導 入 事 例

Cb Defense

Carbon Black.

NVC NETWORK VALUE COMPONENTS

株式会社 電通テック

従来型アンチウイルスをすり抜ける攻撃から守るため「Cb Defense」を採用「生命線」であるさまざまな情報を守りながら、働き方改革を推進、利便性とセキュリティの両立を実現

クライアントとともに、デジタルテクノロジーを活用した新たなプロモーションを次々と生み出している電通テックにとって、さまざまな情報を守るセキュリティは「生命線」だ。同社は、さまざまな多層防御を導入していたにも関わらず発生する「すり抜け」を減らし、一段高いセキュリティレベルを実現するため、米Carbon Black社の次世代型アンチウイルス「Cb Defense」を採用。またそのEDR機能により、状況の可視化、インシデント対応力を強化している。

課題

- 従来型アンチウイルスソフトではマルウェアのすり抜けが発生してしまっていた
- 社外の環境でPCが利用される場合でもコントロールを実現したかった
- インシデントの原因を究明するのに関連するログを突合する手間がかかり作業負担が大きかった

成果

- ストリーミングプリベンションを備えたCb Defenseの導入で、未知のマルウェアや非マルウェア攻撃を高い精度で検出できるようになった
- Cb Defenseにより、社員が社外やオフライン環境で利用する場合も保護を徹底できるようになった
- Cb DefenseのEDR機能を活用し、いつ、どのファイルが問題の原因となったかを速やかに特定可能になった

Profile

DENTSU TEC

■株式会社 電通テック
■設　立　2017年（平成29年）1月4日
■所在地　〒100-8508
東京都千代田区内幸町1-5-3 新幸橋ビル
■ＵＲＬ　https://www.dentsutec.co.jp

常に自由度とのバランスを図りながらセキュリティを強化

さまざまなクライアントとともに広告コンテンツの企画・製作を行っている電通テックは、世界最大規模の広告制作企業であり、最近では、デジタルテクノロジーやソーシャルネットワークを活用した新たなプロモーションを次々と生み出している。その同社にとって、セキュリティは不可欠な要素だ。

電通テック　取締役執行役員CIO　松本卓一氏は「私どもは、クライアントとともにさまざまなサービスやキャンペーン展開を立案し、実施に移していく中で、クライアントさまのさまざまな情報を預かっています。個人情報だけでなく、万一そうしたクライアントさまの情報が漏れるようなことがあれば信頼に関わる事態になります」と述べ、セキュリティについては非常にシビアに考えていると説明した。

こうした考えから情報システム部では、システム運用管理を担うISID-AOとともにさまざまな対策を実施してきた。アンチウイルスソフトやファイアウォールの導入はもちろん、標的型攻撃やランサムウェアといった脅威が顕在化する数年前の時点でいち早く次世代ファイアウォールを導入するなど、多層防御を実施し、セキュリティ対策を図ってきた。

セキュリティ至上主義を取ってガチガチに守りを固めるだけならば、ある意味簡単だ。だが、「われわれの扱う商品やサービスは多種多様です。そのため他人からは遊びのように見えても、実際には業務に関係あるコンテンツにアクセスすることもしょっちゅうで、そういったものを一律に制約するのは非常に難しいと考えています」と、同社のコーポレートマネジメントセンター 情報システム部 部長 中山洋一郎氏は述べる。

株式会社 電通テック
コーポレートマネジメントセンター 情報システム部 部長
中山　洋一郎 氏

株式会社 電通テック　取締役執行役員CIO
松本　卓一 氏

導 入 事 例

Cb Defense
Carbon Black.

