SOPHOS

ランサムウェアにおける バックアップの侵害がもたらす影響

過去 1年間にランサムウェアの被害を受けた 2,974社を対象とした調査分析

ソフォス ホワイトペーパー2024年 3月

はじめに

ランサムウェア攻撃によってデータが暗号化された場合、それを復旧する方法は主に、バックアップから復旧するか、または身代金を支払うかのいずれかです。攻撃者は、バックアップを侵害することで暗号化したデータの復旧を阻み、組織に対して金銭を支払うようにプレッシャーをかけます。

このレポートでは、ランサムウェアにおいてバックアップ侵害がもたらす影響を詳しく分析します。また、ランサムウェア攻撃におけるバックアップ侵害の頻度についても取り上げます。

調査の概要

ここでは、昨年ランサムウェア攻撃の被害に遭った世界 14カ国の IT/サイバーセキュリティ担当者 2,974人を対象に、ソフォスがベンダー不問の調査を実施した結果を紹介します。この調査は、独立調査機関の Vanson Bourne に委託して 2024年 1月から 2月にかけて行われ、回答者の過去 12カ月の体験に基づいています。回答者について詳しくは、本レポート末尾の付録をご覧ください。

エグゼクティブサマリー

ランサムウェア攻撃においてバックアップが侵害されると、財務および業務に計り知れない影響を与えます。バックアップが侵害されると、そうでない場合に比べて身代金を支払う確率は約 2倍に、全体的な復旧費用は 8倍になります。

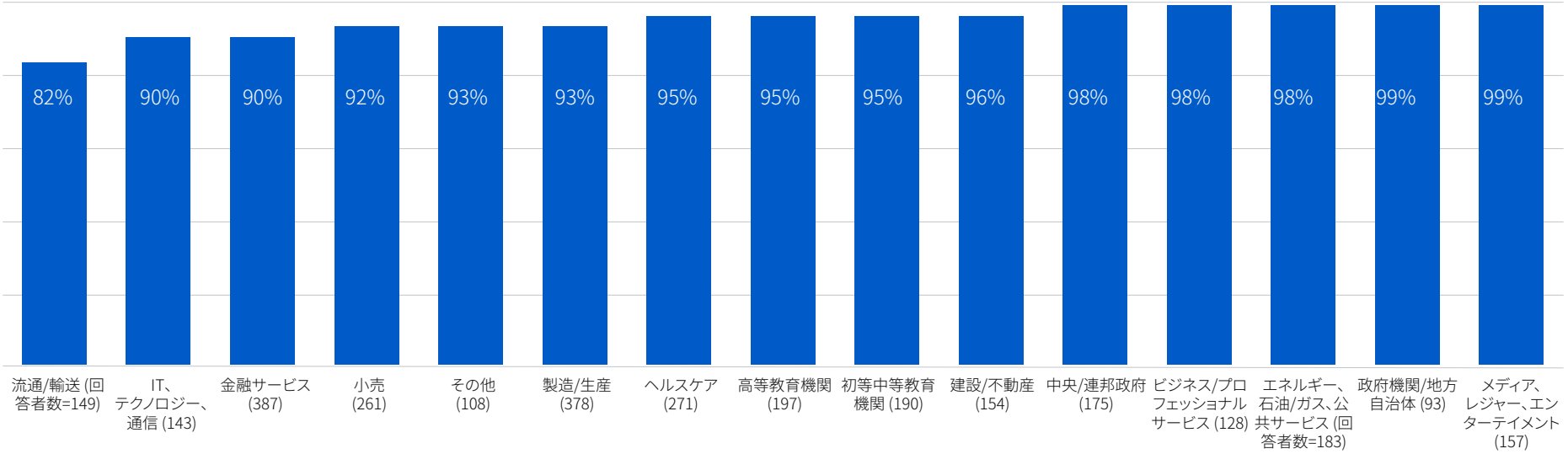
バックアップが侵害される前に悪意のある行為を検出・阻止することで、ランサムウェア攻撃による影響を大幅に軽減することができます。バックアップ侵害の防止策に投資することで、ランサムウェアへのレジリアンスを高めると同時に、サイバーセキュリティの全体的な総所有コスト (TCO) を削減できます。

調査結果 1:

ランサムウェア攻撃では、ほとんどの場合バックアップ侵害が試みられる

過去 1年間にランサムウェアの被害に遭った組織のうち 94% が、同時にバックアップの侵害も試みられたとしています。この割合は、地方自治体/政府機関、メディア/レジャー/エンターテイメントの業界では 99% に達しました。この割合が最も低かったのは流通/輸送業でしたが、それでも 10社中 8社以上 (82%) の組織が、バックアップへのアクセスが試みられたと回答しています。

