أمان الثقة الصفرية [ZERO TRUST SECURITY]

نهج جديد لبنية الأمان

مع تطور التقنية وتكنولوجيا المعلومات أصبح الأمر أكثر تعقيدًا لحماية المعلومات وخصوصيات المستخدم في الفضاء السيبراني. يعد النهج التقليدي لإستراتيجيات الأمان مثل استخدام جدار الحماية والأدوات الأخرى المستندة إلى الشبكة لفحص المستخدمين الذين يدخلون ويخرجون من الشبكة والتحقق من صحتهم غير كافي للاعتماد عليه، والبعض الآخر فشل في توفير مستويات الثقة المطلوبة. وذلك لأن التحول الرقمي والانتقال إلى البنية التحتية السحابية يغيران الطريقة التي تمارس بها المنظمات أعمالها لحماية مواردها كبيانات المستخدم والملكية الفكرية. ثم استحدث نهج جديد لبنية الأمان في الشبكة يساعد على التخفيف من التهديد المحتمل للهجمات وزيادة وضعها الأمني، يسمى بأمان الثقة الصفرية [Zero Trust Security].

ما هو أمان الثقة الصفرية؟

ينص مفهوم أمان الثقة الصفرية على عدم الثقة والتحقق المستمر لجميع المستخدمين والأجهزة بكل محاولة وصل لهم بغض النظر عما كانوا داخل نطاق الشبكة أو خارجها، والمصادقة عليهم باستخدام أساليب مصادقة فعالة وقوية. بالإضافة إلى توفير الحماية من التهديدات.

يظن البعض أن أمان هذا النموذج يقتصر على الشبكة وحمايتها فقط، بالتأكيد الشبكة جزءًا مهم في هذا النموذج، ولكن لا يستند عليه كليًا، فهناك أجزاء أخرى مهمة لتحقيق الأمان وهي: هوية وبيانات المستخدم، الأنظمة والتطبيقات، والحوكمة وطريقة التشغيل.

مبادئ أمان الثقة الصفرية:

- **ضمان توصيل جميع الموارد والوصول إليها بشكل آمن، بغض النظر عن موقع شبكة المتصل**
  يجب حماية جميع الاتصالات بموارد المنظمة، بغض النظر عن موقع الهوية أو موقع البيانات أو تقنية المورد الذي يتم الوصول إليه. فلا يوجد ما يسمى باتصال من مستخدم في داخل الشبكة أو خارجها فجميع المستخدمين في هذا المبدأ سواسية في أسلوب التحقق.

- **الوصول الأقل امتياز (Least Privilege)**
  منح المستخدمين مستوى الوصول الذي يحتاجون إليه لأداء المهام المسندة لهم فقط.

- **تسجيل نشاطات الأجهزة والمستخدمين**
  يتم تسجيل الأجهزة وأنشطة المستخدمين بشكل دوري للتحقق من عدم وجود نشاط مشبوه حيث يجب أن تمر جميع الأجهزة عبر نفس سياسات الوصول والأمان للوصول إلى الشبكة. يمكن للعديد من حلول الأمان مثل الدخول الأحادي (SSO) والمصادقة متعددة العوامل (MFA) أن تعزز أمان الشبكة وتعزز الثقة من خلال التحقق المستمر. كلما زادت نقاط المصادقة التي تمتلكها شبكتك، كلما كانت أكثر أمانًا.

لماذا يجب التوجه إلى هذا النموذج؟

على الرغم من الصعوبات التقنية والإدارية لتطبيق نموذج أمان الثقة الصفرية، إلا أن هناك أسباب كافية للتوجه إلى هذا النموذج وبدء تطبيقه، وذلك يعود لعدة أسباب:

- **أمان المحيط لم يعد كافيًا**

على الرغم من أن المنظمات تفترض في خططها الأمنية أن التهديد يأتي دائمًا من خارج الشبكة، لكن الحقيقة هي عكس ذلك، وأكبر دليل هو حصان طروادة وكيف يمكنه شل نظام بأكمله. لذا، عندما تقوم بتنفيذ مصادقة قوية ومراقبة كل وصول إلى بيانات وأجهزة وخوادم وتطبيقات المؤسسة والتحقق منها، فلن يتمكن أي شخص من الداخل من إساءة استخدام امتيازاته.

- **الانتقال للعمل عن بُعد**

بعد جائحة كوفيد-١٩ شرعت معظم المنظمات لموظفيها بالعمل عن بُعد، وذلك أدى إلى زيادة المخاطر ونقاط الضعف السيبرانية بسبب ضعف الممارسات الأمنية على الأجهزة وشبكات الموظفين الذين يعملون من أي جزء من العالم. حتى جدار الحماية أصبح غير فعال الآن وتتسبب في أخطار على البيانات المخزنة عبر السحابة. فمن خلال تنفيذ نموذج أمان الثقة الصفرية، ستتمكن من تحديد هوية المستخدم والتحقق منه في كل مستوى بغض النظر عن مكان تواجده.

- **ضعف أمان الحوسبة السحابية**

المصادر:

[1] روبدين: Zero Trust Security - لا مكان للثقة

[2] What is Zero Trust Security and Why Is It Necessary