ノートPCを活用した新しい働き方を促進する中エンドポイント保護が課題に

電通テックでは働き方改革も視野に入れつつ、ITを単なるバックエンドを効率化するための役割から、フロントエンドも支援し、独自の価値を生み出すための武器として活用し始めている。「クライアントや取引先と連携しながら仕事をするため、情報を扱う人、やり取りする先が非常に多岐に渡っています。その中でセキュリティは必須の要素です」(松本氏)

その一環として数年前から、社員や関係会社が利用する端末約2500台について、デスクトップPCから持ち運び可能なノートPCへの切り替えを進めてきた。このときも、社員それぞれがクリエイティビティを発揮できるよう、あまり規制を強くしすぎず、積極的に外に持ち出して活用できるようにしてきた。

だが、ファットクライアント単体での活用を前提にすることで、新たな課題が生まれた。重要な情報を保存している社内システムにはVPN経由でセキュアなアクセスを行うことにしているが、場合によっては自社では管理できないパートナーなどのネットワークにつないで利用することもあり得る。「常にわれわれの管理下で活用するとは限りません。われわれIT部門の管理スコープから外れた状態でも、しっかり挙動を守ってくれるエンドポイント製品が必要だと考えました」(中山氏)

もう一つの課題は、パターンマッチングを中心とした従来型アンチウイルスソフトの限界を感じていたことだ。電通テックでは多層防御の一つとして、従来型アンチウイルスソフトを導入し、パターンファイルの更新状況も常に監視する仕組みを取っていた。だが、マルウェアとのいたちごっこが続く中、完璧を期することは難しい。事実、ネットワーク検査を行ったところ、何らかのタイミングですり抜けたマルウェアに感染した端末からの通信を検出したことがあったという。情報漏洩など致命的な事態に至る前に対処できたが、「脅威はかなり近くに来ているという認識を持ちました」(松本氏)

「ランサムウェアにしても他のサイバー攻撃にしてもある種の『経済圏』ができており、簡単に亜種が作成できる状態です。この結果、今までの防御の仕組みだけではとても守りきれない状態になっています。この環境の中で、われわれの生命線である信用、情報をどう守るか。さまざまなアクセス環境がある中、機動性を保ちながらエンドポイントのセキュリティを強化していかなければ、私どものビジネス自体が守れないのではないかと考えました」(松本氏)

実システムに近い検証環境で高い検出率を示したCb Defense EDR機能の有用性も認識

こうした背景から電通テックでは、新たなセキュリティソリューションの検討を開始した。1つ目の条件は、パターンファイル以外の方式で、これまでのセキュリティ対策の水準を大きく引き上げることのできる製品であること。2つ目の条件は、柔軟なワークスタイルを前提に、ゲートウェイではなくエンドポイントで単体で動作することだ。そんな観点でソリューションを探し始めた電通テックが選んだのが「Cb Defense」だった。

当初同社では、AI系アンチウイルス製品をはじめ、他の複数の選択肢も検討していたという。選定に当たって実システムに近い検証環境を構築し、2017年8月から10月にかけてマルウェアの検知率を評価したところ、最も高い検知率を出したのがCb Defenseだった。「当初導入を想定していたAI系製品では取りこぼしが多く、これでは『従来型アンチウイルスの強化』という元々の目的につながらないと判断しました」(中山氏)

検証を担ったISID-ADの笹島佑氏は、「実機と同様の環境を用意し、本物のマルウェア約50種類を用いてどのくらい検出できるかをAI系アンチウイルス、従来型アンチウイルス、Cb Defenseの3製品で確認したところ、Cb Defenseと他の製品とでは検知率にかなり大きな差が出ました。念のため、もう少し古い既知の検体も用いて再検証を行いましたが、2回とも同じで、AI系アンチウイルスでは80%程度にとどまったのに対し、Cb Defenseは100%近い検知精度でした」と振り返る。

特に大きな差が出たのは、最近増加しているPowershellを悪用した攻撃で、AI系アンチウイルスでは全く防御できなかったが、Cb Defenseではストリーミングプリベンション技術により確実に防御していた。またアドウェアについても、Cb Defenseではオフラインでも確実に検出でき、それ以外の二製品とは検出率に著しい違いがあった。

機能比較を進める中で、当初はフォーカス外だったEDR機能の有用性にも気付いたという。「以前、ランサムウェアの感染被害が発生した際には、どういう経緯で侵入し、どのファイルが原因となったかを特定するため、ゲートウェイやファイアウォールなどあちこちに分散している複数のログを付き合わせる必要があり、非常

