加害者にならないためのサイバー攻撃防止法（第6回）

止まらない脅威の多様化。対策概要を解説

2017.05.31

- 企業が取り組むべき情報セキュリティー対策が多岐にわたっている。情報処理推進機構（IPA）が発表した「情報セキュリティ10大脅威 2017」（2017年3月）によれば、企業などの組織への脅威としては「標的型攻撃による情報流出」が1位となった。2016年に7位だった「ランサムウェアによる被害」が2位に急浮上、以下「ウェブサービスからの個人情報の窃取」「サービス妨害攻撃によるサービスの停止」「内部不正による情報漏えいとそれに伴う業務停止」と続く。第8位には「IoT機器の脆弱性の顕在化」が入り、話題のIoTに対する情報セキュリティー対策も考慮しなければならない。多様化し続ける攻撃に、企業としてどう対策を施すべきなのだろうか。

脅威ごとに必要な対策も変わる

特定の組織に狙いを定めて、さもありそうなシナリオを作って社員をだます「標的型攻撃」、悪意を持ったプログラムでパソコンなどを使えなくさせて身代金を取ろうとする「ランサムウエア」、Webサイトのセキュリティー上の弱点を狙って個人情報を盗み取る「脆弱性攻撃」と、主要な脅威だけでもその攻撃手法は異なる。

脅威の手法が異なると、それを防御する仕組みも当然違ってくる。標的型攻撃に遭っても被害を最小化できるようにメールの添付ファイルをいったん隔離する、ランサムウエア対策にバックアップソリューションを活用する、脆弱性攻撃にはアクセスログのリアルタイム分析を導入する、などが考えられる。専任の担当者が24時間365日監視を行うSOC（セキュリティーオペレーションセンター）と呼ばれる組織を活用するといった施策もある。

自社でツールを選んで導入するのは難しい

(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start': new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0], j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src= 'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f); })(window,document,'script','dataLayer','GTM-K9XWQF5'); !function(f,b,e,v,n,t,s) {if(f.fbq)return;n=f.fbq=function(){n.callMethod? n.callMethod.apply(n,arguments):n.queue.push(arguments)}; if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0'; n.queue=[];t=b.createElement(e);t.async=!0; t.src=v;s=b.getElementsByTagName(e)[0]; s.parentNode.insertBefore(t,s)}(window, document,'script', 'https://connect.facebook.net/en_US/fbevents.js'); fbq('init', '996021997138363'); fbq('track', 'PageView'); var yahoo_retargeting_id = 'R26PZOZHRX'; var yahoo_retargeting_label = ''; var yahoo_retargeting_page_type = ''; var yahoo_retargeting_items = [{item_id: '', category_id: '', price: '', quantity: ''}]; /*]]> */ window.dataLayer = window.dataLayer || []; function gtag(){dataLayer.push(arguments);} gtag('js', new Date()); gtag('config', 'AW-686888305'); …
続きを読む