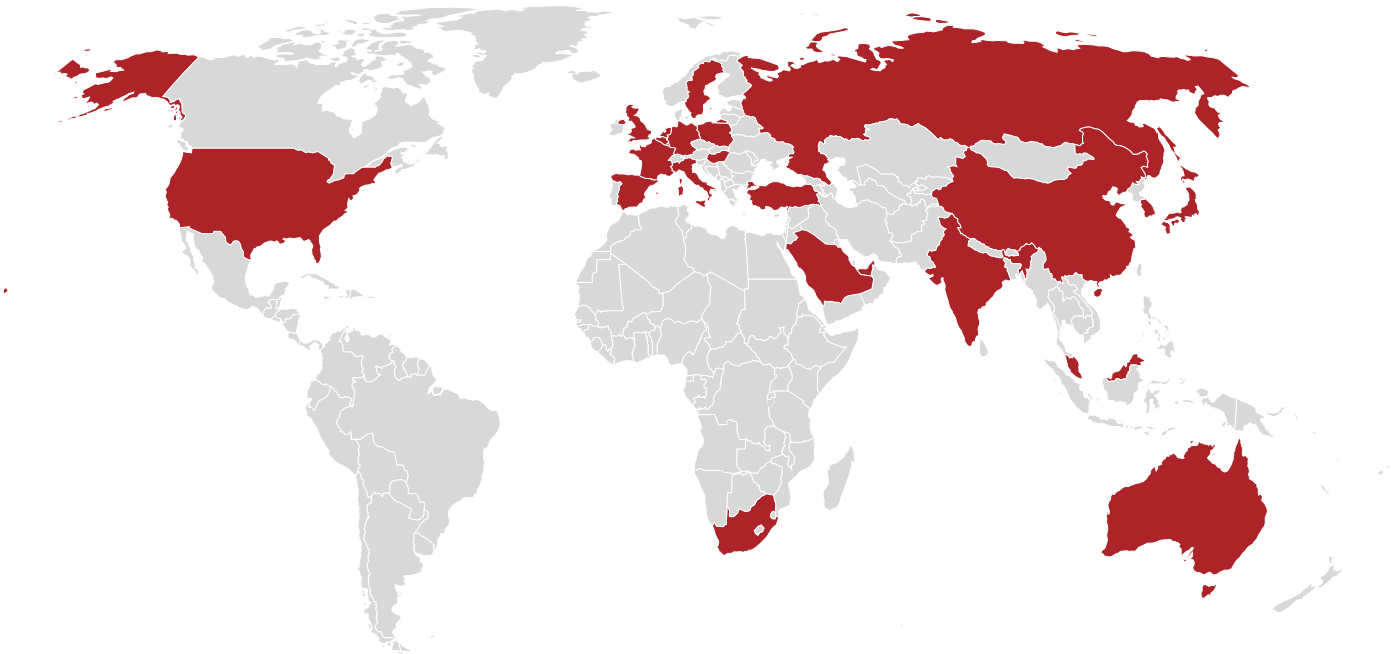
ベリタスのランサムウェア攻撃への対抗策の調査

世界的なパンデミックのために、デジタル変革、特にクラウドの導入が加速しています。企業では、拡大するリモートワークをサポートする必要があるため、生成されるデータが増えるとともに、アプリケーションを自社のデータセンターからクラウドに移行するという必要に迫られています。

この移行が加速する中、継続性対策が追いつかず、対抗策のギャップが生じています。その理由はさまざまですが、重要なのは、クラウドは導入しやすいプラットフォームである一方で、継続性を実現するためのプラットフォームの導入ははるかに難しいと考えられている点です。継続性対策を早期に策定して現在の IT のスピードに対応し、対抗策のギャップを解消することが企業にとって急務となっています。

2020 年 9 月、ベリタスは、ランサムウェア攻撃に対する準備と対抗策のレベルを把握するために、21 カ国の 2,690 名のシニア IT プロフェッショナルおよびエグゼクティブに対して世界的な調査を委託しました。



VERITAS

調査結果の概要は次のとおりです。

- 回答者の 64% が、自社のセキュリティ対策が IT の複雑さに対応できていないと考えています。
- 42% がランサムウェア攻撃を受けたことがあると答え、攻撃を受けた回数の平均は 4.5 回でした。
- COVID-19 パンデミックの渦中、従業員の分散やエッジデータ保護の需要の増加によってセキュリティリソースの負荷が高まっている時期に、多くの企業では IT セキュリティ予算を削減せざるを得なくなっています。
- 過去 2 カ月以内にディザスタリカバリをテストした企業は半数未満であり、大部分の企業がランサムウェア攻撃から完全にリカバリするのに 5 日以上かかると予想しています。
- ランサムウェア攻撃が発生しない安全な場所はありません。オンプレミスリソースとほぼ同じぐらいの頻度でクラウド内のデータとアプリケーションも攻撃の対象になっています。
- データのコピーをオフサイトの 1 つのコピーを含めて 3 つ以上、データセンターとは別の場所に保管している企業は 3 分の 1 をわずかに超えるほどです。
- ランサムウェア攻撃者は大企業を標的としています。潜在的に投資効果が高いとわかっているからです。

データとアプリケーションの配備における迅速さ、柔軟性、俊敏性といったハイブリッドマルチクラウドのメリットは、多くの企業にとって魅力的です。

しかし、メリットを感じている企業の多くがそのメリットを維持できていません。犯罪者はますます効果的かつ破壊的な手段を導入して企業のデータやワークロードを人質に取り続けているため、企業は今すぐに対応が必要です。より確信を持ってハイブリッドマルチクラウド戦略を進められるよう、耐障害性アプローチを直ちに評価し、データとアプリケーションの存在場所に関係なくバックアップとディザスタリカバリプロセスを強固なものにして、対抗策のギャップを解消する必要があります。

VERITAS