信頼される要因

ビジネス推進力を維持する際のサイバーセキュリティの役割

エグゼクティブサマリー

2018年は、サイバー攻撃の危険度合いがこれまでになく高まりました。注目を浴びるようなセキュリティ上のインシデントは、1.7Tbpsを記録した史上最大の分散型サービス拒否（DDoS）攻撃[1]が発生するなど、ニュースに事欠きません。EUでは、一般データ保護規則（GDPR: General Data Protection Regulation）が2018年5月25日に発効され、個人情報（PII）の収集/処理/管理の方法に対して厳格なルールが課せられるようになりました。さらに、クリプトマイナーは手軽な稼ぎを求めてネットワークに侵入しています。

今や、組織や個人がセキュリティの裏付けを額面通りに受け取ることをますます警戒する「信頼の次（ポスト-トラスト）」時代に突入しています。消費者がブランドを目にするときには常に、その企業が自分の個人情報を共有するのに十分信頼できるかどうかを判断します。サイバー攻撃は、企業がブランドと顧客の間で作り上げてきた信頼関係をまんまと破ってしまいます。このような結果を招いたのは、もはやセキュリティ専門家のみの責任ではありません。経営幹部にも、同じく責任があると言えます。

組織が自らのブランド保護に取り組む際、直面する複雑な問題に洞察を提供しようと、ラドウェアはグローバルアプリケーション&ネットワークセキュリティレポートを毎年発行しています。8年目を迎える今回の年次レポートでは、グローバルな業種別調査結果と併せて、ラドウェアによる基本的な調査、実際の攻撃データ、そして表面化してきたトレンドやテクノロジーの分析までを網羅しています。

レポートでは、サイバーセキュリティのもたらすビジネスやテクノロジーへの影響に着目しており、その項目は次のとおりです。

- 最近の攻撃から学んだ教訓
- サイバー攻撃がもたらす量質両面での実コスト
- ネットワークとアプリケーションに対する脅威の現状
- 新たなテクノロジーの脆弱性に対する知見
- 2019年の予測

主な調査結果

コスト対リスクのバランス

サイバー攻撃に対する防御には大きな投資が必要で、それはバランスシートの営業費用として計上されます。組織は常に経費削減の策を求めています。ただ、防御を突破しビジネスに影響をおよぼすサイバー攻撃のリスクを考慮し、どの程度の費用を準備すれば十分なのでしょうか？

ラドウェアの2018年のグローバルな業種別調査で明らかになった次の知見を考えてみましょう。

- わずか1年で、サイバー攻撃に起因する初期コストが52%増加して110万ドルに。
- 自社に対するサイバー攻撃の総コストをモデル化した組織の数は、モデル化していない組織数に比べておよそ2倍に。
- 5分の2の企業が、攻撃により顧客体験の悪化や評価失墜を経験していると回答。
- 回答者の93%が過去12ヶ月間にサイバー攻撃を経験しており、攻撃を受けていないと回答したのはわずか7%。
- 3分の1の組織では、サイバー攻撃を毎週経験。
- 回答者のほぼ半数が、サイバー攻撃で一番影響があったのはサービスの中断であると回答。サービスを完全または一部停止するに至った攻撃は15%増加し、生産性にも悪影響がおよんでいます。
- サイバー身代金要求は、ハッカーにとって引き続き主要な動機となっており、攻撃の51%の理由を占めています。

[1]https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/memcache-ddos-as-a-service/

新たな攻撃ベクトル

攻撃者は、バースト攻撃、増幅攻撃、暗号化攻撃、IoTボットネットなど、サービス拒否を引き起こす効率的な手法を採り入れ、より被害が拡大するアプリケーション層を狙った攻撃をしかけています。

