Détecter et prévenir les menaces externes provenant du darknet

Rapid7, un fabricant renommé pour la gestion des vulnérabilités, a racheté la société de logiciels IntSights. Luca Forcellini explique de quoi il s'agit et où se situe Rapid7 dans le paysage de la cybersécurité.

L'offre de cybersécurité est extrêmement hétérogène et de plus en plus complexe. Ne pourrait-on pas faire plus simple?
Nous constatons de plus en plus que nos clients et partenaires préfèrent couvrir autant d'aspects de la cybersécurité que possible avec des solutions provenant d'une seule main plutôt que d'utiliser différents outils pour toutes les thématiques. Ainsi, chaque innovation ou expansion du paysage de la sécurité ne doit pas nécessiter une nouvelle relation commerciale avec un fabricant supplémentaire et l'équipe de sécurité ne doit pas être obligée de s'adapter à d'autres technologies et philosophies. De nombreux fabricants ont reconnu cette tendance et, par conséquent, élargissent et consolident leurs portefeuilles de produits.

A ce sujet, comment se positionne Rapid7?
Rapid7 est principalement connu pour son rôle leader dans le domaine de la gestion des vulnérabilités. Cependant, avec Insight, le fabricant propose depuis longtemps une plateforme de cybersécurité complète, qui évolue constamment et permet une visualisation centralisée. Outre la gestion des vulnérabilités pour les infrastructures informatiques sur site et dans le cloud, Insight comprend également des solutions pour surveiller et protéger les environnements multicloud, les applications web et Kubernetes. À cela s'ajoutent la détection et réponse étendues (XDR), le SIEM et l'automatisation (SOAR). En somme, une offre bien étoffée et tout aussi intéressante pour les clients et les partenaires.

Rapid7 a maintenant acheté IntSights. Qu'est-ce qui distingue son logiciel?
Les solutions de cybersécurité s'occupent généralement de ce qui se passe dans le réseau de l'entreprise et de

Luca Forcellini, Product Manager, BOLL

ce qui y entre de l'extérieur, par exemple sous la forme d'attaques de phishing et de logiciels malveillants. La solution d'IntSights vérifie ce qui se passe à l'extérieur au nom de l'entreprise – il est question de l'utilisation abusive de la marque pour des campagnes de phishing, de faux profils sur les médias sociaux, de sites web et de boutiques en ligne, ainsi que d'informations confidentielles proposées à la vente sur le darknet. Tout cela peut causer des dommages considérables à une entreprise.

En quoi cette acquisition est-elle importante pour Rapid7?
Avec IntSights, Rapid7 complète son offre avec des plateformes de renseignements sur les menaces externes (external threat intelligence). Il s'agit d'une nouvelle pierre à l'édifice de la plateforme Insight existante, qui fournit aux clients une vue d'ensemble des cyberrisques externes et permet de surveiller le clearnet, le deepnet et le darknet et de prendre des contre-mesures appropriées avant que les dommages ne se produisent ou pour les prévenir avant qu'ils ne deviennent trop importants.

L'external threat intelligence s'adresse à qui?
Principalement aux entreprises actives à l'échelle internationale ou les entreprises possédant une marque forte qui souhaitent protéger leur marque et qui ont peut-être déjà subi des attaques complexes. La solution n'est donc pas seulement intéressante du point de vue de la sécurité informatique, mais aussi pour d'autres départements de l'entreprise comme le service juridique ou le marketing. Les abus sont également de plus en plus souvent commis au nom d'autorités publiques – le renseignement sur les menaces externes est également pertinent pour le secteur public.

Quels autres avantages la solution IntSights offre-t-elle?
En tant que solution purement cloud, elle peut être mise en place très rapidement et n'est pas connectée à l'informatique de l'entreprise. Aucune donnée de l'entreprise n'est exploitée. En effet, le service de renseignements sur les menaces externes (external threat intelligence) ne fait que collecter les données de l'internet qui s'y trouvent de toute façon et en tire une analyse des risques. Les secteurs ayant des exigences élevées en matière de confidentialité, comme le secteur financier, en bénéficient tout particulièrement.

L'analyse des informations trouvées est-elle automatisée?
Dans une certaine mesure oui. L'intelligence du logiciel est complétée par le savoir-faire des spécialistes de Rapid7. Car toutes les occurrences douteuses ne peuvent pas être détectées automatiquement. Dans les cas plus complexes, des connaissances humaines sont nécessaires pour faire face à la situation. Cette combinaison réussie entre un logiciel innovant et l'expérience d'experts est une caractéristique générale de la solution globale de Rapid7.

→ **www.boll.ch/rapid7**

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