Cinq signes vitaux pour la santé de la sécurité réseau

Tout comme les professionnels de santé surveillent vos signes vitaux à chaque consultation, vous devez également surveiller les signes vitaux de votre réseau.

Les principaux signes vitaux habituellement surveillés par les professionnels de santé sont la température corporelle, les rythmes cardiaque et respiratoire et la tension artérielle. Afin de diagnostiquer une maladie, la première chose à faire est de vérifier les modifications de vos signes vitaux. Souvent, le plus intéressant à propos des signes vitaux n'est pas leur valeur spécifique, mais l'évolution de cette valeur dans le temps pour un patient donné.

Voici les cinq signes vitaux essentiels du réseau que vous devez surveiller pour protéger la sécurité de votre organisation.

1 : Nouveaux clients et serveurs

Ce qu'il faut rechercher : votre réseau accueille de nombreux serveurs et clients, et les entreprises en ajoutent sans cesse de nouveaux dans le cadre de leurs activités professionnelles normales. Cependant, des serveurs malveillants sur le réseau et des clients inattendus qui communiquent avec ces serveurs peuvent être le signe que quelque chose n'est pas normal.

Diagnostic : un nouveau serveur de fichiers inconnu sur votre réseau peut être le signe que quelqu'un essaie d'exfiltrer des informations. Un nouveau serveur SubSeven/Back Orifice/SVN pourrait indiquer qu'une porte dérobée est utilisée par un pirate. Un nouveau serveur pourrait être le signe d'un partage de fichiers illicite.

2 : Balayages

Ce qu'il faut rechercher : un comportement de balayage inhabituel ou accru sur le réseau pourrait indiquer que vos systèmes ont été compromis et que vous devez trouver et stopper rapidement les responsables.

Diagnostic : le balayage à la recherche de services ouverts et disponibles est une technique de reconnaissance courante utilisée par les pirates informatiques qui ont trouvé un moyen d'infiltrer votre réseau. Les vers informatiques ont souvent recours au balayage aléatoire pour trouver d'autres systèmes à infiltrer.

3 : Communications sur liste noire

Ce qu'il faut rechercher : des hôtes qui ont des adresses IP connues comme étant malveillantes, comme les réseaux zombies ou les canaux de distribution de programmes malveillants.

Diagnostic : une communication avec un hôte connu pour être malveillant peut signifier qu'un programme malveillant est en train d'être téléchargé, ou même que l'attaquant a déjà trouvé un moyen d'infiltrer le réseau et que le programme malveillant est en train de mettre en place des contrôles et des failles supplémentaires.

4 : Activité en fonction du volume

Ce qu'il faut rechercher : une augmentation inhabituelle et continue du trafic réseau et des connexions peut représenter une attaque par amplification, une attaque SYN Flood, une attaque par réflexion/rebond, une attaque Slowloris, une attaque de type « arbre de Noël », une attaque LAND, une attaque IP/TCP NULL, ou d'autres types d'attaques.

Diagnostic : ces modèles de trafic signalent une attaque DDoS potentielle en cours qui pourrait mettre vos systèmes hors service. Vous devez donc être en mesure de les détecter, de les classer et d'y pallier rapidement.

5 : Exfiltration de données

Ce qu'il faut rechercher : des données entrent et sortent régulièrement de votre réseau. Les volumes de données inhabituellement élevés qui sortent du réseau, particulièrement des données sensibles, doivent faire l'objet d'une enquête immédiate.

Diagnostic : un mouvement important de données peut être le signe que quelqu'un vole des données. Lorsque les entreprises découvrent que des données sensibles disparaissent pendant des semaines ou des mois, les répercussions tant financières que sur leur réputation peuvent être dévastatrices.

Principaux points à retenir

Les nouveaux clients et serveurs, les balayages, les communications externes et les transferts de données sont tous des événements habituels qui ne sont pas nécessairement indicateurs d'un problème. Cependant, lorsque le volume ou le modèle de ces activités change, cela peut indiquer que quelque chose n'est pas normal. Les signes vitaux de votre réseau constituent également un système d'alerte précoce. Leur surveillance vous permet d'identifier et de répondre rapidement aux changements afin de maintenir votre réseau en bonne santé.

Pour en savoir plus sur la façon dont vous pouvez surveiller les signes vitaux de votre réseau avec Riverbed, cliquez ici.