- アプリケーション層攻撃は、最大の被害をもたらしします。回答者の3分の2がアプリケーション層攻撃を経験しており、3分の1が、2019年にはアプリケーションの脆弱性が、特にクラウド環境において大きな懸念材料になると予測しています。半数以上が毎月アプリケーションの変更を行い更新していますが、残りはさらに頻繁に更新を行っているため、セキュリティ自動化のニーズが高まっています。
- 完全な業務停止やサービス中断を引き起こすサイバー攻撃は15%増加し、6分の1の組織が1Tbpsの攻撃にさらされたと回答しています。
- ハッカーは、ネットワークやデータセンターを破壊する新たな戦術を発見しました。HTTPSフラッド攻撃は20%増加し、DNS攻撃とバースト攻撃はいずれも15%増え、ボット攻撃は10%増加しました。
- 3分の1の企業は、動機が特定できない攻撃を受けたと回答しています。

次への備え

企業では、変わりつつある脅威の状勢の深刻さを認め、自らのデジタル資産を守る措置を取っているようですが、セキュリティ脅威の深刻さは厳しさを増しています。

- ほぼ半数が、適所にセキュリティソリューションを導入しているにもかかわらず、あらゆるタイプのサイバー攻撃を防御するには準備不足と感じています。
- 86%の企業が、過去12カ月の間に機械学習や人工知能（AI）ソリューションを検討しました。その理由として、約半数がサイバー攻撃に対してすばやく対応するため、と回答しています。ラドウェアでは、ブロックチェーンを活用する企業が44%増加していると考えています。
- 企業は、引き続き複数のクラウドプロバイダーを活用し、多角的なネットワーク運用を行っています。5分の2の組織が、オンプレミスとクラウドベースの防御を組み合わせたハイブリッド型サイバーセキュリティソリューションを利用しています。
- EMEAの組織の49%は、GDPRに十分備えられていないと回答しています。

唯一の選択肢は成功

あらゆる脅威を常に緩和できなければ、サイバー攻撃のコストは単に増大してしまいます。顧客の信頼はあっという間に消えてなくなり、ブランド評価への影響は大きく、ビジネスを取り戻すためのコストも莫大になります。そしてGDPRやその他の政府の規制は、準拠しない企業を破産させてしまう可能性があります。

サイバーセキュリティを組織の長期成長計画に組み込むことは非常に重要です。デジタル資産の保護は、もはやIT部門のみにその責任を負わせるわけにはいきません。むしろ、セキュリティ計画は新たな製品やサービス、セキュリティ、開発計画、そして新たなビジネス構想に組み込むべきものです。CEOや経営幹部チームは、顧客体験の保護に対する方向付けと投資の方法をリードする必要があります。

経営幹部の展望

CEOは新たな信頼責任者

サイバーセキュリティは、業務執行者として企業のリードを任せられた経営幹部にとっては、極めて個人に依存した問題になりつつあります。顧客と確固たる関係を構築し維持するためには、CEOは「最高信頼責任者（CTO: Chief Trust Officer）」としての新たな役割を引き受けなければなりません。わずか1回のサイバー攻撃で、長年守り続けてきたブランド戦略が消滅してしまう可能性がある際に、最高情報セキュリティ責任者（CISO）にセキュリティ戦略を任せるのでは不十分です。問題が大きすぎます。

Equifax、Yahoo、Moller-Maersk、Anthem Healthcareなど、話題となった攻撃により個人情報が漏洩した企業のCEOの結末を考えてみましょう。組織が自らのブランド価値を高めるためにつぎ込んできた努力のすべてが、攻撃の結果、顧客の信頼失墜の瞬間に水の泡となってしまいました。これらの企業のCEOは、「他の興味深いものに目を奪われていた」のかもしれません。

サイバーセキュリティが企業のビジネスモデルにおいて不可欠であることを保証するため、CEOはセキュリティ対策ならびに対策投資を検証する必要があります。手抜かりなくセキュリティ戦略を委任できるCEOは、自分の責任でそれを実行します。

無料レポートのダウンロード

グローバルアプリケーション&ネットワークセキュリティレポート 2018–2019年