セキュリティの基本とその脆弱性ー守りを怠ればコストが増大

富士通株式会社
脅威予測レポート2017

※当レポートは当社のEMEIAリージョンの分析に基づくものです。

shaping tomorrow with you
社会とお客様の豊かな未来のために

FUJITSU

目次

はじめに

»サイバーセキュリティの世界では、将来を見通すのと同じくらい、過去を振り返ることが大切です。
過去の教訓を学んで、将来の脅威に備える必要があります。

したがって、このレポートでは、2016年の当社の予測を振り返り、実際の出来事とどれほど一致していたかを調べ、2017年の出来事を予測します。

このレポートが過去を振り返るだけでなく将来を見通して、お客様のビジネスを保護する一助になることを願っています。«

ロブ・ノリス（Rob Norris）
EMEIA、エンタープライズサイバーセキュリティ部門長

2016年の予測の正確度評価

当社はモノのインターネット（IoT）の成長が続くため、重大なDDoS攻撃の数が増加すると予測しました。2016年には一部の大規模組織が、DVRとCCTVカメラのIoTボットネットからのDDoS攻撃の影響を受けました。10月には、この攻撃がDynDNSに影響を与えて、Spotify、Twitter、GitHub、PayPalなどのオンラインサービスを妨害しました。KrebsOnSecurityも過去最大級の攻撃を受けました。

当社はWebアプリに対する攻撃が増えるとも予測しました。残念なことに、2016年初頭からロシアのソーシャルメディア会社VKやカタール国立銀行がSQLインジェクションによる攻撃を受けています。

企業にとって貴重なデータが引き続き標的になっています。2016年には、大学や法律事務所も標的になり、主な手口はデータの窃盗やランサムウェアでした。カルガリー大学は、ランサムウェアの被害に遭ったファイルを復号化するために2万ドルを支払ったことを認めました。

当社は生体認証が重要になることも予測しました。富士通は生体認証で世界をリードする技術の開発を続けており、多くのベンダーがハードウェアソリューションの拡張を見据えています。Apple社がiPhoneに指紋認証を採用してしばらく経ちますが、2016年にNISTが2段階認証の2段階目の方法としてSMSのサポートをやめると発表した少し後に、MacBookでも生体認証を採用しました。

当社はFlashは引き続きエクスプロイトキットを使用する攻撃者の格好の標的となることを予測しました。大手のブラウザはFlashをデフォルトオプションで削除し、YouTubeはHTML5をデフォルト設定にしました。その点で、当社の仮定は正しかったといえます。

さらに個人情報がサイバー攻撃に結びつけられるという予測も正しかったといえます。英国の国営宝くじ（UK National Lottery）は、この攻撃の被害者の一例です。26,500人のプレーヤーアカウントがハッキングされ、生年月日やカード情報の詳細が盗まれました。

2017年に企業がサイバーセキュリティの課題に注意を払う必要があることは確実です。
当社のトップ10の予測を次に説明します。

富士通が予測する2017年のサイバーセキュリティトップ10

1

多くの企業に引き続き脆弱性が存在

当社は2017年も攻撃は成功し続けると予測します。それは、SSLインスペクション機能が欠落しているために、暗号化されたチャネル経由の攻撃に存在する脆弱性に企業が対処しないためです。2016年にも、Microsoft PowerShellを使用する企業に対する攻撃が大幅に増えました。PowerShellは、すべてのWindowsコンピュータにデフォルトでインストールされるフレームワークおよびスクリプト言語ですが、悪意のある使用に対する保護が多くの組織で十分に行われていないため、攻撃者が使用しています。これはすでにWindowsシステムの一部であるため、攻撃者にとっては攻撃サイクルの一部として使用しやすく、ネットワークを防御する側にとっては、モニタリングしても、悪意のある使用を識別するのが難しくなっています。侵入テストチームがよく使用するPowerShell Empireなどのツールも、攻撃者がセキュリティ境界を超えて裏口を作り、ネットワーク内を動き回りやすくしています。組織はモニタリング能力やロギングレベルを見直して、ネットワークで使用中の既知の善良なスクリプトを識別し、可能な限り悪意のある攻撃を検知する必要があります。

