rubrik

ユバ郡が語るランサムウェア攻撃を撃退した方法

業界

地方自治体

結果

- ランサムウェアによる身代金の支払はゼロ
- 7日以内にバックアップを100%復元
- 管理時間を90%以上短縮
- ほぼゼロのRTO

課題

- 感染したPCから始まった攻撃
- ADサーバーに潜むKerberos認証の問題
- 約50台のPCと100台のサーバーに対する暗号化攻撃

ビジネス変革

ユバ郡はRubrikを使ってDR戦略を強化できたのはもちろん、ランサムウェア攻撃を撃退し、難局を乗り切りました。Rubrikによりバックアップは100%復旧でき、データの身代金を支払わずに済むと知り、ユバ郡は安心できました。

パートナー

ePlus

ユバ郡はカリフォルニア州北部に位置する小さな町です。郡政府内には医療や公共の安全を指揮するさまざまな部門があり、保安官事務所も含まれています。こうした部門では消防や救急の911番要請に対応しています。保健部門も重要な組織で、新型コロナウイルスの検査や接触追跡、ワクチン接種の管理を担当しています。すべてがユバ郡の住民の生活に欠かせないサービスです。

ユバ郡の元CIO、Paul Lavalley氏は、コミュニティの安全と生活を支えるための、常に利用可能な信頼性の高いインフラストラクチャの提供を担当する16人のチームを監督しています。主にパンデミックの影響でリモートワークが普及して、ランサムウェア攻撃が急増し、サイバー犯罪者にとって利益を生むビジネスになりました。

「2021年2月に私たちを襲ったランサムウェア攻撃は郡の機能を停止させる可能性もありました。しかし、その不安な数週間の中で数少ない達成感を覚えた瞬間がありました。Rubrikがデータをバックアップしていることと、データの復元に身代金を支払う必要がないこととを知ったときです」とLaValley氏は振り返りました。

DoppelPaymer、Dridex、IceIDによる攻撃

ユバ郡はDoppelPaymerランサムウェアのメッセージが複数のサーバーとPCに表示されて、ランサムウェアに攻撃されたことを確信しました。「気付いた頃には、およそ50台のPCと100台のサーバーが暗号化されていました」とLaValley氏は状況を話してくれました。これより前に、侵害されていることを示す複数の兆候がありました。

「まず、Active Directory（AD）サーバーのKerberos認証に問題があり、それが通信を阻害していることに気付きました。その夜遅く、GPOがプッシュされ、エンタープライズAD管理者アカウントが作成されました。フォレンジック分析により、Dridex、Cobalt Strike、IcedID、PowerShellスクリプトのすべてが攻撃の一部に使用されていることが分かりました。それらを基に、この侵害が以前はゴールデンチケット攻撃と呼ばれていたKerberos攻撃であると理解しました。これはADを侵害し、複数の機器を暗号化するランサムウェアを展開する攻撃です」とLaValley氏は付け加えました。

ユバ郡に適したランサムウェアサバイバルキット

ユバ郡はどのように対応したのでしょうか？ 複数のフェーズがあります。LaValley氏は「最初の24時間、すべてのサーバーを切断し、ファイルをバックアップしました。また、管理者アカウントを無効にし、パスワードをリセットしました」と説明しました。「次のステップは部門通知とユーザー通知の再開でした。部門長、郡の管理者、ユーザーに状況を連絡しました。FBIやカリフォルニア州緊急サービス室を筆頭に、州のさまざまな機関にも連絡しました。さらに、米国外のすべての送受信ネットワークトラフィックを遮断しました」

ユバ郡はRubrikを使用して、わずか数回のクリックでランサムウェア攻撃から迅速に復旧し、データを侵害される前の最新の状態に復元できました。「ランサムウェア攻撃に対する防衛手段として、バックアップは1番とは言わずとも最も重要な手段のひとつです。Rubrikのファイルシステムは書き換え不可のため、ランサムウェアがバックアップのデータを暗号化したり、削除したりすることはできません。また、90%が仮想サーバーなので、ライブマウントでRubrik上にあるものをすべて復旧できたことは本当に幸運です」とLaValley氏は述べました。

ユバ郡がRubrikを導入することとなった最初のきっかけは、さまざまな種類の災害対策（DR）が必要だったことです。当時、ユバ郡が整備していたDR戦略は一般的な洪水または地震に対応するためのもので、現在の脅威、特にランサムウェアには適していませんでした。「Rubrikはこの困難な状況下で私たちのデータを守ってくれました。書き換え不可の機能、MFA、リテンションロック機能のおかげです。Rubrikによって、ハッカーがADを制御下に置いていることを把握できたので、私たちはRubrikに結びつくあらゆるもののADを確実に排除し、書き換え不可の保護された保管庫を構築しました」とLaValley氏は説明しました。

「言うまでもなく、私はこのプロセスを通じて多くのことを学びました。再発や別のランサムウェア攻撃のどちらも阻止できるシステムが整っていることが分かっているので、夜はぐっすり眠れるようになりました」とLaValley氏は語りました。その他のメリット

- **ランサムウェアによる身代金の支払はゼロ：**「その不安な数週間の中で数少ない達成感を覚えた瞬間がありました。Rubrikがデータをバックアップしていることと、データの復元に身代金を支払う必要がないこととを知ったときです。これにより郡の費用が、数百万ドルとはいかなくとも、何百ドルも守られたことでしょう」
- **7日以内にバックアップを100%復元：**「Rubrikのネイティブに書き換え不可特性のおかげで、Rubrik上にあるものをすべて復旧でき、身代金を払わなくて済みました」
- **管理時間が90%以上削減（26日分の生産性向上）：**「以前は、バックアップの管理に毎週4～5時間かけていました。Rubrikを使うようになって、今では毎週30分に短縮されました。その結果、チームの生産性は26日分向上しました。小さな事務所なので、専任のバックアップ管理者はいません。時間を少しでも節約して他のプロジェクトに尽力できるのは重要なことです」
- **世界水準のサポート：**「攻撃に気付くとすぐに、Rubrikのサポートチームが加わり、復旧作業を優先してくれました。彼らは24時間体制でシステムの継続性の維持に貢献してくれましたし、いつでもサポートしてくれました。Rubrikチームには感謝してもしきれません」
- **復元可能な隔離されたバックアップ：**「攻撃者がアクセスできない隔離された復元可能なバックアップを所有しておくことは、ランサムウェア攻撃に対する防御の重要要素です。攻撃を止めることはできませんが、少なくともRubrikで復元できるデータを保持できます。この安心感は非常に価値のあるものです」
- **ほぼゼロの目標復旧時間（RTO）：**「従来のソリューションでは、きめ細かいレベルの復元ができませんでした。法的証拠開示手続きのためにオンプレミスのファイルサーバーを復元する責務を負っていましたが、1つのファイルサーバーイメージを復元するために、バックアップ全体を復元するはめになりました。このプロセスを完了するのに1週間かかり、さらに悪いことに、バックアップが停止してしまいました。Rubrikの場合、オンプレミスおよびクラウドからデータを復元するのに数分しかかかりません。雲泥の差です。また必要なものだけを復元できるきめ細かさもあります」

rubrik

本社
3495 Deer Creek Road
Palo Alto, CA 94304
米国

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com/ja

20230202_v1