サイバーセキュリティが物理セキュリティにとって不可欠な理由

Axisは、現実世界の物理セキュリティにおいて便利な製品を世に出すことで知られていますが、ここでサイバーセキュリティを取り上げるのはなぜでしょうか。ハリウッド映画の世界を見ると、スパイや秘密諜報員、カジノの強盗を計画する泥棒、さらにはスーパーヒーローたちでさえ、セキュリティカメラやスマートドア、バイオメトリック認証のキーパッド、その他の華やかな装置を悪用/活用して、世界を救ったり、美女を救出したり、戦利品をまんまと手に入れたりしています。

彼らが使うユーザーインターフェースがどれだけ現実離れしていたとしても (個人的には、MI6やCIAが映画で使っているコンピューターを是非とも手に入れたい)、また本来必要な技術スキルが過剰

にシンプルになっていたとしても (たとえば「国防総省をハッキングする」と書かれたボタンのような形で)、そこには何かしらの真実性が隠されています。

サイバーセキュリティは物理セキュリティにとって不可欠

この投稿と続く幾つかの投稿では、21世紀の物理セキュリティにサイバーセキュリティが不可欠である理由、このコンテキストにおけるサイバーセキュリティの基本パラメーターは何か、そして自分の企業や組織で物理セキュリティシステムを計画する際に念頭に置くべき一般的なサイバーセキュリティの概念について、それぞれ取り上げる予定です。

ここで忘れてはならないのは、**サイバーセキュリティはプロセスであり**、製品ではないということです。脅威はシステムレベルで対処する必要があり、ネットワークとそのデバイスやサービスのセキュリティを確保する責任は、ベンダーのサプライチェーン全体のみならず、ネットワークの管理者やユーザー自身にもあります。テクノロジーは重要ですが、すべてのリスクや脅威を排除することはありません。

基本的なレベルのサイバーセキュリティとはリスク管理のことで、すべてのリスクを排除することはできません。

(余談として、ここで少し思考の実験をしてみましょう。今朝起きてからあなたが直面した潜在的なリスクをすべて書き出してみましょう。飼っている犬につまずいたり、シャワーでやけどしそうになったりしたかもしれませんが、隕石が家を直撃する可能性や、カエルの大群が襲ってくる可能性についてはどうでしょうか。全く予測不可能なリスクもあり、そのすべてに備えることは難しいというよりも、無理なのです)。

たとえできたとしても、リスクによっては多大の費用が生じます (家を隕石から守る防護壁など)。ですから、自分と組織にとって何が大切かをまず考える必要があります。重要な資産を特定して、それを徹底的に守ります。許容できるリスクレベルを検討し、リスクの影響を緩和する方法を導き出し、残りのリスクを保険という形でカバーします。

次の投稿では、物理セキュリティシステムに対するリスクを分析する方法、効果的な緩和策、さまざまな種類の攻撃、そして異なる規模の組織が行える対応策について取り上げます。