株式会社 ISID-AO
協業パートナー
笹島　佑 氏

に苦労しました。Cb Defenseは可視性が高く、いつ、どこで問題が起きたのかやプロセスの遷移といった事柄が一目で分かります。問題となったファイルが実行された時間も分かるので、その前後のログを見れば、簡単に原因の当たりが付けられます」（笹島氏）。

検証環境で試した限りでも、数日かかっていた作業が数分単位でできるようになり、「比較にならないほど楽です」と笹島氏は述べる。「また、Cb DefenseのLive response機能を利用すれば、リモートから管理者が該当端末に入り、あらゆるインシデント対応ができます。わざわざ端末を回収する必要性がなくなるところは大きな魅力でした」（笹島氏）

検証ではまた、リソース消費量やネットワークトラフィックも計測して比較したが、そこでもCb Defenseは満足のいく結果を出した。「電通テックの業務形態では、中には比較的重たいアプリケーションを動かす方もいるので、なるべく動作が軽いことも基準の1つでした。検証環境とは別にわれわれが利用しているPCにも入れて使ってみましたが、既存のアンチウイルス製品とコンフリクトを起こすことも、重たくて動かなくなるようなこともありませんでした」（笹島氏）

徐々に全社へ展開し、社員の利便性とセキュリティの両立を実現

こうしてさまざまな側面からCb Defenseの優位性を確認した電通テックでは正式に導入を決定。2017年12月から、カーボンブラックや販売代理店の支援を得ながら本番導入を開始し、アラートが出た場合の対応フローも含め、運用プロセスの設計を進めている。

導入・構築作業はネットワークバリューコンポネンツ（NVC）が支援した。「担当者が製品について熟知しており、こちらの疑問に確実に回答してもらっています。問い合わせに適切なレスポンスを返すという当たり前のことを、きちんと行ってもらえることに満足しています」と笹島氏は述べ、NVCと話し合いながら、最適なアラートレベルの設定を進めている。

社内ではまず、基幹システムと連携するマクロなど独自の作り込みを加えたファイルを扱う機会の多い経理部門などから先行して、テスト導入、本番導入と進めていく方針だ。「ユーザーには、アラートがしょっちゅう出るわけでも、パフォーマンスが落ちるわけでもなく、今までと何も変わらず使えることを伝えていきたいです」と中山氏は述べ、さらに「一般には、従業員の活動にあまり制約を設けず、かつセキュリティも高めるのは『矛盾』とされていますが、われわれはそれを両立させていきます」とした。

わずか数週間のテスト導入でも、Cb Defenseは早速効果を発揮した。ゲートウェイ的な役割をしているサーバに感染を試みた、ビットコインのマイニング系のマルウェアをブロックし、被害を未然に防いだという。CPUのリソースを膨大に消費するタイプのマルウェアだったので、検知できなければサーバの稼働が止まるところだった。

サイバー攻撃のビジネス化が進んだ結果、攻撃者は彼らにとっての「コストパフォーマンス」を重視するようになった。従って、「無作為に攻撃を行う攻撃者からすれば、自分の痕跡を突き止められる恐れのあるEDRを導入している企業に、わざわざ手間をかけてまで攻撃したくないと思うのではないでしょうか」と、事例に協力した理由を中山氏は述べている。

「これからも攻撃と対策のいたちごっこは続くでしょう。Cb DefenseのEDR機能を活用しながら、今、実情がどうなっているかを可視化し、現状のセキュリティ体制でいいのかチェックした上で、次のアクション、次の一手をどうするかを考え、PDCAサイクルを意識して回していきます」と強調した。

単にバックエンドの業務をITで効率化するだけでなく、フロント業務も含め、強みを生み出す原動力としてのITに軸足を置き、さらにはIoTの活用も視野に入れた電通テック。強固なセキュリティを背景に、これからも積極的にITを活用し、新たな価値を生み出していく。

株式会社ネットワークバリューコンポネンツ
〒144-0035 東京都大田区南蒲田2-16-2　電話: 03-5714-2050　http://www.nvc.co.jp/