SecureAge

中小企業のためのサイバーセキュリティ - データ保護を中心に

SecureAge ホワイトペーパー2021年

概要

このホワイトペーパーでは、以下について説明します。

- 中小企業はデータセキュリティへの意識が低いことが多く、その結果、経営の失敗や大きな損失に繋がっています。中小企業の経営者の66%は、自社はサイバー攻撃の被害に遭わないと考えていますが、データ侵害を受けた中小企業数は、2019年だけを見ても63%増加しています。
- 社員トレーニングやクラウド技術、サイバー保険などは、中小企業にとって効果がほとんど得られない上に、ハイリスクかつ応急処置的なデータセキュリティソリューションが提案され採用されている現状と、それゆえに多くの中小企業が危険な状態にさらされている理由をご説明します。
- SecureAge Technology社が、シンプルなアドバイスとデータに特化したアプローチにより、高額な費用投資や人手に依存することなく、また既存のインフラや仕事のやり方を見直す必要もなく、完全なデータ保護を実現を目指して、世界各地の中小企業を支援してきた方法について、ご紹介します。

データ侵害は想像するよりも頻繁に発生しています。有名な多国籍企業のデータやセキュリティが侵害されたというニュースを、毎週のように目にします。企業や消費者のデータは、不満を抱く従業員、悪意のある内部関係者、プロのハッカーなどによって盗み出されています。あまりにも頻繁に発生しているため、報道機関や世間からすぐに忘れ去られるような事態にすらなっています。大企業へのハッキングがトップニュースとして取り上げられると、データセキュリティの侵害は一時的に注目を浴びますが、大企業と同様に多くの中小企業がデータ侵害やマルウェア攻撃に遭っているという話を聞くことは、滅多にありません。何故でしょうか？

その理由は簡単です。中小企業にとって、サイバー攻撃を受けることは致命的であるからです。

中小企業がデータ侵害やサイバー攻撃に遭った場合、ニュースになるほど長期間耐えられる可能性は非常に低いのです。データ侵害もデータ損失も、中小企業にとっては企業存続に関わる危機と言えるでしょう。データの対価として身代金の支払いを求められたり、罰金が科されたとしても、ビジネス上の決定として対処できる大企業とは状況が大きく異なります。大企業は、サイバー攻撃に遭う前に予防措置としてデータセキュリティソリューションに投資するか、または攻撃を受けた後に身代金や違約金、罰金の支払いをするか、いずれかを選ぶだけの人的、経済的余裕があります。残念ながら、対処する余裕がない企業こそ、最もサイバー犯罪の被害に遭いやすいと言えます。こうした理由から、中小企業にはデータセキュリティに関する正しい情報が最も必要ですが、その経営者達には、データ侵害を受ける可能性や受けた場合の影響に関する認識が大いに不足しています。その結果、歪んだ状況をもたらしています。

数字は嘘をつかない。中小企業でもデータ侵害は発生している。

> - Ponemon Instituteの調査によると、データ侵害を受けた中小企業数は2019年に63%増加しています。
> - またVerizon社の報告によると、データ侵害行為は、3件に1件の割合で中小企業が対象となっています。

中小企業の上層部の意思決定者500人以上を対象に実施された『2019年中小企業へのサイバー攻撃に関する調査』では、中小企業の経営者の66%が自社はサイバー攻撃の被害に遭わないと考えていることが明らかになりました。

このように現実と認識にギャップが生じていることから、多くの有望な中小企業は、効果のあるセキュリティソリューションを導入せずに運営されている可能性が高く、リスクを抱えていることがわかります。これは、経営者の生活や事業の成長性だけでなく、各中小企業が事業を行っている経済にとっても問題となります。

なぜ中小企業はセキュリティリスクを抱えていることに気が付かないのか？

世界的に見ても、中小企業は最も雇用を生み出しており、経済に大きく貢献する存在です。世界貿易機関によると、中小企業は先進国において、企業人口の90%以上、雇用の60~70%、そして国内総生産の55%を占めています。

