Prêts pour les incidents de sécurité

Les solutions EDR contribuent à la sécurité informatique en identifiant et en visualisant les menaces des terminaux et en permettant de prendre des mesures appropriées. Ruedi Kubli, chef d'équipe Fortinet chez le distributeur de sécurité informatique BOLL, explique dans une interview de quoi il s'agit.

Pourquoi EDR est-il nécessaire?
EDR signifie «Endpoint Detection and Response», c'est-à-dire la détection des cybermenaces sur les terminaux et la réaction appropriée. Le trafic de données via Internet étant généralement crypté, les solutions de protection conventionnelles deviennent plus ou moins aveugles aux logiciels malveillants qu'elles peuvent contenir. Cela n'apparaît déchiffré que sur l'appareil final. C'est là que l'EDR entre en jeu.

Comment fonctionnent les solutions EDR?
EDR est basé sur la détection de comportements potentiellement dangereux. Le Machine Learning entre ici en jeu. Par exemple, le logiciel FortiEDR de Fortinet a été formé à l'aide d'innombrables logiciels malveillants existants. Cela lui permet de reconnaître les comportements anormaux. Si tel est le cas, il bloque le trafic du client vers le réseau d'entreprise, l'utilisation d'une application spécifique ou l'ouverture du document potentiellement infecté.

Est-ce suffisant?
Non, le blocage automatique n'est que la première étape. Sur la base des informations fournies par le système EDR, l'entreprise doit réagir de manière appropriée. Il faut par exemple répondre aux questions suivantes: Le client doit il être débarrassé du malware ou entièrement reconfiguré? Doit-on patcher l'application concernée? Et comment traiter le document infecté pour pouvoir l'ouvrir en toute sécurité et fournir des informations importantes pour l'analyse? Une solution EDR ne peut pas prendre elle-même de telles décisions.

Ne faut-il pas disposer d'un vaste Security Know-how pour répondre à ces questions?
Oui, c'est le cas. Cependant, toutes les entreprises ne disposent pas de ressources et des compétences nécessaires en interne. Les entreprises disposant de leur propre équipe de sécurité peuvent s'en occuper elles-mêmes mais d'autres ont besoin d'un soutien extérieur. Un prestataire de services peut apporter son aide avec un service de sécurité géré. Cette solution EDR en place va profiter à ce dernier car elle fournira toutes les informations dont il a besoin pour qu'il puisse réagir de manière ciblée.

Ruedi Kubli, chef d'équipe Fortinet du distributeur de sécurité informatique BOLL

Vous dirigez l'équipe Fortinet chez BOLL. Qu'offre Fortinet en termes d'EDR?
Dans une certaine mesure, le mot EDR fait le buzz actuellement. De nombreux fournisseurs de sécurité proposent une solution EDR, dans laquelle l'aspect de «response» est souvent négligé. Les plateformes EDR offrent de belles visualisations et automatisent les réactions les plus courantes aux logiciels malveillants trouvés via les playbooks. Mais le reste appartient à l'utilisateur. Fortinet va encore plus loin: en plus de FortiEDR, Fortinet propose un service géré de détection et de réponse (MDR), qui, combiné au service de réponse aux incidents FortiGuard, soutient l'équipe du client. En résumé, nous parlons de ce que l'on appelle les «FortiGuard Responder Services».

Qu'entend-on par-là ?
Ces services offrent aux clients une surveillance 24/7 ainsi qu'un triage des alertes et aident à gérer efficacement les incidents. Tant la plateforme EDR chez le client que la plateforme FortiGuard chez Fortinet sont utilisées pour d'autres analyses, ainsi que le savoir-faire des experts Fortinet. Ceux-ci étudient et analysent chaque alerte, prennent des mesures pour protéger les clients et fournissent des recommandations concrètes et détaillées pour la résolution des problèmes ainsi que les étapes de suivi que les administrateurs devraient entreprendre.

Comment les solutions EDR s'intègrent-elles dans le reste de l'infrastructure informatique?
Les plateformes EDR ne sont pas des solutions isolées. Au contraire, elles doivent interagir avec les éléments de sécurité afin que les informations puissent être utilisées par différents systèmes. Par exemple, si EDR détecte une menace, le pare-feu doit également le savoir. Dans le portefeuille de sécurité d'un fabricant, les solutions sont généralement bien intégrées – du moins chez Fortinet c'est toujours le cas. Dans des environnements hétérogènes, les produits tiers doivent être connectés par des API, ce qui implique un effort de développement.

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