21
JAN
2022

CYBERUN
CYBERSECURITY STRATEGIES
cyberun.net

Endpoints

Rassembler des terminaux toujours plus hétérogènes

Bien qu'au cœur des politiques de sécurité, se préoccuper à outrance des *endpoints* ne semble plus être "à la mode". Est-ce la faute du BYOD, de l'omniprésence du *cloud* ou simplement d'une usure des ingénieurs, confrontés depuis des années aux mêmes problèmes (durcissement, patching, antivirus, analyse des remontées d'alertes, etc.), qui ne sont encore que rarement automatisés ?
Pourtant, les négliger conduit irrémédiablement à la catastrophe.

En dehors de l'EDR, souvent présenté comme la réponse à tous les problèmes, les endpoints *illustrent de plus en plus rarement des technologies au marketing flamboyant. D'ailleurs le saut technologique entre antivirus avancés et EDR est finalement assez plus ténu. En revanche, pour utiliser ces nouveaux outils, les organisations doivent évoluer, car il ne s'agit plus de produits qu'on peut laisser tourner sans surveillance. De nouvelles ressources (humaines), internalisées ou externalisées, sont indispensables.*

Contrôler des centaines, voire des milliers de terminaux, que ce soit des postes de travail, des serveurs, des smartphones, des tablettes, mais aussi des objets connectés, est finalement beaucoup plus complexe, mais aussi moins valorisant que de surveiller un réseau. Pourtant, c'est aussi à ce prix que la sécurité globale est améliorée. Et il ne faut plus voir chaque *endpoint* comme indépendant des autres : c'est seulement quand chaque élément renvoie des informations, par exemple à un SOC ou un SIEM, que l'on a une bonne chance de détecter une attaque, qui passerait sinon sous les radars, et de constituer sa propre *threat-intelligence*. N'oublions pas que c'est essentiellement grâce à ce changement de paradigme que l'EDR tire son épingle du jeu, et non en raison d'algorithmes (proches de ceux utilisés dans les antivirus "avancés"). ■

5 idées à retenir…

- **Même si cela peut sembler une évidence, il est indispensable (et pas si simple) de connaître intégralement l'intégralité du parc d'*endpoints* (y compris ceux en BYOD) qui se connectent au SI.**
- **Protéger les *endpoints* ne se résume pas à y installer un antivirus : chiffrement, patching, contrôle d'accès, durcissement sont indispensables.**
- **Les EDR sont une innovation majeure, mais ne doivent pas être choisis à la légère, y compris durant une crise.**
- **La sécurité des *endpoints*, même à grands renforts d'IA ou d'automatisation, nécessite des efforts humains (et donc financiers) importants, conduisant de plus en plus à l'externalisation d'une partie de ces tâches.**
- **Les vulnérabilités nécessitent plus que jamais une gestion efficace et extrêmement rapide des corrections et des contre-mesures, impliquant l'ensemble de la DSI, mais aussi des métiers.**

SOMMAIRE

L'enquête
Problématique et enjeux _02
L'EDR, nouvel eldorado ? _04
Au-delà de la détection des attaques _06

Retours d'expériences
iBanFirst : L'EDR pour déjouer les rançongiciel _08
Grenoble capitalise sur les iOC _09
La Poste : Renforcer l'accès au SI _10
L'indispensable management de l'EDR _11
Les grognements de Cy-Bear _12
Les 10 conseils de nos experts _12

GIUSEPPE BRIZIO | CISO EMEA, Qualys

Optimiser la remédiation des vulnérabilités

La remédiation des vulnérabilités est l'une des tâches les plus complexes sur un parc disparate d'*endpoints*. Il est difficile d'identifier, de prioriser et de remédier efficacement aux vulnérabilités. Avec un nombre croissant de vulnérabilités découvertes chaque année (18 378 vulnérabilités en 2021), nous assistons à une augmentation des attaques par *ransomware* qui exploitent les vulnérabilités non corrigées.

Cette situation a contraint les équipes en charge de l'IT et sécurité de trouver des solutions pour optimiser les délais de remédiation et rendre leur programme de remédiation aussi efficace que possible. De plus, depuis la pandémie, de nombreux employés continuent de télétravailler, si bien que leurs ordinateurs distants et autres actifs doivent être mis à jour en permanence.

Face à ces défis, les équipes IT et sécurité se doivent de travailler ensemble pour optimiser leurs pratiques de gestion des patchs proactive et réactive afin de réduire la surface d'attaque et de renforcer la sécurité de leur entreprise.

Déployer de nouveaux patchs de manière proactive permet de remédier à un grand nombre de nouvelles vulnérabilités, avant même que l'équipe sécurité lance un scan des vulnérabilités. Créer régulièrement de nouvelles tâches de déploiement de patchs améliore la gestion des patchs proactive en termes de simplicité et d'efficacité.

Un *workflow* de remédiation doit permettre de remédier de façon simple et efficace aux vulnérabilités détectées lors de scans de vulnérabilités (gestion des patchs réactive). Dans la plupart des cas, l'équipe chargée d'analyser les vulnérabilités n'est pas celle qui déploiera les correctifs. Il est donc impératif que les solutions de gestion des patchs et des vulnérabilités partagent leurs informations pour garantir un processus de correction efficace.