中小企業は世界経済において重要な役割を担っているにもかかわらず、データ侵害やサイバー攻撃は大手多国籍企業しか遭うことがないという誤った見方をしているのです。

実のところ、このような神話は、大手サイバーセキュリティ企業が、大企業の顧客や政府とのデータセキュリティ契約を取ろうとして、金銭的な理由から提唱しているものです。大企業を中心に調査や報告を行うことで、メディアに取り上げられやすくなり、結果として大口契約を獲得しやすい状況となっています。

パパラッチがトップ記事や注目記事として掲載されることを狙って、最新の有名人の破局情報をスクープしようとするのと同じです。こういったゴシップが大きく宣伝されるからといって、一般人の間でもっと多くの破局が起きていないというわけではなく、ただ報道されていないだけで、中小企業も同じことが言えます。

ハッカーが中小企業を標的にする理由は？

ハッカーが中小企業を標的にするのはなぜなのか、疑問に感じている方もいらっしゃるかもしれません。やはり一般に名が知れた企業は多数の顧客が付いているため、大企業を標的にしたほうがハッカーは多くの利益を得られるのではないかと考えられます。

しかし、現実は大きく異なります。ほとんどの中小企業が攻撃の対象に含まれますし、その攻撃は必ずしも慎重に計画されるわけではありません。だからといって、時間を掛けて準備し、費用が掛かっている攻撃に比べて、被害が少ないわけではありません。

ハッカーは、多くの中小企業がタイムボム型のランサムウェアを検知するためのリソースを持っておらず、セキュリティソリューションを実装していないことを知っています。つまり、ハッカーなどのサイバー犯罪者は、気付かれることなく容易に組織のネットワークに侵入し、データを破壊する準備をしたり、ランサムウェアを仕込んだりすることができるのです。数日から数週間後に身代金を要求されたタイミングで、ようやく中小企業の経営者は状況に気がつくことになります。

IBMおよびPonemon Instituteが2019年に発表したレポートによると、中小企業がデータ侵害を発見してから修復するまでには、平均で9か月掛かることが示されています。また、サイバー攻撃を検知したとしても、中小企業は攻撃を止めるためのリソースやセキュリティソフトウェアを持っていないことが多く、修復することもできません。

一方、大企業は通常は、社内に担当チームが24時間体制で待機しているか、または外部のセキュリティオペレーションセンターに委託しています。さらに、一般的にサイバー犯罪者のやり方を学んでいる社内または社外の人員がセキュリティ管理を行っているという事実も、抑止力となっています。

このように、データ侵害は大企業がターゲットとなることもありますが、中小企業も簡単に攻撃できるターゲットとなるのです。ハッカーは中小企業が自らのデータを保護できないこと、効果的な予防策やセキュリティソリューションがないことを理解しているのです。

内部からの脅威もまた、中小企業のセキュリティを脅かしている

中小企業が心配しなければならないのは、社外のサイバー犯罪者だけではありません。中小企業では、不満を抱く社員や顧客、競合他社などが害を及ぼす可能性もあります。社内の関係者は会社のファイルに簡単にアクセスできるため、当然のことではあります。

当社ではサイバーセキュリティ業界において18年間の実績がありますが、その経験から中小企業から盗まれるデータの大半は、組織内部の犯行により持ち去られていることが判明しています。実際、そういったデータ侵害事件の多くは、社内ネットワーク上に情報が露出した状態になっていた、つまり無防備な状態で放置されていたことが原因でした。

しかし、今日では社員だけでなく、顧客やサプライヤー、ビジネスパートナーが何らかの形で組織のデータにアクセスすることも珍しくありません。人間である以上、間違いも犯します。

それに加えて、キーロガーやIoTやウェブカメラを悪用するためのソフトが従来よりも手頃な価格となり、不満や悪意のある人が簡単に利用できるようになりました。また、RaaS（ランサムウェア・アズ・ア・サービス）が台頭してきたことを考えると、既存のセキュリティソリューションは、中小企業にとって不十分であるという残念な事実を認めざるを得ません。

