ビジネスシーンで役立つ極意（第3回）

セキュリティのプロが指摘する企業がとるべき対策

2023.02.21

企業環境の変化に伴って複雑化・高度化するテクノロジーの活用。新型コロナ禍への対応として浸透しつつあるリモートワーク・テレワークをはじめ、IoT機器活用などによるDX推進が生産性や利便性を高めている。一方、日々、サイバー攻撃の脅威も増している。では、企業はどのような対策を考えればよいのか。今回は、実践的なサイバートレーニングを企画・推進する「ナショナルサイバートレーニングセンター」を率いる国立研究開発法人情報通信研究機構（NICT）の園田道夫氏に近年の攻撃事例やその備えとして企業が取るべき行動などついて伺った。

――企業を取り巻くサイバー攻撃の脅威は、以前と比べてどう変化しているのでしょうか。

近年、DXの推進が企業成長を考える上で重要な要素となり、企業のIT資産が増加しています。このため、サイバー攻撃から守らなければならない対象が拡大し、以前よりも脅威が増していると考えられます。例えば、リモートワーク・テレワークの浸透によって、VPNの利用も裾野を広げました。この脆弱性を利用したインシデントも増加傾向にあります。

例えば、2020年5月頃の大手電機メーカーへのサイバー攻撃では、VPN装置が狙われたとの指摘もあります。攻撃者側は企業環境の変化を俊敏に読み取り、攻撃を仕掛けるべきポイントを綿密に分析しています。その上で弱い部分を的確・巧妙に狙います。このため、どのような規模の企業であっても攻撃の対象となり得ます。総務省や警察庁をはじめ、日本経済団体連合会（経団連）が「経団連サイバーセキュリティ経営宣言2.0」（2022年10月）を発表するなど、さまざまな団体が警鐘を鳴らしているのはこうした背景からです。

また、攻撃者側の分業化・高度化も進んでいます。10年程度前からこの兆候が現れ、誰かが作ったツールを誰かのサポートを受けて使えば誰でもサイバー犯罪に手を染められる状況です。ツールも洗練され、攻撃自体の効率化が確立されつつあります。「攻撃の成功後にどうするか」も犯罪業界に知見が蓄積されてきました。

具体的には「ウィーケストリンク（Weakest Link）」という考え方です。まずは弱いところに入り、関連する人や組織を調べて、使えそうな情報がある企業・団体を洗い出して収集する。こうして情報をかき集め、ビッグデータ的に解析して次の攻撃に生かしたり、データを人質にとったり、欲しがる誰かに売りつけたりします。収集した情報の生かし方にも、攻撃者側では分業化の流れの中でプロフェッショナルが生まれ、巧妙化が加速しています。

●サイバー攻撃を仕掛ける攻撃者の類型（イメージ）

主な攻撃主体	攻撃の主な動機
国家や国家が支援する攻撃組織	政治的・地政学的な動機から攻撃を仕掛ける
犯罪グループ	金銭的な利益を目的として攻撃を仕掛ける
テロリスト	社会的・政治的な主張を目的として攻撃を仕掛ける
ハクティビスト	社会的・政治的な主張を目的とする。「アクティビスト（社会活動家）」と「ハッカー」を掛け合わせた言葉。国際ハッカー集団「アノニマス」なども含まれる
愉快犯	知的好奇心や技術検証のために攻撃を仕掛ける
悪意ある個人	同僚のメールを盗み読むなど悪意を持って攻撃を行う。所属する企業・団体に不満を抱く従業員などが含まれることもある

※取材をもとに作成

――近年の具体的なサイバー攻撃の事例についてについてお聞かせください。… 続きを読む