swisscom

Communiqué de presse

Swisscom renforce la sécurité des entreprises avec Managed Endpoint Detection & Response

Les notebooks, les ordinateurs de bureau et les smartphones sont la cible des cybercriminels. Les mesures préventives à elles seules ne suffisent pas à les arrêter. Afin de contrer les cyberattaques sophistiquées, des mesures de protection supplémentaires s'imposent, telles qu'un système Endpoint Detection & Response (EDR). Swisscom lance un nouveau Managed Service pour les entreprises.

Souvent, tout commence au niveau d'un terminal: 70% des cyberattaques ciblent les endpoints comme point d'attaque initial. Il peut s'agir d'un notebook, d'un PC, d'un smartphone ou d'un serveur local sur le réseau d'entreprise. Telles sont les conclusions d'une étude réalisée par prestataire américain de solutions de sécurité «Absolute Software». Les attaques sont de plus en plus sophistiquées, avec une hausse notable de celles sans fichier. Elles peuvent par exemple consister en un code de programmation qui s'exécute exclusivement dans la mémoire vive de l'ordinateur – sans laisser de traces dans le système de fichiers. «Ce type d'attaque est invisible pour la plupart des programmes antivirus et n'éveille même pas les soupçons des pare-feu», déclare Cyrill Peter, responsable Enterprise Security Services chez Swisscom. «Il est donc essentiel de protéger davantage les terminaux, de détecter les attaques et de les bloquer à temps.»

Élément clé d'une solution de sécurité globale

Un système Endpoint Detection & Response (EDR) est en mesure de le faire. Contrairement aux logiciels antivirus basés sur les signatures, il analyse le comportement des terminaux à la recherche d'anomalies. «Nos clients peuvent suivre toute l'activité en temps réel sur un tableau de bord», ajoute Cyrill Peter. «Les failles de sécurité potentielles de l'ensemble des terminaux deviennent ainsi visibles. Les messages de sécurité sont automatiquement examinés et, si possible, résolus, ce qui permet de soulager l'équipe en charge des opérations de sécurité.»

Un système EDR ne signifie toutefois pas que toutes les attaques seront automatiquement décelées et contrées. L'EDR doit être intégré à d'autres solutions de sécurité, avec un Security Operation Center

(SOC), et requiert souvent une évaluation finale des comportements suspects des terminaux par des Security Analysts expérimentés. Grâce à l'EDR, ces derniers peuvent se concentrer sur un petit nombre d'attaques potentielles (alertes présélectionnées) sans devoir évaluer des milliers d'événements et de journaux d'activité. Leur mission en est grandement simplifiée. En cas d'incident avéré, l'EDR permet à l'équipe de sécurité d'obtenir une vue d'ensemble des infrastructures IT surveillées et de réagir aussitôt sur tous les terminaux – par exemple en isolant un terminal infecté par un logiciel malveillant ou en déplaçant les fichiers suspects vers un répertoire de quarantaine.

L'EDR n'est donc pas un système autonome, mais doit être intégré dans les solutions et les processus de sécurité existants. Chez Swisscom, l'EDR peut par exemple être combiné avec SOC as a Service ou CSIRT as a Service. Les clients Swisscom bénéficient ainsi d'une défense efficace contre les attaques sans fichier, telles que les logiciels malveillants et les zero day exploits.

Voici comment fonctionne Endpoint Detection & Response

Les appareils connectés à des réseaux représentent des cibles potentielles pour des cyberattaques complexes et constituent ce qu'on appelle des endpoints. Le système Endpoint Detection & Response (EDR) surveille en temps réel toutes les activités d'un endpoint, y compris au niveau de l'interface avec le réseau, afin d'examiner et de résoudre automatiquement les alertes de sécurité. Tous les points d'accès au réseau sont ainsi protégés contre les cyberattaques complexes.

Livre blanc:
https://www.swisscom.ch/fr/business/enterprise/downloads/security/endpoint-detection-response.html

Page web produit EDR:
https://www.swisscom.ch/fr/business/enterprise/offre/security/edr.html

Page web produit Services SOC:
https://www.swisscom.ch/fr/business/enterprise/offre/security/threat-detection-and-response.html

Berne, le 14 octobre 2020