L'équipe chargée de déployer les patchs doit utiliser les informations sur les vulnérabilités pour créer des tâches de correction efficaces, mais il faut qu'elle s'affranchisse du travail fastidieux et routinier nécessaire pour transformer les résultats des recherches sur les vulnérabilités en un ensemble exploitable de patchs à déployer. Une plateforme de sécurité intégrée, comme celle de Qualys, utilise les mêmes *workflows* de remédiation et, ainsi, accélère la traduction des vulnérabilités détectées dans vos environnements en correctifs.

Une solution de *Patch Management* doit offrir la possibilité de créer un processus d'automatisation de correction proactive permettant d'être plus efficace et efficient. On peut aussi déployer tous les nouveaux patchs, ou seulement certains d'entre eux, par exemple seulement ceux destinés à des systèmes d'exploitation et/ou des applications tierces en fonction de la gravité de la vulnérabilité ou d'autres critères.

En automatisant le déploiement de patchs simples, l'équipe concernée peut se consacrer à la correction manuelle pour veiller à ce que les patchs à plus haut risque n'engendrent pas de risque opérationnel pour l'environnement.

En s'appuyant sur les données de vulnérabilités et sur les indicateurs de menaces en temps réel, les entreprises peuvent créer des tâches de correction sans intervention (*Zero-Touch*) qui appliquent automatiquement les patchs appropriés à une nouvelle vulnérabilité qui présente un risque spécifique.

Il est légitime que l'équipe sécurité aspire à corriger le plus d'applications possible, mais, en revanche, l'équipe IT a conscience que corriger toutes les applications disponibles peut augmenter le risque opérationnel. L'équipe IT a pour mission de veiller à ce que les applications métier continuent de fonctionner, quel que soit le processus de correction. Résoudre ce dilemme, c'est-à-dire décider quels produits corriger, puis ceux à corriger automatiquement, est difficile à faire. La solution de Patch Management doit donc être en mesure de résoudre ce problème en permettant aux équipes sécurité et IT de visualiser les produits à corriger en priorité, et ceux pour lesquels il est possible de déployer automatiquement des correctifs.

MARINE HARDY | Avocat Directeur des Pôles Innovation & Sécurité, ITLaw Avocats

Sécurité des *endpoints* : quels enjeux juridiques ?

Envisager la sécurité des *endpoints* fait partie des points essentiels en matière de sécurité informatique. Nous constatons qu'en complément des mesures classiques, comme l'usage d'antivirus, existent des outils innovants (EDR, XBR, NDR, EPP, etc.) intégrant des technologies complexes telles que de l'intelligence artificielle. L'apparition de ces outils s'explique notamment par une complexification de la sécurité en matière d'*endpoints*, complexification ayant diverses origines, telles que l'essor du BYOD et de l'Internet des objets qui ont conduit à une augmentation et une diversification du type d'appareils connectés aux systèmes d'information des entreprises et des nouveaux types de menaces cyber. Avant de signer, plusieurs points de nature juridique doivent retenir votre attention.

Gare aux termes de vos contrats

À titre d'exemple, en matière d'antivirus, outre les clauses d'exclusion de responsabilité classiques des contrats IT, la plupart des contrats des prestataires en la matière comportent des clauses d'exclusion qui peuvent apparaître contraires à l'objectif annoncé lors de l'achat de la solution antivirus. On notera ainsi, par exemple, l'exclusion par principe de la responsabilité du prestataire en cas de perte de données, de jouissance du matériel informatique et/ou toute perte d'activité résultant de la prise de contrôle du ou des ordinateurs du client. Par ailleurs, il peut être imposé au client de mettre en place les mesures "adéquates" pour gérer les risques de son système d'information (dont la solution d'antivirus fait partie…), voire certaines mesures sont imposées, par exemple faire des sauvegardes.
En outre, des interdictions et incompatibilités dans le cadre de l'usage de la solution peuvent être précisées, rendant parfois caduc le produit. Il est important de maîtriser ces termes afin que le contrat n'affaiblisse pas l'objectif recherché par l'usage de tels outils.

Gare à l'usage d'une solution innovante non maîtrisée

L'usage des nouveaux outils innovants, incluant notamment de l'intelligence artificielle, est très intrusif sur un système d'information et peut conduire à des conséquences non souhaitées, telles que, par exemple, des modifications, suppressions, altérations ou déplacements de données. Il est dès lors recommandé d'anticiper ces difficultés et d'encadrer leurs conséquences dans un cadre contractuel. À titre d'exemple, on peut définir les résultats et fonctionnalités attendus, les actions interdites à l'outil, mais également la répartition des obligations et responsabilités de chaque partie en matière de paramétrage, de sélection des données alimentant l'outil et de contrôle des résultats.
En conclusion, à ce jour, les mécanismes contractuels apparaissent comme l'un des points clés de la sécurisation juridique, technique et économique concernant la sécurité des *endpoints*. Il est donc plus que nécessaire de veiller à leur parfaite adéquation à vos projets !