「社内でさらに努力するより、外部の専門家に頼るべきでは？」

中小企業の経営者は、実際にこういった助言を受けることが多いようです。

しかし、このような「応急処置」的なアプローチでは、多くの中小企業がさらに費用を費やすことになるだけで、サイバー攻撃からデータを保護することはできません。

中小企業の場合、予防措置としてのセキュリティソリューションを導入する際に通常掛かるコストは、ほとんどの経営者にとっては先送りにしたいものです。リード生成サービスや特典アプリ、生産性向上に役立つソフトウェアなどは魅力的で、より迅速に利益を得られるように思えます。もちろん、投資収益率は重要な指標ですが、サイバー攻撃に遭って会社が存続できなくなった場合、測定する収益自体が無くなってしまいます。

中小企業のためのサイバーセキュリティでやってはいけないこと

当社のアプローチを説明する前に、まずサイバーセキュリティに関する一般的に信じられている神話をご紹介します。

1. 真に効果的なサイバーセキュリティ文化を構築することはできない

多くの中小企業の経営者は、専門家のアドバイスを信じるものです。専門家の多くは、サイバーセキュリティ文化の構築を提唱しており、サイバーセキュリティのベストプラクティスに重点を置いたチームのトレーニングに非常に力を入れています。具体的にどのように行われるのでしょうか。

一般的には、既知の脆弱性やセキュリティ上の弱点を確認し、パッチやアップデートのダウンロードを行ったり、またはサイバーセキュリティ製品·サービスを提供するベンダーと契約を結んだりします。次のステップでは、社員が学び、採用する必要のある関連するセキュリティスキルや方針を洗い出し、トレーニングとテストを繰り返し実施します。

簡単そうに思えるかもしれませんが、新しいハッキング手段が出てくるたびに、社員は新しいセキュリティスキルを学ぶ必要があり、そのためにはさらに多くのトレーニングとテストを実施する必要があります。新しいハッキング手段は際限なく生み出されるため、終わりが見えず、大抵のケースでは、社員は混乱し、疲れ果て、場合によっては不安を感じるでしょう。特に、ミスや社内の抜き打ちテストで引っかかると職を失うことになる場合は、社員に負荷が掛かります。

サイバーセキュリティ文化を構築するためには、多くの労力が必要となります。世界中のあらゆる潜在的な脅威に常に注意を払う必要があることは言うまでもありませんが、社員もまた人間であり、人間は常に間違いを犯すものだということを念頭に置く必要があります。

意欲的なサイバーセキュリティ文化を構築するためには、社員の賛同を得る必要もあります。大半の場合、社員は別の仕事のために採用されているため、データセキュリティを自分の仕事とは考えていません。また、当然ですが長時間の説明やトレーニング、さらにはマニュアルが必要となる場合、ビジネスの妨げになってしまいます。

ここでお伝えしたいことは、中小企業のサイバーセキュリティのツールやノウハウによるチーム武装が大事ではないということでなく、社内チームにサイバーセキュリティの専門家になるよう求めたり、本来の仕事の妨げになったりするような管理的および物理的な制御に依存してはならないということです。

たとえセキュリティの専門家を雇うことができたとしても、技術力が高く、ソーシャルエンジニアリングの手法を駆使して積極的に攻撃を仕掛けてくるハッカーを常に防ぐことは大変困難です。

2. クラウドはすべてのサイバーセキュリティーに関する問題の解決策とはならない

すべての業界は常に変わり続けています。激動の2020年を経て、「新型コロナウイルス」が日常的に話されるようになる前の状態に戻ることは難しいでしょう。メディアが名付けた「新しい常識」がきっかけとなり、クラウド環境への依存度は急激に高まっています。

業界によっては、まさに可能性が広がり、刺激的な時期でしょう。危機的状況がイノベーションを生むこともあります。しかし、イノベーションはセキュリティギャップを明らかにする場合もあり、それが今クラウドで起きています。クラウドテクノロジー自体に問題があるわけではありませんが、必要な箇所で適切なセキュリティ対策を講じられるかどうかは、ユーザー企業だけでなく、クラウドプロバイダー側の社員にも依存することになるため、データがリスクにさらされる可能性が生じます。

