SecurityScorecard

SecurityScorecard社ブログ

発行日：2021年3月29日

執筆：SecurityScorecard 中村 悠
編集：SecurityScorecard 橋本 詩保

10項目のセキュリティ リスク マネジメントに関する考慮事項

セキュリティ リスク マネジメントとは、潜在的なリスクを特定し、リスクの影響を評価し、リスクが現実になった場合の対応方法を計画するプロセスです。このプロセスは、その規模や業界を問わず、すべての組織がセキュリティ リスク マネジメント計画を策定する際にとても重要です。

しかしながら、たとえ事前に潜在的なリスクを特定されたとしても、そのすべてのリスクを除去できることは、残念ながら、ありません。このこともまた、組織が認識しなければならない事実の1つです。ただし、組織の努力によって、潜在的なリスクを低減し、もし、リスクが顕在化した場合でも、その影響を減らすことは可能です。そのために、組織のセキュリティ リスク マネジメントを計画/立案する際に考慮すべき10項目を以下に示します。

1．企業文化の構築

組織のセキュリティ リスク マネジメントを計画する際にまず考慮すべきことは、企業の文化の構築です。現在、サイバー攻撃を受けた企業が被る損害の平均金額は、1億円を超えるとも言われており、攻撃された企業の37%は、風評被害により企業価値が低下しています。このため、組織で働く上層部からパートタイムやアルバイトのスタッフまで、組織全体でセキュリティを日頃から意識し、1人1人が自覚をもって、リスクを低減しようという組織文化を確立する必要があります。

2．責任の分担

セキュリティ態勢を確立し、それを維持するための努力は、IT部門やセキュリティ部門に限ったものではありません。組織内のすべての従業員が、潜在的なリスクを認識し、自身が従事する業務の範囲内で徹底できるリスクの低減に責任を持つ必要があります。例えば、セキュリティ対策を計画する上では、もちろん、フィッシングメールに従業員が反応するといった、人的リスクも考慮する必要がありますが、組織のすべての従業員がセキュリティ意識を高めることで、このリスクを低減できることは言うまでもありません。

続きを見たい場合は
メーカーBlogへ
https://securityscorecard.com/io-considerations-for-cybersecurity-risk-management-jp