バックアップの侵害が試行されたランサムウェア攻撃の割合



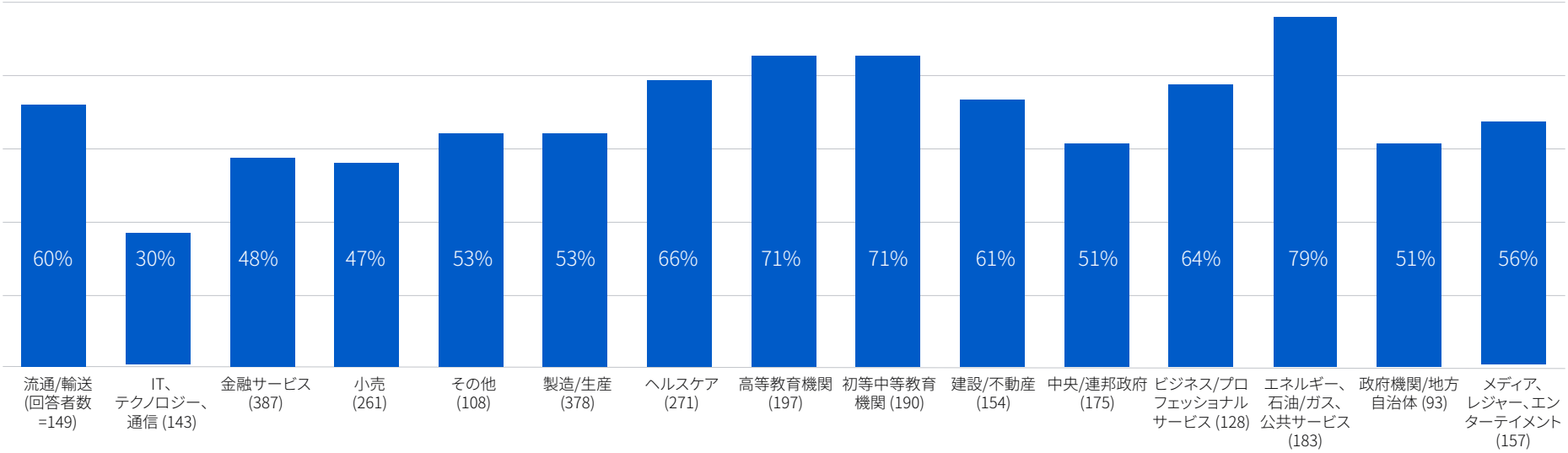
調査結果 2:
侵害の成功率は業界によって大きく異なる

こうしたバックアップ侵害の試行のうち、全体で 57% が成功しています。つまり、半数以上で、ランサムウェアからの復旧作業に影響が及んでいることになります。興味深いのは、こうしたバックアップ侵害の成功率が業界によって大きく異なる点です。

- エネルギー、石油/ガス、公共サービスでは 79%、教育機関では、71% と、被害者のバックアップの侵害の成功率が最も高くなっています
- 一方、IT、テクノロジー、通信では 30%、小売業では 47% と、バックアップの侵害の成功率が最も低くなっています

これには、いくつかの理由が考えられます。IT、テクノロジー、通信では、最初から強力なバックアップ保護対策が整っていたため、攻撃に耐え抜くことができたのかもしれません。または、侵害が試行された段階での検出・阻止が効果を発揮した可能性もあります。あるいは、エネルギー、石油/ガス、公共サービスの組織は、非常に高度な攻撃に遭う確率が高いのかもしれません。理由はともあれ、その影響は甚大です。

バックアップ侵害試行の成功率



調査結果 3:
バックアップが侵害された場合、身代金の要求額や支払い率が 2倍になる

データの暗号化
バックアップが侵害された組織は、そうでない組織よりもデータが暗号化される割合が 63% 高いことがわかりました。バックアップが侵害された組織のうち 85% が、データが暗号化されたと回答したのに対し、バックアップが侵害されなかった組織では 52% にとどまりました。この割合の高さは、全体的なサイバーレジリアンスが貧弱であることの表れであり、ランサムウェア攻撃の各段階にわたる防御が十分でないことを示唆しています。

身代金を要求
バックアップが侵害された組織はそうでない組織に比べ、要求された身代金額が平均して 2倍以上に達し、中央値はそれぞれ 230万ドル (バックアップが侵害された組織)、100万ドル (バックアップが侵害されなかった組織) でした。バックアップの侵害に成功した場合、攻撃者が強気になって高額な身代金を要求することができる、といえそうです。

身代金支払い率
バックアップが侵害された組織では、暗号化されたデータを復旧するために身代金を支払う割合が、そうでない組織に比べて約 2倍でした (67% vs. 36%)。

