DELL Technologies

ホワイトペーパー

サイバー ストームにおける Sheltered Harbor

Sheltered Harborとデル・テクノロジーズによる共同ホワイトペーパー

はじめに

残念なことに、破壊的なランサムウェアベースのサイバー攻撃が日常的に発生するようになり、その被害がニュースで頻繁に取り上げられています。2020年には、身代金として総額3億5000万ドル以上が犯罪者に仮想通貨で支払われました[1]。利益性が高いため、サイバー犯罪者が団結して作り上げた高度で活発な地下経済は、消滅することはないだろうという見解をThreat Postは示しています[2]。

このような攻撃による痛手は、手間や経費だけではありません。世界的な経済活動を後押しする、重要なインフラストラクチャ、機関および組織の存続、消費者の信頼と安心感も脅かされます。また、死傷事故に発展するケースもあります。さらに、ホワイト ハウスが2021年6月に発表した通達は、「組織の規模や所在地を問わず、あらゆる企業がランサムウェア攻撃の対象となる可能性があることを、すべての組織が認識すべき」という内容でした[3]。このきっかけとなったのが、2021年5月に発生した3件の攻撃です。1件目は、米国の重要なパイプライン企業に対するもので、東海岸では攻撃直後からガソリン不足に陥りました。2件目では食肉サプライ チェーンが破壊され、3件目ではアイルランドの大部分で医療サービスが中断しました。

多くの人にとって、攻撃のペースは速まっているように見えますが、攻撃自体は目新しいものでありません。それでも組織は、最善の備えや対応の方法を見い出そうと、悪戦苦闘し続けています。攻撃の防止または範囲を限定的なものにすることを目的としたサイバーセキュリティ制御は、依然として重要ですが、結局のところ、それで十分とは言えません。人間とITシステムとの相互関係、高度なサプライ チェーン攻撃、ゼロデイ脆弱性、その他の高度な技術によって生じる課題がある限り、一部の攻撃は成功してしまいます。組織は、攻撃の被害を受けた後のITシステムをリカバリーして以前の「良好な」状態に戻せるようにするなど、耐障害性（レジリエンス）を備える必要があるのです。

このホワイト ペーパーでは、レジリエンス戦略全般の形成に役立つ2つの類似したフレームワークについて詳しく説明します。

極端だが起こりうる状況に対する唯一のアプローチ

2015年初頭、ある国家が世界的なエンターテインメント企業に仕掛けた今や悪名高いサイバー攻撃をきっかけに、多くの組織がサイバー攻撃による破壊の問題に対処し始めました。かつて、犯罪的なサイバー活動のほとんどは、組織からデータを盗み出すことに重点を置き、攻撃者の存在が明らかになるような検出やあらゆる混乱を回避するため、特別な仕掛けをするのが一般的でした。そのため、ITインフラストラクチャに対する攻撃を通して、直接、組織に害を及ぼしたり、組織を破壊したりするように設計されたサイバー攻撃は、新たな問題を提示したのです。

この事態を受け、2015年には、大手金融機関、業界団体、大手サービス プロバイダーが、このような攻撃による米国金融システムへのリスクを評価し解決することを目的に、Sheltered Harborイニシアティブを確立しました。デル・テクノロジーズ（当時のEMC Corporation）も、金融業界と他の業界の最も重要なお客様から要請を受け、この問題に着手しました。

Sheltered Harborと当社の目標はわずかに異なりますが、両組織とも、同じ基本の3部構成のフレームワークで問題に取り組みました。

- 「極端だが起こりうる状況」に直面した場合に、保護の対象となり、耐障害性を持つ必要がある、最も重要なビジネス サービスを特定し、最終的には、それらのサポートに必要なITデータやアプリケーションにマッピングすること
- 安全性の高いデータ ヴォールト内で、プロセスをサポートするデータやアプリケーションを保護し、このようなヴォールトに必要な要件を定義すること
- 基本目標を達成するために必要なパラメーター（極端な状況に陥った場合のRPOやRTOなど）内で、極端な状況からのリカバリーを可能にする計画とプロセスを有効にすること

このような要件それぞれについて、Sheltered HarborとDellでは若干異なるアプローチを採用しましたが、そのアプローチは、レジリエンスの強化を目指す、すべてのユーザーに役立つはずです。

