swisscom

Communiqué de presse

Cyberdéfense: danger identifié, danger réglé

Swisscom élargit son offre de services de sécurité gérés et propose dès maintenant une solution de détection et de réponse aux menaces à l''intention des entreprises. Ainsi, il devient possible pour les entreprises de détecter au plus tôt les cybermenaces et de se protéger.

Les menaces dues aux malwares, au piratage et au phishing font partie du quotidien pour les entreprises comme pour les administrations.
En sa qualité d'opérateur et de spécialiste majeur de la sécurité, Swisscom bloque des millions d'attaques par malware ainsi que 2250 tentatives de phishing par mois. Alors qu'autrefois, ces attaques étaient le fait de petits malins qui s'ennuyaient, on est aujourd'hui face à des cybercriminels professionnels. Leurs attaques sont tout à fait différentes, du point du vue qualitatif et quantitatif.

Pas de fumée sans feu… ou si?

Avec l'Internet des objets, l'essor de l'intelligence artificielle et les applications du cloud, les cybercriminels ont désormais de toutes nouvelles possibilités de nuire aux entreprises. C'est ainsi que les hackers se lancent à l'assaut d'objets du quotidien, à l'aide desquels ils mettent en place un réseau de machines zombies avant de lancer des attaques par déni de service. De plus en plus souvent, les pirates s'approchent à pas de loup; ils restent inaperçus pendant des mois, voire des années, et provoquent des dégâts conséquents. Le plus perfide, dans tout cela, c'est qu'on ne peut pas combattre ce dont on ignore l'existence. C'est pourquoi il est important de détecter au plus tôt les activités des cybercriminels et d'y apporter une réponse professionnelle.

Parés pour la prochaine génération de cyberattaques

Face à ces cybermenaces, il n'y a qu'une parade: la prévention, la détection anticipée et l'intervention de professionnels en cas de besoin. C'est pourquoi Swisscom propose dès maintenant des solutions de détection et de réponse complètes à ses clients. Depuis sept ans, Swisscom gère un «Security Operation Center» 24 h/24, 7 jours/7 à Zurich pour ses clients entreprises et dispose d'une Security Operation Center (CSIRT). Sa longue expérience bénéficie désormais à la nouvelle solution de détection et de réponse aux menaces proposée sous forme de quatre pans de services modulaires:

1. Security Analytics as a Service
   Les entreprises ont un aperçu des incidents de sécurité potentiels de l'historique des évènements par le biais d'un tableau de bord de la sécurité. Le client fait ainsi appel à l'infrastructure Security

Analytics sous forme de service. Les entreprises se chargent elles-mêmes de l'analyse et de la réaction aux incidents de sécurité.

2. Security Operation Center as a Service

   En complément de Security Analytics as a Service, Swisscom propose des services de processus de sécurité. Des spécialistes de la sécurité expérimentés analysent 24 heures/24, 7 jours/7 les incidents de sécurité potentiels et avérés, les interprètent et fournissent des recommandations concrètes aux entreprises.

3. Computer Security Incident Response Team as a Service

   Pour maîtriser les incidents de sécurité critiques, il est fait appel à des experts de la sécurité expérimentés de Swisscom. Ils lancent et appliquent la procédure de gestion des incidents à l'aide d'outils et de processus établis.

4. Threat Intelligence as a Service

   Des experts Swisscom informent de manière proactive de la présence d'informations commerciales et personnelles sensibles d'une entreprise dans les réseaux publics et fermés (darknet, par exemple). Les clients obtiennent ainsi des informations inédites au plus tôt indiquant des fuites possibles au sein de l'entreprise.

Cyrill Peter, Head of Product Management Enterprise Network & Security au sein de Swisscom Enterprise Customers, explique: «Nous constatons un phénomène marqué de professionnalisation et d'industrialisation chez les pirates. Nous sommes plus que tout autre capables d'y faire face: d'une part, grâce à notre connaissance des réseaux, nous décelons immédiatement les anomalies et les attaques potentielles; d'autre part, les connaissances accumulées suite aux attaques sont automatiquement intégrées à nos services de détection et de réponse. Nos clients profitent ainsi d'une intelligence collective unique en son genre en Suisse.»

Berne, le 26 septembre 2017

Plus d'informations sur la détection et la réponse aux menaces: https://www.swisscom.ch/detection