Comment mettre en place une stratégie efficace de cybersécurité ?

Guide pour petites et moyennes entreprises

Digital Security
Progress. Protected.

Dans les grandes entreprises, des départements entiers supervisent généralement la cybersécurité de l'entreprise et mettent en place des stratégies efficaces. Mais qu'en est-il des petites et moyennes entreprises (PME) qui ne disposent que de quelques spécialistes informatiques en interne ? Comment devraient-elles procéder pour veiller à ce que l'activité soit protégée en conséquence, sans être dépassées par toutes les mesures à prendre ?

Voici quelques conseils de **Michal Jankech, Vice-Président du segment PME et MSP chez ESET**.

Digital Security
Progress. Protected.

Par où commencer ?

Dans la plupart des cas, les PME ne disposent que d'une main-d'œuvre limitée, voire inexistante, pour s'occuper de leur stratégie de sécurité numérique. Il est donc crucial pour elles de se concentrer sur les plus grandes menaces et d'investir leur énergie dans les domaines qui sont importants pour la continuité de leur activité.

« **Elles devraient adopter une approche fondée sur le risque, qui inclut l'identification des vulnérabilités les plus importantes,** » explique M. Jankech, qui ajoute que les PME devraient d'abord s'attaquer aux domaines suivants.

- **Protection et chiffrement des données**
- **Protection multicouche des endpoints et restrictions de l'accès des utilisateurs**
- **MFA et mises à jour régulières**
- **Prestataires de messagerie de haute qualité et sensibilisation des collaborateurs**
- **EDR ou MDR pour les entreprises matures et rigoureuses**

Protection et chiffrement des données

Tous vos appareils sont-ils verrouillés par un nom d'utilisateur et un mot de passe robuste ? Parfait ! Mais vous pouvez encore prendre d'autres mesures pour que la protection de vos appareils soit renforcée autant que possible. « **Tous les endpoints devraient être chiffrés**. Imaginez que quelqu'un vole votre ordinateur. Il ne peut pas pénétrer à l'intérieur puisqu'il ne connaît pas le mot de passe et le nom d'utilisateur, mais il peut néanmoins accéder aux données en retirant le disque dur. Veillez non seulement à ce que les appareils portables mais également les ordinateurs de bureau soient correctement chiffrés, » suggère M. Jankech.

« J'ai visité un établissement de santé un jour, et j'ai vu qu'un ordinateur était placé juste à côté d'une borne d'information. L'appareil n'était pas protégé par un mot de passe. Quelqu'un pourrait facilement entrer par effraction et voler le PC, accédant ainsi à toutes les données des patients. De tels scénarios peuvent être évités en mettant en œuvre des mesures efficaces de protection des données et de chiffrement. »

Protection multicouche des endpoints et restrictions de l'accès des utilisateurs

« Il est crucial de limiter les comptes administrateurs. Dans de nombreux cas, ce sont les personnes qui peuvent causer le plus de dommages. Un saboteur pourrait potentiellement installer n'importe quoi sur l'appareil s'il obtient l'accès au compte administrateur, » explique M. Jankech.

Sachez également qu'une seule couche de protection ne suffit pas. « C'est comme protéger une maison familiale. Dans ce cas, vous utilisez des mesures qui multiplient vos défenses : un portail d'entrée, des portes de sécurité, une alarme, une clôture et des fenêtres. … Beaucoup de gens disent que **l'ère de l'antivirus est révolue**. Oui, l'ère de l'antivirus standard qui n'utilise que des signatures est dépassée. Ces solutions ne sont pas en mesure de couvrir l'immense éventail des menaces actuelles, » poursuit M. Jankech.

Au lieu de cela, **un logiciel de sécurité multicouche pour endpoints** qui repose sur les principes de l'apprentissage machine et qui offre une protection de type comportemental est recommandé. Il devrait

« Pour les PME, il est logique d'investir le plus dans la prévention. Il est essentiel de renforcer vos systèmes, de les maintenir à jour et d'utiliser un bon logiciel de protection des endpoints. »

Michal Jankech,
VP du segment PME et MSP chez ESET

également mettre sur liste noire les sites web dangereux et bloquer l'accès aux domaines à risque, et intégrer une protection contre les attaques réseau ou les vulnérabilités du protocole d'accès à distance qui pourraient être exploitées pour détourner son utilisation.

« Il ne s'agit pas seulement de mettre en place une protection, mais également de la configurer et de la mettre à jour correctement, » ajoute M. Jankech. Il faut par exemple veiller à ce que le logiciel de protection des endpoints ne puisse être désinstallé ou que sa configuration ne puisse être modifiée.

