PRESS RELEASE

2021 年 8 月 5 日

Tenable Network Security Japan K.K

Tenable の新しい Active Directory セキュリティチェックが企業を支援

※本リリースは米国で発表されたプレスリリースの抄訳版です。原文は下記 URL を参照ください。

https://www.tenable.com/press-releases/tenable-helps-organizations-disrupt-attacks-with-new-active-directory-security

昨今のランサムウェアと巧妙なサイバー攻撃の増加を受けて、Cyber Exposure カンパニー、Tenable®, Inc. は、同社のソリューションを対象に、10 項目の基礎となる設定チェックを開発しました。対象のソリューションは、Tenable.io、Tenable.sc、Nessus Professional と Nessus Essentials で、Microsoft Active Directory のセキュリティ体制を評価し、その結果から得られた脅威の状況に応じて修正作業を整合させる機能です。これらのチェックは、Tenable が Tenable.ad で得た Active Directory 環境のセキュリティ確保に関する専門知識を活用したもので、既存のお客様には無償で今すぐ利用可能です。

攻撃を目論む集団は、企業ネットワークのすべての要素 – クラウド、ウェブアプリ、従来の IT、オペレーショナルテクノロジー（OT）– が 1 か所に連結されるシステムを狙っています。そのシステムが Active Directory です。Frost & Sullivan の調査によると、Fortune 1000 の企業のうち、90% が Active Directory をユーザー認証と認可の主要方法として使用しています。Active Directory は、一旦企業環境に侵入した攻撃者が、ほとんどの場合、最初の標的にしています。Solarwinds のハッキングの事件や一連のランサムウェア攻撃によって重要インフラがお手上げ状態になったことによって、Active Directory セキュリティ上の重要性に光があたり、専門知識を活用した適切な設定や、リスクの高い変化や動きを監査・監視しなければ起きる可能性のある問題が明らかになりました。

このように拡大し続ける危機に対応すべく、Tenable は、同社のソリューションを対象に、10 項目の基礎となる設定チェックの利用提供を開発しました。お客様が Active Directory 内でよく悪用される弱点を検出できるようにして、アクセス管理の保護と権限昇格の防止を支援する機能です。チェック機能は今すぐ利用可能で、Kerberos 認証方式を狙った攻撃、設定ミスやパスワード管理の不備、脆弱な暗号処理プロトコルなどを含む、一連のリスクにさらされているかどうかが評価できます。その結果、潜在的な攻撃経路が発見されれば、直ちに対処して、悪用される前に遮断できます。

「新しいランサムウェア攻撃やハッキングが報道メディアの見出しになる度に、Active Directory の武器化が進んでいることを見せつけられています。Active Directory のセキュリティを確保することは、より強力なサイバー防御体制とデジタルビジネスの確固たる基盤を構築するのに必要な、すべての企業がとるべき最も重要なステップの 1 つと言えます」と Tenable の共同設立者で CTO を努める Renaud Deraison は語り、また「当社では、拡大する危機に対処する支援の一環として、新しい Active Directory のチェック項目を開発して、今すぐ実行しなければならないステップを明確にしました。Active Directory のセキュリティを整備して、悪意のある攻撃者が攻撃経路に行かないように阻止する方法をよりわかりやすく提供しています」と結んでいます。

Active Directory のセキュリティ対策チェックは、Tenable.sc、Tenable.io、Tenable.ep、Nessus Professional と Nessus Essentials で一般利用可能です。総合的な Active Directory セキュリティソリューションに関心のあるお客さまには、Tenable.ad の内容を詳しくご確認いただくことをお勧めしています。Tenable.ad は、上述の基礎的なチェックばかりでなく、そのほかの包括的な評価機能を備えています。
ご紹介したチェック機能については、こちらからご覧ください。
https://www.tenable.com/blog/new-in-nessus-find-and-fix-these-10-active-directory-misconfigurations