CXO Guide-JP

CXOのための攻撃対象領域管理ガイド

paloalto NETWORKS | CORTEX

CXO のための
攻撃対象領域管理ガイド

攻撃対象領域の概念は新しいものではありません。しかし、組織や CXO は攻撃対象領域に対する考え方を改める必要があります。従来、IT 部門は組織の攻撃対象領域を内側の視点から捉えて、「インターネットに接続されている資産は何か？」や「防御する必要がある境界はどこか？」といったことを問題にしました。

そうした攻撃対象領域に対する考え方は、リモート ワークやクラウドへのデジタル変革の普及に伴い、良くも悪くも崩壊しています。スタッフや業務は地理的に分散し、新たなクラウド資産が数秒で作成される可能性があります。

CXO は、組織の攻撃対象領域を内側ではなく外側の視点から捉え、「クラウド内の資産やサプライ チェーンに属する資産のうち、自社のネットワークに接続されているものは何か？」や、「そうした資産のうち、未知のものはどのくらい存在するのか？」といったことを問題にする必要があります。

Cortex by パロアルトネットワークス | CXO のための攻撃対象領域管理ガイド | ホワイト ペーパー 1

ASMに取り組むCXOに向けた知見攻撃対象領域という考え方は新しくはありません。しかし、組織やCXOに求められる攻撃対象領域との対応は必要です。従来はITチームが「広大なインターネットに接続する資産はどれか」、「防御が必要なネットワーク境界はどこか」という観点で、組織の内側から攻撃対象領域を捉えてきました。CXOには、「外部から企業ネットワークに接続されている、クラウド上の資産やサプライチェーンが所有す

る資産はどれか」、「こうした資産のうち、把握していないものがどれだけ存在するか」という観点で、組織の外側からリスクを捉えることが求められるのです。このガイドでは、次のポイントを解説します。警戒すべき高リスク要素攻撃対象領域管理(ASM)計画の成否を判断する方法