2017年にセキュリティ研究者が、保護されていない状態のAmazon S3ストレージバケットを発見したことをニュースでご覧になった方も多いと思います。アクセンチュア社の顧客認証情報など、機密性が高いデータが格納されていました。これは、バケットが一般からアクセスできるように誤って設定されていたために発生しました。

アクセンチュア社だけではありません。その後、多くの企業が、クラウド上にあるデータのセキュリティに問題があり、データが一般に公開されてしまったことを報告しています。ダウ・ジョーンズやベライゾン、軍事諜報機関であるアメリカ陸軍情報保全コマンド（INSCOM）も含まれます。

クラウド上にデータを保存した場合でも、ローカルであっても、セキュリティ上の問題点は、一般的にセキュリティの「ドア」を用いて保護されているということです。認証やアクセス制御などのセキュリティの「ドア」が開いたままだったり、バイパスされたり、侵入されたりすると、格納されているデータが盗み出されてしまいます。

3. サイバー保険は魅力的に見えるものの、中小企業の存続には役立たない可能性がある

残念なことに、企業の大半は予備措置としてデータセキュリティソリューションに投資するよりも、保険に加入するほうが安く済むと考えているようです。サイバー保険は魅力的に見えますが、冷静に考えると、保険の掛け金では、中小企業に必要な補償内容を提供することはできません。サイバー保険に頼っている企業は、防ぐことができるものと制御できないものは微妙に異なることを理解しておらず、誤った判断をしています。中小企業の経営者の中には、保険金が支払われる前に、調査官にセキュリティに関するベストプラクティスを実施していたことを証明する書類を提出する必要がある事実をご存知ない方が多いのです。証明するには、当然ですが時間や費用が掛かり、面倒な作業が発生するため、大抵の中小企業では対応するのは難しいと考えられます。サイバーセキュリティのソリューションに関する深い知識だけでなく、法的な専門知識も必要となります。

他にも、仮に保険会社が罰金や広報費用を補償したとしても、システムがダウンしたり、評判が損なわれたりした場合、中小企業は存続できるのかという疑問もあります。売上を維持するためには、会社の評判がどれほど重要でしょうか？貴社のビジネスは、保険会社にとってどのくらい重要でしょうか？こういった点を考えてみると、データ侵害を未然に防ぐことがより良い方法であることがわかります。

試行錯誤されたサイバーセキュリティソリューションは信用できない

中小企業が新たな取り組みを開始し、新たな顧客に働きかけ、デジタルイノベーションによって差別化を図ろうとしのぎを削る中、全社に共通するのは、データセキュリティへの脅威に対処する必要があるということです。アフリカの中小企業であろうと、ロンドンの多国籍企業であろうと、ビジネスの生命線であるデータを保護することは、効率的で効果的なサイバーセキュリティソリューションです。

残念ながら、業界ではデータセキュリティは厳しいビジネスであるという幻想が信じられています。確かに色々行わなければいけないことは多いですが、Visaの創業者であるDee Hock氏の言葉が非常に上手く言い表しています。

> 「単純で明確な目的と原則は、複雑で知的な行動を生む。複雑なルールや規制は、単純で愚かな行動を生む」

そこで、当社ではデータセキュリティと使いやすさを両立させたシンプルなソリューションを中小企業向けに開発して、セキュリティ業界に衝撃を与えました。

データ暗号化は本質的で意識されず、透過的かつ直感的であるべきだという原則を固く守ってきました。当社の暗号化技術「SecureData」とデータセキュリティソフトウェア「SecureAge Security Suite」により、すべてのデータを常に保護することができます。データが「転送中」「使用中」「保管中」どの状態であって保護は継続します。

当社では、過剰な費用投資や人手に依存することなく、また既存のインフラや仕事のやり方を見直すことなく、中小企業に付加価値をもたらす新しいデータセキュリティソリューションが正しいと考えました。結果として当社の予測は正しく、今まで以上に中小企業ではこのようなセキュリティソリューションが必要とされています。

