Livre blanc

Bitdefender®

COMMENT AMÉLIORER VOTRE CYBERSÉCURITÉ GRÂCE À L'ANALYSE DES RISQUES DES ENDPOINTS

Sommaire

Conformité ne rime pas toujours avec sécurité

Ces temps-ci, on ne compte plus dans les médias les articles qui signalent des attaques exposant d'impressionnantes quantités de données. Les statistiques compilées par les professionnels du secteur montrent que le nombre de dossiers concernés a plus que doublé entre 2017 et 2018. En examinant de plus près les attaques récentes les plus médiatisées, on constate qu'un grand nombre d'entre elles ont visé des entreprises aux critères de conformité particulièrement stricts, comme Target ou Equifax. On peut donc en déduire que le respect de ces critères ne suffit pas à éviter les cyberattaques. Conformité ne rime ainsi pas toujours avec sécurité. Les cybercriminels n'ont que faire des normes et des obligations réglementaires que votre entreprise applique. Ils cherchent seulement à repérer et exploiter les points faibles de votre environnement, par exemple un endpoint à risque. D'après les experts, ces attaques ont un point commun : dans tous les cas, les hackers ont profité de la faiblesse d'un « endpoint à risque » pour s'introduire dans un environnement informatique.

Les entreprises utilisent une grande variété de composants informatiques. Chaque élément connecté à Internet peut être attaqué de multiples manières. Les mots de passe faibles, les logiciels vulnérables et les problèmes de configuration ne sont que quelques-uns des moyens permettant de compromettre un appareil et de pénétrer sur votre réseau. Une fois qu'il y a accès, un hacker peut rapidement repérer dans votre infrastructure un élément majeur et déclencher une violation de données de grande ampleur. Vos adversaires peuvent utiliser plusieurs millions de permutations et combinaisons de méthodes pour attaquer et compromettre votre infrastructure.

La plupart des violations de données se produisent dans des entreprises qui ne sont pas conscientes de l'étendue de leur surface d'attaque et ne savent pas que certains de leurs endpoints sont vulnérables. Il est très difficile d'évaluer le risque global - cela revient à naviguer à vue.

Des difficultés universelles

À mesure que les entreprises, quelle que soit leur taille, poursuivent leur transformation numérique et optent de plus en plus pour des applications mobiles ou dans le cloud, leur infrastructure informatique s'étend et devient plus complexe. Pour preuve, 68% des entreprises ayant répondu à une enquête menée par le cabinet d'analyse ESG affirment que leur environnement informatique s'est complexifié aux cours des deux dernières années.

Figure 1.

Une surface d'attaque qui s'étend

L'époque où il suffisait de protéger vos endpoints et de surveiller vos réseaux internes abrités derrière un pare-feu pour assurer votre sécurité est bel et bien révolue. Les entreprises se sont développées en ligne et dans le cloud, et par conséquent leur surface

d'attaque est désormais bien plus grande. Les hackers qui aiment innover ont donc une multitude de nouvelles voies à explorer.

Les entreprises modernes doivent disposer d'un environnement numérique en lien avec des services externes, parfois sous la forme d'applications « maison » hébergées dans le cloud, ou bien en lien avec des applications gérées par des entreprises tierces. Pour les responsables IT et les administrateurs de la sécurité, la principale difficulté consiste à obtenir une vue d'ensemble suffisamment précise de la surface d'attaque, afin d'identifier les endpoints à risque et de détecter les problèmes de configuration.

Pour lutter contre les acteurs malveillants, les entreprises doivent faire évoluer leur sécurité. Il ne s'agit plus seulement de protéger les endpoints. Il faut changer de perspective et comprendre que l'environnement des endpoints et des installations joue un rôle bien plus important qu'il n'y paraît. Il n'est plus possible de miser uniquement sur la protection des endpoints. Pour comprendre les risques auxquels s'exposent les entreprises et contrôler la surface d'attaque il faut disposer d'une bonne visibilité sur l'ensemble des composants de l'infrastructure, mais aussi connaître la configuration de chacun d'eux, les applications utilisées, les contrôles de sécurité mis en œuvre et les comportements des utilisateurs, entre autres.

