これからを創造するお役立ち情報
イノベーションラボ News
発行 あいおいニッセイ同和損害保険株式会社
編集 DREAMJOB Innovation Lab

『 建設・土木業のすぐに始めるサイバーセキュリティ 』

コラム読者の皆様こんにちは！
内山会計の内山でございます。

この記事では建設・土木業の方へ向けて、税理士・会計士としての立場から、専門的な知識・情報をわかりやすく解説してまいります。

建設・土木業界にも働き方改革の波が押し寄せ、同時にIT化も進んでいるというお話は以前からお伝えしている通りですが、皆さんの会社ではサイバーセキュリティに対するリスク管理は行っているでしょうか？

様々な機器がネットにつながる今日において、サイバーセキュリティはIT関係の企業だけが取り組めばよいという問題ではなくなりました。さらに、建設・土木業はサイバーセキュリティインシデントが増えているという実態も存在します。
一般的な会社と比べ、関連企業や下請け、孫請けなど様々な組織でプロジェクトを進めるために、例え自社の取り組みが完璧でもどこかに穴があれば簡単に攻撃を受けてしまうものです。

ひとたび攻撃を受けてしまうとプロジェクトはストップする可能性がありますし、何より膨大な時間と費用をシステム復活に充てる必要性も出てくることから、企業にとって死活問題とも言えます。

そこで今月のコラムでは『建設・土木業のすぐに始めるサイバーセキュリティ』と題し、中小の建設・土木業者がすぐに取り組めるサイバーセキュリティを高める取り組みをいくつかご紹介します。ぜひ最後までお付き合いください。

サイバー攻撃を受けると…

近年世界中で行われている攻撃の一つにランサムウェアというものがあります。これは、攻撃者が社内システムに侵入、データを勝手に暗号化し復号してほしければ身代金を支払うよう要求してくるという悪質なものです。
例え身代金を支払ったとしても復号される保証はありませんし、何より再度攻撃を受ける可能性も大いに存在します。

また、身代金の支払い有無に関わらずデータは流出しているわけですので、一定数以上の個人情報漏えい等が発生した場合は、個人情報保護委員会への報告義務と本人に対する通知義務が必要です。

顧客からの問い合わせ窓口の設置。上記委員会への届け出。暗号化されたデータの復号。再発防止策。これらを短期間に実行しなければなりませんので、工期を気にしている余裕はないと言えるでしょう。

サイバー攻撃はそれだけ恐ろしいものですが、どこか他人事のように感じてしまうかもしれません。しかし、既述の通り関連企業が多ければ多いほどリスクは増えていくものですので、ピンと来ていなくても関連企業と併せて高い意識を持ち、どのような取り組みを行えばリスク軽減につながるのかを探っていくべきですね。

今日からできるサイバーセキュリティ対策

まずは従業員の意識向上が重要です。
たった一回のサイバー攻撃で自社が倒産してしまうかもしれないということを全社員に認識してもらいましょう。そのために、基本的な項目として次の事項を社内ルールとして制定すると効果的です。

パスワード・二段階認証のルール化

最も基本的なこととして、複雑なパスワード設定と二段階認証システムの導入が挙げられます。銀行の暗証番号も誕生日は設定出来ないのと同じように、社内システムのパスワードも単純なものは避け、大文字小文字数字記号を含めた10桁以上の複雑な文字列とするべきでしょう。

また、二段階認証もスマホアプリで対応できるシステムが増えてきましたので、同じように導入することも重要です。もっとも、従業員のスマホもパスコードロックが有効かを調査し、出来ることなら必要な社員には業務専用のスマホを支給すべきと言えます。

業務専用スマホであれば、アクセスログの管理や使用状況の管理も可能となりますので、個人のスマホを業務利用するよりも安全と言えます。

サイバーセキュリティ研修の実施

これは座学の研修だけを行うのではなく、研修後のテストも兼ねたものが良いでしょう。私の知人の会社では実際にテストも行っており、昇進・昇給材料の一つとしているそうです。それだけ、サイバーセキュリティに対する取り組みを強化しているという事になりますが、同時に社員もサイバーセキュリティの意識を高めると昇進・昇給の可能性があるということになりますので、取り組み度合いも違ってくることでしょう。

関連企業も一緒に

これは今すぐできることでは無いかもしれませんが、関連企業も一緒に研修受講や各種取り組みを実施していけるとよいですね。冒頭お話しした通り、関わる組織・人が増えれば増えるほどセキュリティに穴も出来やすくなりますので、日ごろからの啓発活動が非常に重要と言えるでしょう。

システムや保険の活用も視野に

近年ではEDRというシステムを導入する企業も増えてきました。これは業務で使うPCなどに常駐監視するシステムであり、侵入を検知するとマルウェアの侵入経路やデバイスの隔離を行ってくれるものです。中には専門家チームへ連携してくれるものもありますので、非常に心強いシステムと言えます。

また、損害保険の分野ではサイバーセキュリティ保険も存在します。上記EDRとセット販売を行っている保険もあるようですので、加入を検討してみてはいかがでしょうか。

今回のまとめ

まずはお金をあまりかけずに出来るところからスタートするのが現実的と言えますが、大きなプロジェクトであればあるほど、攻撃を受けた際のリスクは計り知れません。
どこまで予算をかけたらよいか？　については、自社のキャッシュフローと抱えている案件を元に計算し、システム会社や保険代理店とも連携しながら決定していくとよいでしょう。

とにかく、ノーガードでは済まされないものでもありますので、未対策という事業者様は今回のコラムを参考に自社の対策を進めていただければと思います。

今回も最後までお読みいただきありがとうございました。

税理士法人内山会計 公認会計士・税理士 内山典弘