「SecureData」の暗号化技術

当社のパートナー企業である北米の会社は、設計とテストの拠点であることから、データを100%保護できるソリューションを必要としていました。いかなる種類であってもデータ侵害が発生すれば、技術的努力と貴重な知的所有権が大きなリスクにさらされることになります。場合によっては、予定されていたランチミーティングが公開されただけでも、他の機密データにアクセスするための経路となる可能性があります。

同パートナー企業はこれまで努力して名声を築き上げ、ビジネスを拡大してきましたが、競争の激しい業界では破壊工作やサイバースパイのリスクがあることを認識していました。そのため、以下の要件を満たす、実績があり同社の環境に適したデータセキュリティソリューションを探し始めました。

- 内部および外部の脅威から自社のデータを保護するためのセキュリティソリューション
- 同社の比較的小さめな企業規模（ワークステーションとサーバーが40台以上）に対応しつつ、成長に合わせて拡張できる
- 専任のIT部門の設置やインフラの追加を行う必要がなく、手頃な価格で簡単に導入できる

様々なアプローチを比較検討した結果、SecureDataの暗号化技術が搭載されたSecureAge Security Suiteが最適なソリューションであると判断しました。SecureDataは、既存のシステムや社員の作業を妨げることなく、また追加のインフラを必要とすることなく、保存場所を問わず、すべてのファイルを常に保護しています。また、世界で最も過酷な環境下で18年間にわたり、データ侵害が一度も発生していないという実績からも、有効性をおわかりいただけるでしょう。

結論：中小企業にはより優れたサイバーセキュリティツールが必要

上記の通り、中小企業向には、予防措置としてのサイバーセキュリティおよびデータセキュリティソリューションが必要であることを説明してまいりました。これは法規制により必要となっているからではありません。脅威が増えているからというわけではなく、脅威は常に存在しています。それなのに、既存のソリューションは機能していません。

恐ろしいのは、多国籍企業が注目され続けている一方で、中小企業が直面するデータセキュリティの脅威が増加していることは無視されているということです。ニュースには取り上げられないものの、以下は実際に起こった事件の一例です。

- 地元で活動するある弁護士は、破壊的なマルウェアによる攻撃を受けたことにより、1週間コンピューターを使用できなかった
- ある保険ブローカーは、顧客の機密情報を身代金として要求された
- ある広告代理店経営者は、朝起きたら銀行口座に入っていたお金がすべて無くなっていることに気が付いた

ニュースで報じられなくても、こういったサイバー攻撃は実際に起こっています。

2008年の世界金融危機以降、「コンシューマーフレンドリー（消費者の立場で考える）」が売り文句になったと言われていますが、2020年から始まったコロナ禍をきっかけに、「データフレンドリー」が売り文句となり、ようやく緊急性を持って対処されるようになるでしょう。昨年、米国の大手銀行のトップが議会でサイバーセキュリティの重要性を強調したのも、2020年7月に欧州連合がサイバー攻撃に対して史上初となる制裁措置を発動したのも、そのためです。

データセキュリティは複雑であるべきではありません。SecureAge Security Suiteは中小企業、政府機関、多国籍企業を問わず、複雑な作業を省き、予防措置として効果的にデータを保護することができます。

データを安全に保護しましょう。

SecureDataの暗号化テクノロジーの詳細については、こちらをご覧ください。

データセキュリティソフトウェア「SecureAge Security Suite」の詳細については、こちらをご覧ください。

ご意見・ご感想、デモのご希望、またパートナーシップのご相談については、contactus@secureage.co.jpまでご連絡ください。

ウェブサイト www.secureage.com
お問い合わせ contactus@secureage.co.jp

SecureAge

シンガポール 3 Fusionopolis Way, 05-21 Symbiosis, Singapore 138633
英国 74 Mackie Avenue, Brigton, BNI 8RB, Company No. 11734665
日本 105-0001 東京都港区虎ノ門1-16-6 UCF7F
北米 1801 Old Reston Ave Suite 301 Reston, VA 20190, USA