Pas assez de spécialistes de la sécurité

Dans une récente enquête du cabinet ESG sur les principales difficultés rencontrées par les services informatiques des entreprises, il a été demandé aux responsables d'identifier les domaines dans lesquels ils constataient une pénurie de compétences. En 2018-2019, la cybersécurité est arrivée en tête de liste (53% des réponses). Le domaine de l'architecture informatique/de la planification occupait la deuxième place (38%). Fait inquiétant, le déficit de compétences en cybersécurité est systématiquement la principale difficulté mentionnée dans l'enquête annuelle d'ESG depuis que celle-ci existe. Dans le même temps, le pourcentage d'entreprises signalant une pénurie problématique de compétences en cybersécurité continue d'augmenter.

C'est un enjeu important dans le monde entier, car les entreprises concernées sont davantage exposées au risque de cyberattaque. Selon différents rapports, à l'échelle mondiale la cybercriminalité devrait coûter $2 mille milliards de dollars par an d'ici 2020. Si la pénurie de compétences continue de s'aggraver, les entreprises seront de plus en plus exposées et mettront en danger leur infrastructure et leurs clients. Les entreprises qui cherchent à recruter peuvent mettre entre six et neuf mois pour trouver des candidats qualifiés. Ce délai a parfois des conséquences graves, puisque les équipes informatiques n'ont pas suffisamment de personnel. Elles manquent donc souvent de compétences avancées dans les domaines majeurs que sont l'analyse, la réalisation d'enquêtes sur les attaques et le cloud computing. Par ailleurs, étant donné la pression exercée sur les ressources existantes, les entreprises consacrent trop de temps à la formation continue des équipes chargées de la cybersécurité, parfois au détriment de la satisfaction professionnelle de leurs employés.

De trop nombreux outils

On est souvent attiré par tout ce qui brille, tout ce qui est nouveau. Et le secteur de la cybersécurité ne fait pas exception : le marché regorge d'outils soit disant innovants et promettant de régler toutes sortes de problèmes. Votre équipe de sécurité est-elle fatiguée d'avoir à jongler entre tous ces outils ? Est-elle débordée par le nombre d'outils qu'elle n'arrive pas à gérer ? A-t-elle du mal à suivre toutes les informations communiquées et à appliquer les procédures et mises à jour en temps voulu ?

D'après la dernière enquête d'ESG, 40% des équipes de sécurité utilisent entre 10 et 25 outils, et 30% disent même qu'elles utilisent entre 26 et 50 outils. C'est dans le secteur de la finance que ce chiffre est le plus impressionnant : 73% des entreprises utilisent au moins 35 outils. Mais le problème n'est pas tant leur nombre que l'absence d'intégration entre ces différents outils et l'incohérence entre leurs multiples fonctionnalités (https://www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf).

Les cyberattaques modernes

Le ransomware WannaCrypt (WannaCry), créé en 2017, a fait des ravages dans le monde entier. Il s'agit d'un ver qui se propage rapidement à travers un grand nombre de réseaux informatiques. Une fois qu'il a infecté un ordinateur Windows, il chiffre des fichiers sur le disque dur pour les rendre inaccessibles. Les attaquants adressent alors une demande de rançon en Bitcoin au propriétaire de ces fichiers, qui doit payer pour obtenir leur déchiffrement.

Le ransomware Wannacry se compose de plusieurs éléments. D'abord, un programme malveillant qui infecte l'ordinateur, puis le ransomware proprement dit qui chiffre les dossiers du endpoint et enfin le ver qui se propage sur d'autres systèmes connectés en exploitant une vulnérabilité SMB non corrigée des systèmes Windows.

Une fois qu'un endpoint est infecté, WannaCry tente d'accéder à une URL codée en dur (kill-switch). S'il n'y parvient pas, il recherche et chiffre des fichiers de formats courants (Microsoft Office, JPEG, MP3, MKV, etc.) pour que l'utilisateur ne puisse plus y accéder. Il affiche ensuite une demande de rançon (300$ en Bitcoins) pour le déchiffrement et la restauration des fichiers.

La propagation de WannaCry aurait pu être évitée

Le ver permettant au ransomware d'infecter d'autres ordinateurs est basé sur l'exploit EternalBlue, qui aurait été développé par la NSA, l'agence gouvernementale américaine responsable du renseignement et de la sécurité des systèmes d'information, et qui

cible une vulnérabilité SMB. Cet exploit a été dérobé et mis en ligne sur le dark web par un groupe de hackers connu sous le nom de Shadow Brokers. Après avoir pénétré un réseau Windows, WannaCry a pu se propager et infecter d'autres machines sur lesquelles cette vulnérabilité n'avait pas été corrigée, sans aucune intervention humaine. C'est grâce à ce mécanisme de propagation autonome que ce ransomware s'est répandu si rapidement.

