースが多いからだ。しかし「インターネットでビジネスを行う際には万全の心構えと対策が必要。サイバー犯罪集団の活動には特定企業を狙うケースがある一方、AI（人工知能）などを使い、自動的に攻撃経路が存在するサイトを発見・攻撃するケースもあることを忘れてはならない」とブロードは警鐘を鳴らす。

多角的なセキュリティ対策を

サイバーセキュリティに関するリスクを軽減するため、多くの企業はこれまで脆弱性管理に注力してきた。しかし、使用されるソフトウェアのセキュリティ上の欠陥や設定ミスを調査し、すべてに対策を講じることは容易ではないし、対策が必要な部分を的確に見出すには非常に高度なスキルが求められる。

そこで、注目されてきたのがペネトレーションテスト（侵入検査）だ。これは専門家による侵害経路を探す検査で、通常、定期的に行われているもの。しかし、この手法においても高度な技術が必要になるため、対応可能な人材がかぎられるし、進化しつづける攻撃側の手口に追いつくことが困難という問題がある。

だが、ここにきて「AIの進化でペネトレーションテストをより簡便にできるようになった」という。たとえば、とブロードの担当者は米国のRidge Security社製の『RidgeBot』の使用をすすめる。AIが最新の攻撃パターンを反映したペネトレーションテストを自動的かつ継続的に運用してくれるからだ。しかし、「サイバー攻撃の多くがメールに添付されてくる」ことをご存じか。それを防御するにはHP社製の『HP SCE』もオススメ、だと話す。ITを活用した新規事業やDXを推進する際には、こうした観点からセキュリティ対策を盤石にしてほしい。