ランサムウェア攻撃から学んだ5つの教訓

DXC Technology上級副社長、マーク·ヒューズ

ランサムウェア攻撃ではダウンタイムによる大きな被害が発生するため、すばやい対応が必須です。

ランサムウェア攻撃の増加はこれまでにも多く報告されていますが、ランサムウェア攻撃は企業の顧客、事業運営、ブランド価値、さらには取締役会に至るまで、ビジネスのあらゆる部分に影響する深刻な被害をもたらす恐れがあります。

DXC Technologyでの職務の一環として、私はDXCのセキュリティビジネスを監督し、お客様が受けるサイバー攻撃にたびたび対応しています。しかし、2020年7月4日土曜日、家族とのバケーションに向かう車から降りようとしていたとき、当社がランサムウェア攻撃の標的になりました。

当社への攻撃は、英国を拠点とするDXCの子会社であるXchanging社に関係するものでした。Xchanging社は、商業保険業界にテクノロジーを活用したビジネスサービスを提供しています。攻撃者はこういった攻撃でよく使われる、人気のアニメキャラクターが不快な手ぶりをしている画像とともに、次のメッセージを送りつけてきました。「あなたのデータをいただきました。あなたのファイルを暗号化しました。交渉が必要な場合は、安全なツールまたはチャットセッションで話し合えます」

Xchanging社のネットワークはDXCの非常に大規模なIT環境からは分離されていたとは言え、ロンドンの保険会社の事務所が月曜日に業務を開始した際に、この攻撃がXchanging社のお客様の業務に影響を与えることがないかを私たちは懸念していました。

ランサムウェア攻撃ではダウンタイムによる大きな被害が発生するため、すばやい対応が必須です。Emsisoft社によると、ランサムウェア攻撃による重要なシステムの停止は平均で16日間に及び、2020年の世界のランサムウェア総被害額は1,700億ドルに達する可能性があると予測されています。

Xchanging社のケースでは、ハッカーが最初に侵入したのはわずか2日前でした。侵入されたシステムはほんの一部であり、私たちは脅威をすばやく分離して制御できたため、データは何も盗まれず、身代金も支払いませんでした。私たちはすぐにお客様や司法当局と連携を取り、7月5日の日曜日には影響を受けた環境をクリーンアップして復旧したことにより、月曜日の朝までにはXchanging社は平常通りに保険証券の処理が可能になっていました。

安全を維持するためのヒント

本件の捜査は進行中であり、私たちはあらゆる場面で当社の管理手順を見直してきましたが、ほぼすべてが計画どおりに機能していたと言えます。ところが、残念ながら多くの企業組織では状況が異なります。

私たちは、適切に機能したこと、機能しなかったこと、そして改善できることを分析しました。以降に、重要な5つのポイントを説明します。

インフラストラクチャの把握: 基本的なソフトウェアパッチのハイジーン (衛生管理) に重点を置き、悪意ある動作を検出するためのエンタープライズセキュリティツールがすべてのネットワークとファイアウォールに展開されていることを確認します。今回の攻撃者は「グレイウェア」と呼ばれる公開セキュリティテストツールを足掛かりとしていました。グレイウェア自体は悪意のあるものではありませんが、本事例ではMicrosoft Windowsを悪用し、新しい暗号化マルウェアの亜種を展開するためのバックドアを作成する目的で利用されました。私たちは攻撃を阻止することはできませんでしたが、異変について警告を受け、攻撃の進行中にネットワークの侵害部分をすばやく特定することができました。

当局は身代金を支払わないことを強く助言しています。実際、米国と英国は身代金の要求に対して民事処分のみならず刑事処分までをも課す方向に向かっています。

初期対応から上級管理職が関与する: 私たちのグローバル危機対策チームは状況を把握するために集まりましたが、重要な決定を迅速に下せるように上級管理職を直接関与させたため、この集まりは私たちにとって重要なことでした。たとえば、リモートアクセスを遮断する必要があったため、Xchanging社のシステムへの接続をすべて切断する決定を下しました。これは簡単に聞こえますが、英国だけでなくインドのITチームによる緊急対応が必要であり、双方のチームリーダーを関与させたことで迅速かつ効率的に遮断できました。今回の対応全体を通じて、DXC CEOのマイク・サルヴィーノを含むリーダーたちが状況の判断と重要な決定に加わりました。今の時代には優れたガバナンスが不可欠であり、説明責任や誰が何を担当しているのかが明確でないと、貴重な時間を無駄にし、攻撃者にその隙を悪用されてしまいます。

司法当局や専門家との早期の連携: 司法当局とセキュリティの専門家は、サイバー攻撃への対処方法や、迅速な法的介入を可能にする方法について貴重な知見を提供してくれます。たとえば、今回のランサムウェアではXchanging社のデータを米国のWebサイトドメインに送信するように設定されていたため、祝日と重なった週末に勤務している司法当局者に連絡し、その日の夜に攻撃者のインターネットドメインを掌握する裁判所命令を得ました。

できるだけ多くのサポートを得て、身代金を支払わない: 司法当局は身代金を支払わないことを強く助言しています。実際、米国と英国は身代金の要求に対して民事処分のみならず刑事処分までをも課す方向に向かっています。私たちの場合、攻撃者は最初に金銭を要求せず、交渉を望んでいました。私たちは、攻撃を遮断したこと、攻撃者が私たちのデータを盗んでいないこと、そして私たちにはバックアップデータがあることを把握しており、強い立場にあったので交渉する必要はありませんでした。もし、あなたがサイバー犯罪者と交渉することを選択した場合は、単独で交渉してはいけません。経験豊富な身代金ブローカーを探して確保してください。できれば攻撃を受ける前に、インシデント対応の準備の一環として行うことが推奨されます。

透明性の確保: すべての事実を明らかにする必要はありませんが、一般的にオープンであることは有効な手だてあり、実際に私たちは攻撃者の侵入の痕跡 (IoC) を数百のお客様と共有しました。確かに公開できない情報もあるかもしれませんが (たとえば、顧客の守秘義務制限の対象である場合や司法当局の指示など)、公開できる情報を共有することは、他の人々の安全を守るだけでなく、多くの同僚、司法当局、セキュリティコミュニティに支援を求める場合にも役立ちます。私たちは7月5日の日曜日にランサムウェア攻撃に関するニュースリリースを公表した後、数週間後にもう一度封じ込めの確認に関するニュースリリースを公表しました。

その週末に私が話した司法当局者は、攻撃がすでに封じ込められていることに驚いていました。司法当局者が受ける電話のほとんどはCEOからのものですが、これはITチームとセキュリティチームが必死に奔走しており、企業は業務を停止してから3〜4日経っても通常は終わりが見えないためです。

7月4日のランサムウェア攻撃の被害はもっと大きくなっていた可能性があると考えています。迅速なインシデント対応、セキュリティ管理、ガバナンスに加えて、技術ツールと業界におけるベストプラクティスの活用が、私たちに優位に働きました。

「新しいDXC」は、常にお客様のことを第一に考え、サイバー脅威の課題に対処します。

以上が私が夏休みに経験したことです。

最新のサイバー脅威について常に把握しておくことが大切です。**www.dxc.technology/threats_HBR** (英語) でDXCのセキュリティ脅威インテリジェンスレポートをご購読ください。

著者について

マーク・ヒューズ
DXC Technologyのオファリング・戦略パートナー担当上級副社長。サイバーディフェンス、セキュアインフラストラクチャ、デジタルID、データ保護など、DXCのグローバルセキュリティ組織およびオファリングの責任者。以前は、BT Security社の最高責任者を務めていました。

DG_8078a-21。2020年11月