身代金額
バックアップが侵害された組織が支払った身代金額の中央値は 200万ドルで、そうでない組織 (106.2万ドル) の約 2倍でした。また、身代金額の引き下げ交渉においても、バックアップが侵害された組織では平均して要求額の 98% にとどまったのに対し、バックアップが侵害されなかった組織は、82% まで引き下げることに成功しています。

データが暗号化される割合

89%
バックアップが侵害された場合

52%
バックアップが**侵害されなかった**場合

要求された身代金 (中央値)

$230万 バックアップが侵害された場合

$100万 バックアップが**侵害されなかった**場合

データを復旧するために支払った身代金額

67%
バックアップが侵害された場合

36%
バックアップが**侵害されなかった**場合

身代金の支払額 (中央値)

$230万 バックアップが侵害された場合

$106.2万 バックアップが**侵害されなかった**場合

調査結果 4: バックアップが侵害された場合、ランサムウェアからの復旧費用総額が 8倍になる

ランサムウェア攻撃がすべて、身代金の支払いという結果につながるわけではありません。また、たとえ身代金を支払った場合でも、それはランサムウェア攻撃への対処や復旧にかかる全費用の一部でしかありません。ランサムウェアによって引き起こされる運用停止は、日々の業務に大きな影響を及ぼし、IT システムの復旧作業は複雑で、多額の費用がかかります。

ランサムウェアからの復旧費用総額の中央値は、バックアップが侵害された組織で 300 万ドルと、そうでない組織の 37万 5千ドルに比べ、8倍に達しています。この差にはいくつかの理由が考えられますが、主に、あらかじめ準備されたバックアップからの復旧に比べ、データを解読して復旧する場合は余分な手間が発生するということが挙げられます。また、バックアップの保護対策が不十分であるということは、堅牢な防御が不足している可能性を示し、再構築にかかる手間が大きくなります。

さらに、バックアップが侵害された場合は、復旧にかかる時間も大幅に長くなります。具体的には、1週間以内に完全復旧する割合が、バックアップが侵害されなかった場合は 46% であるのに対し、バックアップが侵害された場合はわずか 26% にとどまっています。

ランサムウェアからの復旧費用総額 (中央値)

$300万 バックアップが侵害された場合

$37.5万 バックアップが**侵害されなかった**場合

ソフォスの提言

バックアップは、サイバーリスク軽減のための全体的な戦略の重要な要素ですが、バックアップにオンラインでアクセスできるようにしている場合は、攻撃者にも見つけられる可能性があると考えたほうがよいでしょう。組織には以下の対策をとることをお勧めします。

- 定期的にバックアップをとり、複数の場所に保管する。クラウドのバックアップ用アカウントに MFA (多要素認証) を追加し、攻撃者からのアクセスを防止しましょう。
- バックアップから復元する練習をする。復元手順に慣れるほど、攻撃に遭ったときにすばやく簡単に復元できるようになります。
- バックアップを保護する。バックアップに対する不審なアクティビティは、侵害の兆候である可能性があります。こうしたアクティビティに監視の目を光らせて対応するようにしましょう。

ソフォスが提供する支援

Sophos MDR: ソフォスのエキスパートがバックアップを防御

Sophos MDR は、ソフォスのエキスパートが 24時間 365日体制で提供する Managed Detection and Response サービスであり、テクノロジーだけでは防止しきれない高度な攻撃の阻止を専門としています。500人以上のスペシャリストが、社内の IT/セキュリティチームではカバーしきれない部分まで幅広く対応し、社内の環境を監視するとともに、不審なアクティビティや警告が見られた場合は調査・対応にあたります。

Sophos MDR のアナリストが、既存のバックアップおよび復旧ソリューションから得たテレメトリ情報を活用しながら、バックアップの侵害を検出・阻止し、大きな被害が出る前にランサムウェアを無効化します。また、エンドポイントやメール、ファイアウォールの既存のセキュリティツールからのシグナルも活用して、ランサムウェアや不正行為を検出します。Sophos MDR が脅威を解決するまでの平均時間は 38分であり、次に襲いかかる脅威を上回るスピードで対応します。

Sophos XDR: 攻撃防止に役立つ可視性とツールを IT チームに提供

社内のセキュリティチームは、Sophos XDR が提供する可視性、分析情報、ツールを駆使することで、主な攻撃ベクトルの複数段階にわたる脅威を短時間で検出、調査して対応することが可能となります。具体的には、バックアップおよび復元ソリューションや、他のセキュリティ製品からのテレメトリ情報を活用することで、攻撃にすばやく気が付いて対応できるようになります。

付録

この調査は、以下の世界 14カ国の従業員数 100〜5,000人の中小企業を対象に実施されました: オーストラリア、オーストリア、ブラジル、フランス、ドイツ、インド、イタリア、日本、シンガポール、南アフリカ、スペイン、スイス、英国、米国。

2024-03-18 (WP-NP)

SOPHOS