# Protéger proactivement les terminaux grâce aux évolutions de l'EDR

Ces dernières années, le paysage des cybermenaces a radicalement changé, avec notamment l'apparition de nouvelles menaces, les ransomwares, les mineurs de cryptomonnaie, les attaques sans ficher etc. Tout particulièrement, les attaques ciblées vers les entreprises représentent un danger sans précédent. Les cybercriminels exploitent le fait que les entreprises ne soient pas capables de gérer leur environnement informatique, de plus en plus complexe. Il est en effet difficile pour les entreprises n'ayant pas la situation en main, de faire face, d'analyser et bloquer immédiatement toute forme d'attaques, ni d'en réduire les dommages potentiels.

Un principe de base : toutes les entreprises, quelle que soit leur taille ou leur secteur d'activité peuvent être attaquées par des cybercriminels. Le défi pour les PME en particulier est que bien souvent elles n'ont pas connaissance des menaces auxquelles elles sont réellement exposées, alors que leurs ressources et expertise en matière de cyberdéfense sont souvent très limitées. Il leur est donc plus difficile de faire face à des menaces complexes.

## La simple protection des terminaux n'est plus suffisante

D'une manière générale, le logiciel de sécurité en place doit assurer une protection complète (pour tous les terminaux et serveurs, qu'il s'agisse de Windows, Mac, Android ou Linux), mais également être intuitif et facile à utiliser. Une fois qu'un logiciel malveillant ou malware a contourné la détection basée sur les signatures et les scanners binaires, les cybercriminels ont tous les accès requis pour modifier à loisir les fichiers et crypter les données.

En outre, ils utilisent fréquemment des malwares basés sur la mémoire vive qui ne laissent aucune trace sur le disque dur. Ce type d'attaque est donc rarement détecté par les solutions de sécurité traditionnelles. En fait, se contenter de bloquer les menaces génériques au niveau du terminal ne suffit plus, les entreprises ont désormais besoin d'outils capables de détecter les menaces les plus récentes et les plus sophistiquées et d'y répondre.

## L'EDR, une solution complémentaire nécessaire pour une protection proactive

La technologie EDR de détection et de réponse aux points d'accès est une technologie de cybersécurité qui répond au besoin de surveillance en temps réel et se concentre sur l'analyse des points d'accès et la réponse aux incidents. Une solution EDR propose une visibilité complète sur l'activité de chaque terminal ou point d'accès de l'infrastructure à partir d'une console centrale unique, qui délivre des informations sur la sécurité pour des enquêtes et des réponses plus approfondies. L'EDR permet de détecter de manière proactive les menaces nouvelles et inconnues

mais aussi les infections non identifiées auparavant qui s'infiltrent directement par le biais des terminaux et des serveurs. Pour ce faire, elle analyse des événements qui n'ont pas encore été attribués et qui ne peuvent être classés comme « dignes de confiance » ou « définitivement malveillants ».

Les règles et les restrictions qui étaient auparavant suffisantes pour contrer les attaques, connaissent des limites à l'heure des attaques ciblées et intervenant à plusieurs niveaux du réseau de l'entreprise. Les solutions de protection des terminaux et EDR doivent fonctionner main dans la main afin d'assurer une protection fiable et efficace contre ces menaces sophistiquées. Ces solutions permettent par exemple de déterminer s'il existe des signes d'intrusion éventuelle de personnes ou d'activités non autorisées venues du côté de l'interne et des employés ou de partenaires à l'extérieur de l'entreprise.

Dans un futur proche, la prise en charge des solutions EDR va dépendre des fournisseurs du marché et de leur capacité à automatiser l'analyse, la compréhension et la réponse, et à les reproduire sans intervention humaine.

Une solution EDR est une réelle opportunité pour contrer efficacement les cybermenaces avancées, en particulier pour les entreprises de taille moyenne. Dans la mesure où ces dernières ne peuvent pas couvrir à elles seules, avec leurs experts internes, tous les niveaux de cybersécurité, les solutions EDR en tant que service de sécurité managé (MDR = managed detection & response) offrent une réelle alternative efficace.

La sécurité des points d'accès ainsi externalisée est alors confiée à des fournisseurs de services ce qui permet au département informatique interne de concentrer ses ressources sur les compétences quotidiennes nécessaires à la continuité du business/activité de l'entreprise sans compromettre sa sécurité. Cette approche permet parallèlement d'améliorer la posture de l'entreprise en matière de cybersécurité. Plus la protection est pro active et qualitative, plus les spécialistes disposent de temps et de ressources pour faire face à des attaques difficiles.

Il est d'ailleurs intéressant de constater que plus d'un quart (28 %) des entreprises qui ont déjà mis en œuvre une solution de détection et de réponse des points d'accès (EDR) ont été en mesure de détecter des cyberattaques en quelques heures seulement, voire presque immédiatement après qu'un incident se soit produit {1}.

{1} Kaspersky IT Security Risks Survey 2019