Ensuite, **utilisez une console d'administration pour les endpoints**. « De nombreuses entreprises pensent qu'il suffit d'utiliser un client de protection des endpoints. Mais si vous ne le gérez pas via une console qui vous permet de superviser l'ensemble du réseau, vous ne saurez jamais s'il fonctionne correctement. Même si vous n'avez que 10 ordinateurs dans l'entreprise, vous ne serez pas en mesure de les contrôler correctement, surtout de nos jours avec des collaborateurs qui travaillent de plus en plus à domicile et se déplacent, » propose M. Jankech. La console devrait vous fournir des rapports que vous pouvez consulter pour être sûr à 100 % que vos systèmes et le trafic réseau sont dans des conditions idéales.

MFA et mises à jour régulières

L'authentification multifacteur (MFA) devrait être en place sur tous les appareils professionnels et personnels. De même, veillez à ce que tous les systèmes d'exploitation soient mis à jour vers leur toute dernière version. « La plupart des atteintes à la sécurité apparaissent à la suite d'un vol d'identité et de mot de passe, ou d'une vulnérabilité connue du système d'exploitation qui peut être exploitée, » explique M. Jankech.

À chaque nouvelle version du système d'exploitation, l'éditeur corrige les éventuelles lacunes et vous augmentez les chances d'empêcher les cybercriminels de s'introduire dans les appareils de l'entreprise. **Les mises à jour automatiques sont recommandées.** « Les PME constatent rarement des attaques de type zero-day. Si vous utilisez un logiciel spécialement conçu, les chances que les cybercriminels mènent une telle attaque ciblée sont plutôt faibles. Dans la plupart des cas, les vulnérabilités répandues dans les logiciels couramment utilisés ou les logiciels libres constituent la porte d'entrée de votre entreprise, » déclare M. Jankech.

« Médecins, architectes, agences de relations publiques... tous ont besoin d'une stratégie de cybersécurité. Beaucoup de gens ne savent par exemple pas que certains documents sont protégés par le droit d'auteur et devraient donc être sécurisés en conséquence. »

Michal Jankech,
VP du segment PME et MSP chez ESET

Prestataires de services de messagerie de haute qualité et sensibilisation des collaborateurs

Des prestataires de messagerie fiables sont également essentiels. « Les collaborateurs devraient savoir comment repérer un email d'hameçonnage. Vous pouvez également faire savoir à chaque destinataire qu'un message provient de l'extérieur de l'entreprise. Même Office 365 vous permet de libeller les emails avec la mention "externe", » recommande M. Jankech. De temps en temps, il est utile d'investir dans la formation des collaborateurs pour les sensibiliser davantage à la cybersécurité. **Vous pouvez découvrir quelques conseils** sur la façon d'améliorer l'efficacité des formations et les rendre plus ludiques en consultant le Digital Security Guide d'ESET.

M. Jankech souligne que la plupart des entreprises n'ont pas mis en œuvre ces mesures de base et que, parfois, la sécurité numérique des grandes entreprises présente des lacunes encore plus importantes. « Certaines entreprises hésitent encore à investir dans des solutions de cybersécurité ou estiment qu'elles ne deviendront pas une

cible car leur secteur d'activité est plutôt peu attractif. Mais généralement, les cyberattaques ne sont pas ciblées. Tout le monde peut en être victime, » souligne l'expert en cybersécurité.

EDR ou MDR pour les entreprises matures et rigoureuses

Une fois que vous avez mis en place tous les éléments de base de la cybersécurité, il est temps de considérer des outils de cybersécurité avancés, **tels que les solutions de détection et de traitement pour endpoints (EDR)**. « C'est un tout nouveau sous-marché, reposant sur le principe que la prévention n'est plus suffisante. Ce segment de produits s'adresse principalement aux grandes entreprises qui peuvent se permettre le luxe de disposer de nombreux services informatiques internes et d'un SOC [centre opérationnel de sécurité] interne opérationnel 24 heures sur 24 et 7 jours sur 7. Suivre cette approche revient généralement à se dire qu'un jour ou l'autre, les cybercriminels réussiront à s'introduire dans votre système, » ajoute M. Jankech.

