Surfer avec 100% de sécurité grâce à l'isolation

L'isolation promet une protection parfaite lors de l'utilisation du web et des e-mails. Patrick Michel, Principal Consultant chez le distributeur de sécurité informatique BOLL, explique en quoi consiste ce concept de sécurité innovant, quels en sont les avantages et quels fournisseurs proposent des solutions d'isolation solides.

Que signifie l'isolation en relation avec la sécurité?
Il s'agit du fait qu'aucun code malveillant ne parvient à l'utilisateur lors de l'accès au web et de la lecture d'e-mails. De plus, tout ce qui est exécuté dans le navigateur local s'exécute sur une plateforme d'isolation dans un environnement hautement sécurisé sous la forme d'un conteneur virtuel dans lequel un navigateur est exécuté pour l'utilisateur. Cela signifie qu'aucun code malveillant n'est exécuté sur le client, mais dans un conteneur d'isolation. On ne cherche donc pas à identifier un code malveillant, mais à l'isoler complètement. Un nouveau code propre et sûr est généré afin d'être envoyé sur le dispositif final. La procédure est différente pour les documents téléchargés par les utilisateurs. Les documents sont privés de fonctions de script dangereuses qui, dans la plupart des cas, ne sont pas nécessaires. Toutefois, dans certaines situations, l'utilisateur a la possibilité de télécharger malgré tout le document original par une action manuelle et volontaire.

Quelle est l'importance de l'isolation pour la sécurité informatique?
L'isolation entraîne un véritable changement de paradigme. Au lieu de faire la distinction entre le bon et le mauvais, comme le font les solutions de sécurité conventionnelles basées sur la détection, l'utilisateur est isolé à 100% de tout code potentiellement dangereux. Tout le trafic web et les liens dans les e-mails passent par la plateforme d'isolation. Vous pouvez surfer à votre guise où vous le souhaitez, sans crainte de code malveillant. En bref: l'isolation est un concept technologique très intéressant et corrige les faiblesses des produits de détection ou les complète.

L'isolation rend-il les autres logiciels de sécurité superflus?
Avec une plateforme d'isolation, les filtres URL ne jouent plus aucun rôle du point de vue de la sécurité. À d'autres fins – telles que le blocage de contenus qui ne sont pas souhaités par l'entreprise pour d'autres raisons – le filtrage web reste bien sûr utile. La question qui se pose aujourd'hui pour le trafic internet des utilisateurs est de savoir où celui-ci doit être protégé. Dans les architectures classiques, cela se fait sur des firewalls ou des passerelles web sécurisées (proxys). À l'ère du cloud et du télétravail, il est de plus en plus disponible en tant que service Secure Access Service Edge (SASE). Les fournisseurs de solutions web sécurisées et de passerelles de messagerie sécurisées ont commencé à les compléter par des fonctions ou des produits d'isolation appropriés.

Comment les contenus «nettoyés» parviennent-ils à l'utilisateur?
Il existe deux variantes: soit le site web est préparé dans la plateforme d'isolation puis envoyé au navigateur comme un pur document HTML/CSS – c'est ce qu'on appelle le clientless rendering. C'est très efficace et totalement transparent pour l'utilisateur, c'est-à-dire que les utilisateurs ne remarquent même pas l'isolation. Ou bien le contenu est transmis dans une sorte d'émulation de terminal sous la forme d'un flux de pixels, ce qui nécessite plus de ressources, génère plus de trafic et entraîne une perte de convivialité. Certains prestataires mélangent également les approches. Par exemple, la méthode des pixels est utilisée comme technologie de secours si la méthode de rendering crée des problèmes d'affichage.

Quel est le degré de maturité de la technologie d'isolation?
C'est un concept relativement récent, mais la technologie a maintenant mûri. L'isolation n'est plus une technologie de niche et est utilisée de manière productive par les entreprises et les autorités. C'est également le cas en Suisse – par exemple dans les banques, les centrales nucléaires et d'autres organisations soucieuses de la sécurité. La préoccupation initiale selon laquelle il y aurait trop de problèmes de rendu avec les sites web n'a pas lieu d'être.

Qui propose des solutions basées sur l'isolation?
Le pionnier a été et reste Menlo Security avec sa plateforme d'isolation, qui protège de manière fiable le trafic web et les e-mails. Aujourd'hui, le concept est utilisé par de nombreux fabricants de sécurité, par exemple Fortinet, Proofpoint et Symantec. Pour les fournisseurs de cloud tels que Zscaler, l'isolation est également présente – la technologie est entrée dans le portefeuille de Zscaler grâce à l'acquisition d'Appsulate. Lorsque des géants de l'industrie achètent des start-up innovantes et intègrent leurs technologies dans leurs propres solutions, cela indique clairement l'importance croissante d'une technologie.

Et selon vous, qui a la meilleure plateforme d'isolation?
D'après notre expérience chez BOLL, il s'agit clairement de Menlo Security. Surtout lorsque tout le trafic web doit être isolé. La technologie de rendering de Menlo s'est avérée être le leader des tests. Le marché s'intéresse de plus en plus à la solution d'isolation de Menlo. Le département américain de la Défense a récemment signé un contrat de 199 millions de dollars avec un partenaire de Menlo. De plus, Menlo Security élargit en permanence son portefeuille de solutions, toujours basées sur la plateforme d'isolation comme élément central.

Patrick Michel, Principal Consultant, BOLL.

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60
vente@boll.ch
www.boll.ch