2

人工知能がセキュリティオペレーションセンター（SOC）の分析を変える

2017年は組織が人工知能（AI）や機械学習を使用しはじめるので、セキュリティイベントを分析する方法が変わります。「善良さの特徴（what good looks like）」というサイバーセキュリティの用語は長い間知られています。機械学習ではこの概念を拡張して、特定のシステムコールをどのように発行するべきか、またはするべきでないか、特定のファイルタイプをどのように一緒に配置するべきかなど、善良な振る舞いのアルゴリズムを設定し、これから逸脱した場合に疑わしいと見なします。大規模トランザクションやデータベースへの初回アクセスなど、コアネットワークの特異な振る舞いのモニタリングに対するセキュリティオペレーションセンターのアプローチは、インテリジェンス主導のアプローチに変化するでしょう。ウィルス対策や侵入検知で「悪意のある既知の」トラフィックに反応してトリアージを行うのではなく、機械学習アルゴリズムに基づいて、特異な事象が発生したことを周知するアラートを調査することが必要になるでしょう。2017年に注意が必要なもう1つの分野は、ネットワークやセキュリティコントロールを破るために、攻撃者も同等のAI機能を使用することです。

3 銀行のコアアプリケーションが引き続き犯罪者の標的に

銀行のコアアプリケーションは2016年も標的にされました。SWIFTのグローバル支払ネットワークに弱点があったため、国際的な金融機関が大規模に侵入されて多額の資金が直接盗まれました。最大の被害は、バングラデシュ銀行から盗まれた8,100万ドルです。

また、銀行向けのトロイの木馬が「バックオフィス」アプリケーションを標的とし、レガシーテクノロジーを悪用して銀行から直接資金を盗む手口も増加しました。

当社はこれが2017年の金融部門の大きなリスクと見ています。

SWIFTは16項目の必須管理項目を設定して、銀行が遵守しているかを2018年に調査しますが、依然としてサイバー犯罪者にはチャンスが残されています。研究者は2016年後半にSWIFTを標的にしたOdinaffというトロイの木馬を特定しており、当社はその変種や新しい攻撃方法が今年現れると予測しています。

4 攻撃者の標的はモバイルマーケットで増加

新しいオペレーティングシステムのセキュリティが向上し、スマートデバイスで個人データやビジネスデータを扱う機会が増えるため、2017年はモバイルプラットフォームが標的になるでしょう。

多くの組織は、以前頻繁に標的になった脆弱なMicrosoftのレガシーオペレーティングシステムをアップグレードして、Windows 10、Edgeブラウザ、サーバーオペレーティングシステムで優れたセキュリティ機能を利用しています。特にエクスプロイトキットで頻繁に標的にされるAdobe Flashなどの小さなアプリも、エンタープライズネットワークやブラウザプロバイダから削除され、2016年12月にはGoogle ChromeのデフォルトオプションもHTML5になりました。個人が複数のスマートデバイスを持つようになり、最近のストレージ機能の進歩で膨大な量の個人データとビジネスデータが保存されています。そのため、攻撃者がモバイルプラットフォームに対する攻撃を進化させて、個人の写真の返還や復号化の見返りに金銭を求めるモバイルランサムウェアによる攻撃が続くでしょう。特にビジネスデバイスについては、モバイルデバイスマネジメントを強固なセキュリティコントロールで補う必要があります。

ハッカーはスマートシティを標的に

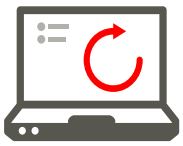
5

IoTのデバイスが爆発的に増えるにつれて、以前には考えもしなかったセキュリティ問題が発生してくるでしょう。スマートモーターウェイの電光板を設置したときには、ドライバに対する道路の警告表示をハッカーが政治的なメッセージに変えるとは考えていませんでした。IoTの「Mirai」ボットネットを構成するようになったCCTVカメラ、DVR、SOHOルーターを多数生産するIoTメーカーにも同じことがいえます。

Miraiから学べる明らかな教訓は、デフォルトパスワードのハードコーディングを避けることですが、Zyxelルーターに見られるように、つながるスマートデバイス用に設計された多くのプロトコルには潜在的な欠陥と脆弱性があります。これらの脆弱性が2017年にはさらに増えると思われます。

攻撃者がこれらの脆弱性を悪用して、つながる「スマート」な都市を破壊することなど、12か月前にはあり得ないことでしたが、最近の出来事はその見方を変えました。スマートデバイスの潜在的な脆弱性に対処するだけでなく、これらのプラットフォームを制御する必要もあり、これらの制御プラットフォームの管理に関するガバナンスが非常に重要になります。これには、つなごうとしているスマートシティのすべての部分の配送や制御に関連するサプライチェーンのセキュリティコントロールが含まれます。サプライチェーンの一部に侵入すれば、スマートデバイスの管理プラットフォームも乗っ取れるとすれば、このような攻撃は増え続けることでしょう。攻撃者が、つながる都市の脆弱性を悪用しようとしなくても、インフラの重要な部分にランサムウェアをインストールしようとするかもしれません。