Les solutions d'EDR identifient les anomalies et les comportements suspects sur le réseau, et vous permettent idéalement de réagir en bloquant les

Les éléments essentiels de la stratégie de cybersécurité des PME

- **Données protégées et chiffrées**
- **Règles de restriction des accès pour les utilisateurs**
- **Sécurité multicouche pour les endpoints**
- **MFA et mises à jour du système d'exploitation**

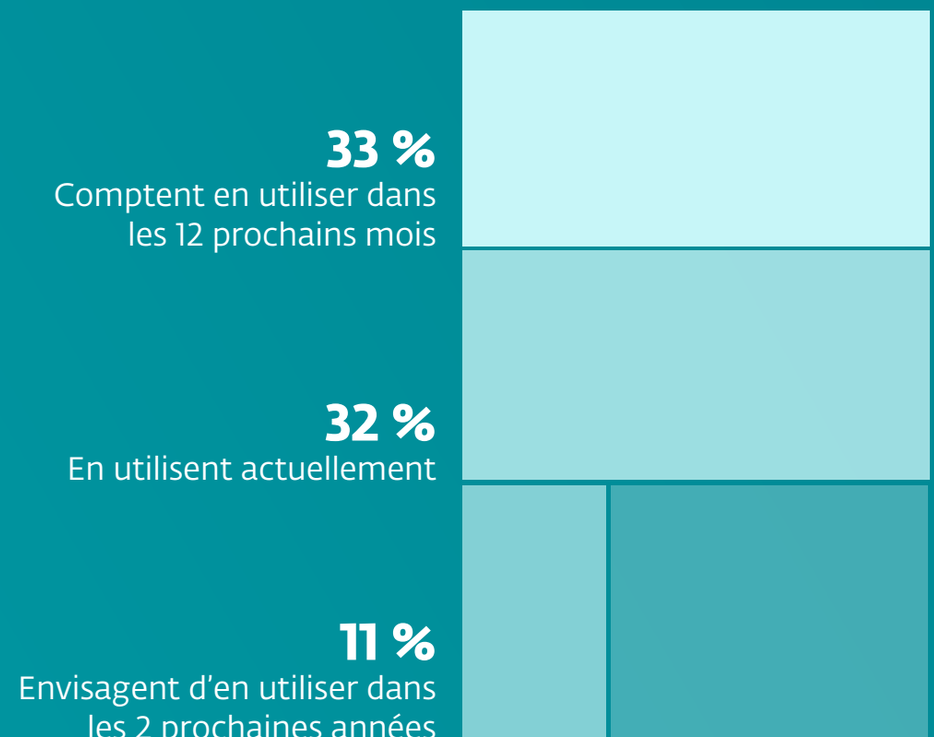
processus, ou bien les systèmes gèrent ces tâches via des règles personnalisées et automatisées. « Si elles sont généralement utilisées dans les grandes entreprises, ces solutions peuvent également être bénéfiques aux petites entreprises.

Quoi qu'il en soit, étant donné que vous avez besoin de personnel pour gérer votre plateforme d'EDR, il est recommandé aux petites entreprises d'envisager l'externalisation de ces services, » ajoute M. Jankech.

C'est là qu'intervient le MDR (détection et traitement managés). Le MDR est un système de détection et de traitement géré par un tiers. « Un seul centre de surveillance permet de superviser des dizaines, voire des centaines de clients, et il existe généralement une ligne d'assistance téléphonique accessible 24 heures sur 24 et 7 jours sur 7, » explique M. Jankech.

Néanmoins, l'EDR ou le MDR ne devraient être envisagés que si vous disposez déjà des couches de protection de sécurité de base. Lorsque vous êtes prêt, l'utilisation de l'EDR ou du MDR augmente les chances de votre entreprise de résister aux cyberattaques. Elle reste ainsi protégée mais toujours en alerte.

Utilisation de solutions EDR / XDR / MDR



Source : Rapport ESET sur le sentiment de sécurité numérique des PME en 2022

À PROPOS D'ESET

Depuis plus de 30 ans, **ESET®** développe des logiciels et des services de sécurité informatique pour protéger le patrimoine numérique des entreprises, les infrastructures critiques et les consommateurs du monde entier contre des cybermenaces. Nous protégeons les terminaux fixes et mobiles, les outils collaboratifs, et assurons la détection et le traitement des incidents. Établis dans le monde entier, nos centres de R&D récoltent et analysent les cybermenaces pour protéger nos clients et notre monde numérique. Pour plus d'informations, consultez le site **www.eset.com/fr/** ou suivez-nous sur **LinkedIn**, **Facebook** et **Twitter**.

Digital Security
Progress. Protected.