Paradoxalement, Microsoft a découvert cette vulnérabilité et a mis à disposition un correctif efficace contre WannaCry avant même que l'attaque ne commence. Le bulletin de sécurité MS17-010, publié par Microsoft le 14 mars 2017, annonçait une mise à jour du protocole SMB sur Windows pour éviter une infection via EternalBlue. Microsoft avait signalé que ce patch était essentiel. Malgré cette mise en garde, il n'était toujours pas appliqué sur un grand nombre de systèmes en mai 2017, lorsque WannaCry a commencé à se propager. En cas d'infection d'un système non protégé il n'y a pas grand-chose à faire, si ce n'est restaurer les fichiers chiffrés à l'aide d'une sauvegarde. On peut tirer une leçon fondamentale de cette expérience : il faut toujours appliquer les derniers correctifs de sécurité.

Malgré une médiatisation massive, sans oublier la publication d'un grand nombre de patchs et de bonnes pratiques visant à endiguer sa propagation, le ransomware WannaCry est encore actif et continue à infecter des systèmes. Une solution existe pourtant, mais c'est justement parce que ces patchs ne sont pas appliqués que des malwares comme WannaCry peuvent encore faire des dégâts bien après la mise à disposition de cette solution. Cela montre bien qu'il est essentiel d'avoir une bonne visibilité sur les risques posés par les endpoints qui composent votre infrastructure, afin de les éliminer à temps.

Aujourd'hui le principal danger vient des variantes de WannaCry, ou plus précisément des nouveaux vers utilisant le même exploit EternalBlue. Tous les malwares basés sur EternalBlue ciblent la même vulnérabilité de Windows. La multiplication de ces attaques laisse penser qu'un grand nombre de systèmes Windows ne sont pas encore protégés par les correctifs adéquats. Il ne faudra pas longtemps à un attaquant pour les repérer.

Critères essentiels pour la sécurité des endpoints

Analyse des risques des endpoints et renforcement

Toute approche globale visant à protéger l'environnement informatique d'une entreprise doit commencer par une analyse de la surface d'attaque. Vient ensuite la phase d'identification et de sécurisation des endpoints à risque, l'objectif étant de les rendre moins vulnérables aux cyberattaques. Pour Bitdefender, c'est une première étape essentielle à la mise en place d'un système complet de protection.

La sécurisation renforcée des endpoints est le processus qui consiste à réduire la surface d'attaque, notamment par les opérations suivantes :

Sécurisation du système d'exploitation – Mise à jour complète du système d'exploitation : installation des dernières fonctionnalités, suppression des programmes inutiles, actualisation des paramètres de sécurité, vérification des configurations, etc.

Sécurisation des services – Suppression des services, processus, fonctions et fonctionnalités inutiles et indésirables.

Analyse des problèmes de configuration des endpoints – Contrôle continu de la configuration des endpoints, puis signalement et résolution des problèmes éventuels.

Sécurisation des applications – Mise en place des correctifs les plus récents et correction des bugs.

Pour tout maintenir à jour, de nombreuses entreprises utilisent les outils intégrés à leurs systèmes d'exploitation ou des logiciels vendus par le fournisseur (Microsoft SCCM, par exemple). D'autres font appel à des applications tierces de gestion des correctifs, capables d'appliquer les mises à jour nécessaires sur les systèmes d'exploitation et les applications les plus courantes. Quelques outils permettent d'identifier les problèmes de configuration des endpoints et d'y remédier. On peut notamment citer Defender ATP Threat & Vulnerability Management, récemment annoncé par Microsoft, qui analyse les endpoints pour y détecter d'éventuels problèmes de configuration du système d'exploitation ou des applications ou encore les mises à jour manquantes/patchs non appliqués, afin de créer un index des vulnérabilités.

Les quelques outils qui permettent d'effectuer toutes ces actions de sécurisation - ou une partie seulement - ne sont pas cohérents les uns avec les autres, ils nécessitent des consoles de gestion distinctes et ils sont souvent administrés par des équipes qui ne communiquent pas entre elles. Résultat : les actions sont souvent confuses et tardives, et la protection n'est pas toujours complète. L'idéal est donc une solution intégrée capable d'assurer une couverture totale.

