N ニュータニックスニュース!

役立つニュータニックス！ from「THE FORECAST by NUTANIX」

サイバー犯罪との戦い――自治体の新たなアプローチ

ジョエル・ケラー */ フリーライター

スマートシティテクノロジーは、米国では都市部ではない、地方の住民にも新しいサービスをもたらしている。こうした変化に伴い、各自治体の CIO はセキュリティを再検討し、エンドポイント型から一元管理型への移行を目指している。

Microsoft のサーバーや PC が世界初と謳われる大量拡散型ウイルス、メリッサ・ウイルスの攻撃を受けた日のことを、1999 年にカリフォルニア州サンノゼ市で CIO 代行を務めていたジョン・ウォルトン氏は今でも鮮明に覚えている。

それは最悪の 1 日だったとウォルトン氏は当時を思い出し、次のように述べている。

ウォルトン氏 「ネットワーク全体をシャットダウンする必要がありました。部署という部署に設置されたあらゆる機器のコンセントをひたすら抜いて回ったことを覚えています」

メリッサ・ウイルスは、仕込んだ添付ファイルを電子メールに乗せて大量送信するマクロウイルスで、数時間のうちに遠隔地にまで拡散を拡げた。

Word のあらゆる保護機能を無効化した後、ユーザーのアドレス帳に登録されているメールアドレスに対し、自らを再送信させる仕組みだ。

この出来事には 1 つだけポジティブな面があった。

「これをきっかけとしてようやく、サンノゼ市内の PC すべてに対し、ウイルス対策のセキュリティソフトがインストールされることになったのです」とウォルトン氏は説明する。

現在、カリフォルニア州サンマテオ郡の CIO を務めるウォルトン氏は次のように述べている。

ウォルトン氏 「対処すべきは、プロパガンダ活動の一環としてウイルス拡散を目論む単独ハッカーだけではありません。ハッキングはより組織化し、アトランタやボルチモアなどの主要都市がランサムウェアによって攻撃された事例も報告されています」

ウォルトン氏を始めとする地方自治体の CIO はこうした事態に対処し、複数のセキュリティ課題を解決する必要に迫られているものの、与えられた予算ではカバーしきれないのが現状だ。

損害をもたらす問題の修復は必須とはいえ、それ故に、それ以外の重要な計画を犠牲にしなければならない

Nutanix で公的機関向けソリューションの責任者を務めるティム・ウォレスは、次のように説明する。

ウォレス 「ランサムウェアは 20 年が経過した現在も、メリッサがとった手法によりネットワークに侵入しています。メール、あるいはソーシャルメディアに添付されたリンクをエンドユーザーにクリックさせるのです。システムへのアクセスが成功すると、攻撃者による侵入を容易にするバックドアを仕込みます。攻撃者は開かれたドアからシステムに侵入し、別の穴を探す行為に及びます」

「サイバー強盗は探し当てたデータを暗号化し、多くの場合、ビットコインで何万ドルもの身代金を要求します」とウォレス。

＊

ランサムウェアの攻撃によって自治体のシステムが停止すると、重要なシステムがダウンし、税金の徴収ができない、あるいは裁判所や警察に向けて情報提供ができないといった事態を引き起こす。

そして、復旧にあたっては多額の費用がかかることも少なくない。2016 年、SamSam と呼ばれるウイルスの攻撃により、アトランタ市を含め、200 を超える組織が被害を受けた。

アトランタ市は緊急対応サービスを契約し、復旧のために新たなテクノロジーを導入した。計上された費用は 1,700 万ドルに上ったと、State Scoop の記事が伝えている。

「ライブラリの構築や人員の増員・雇用は、対策として現実的ではありません」とウォルトン氏。

地方自治体の予算は各年度が始まる前に決定されることが多く、四半期ごとに見直しが可能な企業と比べて、支出を柔軟に調整することがはるかに難しいという。

「損害をもたらす問題の修復は必須とはいえ、代わりに、それ以外の重要な計画を犠牲にしなければならないのです」とウォルトン氏は話した。

＊

ネットワークの強化が図られた過去 20 年間に、サイバー攻撃の手口も、より巧妙かつ高度に進化した。

脆弱性（ファイアウォールの保護対象外とされた古いサーバーなど）を発見する能力を進化させてはいるが、一方ではユーザーに不正リンクをクリックさせるという従来の手法も依然として使用している。

巧妙化が進む、膨大な数の脅威への対応を迫られるなか、公的機関の CIO は IoT（モノのインターネット）やいわゆるスマートシティ関連テクノロジーなど、新たなイノベーションを継続的に展開している。

ウォレス 「センサーを通して情報を収集する IoT の普及は、大量のタッチポイントを生み出すことになりました」

「地方自治体を統率する立場として、交通管制システムを始めとするインターネット接続機器を攻撃者の侵入から守らなければなりません」とウォレス。

現在は防衛手段の 1 つとして、コンピューターサーバーやストレージを仮想化し、VDI（仮想化デスクトップ）や DaaS を活用している。

ウォルトン氏によると、こうした新しいテクノロジーを使うことで、感染した領域を切り離すことができるだけでなく、すべてを再フォーマットすることが可能になったという。

「ある一定期間に発生したものであれば、ウイルスや感染の種類を問わず一掃することが可能です。ウイルス

感染の機会を減らすとともに、ネットワーク上の端末間での感染拡大を防止するため、業務への影響を考慮しながら、できる限り頻繁に対応していきたいと考えています」とウォルトン氏は話した。

＊

従来の方法では、各デバイスに対してウイルス対策のアプリケーションを個別にインストールしていた。新たなテクノロジーにより、これを確実に上回る効果が期待できるだろう。

（2019 年 12 月 16 日 , THE FORECAST by NUTANIX）

記事構成：ニュータニックス・ニュース！ 編集部 , Nutanix Japan

＊ケン・カプランは、ニュータニックスが発行するメディア The Forecast by Nutanix, 編集長。

NUTANIX
YOUR ENTERPRISE CLOUD

お問い合わせ：03-4588-0520
info-jp@nutanix.com | www.nutanix.com/jp | @NutanixJapan
東京都千代田区大手町 1-1-1 大手町パークビルディング 7F