事例で学ぶセキュリティインシデント（第15回）

安心な端末利用を支援する「エンドポイントセキュリティ」

2024.08.15

関西で不動産業を展開するO社では営業担当者にノートパソコンを支給し、顧客ニーズ合わせて物件の案内などがスムーズに行えるIT環境を整備してきた。本社のIT担当者は出社直後、支店の営業担当者から電話連絡を受けた。「パソコンを立ち上げようとしたところ、動作がおかいしいので見てもらえませんか」。IT担当者は本社までパソコンを持参するように伝え、ウイルス感染を疑った。

端末レベルでのウイルス/マルウエア対策が課題

O社では社内ネットワークとインターネットの境界となるゲートウェイでウイルス対策などのセキュリティを講じている。支店の営業担当者によると、最近は定義ファイルの更新を行っておらず、外出先でインターネットアクセスした際にウイルスに感染したようだ。ただ、感染後、営業担当者はパソコンを社内ネットワークに接続しておらず、現段階では他のパソコンやサーバーへの感染は免れたと判断した。だが、IT担当者はこのインシデントを通じ、端末レベルでのエンドポイントセキュリティ対策の必要性を痛感した。

近年、サイバー攻撃の手口が巧妙化し、ウイルス/マルウエア感染被害が深刻化している。どの企業でもウイルス対策を行っているはずだが、従来のパターンファイルベースの対策では、未知のウイルスの防御が困難だ。また、ゲートウェイでファイアウォールやアンチウイルスなどのセキュリティ対策を行う企業も多いが、暗号化されたファイルにウイルスが埋め込まれた場合、ゲートウェイレベルでのセキュリティ対策では検知・防御が難しいのが実情だ。

攻撃者はメールの添付ファイルにウイルスを埋め込み、受信者はうっかり添付ファイルを開いて感染したり、悪意のあるWebサイトに誘導してファイルを開かせて感染させたりする手口もある。その感染端末から社内の他のパソコンやサーバーにウイルス感染を広げるリスクもある。そこで、端末に感染したウイルスを検知し、感染端末の隔離やウイルスの除去といった対処を迅速に行い、感染の拡大を防止する仕組みが必要になる。

端末のウイルス感染の検知と対応を支援するEDR… 続きを読む