Prévention intégrée des violations, s'appuyant sur l'analyse des risques

Les exigences d'une entreprise en matière de sécurité dépendent d'un grand nombre de facteurs. Dans certains secteurs, notamment la finance et la santé, ce sont les réglementations en vigueur qui déterminent les précautions à prendre. D'autres entreprises peuvent revoir leurs exigences à la hausse parce qu'elles ont subi une violation de données ou parce qu'elles adoptent une posture préventive.

Ces approches sont utiles, mais elles ne permettent pas de garantir une sécurité totale car elles sont trop restreintes. Pour assurer une sécurité totale, il faut opter pour une approche globale reposant notamment sur l'identification des éléments à risque dans l'environnement, la recherche de vulnérabilités sur l'ensemble des endpoints, la vérification des paramètres de sécurité et la mise en place d'un système d'aide ou d'automatisation pour la résolution des problèmes. Elle doit être associée à une visibilité accrue et à une politique de prévention plus efficace.

GravityZone donne aux équipes informatiques les outils nécessaires pour mettre en place des processus de sécurité optimaux. Endpoint Risk Analytics est l'une des dernières technologies venues compléter notre solution de sécurité. Ce module s'ajoute à d'autres qui ont déjà fait leurs preuves, parmi lesquels Full Disk Encryption, Web Threat Protection, Device Control, Application Control et Patch Management.

Figure 2.

Comment fonctionne l'analyse des risques par Bitdefender ?

Le module Endpoint Risk Analytics (ERA) analyse en continu tous les endpoints à la recherche de plus de 200 indicateurs de risque, afin d'obtenir le score de chaque endpoint mais aussi un score global. Ces scores apparaissent sur un tableau de bord dédié, avec des informations sur la gravité des risques encourus. L'analyse des risques repose principalement sur l'identification des problèmes de configuration des endpoints, qui constituent le principal talon d'Achille des entreprises.

Problèmes de configuration des endpoints

Les problèmes de configuration sont à l'origine de la plupart des failles de sécurité. Plus de 90% des attaques recensées ont pu se produire parce qu'un endpoint était mal configuré et a servi de « porte d'entrée ».

Parmi les problèmes pouvant être exploités par un hacker, on peut citer :

- **La désactivation de la protection**
- **L'activation du protocole Telnet sur Windows** pour les connexions entrantes non chiffrées au lieu d'utiliser des serveurs SSH. Cela permet à des tiers non autorisés d'accéder à l'ordinateur.
- **L'activation de l'option Connexion automatique** réduit la protection des comptes car n'importe qui peut y accéder.
- **La désactivation ou le manque de fiabilité de la fonction de contrôle du compte utilisateur (UAC)** n'informe pas l'utilisateur si un tiers tente d'installer un nouveau logiciel sur son ordinateur ou d'en modifier les paramètres.
- **L'activation du LM Hash** quand il devrait être désactivé par défaut pour éviter de compromettre le chiffrement et l'authentification du mot de passe.
- **La désactivation de la fonction ASLR (distribution aléatoire de l'espace d'adressage)** corrompt la sécurité du système, alors que cette fonction devrait être toujours activée.
- **La désactivation du mode de protection Session Manager**
- **La possibilité d'ouvrir une session invité non sécurisée** affaiblit la sécurité des clients Windows. L'ouverture de sessions invité non sécurisées ne devrait jamais être autorisée car ces comptes sont plus vulnérables aux attaques dites « de l'homme du milieu ».
- **L'activation de la fonction Autorun** – alors que cette fonction devrait être désactivée. Sinon, du code malveillant pourrait être exécuté sans que l'utilisateur ait à intervenir ou puisse s'en rendre compte.

Quand l'un de ces cas de figure - ou tout problème de configuration parmi les 206 autres prédéfinis par le module ERA - est détecté sur un endpoint, le score de risque de ce dernier augmente d'un certain nombre de points en fonction de la gravité du problème.

