TOPICS

法的リスクマネジメント講座 第90回

中小企業を狙い撃ちにするサイバー攻撃にどう備えたらよいか（続々々編）

長谷川俊明法律事務所
弁護士
長谷川 俊明

はじめに――「脅威」の内容を知りましょう

日本が抱えるサイバーリスクは、世界２位の大きさといわれています。比較的に防御の甘い中小企業を標的に、世界中のハッカーがさまざまな攻撃を仕掛けているようです。

独立行政法人情報処理推進機構(IPA)の「情報セキュリティ10大脅威2023」【組織】は、以下のような順位表を掲げています。

1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	標的型攻撃による機密情報の窃取
4位	内部不正による情報漏えい
5位	テレワーク等のニューノーマルな働き方を狙った攻撃
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7位	ビジネスメール詐欺による金銭被害
8位	脆弱性対策の公開に伴う悪用増加
9位	不注意による情報漏えい等の被害
10位	犯罪のビジネス化（アンダーグラウンドサービス）

これだけの脅威にさらされていながら、対策を講じず、手を拱いているわけにはいきません。本講座では、第87回(2022年5月)から第89回(2023年6月)まで、3回にわたり、中小企業がコストをあまりかけることなく、身近なところから効果的に行える具体的な対策を、紹介してきました。

連続講座の4回目の今回は、「ウェブサイトの改ざんをどう防いだらよいか」を中心に、有効な対策を検討してみます。

ウェブサイトはどのように改ざんされるか

2023年5月、警察庁と経済産業省が、「サイバー警察局便り」（Vol.6）のなかで、「御社のウェブサイト改ざんされていませんか？」と題して、企業に注意喚起しています。

こうした注意喚起が必要なほど、ウェブサイトへのサイバー攻撃が多くなったとみられます。この手の攻撃にどう備えたらよいかを探るにあたっては、まずは攻撃の手口を知る必要があります。

警察庁公表の資料によりますと、次のような手口が認められます。

- 窃取したアカウント情報を悪用し不正アクセスをする
- ソフトウェアの脆弱性をつく
- 組織内の制御機能の不備をつく

これらの手口にどう備えるのがよいかと問われれば、アカウント情報を盗まれないようにする、ソフトウェアの脆弱性をなくす、アクセス制御機能の不備をなくすといった答えが、すぐに浮かびます。しかし、問題はそれほど単純ではありません。各備えを具体的にどう進めたらよいかまで考える必要があるからです。

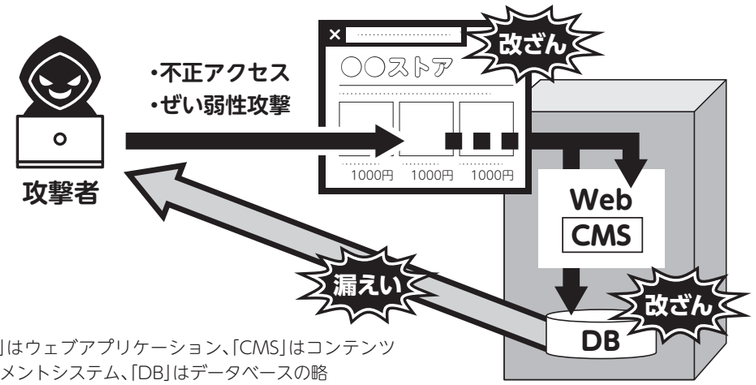
ウェブサイトの改ざんを防ぐための具体策

ウェブサイトの改ざんは、サイトのコンテンツを、運営者の承諾なく、追加や削除、変更することを指します。改ざんをしただけであれば、サイバー攻撃は、単なる嫌がらせを目的とするものでしたで終わるのですが、ほとんどこれは期待できません。

ウェブサイトを改ざんすることによって、個人データを流出させたり、サイト閲覧者をウイルスに感染させたりするのが攻撃者の狙いだからです。なかでも深刻なのは、近時急増しているEC（電子商取引）サイトの閲覧者情報・データの漏洩であり、これらについての対策の詳細は、次号以降で取り上げます。

ランサムウェア攻撃の一例

攻撃者は、窃取したID・パスワードを悪用したり、ソフトウェアのぜい弱性をついたりすることなどにより、ウェブサイトへの攻撃を行います。



※「WEB」はウェブアプリケーション、「CMS」はコンテンツマネジメントシステム、「DB」はデータベースの略

出典：経済産業省 注意喚起「サイバー警察局便りVol.7 御社のウェブサイトが狙われています！」

重大な被害を生じさせないためには、なんといってもウェブサイトを改ざんされないようにすることです。参考になるのは、IPAの公式サイト「安全なウェブサイトの作り方」であり、警察庁が、「ウェブサイト安全性向上のための対策」として抜粋して紹介しています。その内容を、以下のとおり、さらに箇条書きで要約してみました。

対策1	ウェブサーバーに関し、OSやソフトのぜい弱性情報を継続的に入手し、ぜい弱性の修正などを行う
対策2	DNSに関し、ドメイン名やDNSサーバの登録情報を調査し、必要に応じて対処するなど
対策3	ネットワーク盗聴に関し、ウェブサイト運営者がメールで受け取る重要情報を暗号化するなど
対策4	フィッシング詐欺に関し、EV SSL証明書を取得し、サイトの運営者が誰であるかを証明するなど
対策5	パスワードに関し、伏せ字で表示されるようにし、サーバ内で保管する際は、平文ではなくソフト付きハッシュ値の形で保管するなど

こうした予防策を講じていても、自社のウェブサイトの改ざんは、不可避的に起こりえます。その場合、改ざんをなるべく早く察知し、いち早く対処して、個人データの漏えいなどの発生を防止しなくてはなりません。

いち早くウェブサイトの改ざんを発見するには、自社ウェブサイトを検索し見覚えのないページが設置されたりしていないかを日頃からチェックすることです。

検索結果に反映されるタイプの改ざんを、コストをかけずに調べる方法として、警察庁は、検索エンジンに意図しない情報が登録されていないか確認することをすすめています。また、改ざんに気づいたら、直ちにサービスを停止し、管理者画面やデータベースへのアクセスログの保存、警察への相談を呼びかけています。

＊裏表紙の参考サイトをご参照ください

おわりに

サイバー攻撃の手口は、日々巧妙化しています。対して、中小企業のセキュリティ対策は、一向に進められないのが実情です。大半の企業はセキュリティ対策の第1歩をセキュリティソフト導入から踏み出します。ただこのレベルの対策で大丈夫と安心しないことです。

ウィルス対策ソフトで、過去のマルウェアは検知できますが、IPA（独立行政法人 情報処理推進機構）によれば1日でおよそ１２０万件生成されるという新種のマルウェアを検知できないためです。ウィルス感染をいち早く発見し次のレベルの対策を打てるようにすべきでしょう。その詳細は、次号にて取り上げることにします。

参考URL
・独立行政法人情報処理推進機構(IPA)「情報セキュリティ 10大脅威 2023（組織）」
https://www.ipa.go.jp/security/10threats/10threats2023.html
・経済産業省―サイバーセキュリティ政策―サイバーセキュリティの強化について（注意喚起）
https://www.meti.go.jp/policy/netsecurity/cyberpoliceagency letter0508.pdf
・警察庁―サイバー警察局―ウェブサイト改ざん対策―ウェブサイト改ざんの手口
https://www.npa.go.jp/bureau/cyber/countermeasures/hacked-website.html
・警察庁―サイバー警察局―ウェブサイト改ざん対策―ウェブサイト安全性向上のための対策
https://www.ipa.go.jp/security/vuln/websecurity/about.html