次世代ファイアウォールが IT ソリューションプロバイダを 大規模ランサムウェア攻撃から救う

マネージドアプリケーションの小規模プロバイダとして創業したこの企業は、わずか 10 年で大手クラウドホスティング / サービス会社へと成長し、VoIP ソリューションをはじめとする総合 IT サービスを手掛けるようになりました。

大規模ランサムウェア攻撃に突如襲われる

同社のインフラストラクチャには、業界大手のネットワークベンダーのファイアウォールの中でも最上位モデルの 1 つが導入されており、30,000 件の電子メールボックスを管理し、50,000 以上の Web サイトを運用していました。2 か所のデータセンター、5,000 の仮想マシン、300 台の物理サーバーで構成される、盤石と思える環境だったのです。

ところが、セキュリティ対策は十分ではありませんでした。突如として、データセンターが大規模ランサムウェアに攻撃されたのです。4,000 のアクセスポイントが CryptoLocker ランサムウェアによってブロックされ、14,000 を超えるクライアントのユーザーが 3 日以上にわたってアクセス不能になりました。

同社の最高技術責任者は、悪夢と言うべき当時の状況を次のように振り返ります。「システムに侵入した攻撃者に、私が使っている認証情報を不正取得されてしまったことが致命的でした。攻撃者は事実上、ランサムウェアを拡散させる完全な制御を手に入れたのです。サポート窓口への問い合わせは 2 日間で 20,000 件を超え、5 日間もアクセス不能になるエンドユーザーもいました」

フォーティネットが救世主となる

同社のある従業員が、何とか事態を収拾する方法はないかと考え、自宅で使っていた FortiGate ファイアウォールを持ち込んで試してみることを思いつきました。そのモデルは小規模企業向けではありましたが、同社のセキュリティチームは、当時使っていたファイアウォールの前にそのデバイスを置くことを決断したのです。「目の前に迫る巨人に子供が戦いを挑むような、運を天に任せて祈るばかりの状況でしたが、不正侵入検知と防御、ウイルス対策、Web コンテンツのフィルタリング機能を FortiGate がすべて提供してくれたおかげで、ネットワーク全体のセキュリティを確保し、制御を取り戻すことができました」と CTO は説明します。

「フォーティネットがなければ、今日という日を無事に迎えることはできませんでした。フォーティネットのソリューションは本当に素晴らしい働きをしてくれています」

– クラウドホスティング / サービス会社 最高技術責任者

事例の詳細

顧客：クラウドホスティング / サービス企業

業種：IT

所在地：米国

導入の効果

- 既知および未知のグローバルな脅威への緊急対策
- エンタープライズ規模のインフラストラクチャ全体を保護
- 既存の環境を変更することなく容易に実装
- ビジネスのダイナミックな成長をサポートするスケーラブルなセキュリティソリューション

ソリューション

- FortiGate
- FortiAnalyzer
- FortiManager
- FortiDDoS
- FortiADC

同社は直ちにフォーティネットの採用を決断し、FortiGate 1500D エンタープライズファイアウォールと FortiAnalyzer を購入して、ランサムウェアの侵入を防ぐことのできなかった既存のファイアウォールをリプレースしました。

CTO は興奮気味に、次のように説明しています。「当社の環境は非常に複雑であるにもかかわらず、FortiGate 1500D への切り替えはわずか 30 分で完了し、本当に驚くほど簡単でした。我々の環境のどのような要素の再構築もまったく必要ありませんでした」

同社のセキュリティチームは、既知の国家主導の攻撃者からのリスクを軽減するために、直ちに FortiGate の位置情報に基づくジオロケーションブロック機能を実装しました。また、ユーザーを保護する目的で多要素認証を導入し、ウイルス対策の機能やその他の対策も提供することにしました。

同社の IT 担当者は、これまで侵入者がどこから来たのか判断できませんでしたが、FortiAnalyzer をインストールした直後から、実用的なインテリジェンスを活用できるようになりました。CTO は、次のように説明します。「これこそが我々の必要としていた機能であり、攻撃の発生元を正確に特定できるようになりました」

保護領域の拡大

フォーティネット セキュリティ ファブリックを導入した同社は、FortiManager の実装によって、今ではインフラストラクチャ全体のすべてのフォーティネットデバイスを一元管理できるようになりました。また、FortiADC の追加によって安全で無駄のない方法でアプリケーションを配信できるようになりました。さらに、FortiDDoS の導入によって既知 / 未知のどちらの分散型サービス拒否（DDoS）攻撃からの保護も可能になったのです。

「フォーティネットがなければ、今日という日を無事に迎えることはできませんでした。フォーティネットのソリューションは本当に素晴らしい働きをしてくれています。当社は、社内の極めて大規模なセキュリティスタック全体でフォーティネットのソリューションを活用しているだけでなく、自らの実体験に基づき、お客様にもこのソリューションを推奨しています」と、CTO は語っています。

また最高経営責任者（CEO）は、今回の件を次のように振り返ります。「ランサムウェア攻撃は、我々にとって一種のテロ行為と言えるものであり、結果として 300 万ドル以上の損害を被ることになりました。しかしながら、我々のセキュリティ対策を見直す大きなきっかけにもなりました。セキュリティベンダーを名前や規模だけで選ぶべきではなく、ベストインクラスのソリューションを選択する必要があると気付くことができました 」

「 フォーティネットは、セキュリティスタックのあらゆる層を対象とする、我々が必要としていたソリューションを提供してくれます。これにより、我々自身もお客様に対して比類のないレベルのサービスとサポートを常に安心して提供できるようになりました」

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.co.jp/contact

お問い合わせ