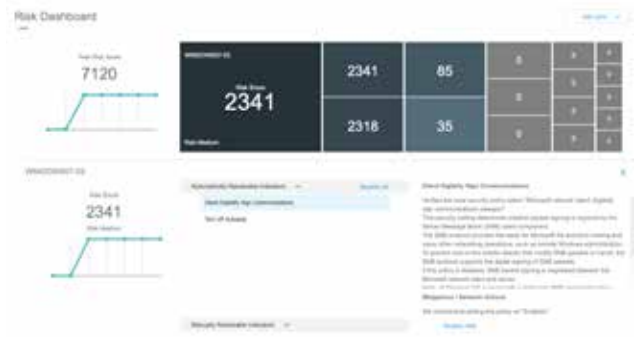
Grâce au module ERA, les équipes informatique peuvent désormais obtenir une vue d'ensemble de la sécurité de leur entreprise. Le score de risque global affiché sur le tableau de bord correspond à la somme des scores de chaque endpoint. L'interface utilisateur du module ERA permet aux administrateurs de décomposer ce score global et de connaître le niveau de risque de chaque endpoint.

Le tableau de bord de GravityZone (Figure 3 ci-dessous) permet aux administrateurs d'accéder au profil de risque de chaque endpoint protégé par GravityZone. Le tableau de bord permet de visualiser un profil de risque global à l'échelle de l'entreprise. La première ligne indique le nombre total d'appareil protégés, le score de risque et son évolution, les appareils propres à chaque système d'exploitation, le type d'appareil (endpoint ou serveur), etc.

Figure 3.

Figure 4.

Figure 5.



La deuxième ligne (Figure 5) indique le score de risque global et les briques montrent le score de risque de chaque endpoint. Celui qui a obtenu le score le plus élevé s'affiche en haut à gauche. En passant la souris sur chaque brique on obtient des informations complémentaires : nom et type de d'endpoint, catégorie de risque, etc. En cliquant sur le bouton « Détails », on accède à une description précise. C'est aussi depuis cette fenêtre que l'on peut déclencher le processus d'élimination du risque ou découvrir la marche à suivre pour l'éliminer. Les responsables IT disposent ainsi d'une meilleure visibilité des risques auxquels les endpoints sont exposés mais également d'informations permettant d'éliminer ces risques. Il est même parfois possible de déclencher leur élimination automatiquement.

La troisième colonne du tableau de bord (Figure 6) recense les indicateurs de risque (IoR). Cela permet de savoir quels sont les types de risques détectés dans l'environnement de l'entreprise. La couleur de la brique indique la sévérité du risque, et le chiffre qui se trouve au milieu correspond au nombre d'endpoints concernés. En cliquant sur le bouton « Détails » on ouvre une fenêtre qui contient une description précise des risques,, ainsi qu'un bouton permettant de déclencher le processus d'élimination de ces risques.

Figure 6.

Résumé

Le déploiement de solutions de types EPP ou EDR ne suffit pas à assurer une cybersécurité complète et efficace. Pour garder une longueur d'avance sur des menaces qui évoluent constamment, il est important d'analyser les risques des endpoints. Cela peut se faire en évaluant en continu les endpoints pour repérer notamment les problèmes de configuration, sur la base des recommandations de Microsoft en matière de sécurité ou d'autres critères permettant de détecter des vulnérabilités. Une analyse complète des risques permet aux administrateurs de visualiser la sécurité globale à l'échelle de l'entreprise mais aussi au niveau de chaque endpoint. Le module Endpoint Risk Analytics permet d'éliminer un certain nombre de risques en un clic, et indique la marche à suivre pour traiter les risques plus complexes (aide à la remédiation). Face au risque d'une attaque de grande ampleur, la meilleure stratégie consiste à identifier les endpoints les plus à risque dans votre environnement et à corriger rapidement les problèmes détectés. La gestion des risques numériques auxquels s'expose une entreprise fait partie des mesures qu'un administrateur peut prendre dès aujourd'hui pour éviter des cyberattaques de demain.

Pour plus d'informations, veuillez consulter www.bitdefender.fr/business

Bitdefender est une entreprise mondiale de sécurité qui développe des solutions de cybersécurité de pointe et qui protège plus de 500 millions d'utilisateurs dans plus de 150 pays. Depuis 2001, Bitdefender développe des technologies régulièrement récompensées, pour les marchés des entreprises et des particuliers, et est un fournisseur recommandé pour sécuriser les infrastructures hybrides et protéger les endpoints. Grâce à ses équipes R&D et celles en charge des alliances et des partenariats avec les principaux fournisseurs de technologies de virtualisation et de Cloud, Bitdefender a su réhausser les standards de sécurité les plus élevés de l'industrie et est reconnu comme étant un éditeur innovant, proposant des solutions de sécurité fiables, performantes et efficaces. Plus d'informations sur www.bitdefender.fr.

Bitdefender-WhitePaper-WCPERA-CREAT3790-fr_FR