懸念事項1：保護対象を特定する

最初は、組織の存続に最も重要なもの、つまり、極端な状況からのリカバリーを可能にするために保護対象を特定するのは簡単なように思えます。ところが実際には、非常に複雑なプロセスになることがあります。それでも、その後のプロセスを進めるためには、この最初のステップを正しく実行することが不可欠です。

[1]Ransomware Task Force、『Combating Ransomware A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force』：https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force_Final_Report.pdf

[2]Threat Post、『A Peek Inside the Underground Ransomware Economy』：https://threatpost.com/inside-ransomware-economy/166471/

[3]ホワイト ハウスの発表、2021年6月2日、「What We Urge You To Do To Protect Against The Threat of Ransomware」：https://docs.google.com/viewerng/viewer?url=https://www.mainstream-tech.com/wp-content/uploads/2021/06/White-House-Memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware17.pdf&hl=en

第1の鍵は、作業の主な目標を具体的な言葉で明確に示すことです。このためには、生き残るために不可欠なビジネス ニーズを幅広く把握する必要があります。つまり、IT部門の垣根を超え、サイバーセキュリティ、さらにはリスクやコンプライアンスに関与している人に限らず、幅広い視点が必要です。このステップから、サービスのサポートに必要な機能を特定できます。このデジタル世界では、ほとんどの場合、情報技術に重点が置かれます。

ビジネス プロセスと情報技術に必要なコンポーネントについても、非常に細かく決定する必要があります。そのなかには、急速または頻繁に変化する可能性のあるデータ（預金者とその口座残高のリストなど）が含まれます。そのデータを使ってやり取りを行う既製のアプリケーションやカスタム アプリケーション（データベース アプリケーション、コア バンキング アプリケーション、取引プラットフォーム）が必要になる場合があります。また一般に、ドメイン コントローラーや認証テクノロジー、サーバー名を解決するためのDomain Name Service (DNS)などのテクノロジーに「接続」する必要もあります。

Sheltered Harborは、消費者の信頼感を保つという非常に明確で焦点を絞った目標を持っていました。これがさらに洗練され、機関自身による復旧ができるようになるまで、または最悪でも問題が解決されるまでは、プロセスを機能させるといった目標になりました。このように目標と運用期間を絞ったことにより、Sheltered Harborは、すべてを2つの機能と基本的なサービスにまとめることができました。顧客は、引き続き、口座の残高情報と資金にアクセスできるようにするということです。その結果、Sheltered Harborの仕様は、具体的な業界標準データ セットに焦点を当てることが可能になりました。この具体的なデータ セットに絞ったことで、無数のアプリケーションと基盤となるテクノロジーも保護しなければならないという困難な状況に陥らずにすみ、これら2つの重要なビジネス サービスに共通のリストア プラットフォーム（パート3で説明）を作成できるようになったのです。

Sheltered Harborの基準では、重要な顧客口座情報の安全なデータ ヴォールトと、レジリエンス計画を組み合わせ、最悪のシナリオでもお客様がデータと資金にタイムリーにアクセスできるようにします。Sheltered Harborのレジリエンス基準は実証済みで成熟しており、導入、実装、認定をサポートするエコシステムを備えています。基準の実装に成功した金融機関は、Sheltered Harbor認定を取得できます。Sheltered Harborは現在、米国のあらゆる種類の金融機関を対象にしています。その範囲は、当初の基盤である銀行、信用組合、ブローカーディーラー、業界団体、コア サービス プロバイダーを超えて拡大しています。最新の基準では、今や、保険会社、証券保管機関、資産管理会社、手形交換所などにも対応しています。詳細については、「shelteredharbor.org」を参照してください。

Dellのプロセスは、開始方法こそSheltered Harborと似ているものの、それ以降はすぐに違うものになります。プロセスは、お客様に固有であり、通常は、お客様独自の生存能力の維持に重点を置いているためです。さらに、Dellのお客様は、業界、規模、洗練度がそれぞれ異なります。そのため、実際に使用する質問も若干異なり、組織を動かすために最も重要なサービスは何かを尋ねます。重要なサービスの決定は、組織ベースで行うことができ、多くの場合、収益や利益、ブランドや知的財産の保護、規制当局への対応に重点が置かれます。

