ネットワークセキュリティの健全性を維持するための5つのバイタルサイン

医療提供者が患者の来院の度にバイタルサイン（重要ポイント)を検査するのと同じように、ネットワークのバイタルサインも監視する必要があります。

医療提供者が常に検査する主なバイタルサインには、体温、心拍数、呼吸数、および血圧があります。疾病の診断における最初の手順は、バイタルサインの変化を確認することです。バイタルサインについて最も興味深いことは、多くの場合、特定の値ではなく、所定の患者の経時的な値の変化が重要になることです。

以下は、組織を常に保護するために監視する必要がある5つの主なネットワークのバイタルサイン（重要ポイント）です。

1: 新しいクライアントとサーバー

確認事項: ネットワーク上には多数のサーバーとクライアントがあり、企業は、通常の業務運営の一部として常に新しいサーバーとクライアントを追加します。ただし、ネットワーク上に孤立した見慣れないサーバーがあり、これらのサーバーと通信する予期しないクライアントがある場合、何らかの問題を示している可能性があります。

診断: ネットワーク上に新しい未知のファイルサーバーがある場合、誰かが情報を密かに抽出しようとしている可能性があります。新しいハッキングツールやワーム、バックオフィスサーバ、リモートアクセスサーバーは、ハッカーが使用するバックドアを示している可能性があります。新しいサーバーがある場合、不正なファイル共有が実行されている可能性があります。

2: スキャン

確認事項: ネットワーク上に普段とは異なるスキャン動作がある、またはスキャン動作が増加している場合、システムが不正アクセスされている可能性があり、犯人を素早く見つけて阻止する必要があります。

診断: 公開され、利用可能なサービスのスキャンは、ネットワークへの侵入方法を見つけたハッカーが使用する一般的な偵察手法です。多くの場合、ワームはランダムスキャンを用いて侵入先の他のシステムを見つけます。

3: ブラックリストに登録された通信

確認事項: ボットネットやマルウェアの配布チャネルなど、既知の不正なIPアドレスであるホスト。

診断: 既知の不正なホストとの通信が行われている場合、マルウェアがダウンロードされている、あるいは攻撃者がネットワークへの侵入方法を既に見つけた、およびマルウェアがさらなるコントロールと悪用手段を確立している可能性があります。

4: 数量ベースのアクティビティ

確認事項: ネットワークトラフィックと接続が継続的に異常に増加している場合、増幅、SYNフラッド、スマーフ（ICMPのブロードキャスト）/フラグル(ICMP Echoの偽造)、スローロリス(スローHTTP攻撃)、クリスマスツリー(TCPフラッグを使った攻撃)、LAND(送信元と宛先を同じアドレスにする攻撃)、IP/TCP NULL(値Nullに設定した攻撃)、またはその他の攻撃が発生している可能性があります。

診断: これらのトラフィックパターンは潜在的な進行中のDDoS攻撃の前兆であり、システムがダウンする可能性があるため、これらを素早く検出、分類、軽減できる必要があります。

5: データの引き出し

確認事項: データは定期的にネットワークを出入りしています。ネットワークの境界を出ていく不自然なほどの大量のデータ（特に機密データ）がある場合、直ちに調査する必要があります。

診断: データが大規模に移動している場合、誰かがデータを盗んでいる可能性があります。数週間または数か月にわたって機密データが流出していることに組織が気づいた場合、財務的および評判上の影響は壊滅的なものになる場合があります。

重要なポイント

新しいサーバー、スキャン、外部通信、およびデータ転送はすべて定期的なイベントであり、必ずしも問題の兆候ではありません。ただし、これらのアクティビティの量またはパターンが変わった場合、それは何らかの問題がある可能性を示すサインです。ネットワークのバイタルサインは、早期警告システムでもあります。これらのバイタルサインを監視することにより、変化を素早く特定して対処できるようになるため、これによってネットワークの健全性を維持することができます。

リバーベッドによる、ネットワークのバイタルサインの監視方法の詳細については、こちらをクリックしてください。