セキュリティ

ITマネジメント（内部統制）

ターゲットは2020年？

IoT、リモートの普及で、サイバー攻撃への対策が急務に

2019年、2020年に様々なイベントが立て続けに日本で開催されます。いまから楽しみにしている方も多いかと思いますが、一方で注目度の高いイベントだけに、サイバー犯罪者は日本へ攻撃を仕掛けるチャンスと考えています。そこで2020年に向けて増加すると思われるサイバー攻撃への対策について解説します。

注目のイベントはハッカーにとっても“祭典”

注目度の高いイベントが開催されると、多くのファンが現地に詰めかけるほか、テレビなどの中継映像を多くの人が視聴します。サイバー犯罪者は、これを絶好の機会と考えているのです。個人で活動しているサイバー犯罪者にとっては、こうしたイベントが行われている地域を攻撃し、それが報道されれば、己の名を馳せることになります。組織化したサイバー犯罪集団にとっては、組織のアピールとなり、スポンサー獲得につながります。

イベントを開催する国では、サイバー攻撃が日を追うごとに増加し、会期中にピークを迎える傾向にあります。中でも多いのは、偽のチケット販売や中継動画などのフィッシングメールでしょう。これは、格安のチケットや動画などを売り込み、代金をせしめるという詐欺です。また、テレビ局や動画サービス会社などへのサイバー攻撃も多発する傾向にあります。たとえば、それらの会社へDDoS攻撃を仕掛けてサービスを利用不能に追い込みます。その後、攻撃を止めることと引き換えに金銭を要求することでしょう。

さらに、「ハクティビスト」のサイバー攻撃も増加することが予想されます。ハクティビストとは、特定の思想を持った活動家のことで、ハッカー+アクティビストの造語です。ハクティビストのサイバー攻撃は、政府機関や企業などのWebサイトを改ざんして、自分たちの思想などをアピールする内容に書き換えたり、同様の内容のスパムメールを大量送信したりします。

かつてない手法のサイバー攻撃が行われる可能性も

近年開催されているイベントのいくつかはサイバー攻撃の対象となってきましたが、2019年から2020年で大きな変化があると予測されています。その理由の1つが、開催地が日本であるという点です。

日本はGNI(国民総所得)が世界第3位の経済大国であり、世界的な規模の企業の拠点が数多く存在します。当然、(実際はともあれ)それらに堅牢なセキュリティ対策が行われていると、ハッカーは考えているでしょう。そんな国で大規模なサイバー攻撃を成功させることができれば、サイバー犯罪者は実力を大いにアピールできます。こうした背景から、前回とは比較にならないほどの質と量の攻撃が行われるおそれがあるのです。

そして、もう1つの理由がIoT(Internet of Things ／モノのインターネット)の普及です。2020年は、現在よりもはるかにIoTが普及しているでしょう。テレビ中継・報道、運営など、さまざまな場面でIoTの技術が使われるはずです。それ以外でも社会システムや観衆を含む一般人へも普及しているでしょうから、それらもターゲットにされる可能性があります。IoTは適用範囲が非常に幅広く、攻撃を受けた場合の被害も甚大になる可能性があるため注意が必要です。

ポイントは、IoT機器やリモートデバイスの「棚卸し」

それではこれからの2年に向けて、企業はどのようなセキュリティ対策をとればよいのでしょうか。

現状、サイバー攻撃はメールとWebサイトによる脅威が大きな割合を占めています。特にメール経由は、全体の9割を占め、巧妙化･複雑化しています。「なりすまし」などの手法を活用した攻撃も増えているのです。そのためメールの文面に乗せられてうっかり添付ファイルを開いてしまったり、リンクをクリックしてマルウェアに感染するなどのケースが後を絶ちません。やはり、「請求書」「見積書」「(宅配便の)不在連絡」などを騙るメールが届けば気になってしまうので、こうした被害がなくならないのでしょう。

メール経由では新種のマルウェアもあります。マルウェアは表向きには問題を起こさず、その裏でシステムの脆弱性を悪用して感染を広げる活動を行うものです。ウイルス対策ソフトによる防御を回避されてしまう可能性が高い攻撃の1つです。さらに最近ではSNSを利用したアタックも増えているため、こうした攻撃に対応した最新の製品・サービスを導入した上で、従業員へ適切なセキュリティ教育を施す必要があります。もちろん、DDoS攻撃やWebサイト改ざんなどへの対策も重要です。

IoT機器では、ユーザーがインターネット接続を意識せずに使用しているケースが多く、攻撃に気づいていないことがあります。家電への攻撃方法としては、家庭用のブルーレイレコーダーへインターネットから不正アクセスを実施し、マルウェアに感染させ、DDoS攻撃に利用する手法が確認されています。企業においても、部署単位で無許可の無線LANアクセスポイントやリモートアクセス機能を持つ外付ハードディスクを設置していたり、会議室に家庭用ブルーレイレコーダーを設置していることもあるでしょう。これによって外部から不正にアクセスされる危険性が高まります。

昨今では、従業員が個人保有のスマートフォンやタブレット、ノートPCなどのリモートデバイスを職場に持ち込み、業務使用するBYOD (Bring your own device)も拡大しています。それらをオフィス外で使用する時、暗号化が施されていないWi-Fiサービスに接続していないでしょうか。

こうした攻撃への対策としては、まず社内にあるIoT機器や個人保有のリモートデバイスを洗い出し、設定を確認したり、ファームウェアをアップデートする、あるいは社内ネットワークと直接接続しないようにするなど、セキュリティーリスクを軽減するための「棚卸し」が第一歩となるでしょう。

関連サービス

マイセキュア ビジネス	クラウドにある最新のセキュリティテクノロジーを最小の管理コストで実現します。 先進の「ファイル形式＆行動認証テクノロジー」を、クラウドコンピューティングのパワーと組み合わせることで、既知の脅威をブロックし、ゼロデイ攻撃を防止します。
Arcstar Universal One クラウドWi-Fi	アクセスポイントのレンタルから認証基盤まで、セキュアなWi-Fi環境に必要なすべてをNTTコミュニケーションズが一元的に提供します。 さらにアクセスポイント設置やLAN配線工事などを行い、ネットワークと合わせて24時間365日保守対応するプランも提供することで、お客さまの負担を軽減し最適なWi-Fi環境の構築を実現します。
WideAngle マネージドセキュリティサービス	人工知能搭載のSIEMエンジンとセキュリティオペレーションセンター(SOC)のリスクアナリストが、ICT環境を24時間365日サポート。高度なセキュリティ監視により、実在するリスクと潜在リスクを可視化します。 また、「NWセキュリティ」をはじめとするセキュリティ対策パックメニューや、「リアルタイムマルウェア検知」などの機能をご用意、様々なご要望に応じて総合的なセキュリティソリューションを提供します。