重要なサービスが定まったら、それらのアプリケーションの基盤となるテクノロジー コンポーネント（データベース、設定ファイル、アプリケーション コードなど）も特定し、保護されるようにする必要があります。最終的には、アプリケーションに必要な主要基盤テクノロジー（Active Directory、DNSなど）も特定します。

懸念事項2：データ ヴォールトの特徴

保護対象を特定したら、次はどのように保護すべきかを考えます。組織は、さまざまな方法でデータを保護します。たとえば、ロール ベースのアクセス制御、暗号化（転送中、保存中、場合によってはアプリケーションまたはデータベース レベル）、レプリケーションとバックアップといった方法です。一般的な制御の多くは、不正アクセスを防ぐため、データの機密性を保護するように設計されています。この目的では、データの可用性と整合性が最も重要になります。

このユース ケースでは、データを可能な限り最強の方法で保護する必要があることが直ちに判明しました。データは、高度で意図的な最悪の状況、つまり、本番環境を完全に制御し、最も一般的なセキュリティ方法を回避できるアクセス権と知識を持つ攻撃者からの侵害を、乗り切る必要があったのです。このため、Sheltered HarborもDellもすぐに、データ ヴォールトの概念を採用しました。データ ヴォールトとは、データを安全に保管できる、非常に安全性の高い環境です。アクセスできない状態を保ちますが、更新中でも、安全です。

Sheltered Harborは、データ ヴォールトについて重要な要件をいくつか規定しています。

- 不変（変更不可、削除の対象外）
- エア ギャップを設ける（本番環境およびバックアップ システムから分離）
- 存続可能、アクセス可能（侵害される可能性のあるインフラストラクチャに依存しない）
- 分散型（単一の本番環境に依存しない）
- 金融機関による、データの完全所有とヴォールト制御

これらの主要原則は、Sheltered Harborのデータ ヴォールト仕様の基盤となっています。

Dellも同様の要件に行き着き、最終的に次の3つの主要機能となりました。

- **分離：**ヴォールトのコンポーネントは分離し、攻撃者からアクセスできないようにする必要があります。この結果が「エア ギャップ」です。この用語は、ヴォールトのコンポーネントが物理的に分離された領域にあり、通常はアクセスできないように「オフ」状態になっていることを示します。さらに、このオン/オフ メカニズムを安全な場所から制御し、本番環境を制御する攻撃者が操作できないようにする必要がありました。

- **不変性：**ヴォールトに書き込まれたデータは「不変」である必要があります。Dellにとってこれは、Data Domainプラットフォームのコンプライアンス保存ロック機能を意味していました。この機能は、17a-4(f)(ii)下で広く知られた記録基準を満たしていると何年も前から証明されています。そこに、時間ベースの攻撃など、記録基準では必要なかったさまざまな攻撃ベクトルを考慮できるよう、さらなる強化が加えられました。

- **インテリジェンス**：この機能は、保護されているデータがリカバリーに有効かどうかを判断するためのものです。これには、マルウェアではなく、ヴォールトのデータをスキャンして破損の証拠を探す機能が必要です。

懸念事項3：データ ヴォールトの特徴

最終的な目標は、データの保護ではなく、予期せぬ状況や攻撃の後に、保護されたデータやその他のシステムを使用し、重要なオペレーションとサービスを可能な限り迅速かつ効率的にリストアすることです。目標が異なるため、Sheltered HarborとDellではプロセスも異なりますが、出発点は同じ懸案事項でした。

Sheltered Harborは、当初、預金口座および証券口座の所有者を対象にし、一般社会からの信頼の維持に重点を置いていたため、口座の残高情報の提供とその口座からの資金利用を可能にするビジネス プロセスに専念できました。このようなプロセスは非常に普遍的なものであるため、Sheltered Harborコミュニティーでは、証券口座または預金口座の標準化されたデータ セットを理解する共通の「リストア プラットフォーム」の仕様を定義できました。また、このようなサービスに頼るように業界が調整されたため、既存の業界サービス プロバイダーがこのような「リストア プラットフォーム」を構築して利用できるようになり、あらゆる人のコストとリスクを削減する共通のソリューションが実現したのです。このとき、Sheltered Harborコミュニティーでは、重要なビジネス プロセスと、参加しているすべての機関にメリットをもたらす迅速なリストアに欠かせない技術的機能を定義しています。

