masuda funai

News & Types: クライアント・アドバイザリー

サイバー攻撃を受けた日本企業が支払った身代金の平均は、なんと117万ドル！ ～ サイバーリスクから貴社を守るためのチェックリスト

4/6/2021

By: ケントン クノップ

Practices: 知的財産テクノロジー

概要

サイバーセキュリティ上のリスクは、今に始まったことではありません。しかし、新型コロナウイルス感染症によるパンデミック発生以降、企業においては従業員の在宅勤務に対応することが急務となりました。その結果、より多くの従業員が会社のサーバーにリモートで接続し始めたことで、新たな脆弱性が生み出されることになったのです。昨年中に発生した事件から明らかになったことは、業務データ、社会保障番号、クレジットカード情報等の機密情報を入手しようとするサイバー犯罪者は、企業規模の如何にかかわらず、いかなる企業をも標的とする可能性があり、さらにはベンダー宛の電子送金やACH送金を虚偽の銀行口座に振り込ませるためにベンダーの従業員になりすますことさえも厭わないということです。

増大するサイバーセキュリティ上のリスクから会社を守るには、小規模企業から大企業まで、各企業で早急に次の措置について検討されることを強くお勧めします。

1. **IT 脆弱性評価(IT Vulnerability Assessment)の実施:**
   企業においては、オンライン・コンピュータ・ネットワークがどのように機能し、そこにどのような脆弱性があるのか（特に従業員が自宅からリモートで作業することで生じる脆弱性）を把握することが重要です。そして、脆弱性を特定でき次第、速やかに対処すべきです。また、ベンダーから派生する脆弱性についても検討すべきでしょう。

2. **従業員向けのサイバーセキュリティ研修の実施:**
   オンライン詐欺事件の多くは、従業員を騙して不正な口座に送金させたり、マルウェア（悪意のあるソフトウェア（malicious software））をインストールさせたり、またはパスワードを提供させたりす

© 2025 Masuda, Funai, Eifert & Mitchell, Ltd. All rights reserved. 本書は、特定の事実や状況に関する法務アドバイスまたは法的見解に代わるものではありません。本書に含まれる内容は、情報の提供を目的としたものです。かかる情報を利用なさる場合は、弁護士にご相談の上、アドバイスに従ってください。本書は、広告物とみなされることもあります。

ることを試みるものです。従って、従業員の「意識」が、オンライン詐欺に対する最強の抑止力の一つになると言えます。注意深い従業員がサイバー攻撃から会社を守る最後の砦となることも少なくないことから、従業員向けにサイバーセキュリティ研修を定期的に実施することは、強力なサイバーセキュリティ・プログラムを構築する上での「鍵」となります。

3. **次世代エンドポイントセキュリティソフト（Next Gen Endpoint Security Software）のライセンス取得:**
   新種のウイルスが発見された後でのみアップデートされる従来のウイルス対策ソフトウェアとは異なり、AI（機械学習）を活用した次世代エンドポイントセキュリティソフトは、より迅速にサイバーセキュリティ上の問題を検知することが可能と言われています。

4. **多要素認証の導入:**
   多要素認証（multi-factor authentication （MFA））をサポートする全てのシステム、プラットフォーム、およびアプリケーションにおいてMFAを導入することをお勧めします。

5. **サイバーセキュリティ保険への加入:**
   サイバーセキュリティ保険は、サイバーセキュリティ事件（ランサムウェアを含む）の被害に遭ってしまった場合の費用の相殺に役立つものです。しかし、サイバーセキュリティ保険は、通常、標準的な企業保険に加えて別途加入が必要になるもので、別個の引受要件が適用されます。従って、企業においては、実際に被害に遭う前にサイバーセキュリティ保険を検討し、加入しておく必要があります。

6. **会社データの定期的なバックアップ:**
   サイバーセキュリティ事件の被害者となってしまった場合、重要データが、（ランサムウェア攻撃のように）サイバー犯罪者によりロックされたり、削除されたり、または安全にアクセスすることができない状態にされたりする可能性があります。そのため、企業では、信頼できるプロバイダーを通じて、安全な場所に重要データを定期的にバックアップすることが重要です。その場合、可能であれば、サイバーセキュリティ事件に対処した後で重要データを迅速に復元することができるよう、オフサイトまたはクラウドにバックアップすることが理想と言えます。また、バックアップにアクセスするための認証情報は、プライマリサーバーにアクセスするための認証情報（primary active directory credentials）とは異なるものにすることも検討すべきでしょう。

7. **物理的なセキュリティ対策の維持:**
   すべてのサイバーセキュリティ事件がオンラインで発生するわけではありません。機密データが含ま

© 2025 Masuda, Funai, Eifert & Mitchell, Ltd. All rights reserved. 本書は、特定の事実や状況に関する法務アドバイスまたは法的見解に代わるものではありません。本書に含まれる内容は、情報の提供を目的としたものです。かかる情報を利用なさる場合は、弁護士にご相談の上、アドバイスに従ってください。本書は、広告物とみなされることもあります。

れた会社支給のノート型パソコンやストレージデバイス（記憶装置）が従業員の自宅もしくは車、または公共の場から盗まれた場合にも、会社データにリスクを生じさせる可能性があります。会社のデバイスへのアクセスは、強力なパスワードで保護するだけでなく、データの暗号化も講じることで、会社所有物が盗難に遭った際のリスクを軽減することができるでしょう。

8. **会社のプライバシー・ポリシー（方針）の更新:**
   貴社のプライバシー・ポリシーを更新し、カリフォルニア州消費者プライバシー法（CCPA）等の該当法に準拠させるようにして下さい。こうすることで、サイバーセキュリティ事件が発生した場合に提起され得る請求や損害賠償のリスクを最小限に留めることできます。

9. **（万が一、サイバーセキュリティ事件の被害に遭ってしまった場合の）対応計画の設置:**
   全米50州の各州では、個人の機密情報への不正アクセスまたはかかる情報の漏えいが発生した場合には、住民にその旨を通知するよう何らかの要件が規定されています。州の通知要件に迅速に従うには、どのような情報が漏えいまたは不正アクセスの対象になったのか、誰の情報が影響を受けたのか、そしてそれらの個人がどこに住んでいるのかを速やかに特定することが重要となります。それには、サイバーセキュリティ事件が発生する前に、適切な対応計画を設置しておくことが必須です。

上記の措置を講じることで、サイバーセキュリティ事件の発生を未然に防ぐだけでなく、実際に被害者となってしまった場合でも、そのリスクと責任を最小限に抑え、通常業務への迅速な復帰を可能にする体制を整えておくことができるのです。

© 2025 Masuda, Funai, Eifert & Mitchell, Ltd. All rights reserved. 本書は、特定の事実や状況に関する法務アドバイスまたは法的見解に代わるものではありません。本書に含まれる内容は、情報の提供を目的としたものです。かかる情報を利用なさる場合は、弁護士にご相談の上、アドバイスに従ってください。本書は、広告物とみなされることもあります。