6

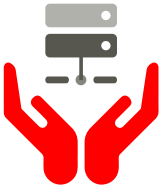


レジリエンスとリカバリがビジネス差別化の鍵

サイバー攻撃は非常に強力になったため、最もセキュリティの厳しい組織でも攻撃される可能性があります。2017年に大切になるのは、どれほど速く回復できるかです。

迅速かつ完全に回復すれば、マーケットの同情と敬意を得ることができますが、リカバリに手間取ると批判や訴訟を招きます。11月末に、サンフランシスコ市営交通局が大規模なランサムウェアの攻撃を受けましたが、バックアッププロセスがしっかりしていたため、1日以内にほとんどの機能が回復しました。

2017年は、企業が防御・検知・対応を組み合せた組織的なアプローチを取っているかどうかで、この課題に真剣に取り組んでいるかどうかが明らかになるでしょう。



7 データリッチであるだけでなく、データのキュレーションにすべての組織が注目

2017年には、さらに多くの投資家、株主、顧客、規制当局が、機密データを注意深く扱うことを求めるでしょう。これは一般データ保護規則（GDPR）のアプローチで特に重要になります。スペシャリスト向けのデータ損失防止（DLP）ツールは正しく使用すれば有効ですが、多くの企業では、DLPに個別にアプローチするか、DLPツールを使用するだけで十分だと考えています。組織はリスクを見極め、保護するデータを特定して、ネットワークを注意深く見守る必要があります。また、サードパーティの機密情報も自社のデータと同様に保護する必要があります。

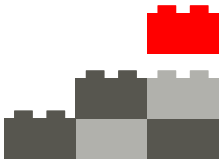
8 グローバル企業が自社のサプライチェーンのデータセキュリティ調査を要求

ほとんどの組織は、機密データが社内だけで保有されているのではないことを知っています。サプライチェーンにも保有されています。しかし、多くの場合、組織が自分のサプライヤに期待することと、サプライヤが契約上行う必要があることの間には大きな違いがあります。

サイバーセキュリティリスクの増大が認識されるにつれて、グローバル企業は専門的なアドバイザーからデータセキュリティが良好であるという明確な保証を得たいと考えるようになっています。これらには、法律事務所、公認会計士、ビジネスコンサルタントが含まれます。大企業はそのようなアドバイザーを利用する条件として、データセキュリティの確保を求めます。このトレンドは、2017年以降長く続いていくと思われます。

9 経営会議でITセキュリティが通常の議題となる

大規模組織に対するサイバー攻撃があまりに多いため、テクノロジー恐怖症の経営幹部でも、これをIT部門のみで処理する問題として片付けることはできません。
2017年は、脆弱なITセキュリティがどれほどビジネスに悪影響を及ぼすかを経営幹部が理解する年になるでしょう。組織はシニアITスタッフをトレーニングして、経営幹部の要求を理解し、経営幹部が理解できる言葉でITを議論できるようにする必要があります。



10 日常のIT運用の不備で避けられるはずの問題が発生

ほとんどの場合、組織で発生するサイバーセキュリティの問題は、新しいサイバー攻撃の手法や悪意を持った社員が引き起こすのではありません。驚くほど多くの企業が、リスクを減らす簡単で重要な基本的管理作業を実行していません。
有効な脆弱性のパッチが適用されておらず、脅威に対する適切なインテリジェンスが欠如しています。現在有効なユーザーのみを許可するようなアクセス管理システムも使用していません。「最小権限」のアクセス権を設定せず、侵入テストの助言に基づいて対処しています。
そのため、システムのデータ損失、データ窃盗、外部からの妨害に対する脆弱性が必要以上に大きくなっています。
残念ながら、この傾向は2017年も続きます。つまり、大きく報道されるセキュリティ侵害のほとんどは実際には回避可能です。

攻撃は発生します。備えはできていますか。

2017年は、より強力なセキュリティ侵害が日常的に発生するでしょう。世界中のすべての主な業界の企業が影響を受けるでしょう。これには、一流の巨大企業、政府、誰でも知っているブランドが含まれるでしょう。不運にも被害を受ける場合もあります。しかし、多くの場合、もう少し注意を払っていれば、避けることができた攻撃を受けてしまうでしょう。

セキュアシンキングのWebサイトで、刻々と変わるサイバー脅威から
お客様のビジネスを保護する方法、そして富士通がどのようにお役に立てるかをご覧ください。

お問い合わせ

富士通株式会社

富士通コンタクトライン（総合窓口）
0120-933-200
受付時間 9時～17時30分
（土曜・日曜・祝日・当社指定の休業日を除く）

http://www.fujitsu.com/jp/solutions/security/

FUJITSU

22 Baker Street
London W1U 3BW
Tel: +44 (0) 1235 79 7711
Email: askfujitsu@uk.fujitsu.com
Web: **uk.fujitsu.com/securethinking**
Ref:3684