Dellのモデルは、攻撃後のリカバリー プロセスに適した基盤の構築を促し、お客様がサイバー攻撃固有の目標リカバリー ポイント(RPO)と目標リカバリー時間(RTO)を合理的に確立できるようにしています。通常、このRPOとRTOはディザスター リカバリー(DR)のものとは大きく異なります。DRのアクティブ/アクティブ アーキテクチャは、RPOはゼロまたは最小限にし、即座のRTOで構築されます。このような設定は高度なサイバー攻撃には通用しません。高度な攻撃を調査している間は、データ センターを一時的にシャットダウンしなければならない場合があります。また、フォレンジック プロセスを完了する必要があり、根本原因を特定してからクリーンアップ/リカバリー手順が開始されます。

そこから、リカバリーにさまざまな形式を取ることができますが、通常は、リストア用の重要な再構築材料（AD、DNSなど）、アプリケーション、データの安全性を再度確認した後、元の環境に安全に戻されます。このプロセスは一般に、攻撃の範囲と洗練度、関連する破壊の規模に大きく依存します。アプリケーションは、本番環境に直接リストアされることも、「クリーン ルーム」環境で一旦リカバリーされ、詳細なフォレンジック テストを実行してから本番環境に戻されることもあります。組織がリカバリー シナリオの進め方を確実に理解できるよう、ラン ブックが作成され、テストされます。

Dellは、パブリック クラウドやプライベート クラウドなどの別の場所へのリカバリー、またはITサービス プロバイダーなどのサード パーティーが提供する共有インフラストラクチャといった利用可能なインフラストラクチャへのリカバリーが可能になっていることに注目し、リカバリー プロセスが成熟し始めていると考えています。たとえば、オンプレミス アプリケーションを保護するデータ ヴォールトを使用することで、フォレンジック、根本原因の追求、クリーンアップなどを待たずに、共有インフラストラクチャ環境へのリカバリー操作を直ちに開始できます。これにも安全なリカバリー プロセスが必要であり、フェールバックに関する考慮事項を解決しなければなりませんが、RTOをしっかりと最小限に抑える機会はあります。

この代替リカバリー プロセスは、Sheltered Harborモデルと興味深い類似点がありますが、インフラストラクチャが関与する可能性が高く、データのみを操作する必要がある完全なリストア プラットフォームではありません。

まとめ

金融機関に対するランサムウェア攻撃または破壊的なサイバー攻撃が成功すると、コンプライアンス、財務、法務、規制、評判に大きなリスクが生じ、組織の運営能力が妨げられ、消費者の信頼と、おそらく組織の存続が脅かされる可能性があります。金融機関としては、お客様の口座を保護する責任があります。米国金融システムに対する世間の信頼を守るため、ご協力ください。Sheltered Harborへのご参加をお待ちしております。

もたらされるメリット

- 顧客口座データの保護およびリカバリーを目的とした、業界で開発された標準への排他的アクセス
- 仕様、該当する分野のエキスパート、ワーキング グループ、フォーラム、実装ガイド、インシデント プレイブック
- レジリエンスに優れたデータ保護の継続的な開発のサポートと、保護対象の資産クラスと地域を拡張するSheltered Harborを利用しての成長
- 極端な状況への対応とリカバリーに備える
- データ保護とレジリエンスに対する米国金融規制機関による認知
- 実装しやすく、認定されやすい
- 金融機関のレジリエンスと評判の向上
- 低コスト、高価値
- Sheltered Harborの極端なケースだけでなく、そのベスト プラクティスも活用

費用

Sheltered Harborへの参加費はわずかです。年間参加費は、資産規模に応じて250ドル～50,000ドルです。実装コストは、組織の規模と複雑さ、インフラインフラストラクチャ、運用、スキル ベースによって異なります。データ ヴォールトの詳細については、Dell Technologiesのアカウント担当者にお問い合わせください。

作成者

Sheltered Harbor
プレジデント兼CEO
Carlos Recalde氏

Dell Technologies
サイバーセキュリティおよびコンプライアンス プラクティス担当ディレクター
Jim Shook

Dell EMC Power Protect Cyber Recoveryの詳細を確認する

お問い合わせ先
デル・テクノロジーズ エキスパート

サイバー レジリエンス評価を受ける

#PowerProtectで会話に参加