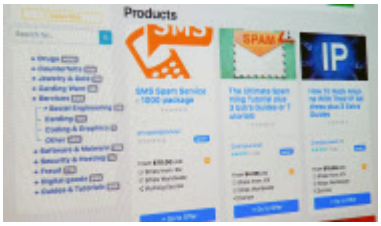
日本経済新聞

サイバー攻撃、専守防衛は限界　「敵陣潜入」新潮流に

2018/10/31 12:05 | 日本経済新聞　電子版

企業のサイバー攻撃対策に新たな潮流が生まれている。犯罪者集団が情報をやりとりする闇サイト群「ダークウェブ」に潜入し、人工知能（ＡＩ）などで情報を分析して攻撃の予兆をつかむという手法だ。情報流出などのリスクが高まるなか、巧妙化するサイバー攻撃に対して「守り」だけでは限界を迎えている。企業にとっては、事前に入手した情報を生かすための専門人材の確保が課題になる。

■「標的型攻撃」、１カ月前に予兆



サイバー攻撃用ツールなどが集まるダークウェブの情報を収集し、事前に対策を打つ「脅威インテリジェンス」と呼ばれる手法が新たな潮流に

ある大手金融会社のＩＴ（情報技術）部門に８月、内部情報を盗むウイルス付きメールを送りつける「標的型攻撃」に狙われる可能性が高いとの連絡が入った。東京五輪関連イベントへの招待を装ったメールのサンプルなどがダークウェブで売買されていることを、セキュリティー会社がつかんだ。

この金融会社は攻撃メールを検出する機能を社内のセキュリティー機器に追加。９月に予想通り攻撃を受けたが、先回りしての対策が功を奏し被害を免れたという。

サイバー攻撃の手口や標的を事前に予測するこうした手法は「脅威インテリジェンス」と呼ばれる。検索サイトなどにも表れず特別なソフトウエアがなければアクセスできないダークウェブを巡回し、狙われている企業や攻撃用ツール、犯罪者の目的などの情報から将来の攻撃を予測する。「ＡＩなどで分析作業がある程度自動化できるようになった」（ＩＤＣジャパンの登坂恒夫リサーチマネージャー）ことで予測の精度が高まっている。

2017年に世界で猛威をふるい、ホンダの工場が生産を一時停止するなど企業活動にも影響を与えたランサムウエア（身代金要求型ウイルス）「ワナクライ」。シンガポールのセキュリティー企業、アントゥイットホールディングスでは「数カ月前に予兆をつかんだ」（同社日本法人の剣持祥夫代表取締役）。最近では、サーバーの管理ソフトの弱点を突く攻撃用ソフトやその管理ソフトを使う企業のリストが頻繁に売買されている状況から攻撃が近いと予測。弱点を埋める対策ソフトの導入などを助言しているという。

こうしたサービスは米国やイスラエルなどのセキュリティ会社が先行し、世界的に広がりを見せている。米グランド・ビュー・リサーチによると、脅威インテリジェンス関連の16年の市場規模は16年の30億2000万ドル（約332億円）。年平均17%増の勢いで成長し、25年に126億ドルに達すると予想する。

日本でもセキュリティー大手のラックが８月に参入したほか、ＳＯＭＰＯホールディングス傘下のＳＯＭＰＯリスクマネジメント（東京・新宿）が2019年１月にサービス提供を始める。この分野で世界最大手とされる米レコーデッド・フューチャーも日本法人を設立した。

サービスの利用料金は１年間当たり数百万～1000万円程度で、セキュリティー意識が高い大手金融やサイバーテロに狙われやすいインフラ企業、あらゆるモノがネットにつながるＩｏＴ導入を進める製造業を中心からの引き合いが増えているという。

■専門人材の確保がカギに

総務省によると、国内の半数以上の企業は過去１年間に何らかのサイバー攻撃の被害に遭っている。従来のサイバー対策は犯罪者の攻撃を素早く検出して食い止める「専守防衛型」だった。ただこれだけでは限界を迎えつつある。

野村総合研究所系のセキュリティー企業、ＮＲＩセキュアテクノロジーズの斎藤大地氏は「取引先や上司になりすまして偽メールを送るビジネスメール詐欺など、攻撃の手口が多様化している」と指摘する。ＡＩやＩｏＴをビジネスに取り入れる企業が増え、守るべき対象も増えている。全ての社内システムをあらゆる攻撃から守るのではなく、どこを重点的に守るかという発想の転換も欠かせなくなっている。

企業にとっては、事前に得た情報を生かして迅速に対策を打てるかが課題になる。サイバーディフェンス研究所の名和利男上級分析官は、「公的組織が無償公開するセキュリティーの情報さえ満足に使いこなせない企業が多い」と指摘する。

ＫＰＭＧコンサルティングが国内の上場企業と売上高400億円以上の未上場企業に４～５月に実施した調査では、「知見のある実務担当者が足りない」ことをサイバーセキュリティ対策の課題に挙げる企業が約60%に達した。新潮流がさらに広がるかは、企業が有能な人材を確保できるかにかかっている。（島津忠承）