事例で学ぶセキュリティインシデント（第10回）

社内ネットワークにつながる複合機のセキュリティリスク

2024.03.12

J社では、複写機、スキャナー、プリンター、FAX機能を備える複合機を本社・工場に設置。総務兼IT担当者は定期的に複合機の操作ログを調べ、利用状況を確認していたところ不審な操作ログに目が留まった。

文書データを一時保存するハードディスクから、データがダウンロードされた形跡があったのだ。「不正アクセスかもしれない」。重要な情報が外部に漏れていれば大変なことになる。IT担当者は上層部にインシデントの可能性を報告するとともに、IT事業者のサポートを得ながら調査に着手した。

メモリーに一時保存された情報が不正利用される恐れ

J社は大阪に拠点を構え、従業数を30名ほど抱える部品製造会社だ。工作機械メーカーなどとの取引があり、顧客から預かった設計データなどを扱うことからセキュリティ対策にも留意してきた。パソコンやサーバーのウイルス対策や、社内ネットワークと外部ネットワーク（インターネット）の境界にファイアウォールを設置し、これまでセキュリティ上の問題が起こることはなかった。

ただ、IT担当者はパソコンやサーバーと同様に社内ネットワークにつながる複合機のセキュリティリスクは以前から耳にしていた。工場では設計・製造にかかわる技術情報などを複合機で印刷したり、コピーしたりして従業員が参照するといった使い方をしている。すべてが機密情報というわけではないが、取引先にかかわる情報も含まれるため、適正に使われているかどうか複合機の操作ログを定期的に確認していた。

複合機にかかわるリスクはさまざまある。その1つが出力した文書・資料の取り扱いがずさんで複合機の操作後、置き忘れたり、紛失したりして情報漏えいする恐れがある。複写機、プリンター単体でも同じことが言える。

また、作業者のパソコンから社内ネットワークを介して複合機へデータを転送する際の盗聴・改ざんリスクや、複合機のハードディスク/メモリー領域に一時保存されるデータが不正アクセスされ、管理者の権限が奪われたり、悪意のあるコードが埋め込まれたりして情報漏えいするといったリスクもある。

さらに、役員会議用にプリントアウトした経営にかかわる機密情報や知財情報、顧客情報などが含まれるデータが社外に流出すれば、それこそ取り返しのつかない事態を招くことになりかねない。

管理者権限が奪われて悪用されるリスクも… 続きを読む