SecurityScorecard

SecurityScorecard社ブログ

発行日：2021年9月24日

執筆：SecurityScorecard 中村 悠
編集：SecurityScorecard 中島 朝可・橋本 詩保

「Attack Surface Management」を実践するには？

皆様は、「Attack Surface Management」という用語を聞いたことがあるでしょうか。

実は、私も最近、耳にするようになった言葉なのですが、当たり前のようでこれまでちゃんと語られなかった用語なので、このブログで皆様と一緒に掘り下げてみたいと思います。
「皆様が所属している組織では、侵害が発生する可能性を把握するためには、どのような視点を持ったらよいでしょうか？」
抽象的な質問で、答え方も様々ありますが、以下のような回答は、皆様にどのように響くでしょうか。
「自組織が保有するデジタル資産の中で、“攻撃者から接点を持たれる可能性のある資産”に着目する。」
“攻撃者から接点を持たれる可能性のある資産”。つまり、“外部に公開しているデジタル資産”に着目するということです。
組織における侵害発生の可能性、サイバー攻撃を受ける可能性は、その組織が外部に公開しているデジタル資産（IPアドレスやドメインなど）にセキュリティ的に脆弱な点が多く存在すればするほど高まる、というのは容易に想像がつくと思います。
その“組織が外部に公開しているデジタル資産に存在するセキュリティ的に脆弱な点”に注目して、セキュリティリスクをマネジメントしようとする取り組みが、「Attack Surface Management」です。
文字にすると、当たり前のように感じますが、実は、今までに存在しなかった新たな概念ではないでしょうか。のような対策を取っているでしょうか。

「Attack Surface Management」を実践するには？

「Attack Surface Management」を実践するにはどのようなステップで取り組めばよいでしょうか。
まずは、組織が保有しているデジタル資産の中で、外部に公開された状態にある資産を把握します。

続きをご覧になりたい場合は
メーカーBlogへ
HTTPS://SECURITYSCORECARD.COM/ATTACK-SURFACE-INTELLIGENCE-JP