LeMagIT
L'informatique pour et par les pros
TechTarget
E-handbook
Contenu PRO+

Gestion des vulnérabilités :

« un impératif en forme de défi »

Comprendre, choisir sa solution et agir

Dans ce guide

Introduction

La gestion des vulnérabilités s'impose comme l'une des pratiques de référence incontournables pour assurer une bonne de posture de sécurité à son système d'information. Mais l'exercice n'a rien de trivial entre inventaire à jour des vulnérabilités à corriger, suivi des correctifs disponibles, planification de déploiement, etc.

Et c'est sans compter avec ces composants logiciels patrimoniaux trop vieux pour recevoir le moindre correctif, mais trop critiques pour être simplement arrêtés.

Heureusement, le marché prend ces questions de plus en plus en compte et adapte ses réponses à la réalité des entreprises.

Dans ce guide

Comprendre les tendances

La gestion des vulnérabilités reste le point noir de la sécurité

Valéry Marchive, Rédacteur en chef adjoint

Se concentrant sur les logiciels présents dans l'environnement des utilisateurs de ses solutions de gestion des vulnérabilités, Flexera a identifié, l'an passé, 17 147 vulnérabilités dans 2 136 applications produites par un peu moins de 250 éditeurs. C'est une progression de 6 % sur un an, et de 33 % sur cinq. La progression du nombre de vulnérabilités observées est donc régulière. Elles peuvent donner l'impression de se concentrer sur un nombre de plus en plus restreint d'éditeurs et de produits : le nombre de produits vulnérables a reculé de 14 % en 2016, et celui d'éditeurs concernés, de 7 %. Mais Flexera relativise ce résultat en soulignant avoir cessé, l'an passé, de suivre les logiciels absents de son parc installé.

Reste que les vulnérabilités apparaissent de plus en plus sévères. Ainsi, l'an passé, 0,5 % des vulnérabilités étaient « extrêmement critiques », et 18 % « hautement critiques », soit 5 points de mieux qu'en 2015. Dans plus de la moitié des cas, les vulnérabilités peuvent être exploitées à distance, depuis l'extérieur du périmètre de l'entreprise (56 %).

Dans ce guide

Mais Flexera propose aussi d'autres indicateurs, peut-être plus représentatifs de l'état du risque, en se concentrant sur les 50 applications les plus souvent présentent sur les postes de travail surveillés avec ses solutions. Là, les applications Microsoft trustent 69 % du classement. La bonne nouvelle, c'est que sur ce Top 50, le nombre de vulnérabilités découvertes a été de 1 626 en 2016, soit 21 % de moins que l'année précédente. Et celles affectant des applications Microsoft n'ont pesé que pour 22,5 % du total.

Las, les vulnérabilités hautement et extrêmement critiques ont représenté 72,5 % du lot, avec des possibilités d'exploitation à distance, depuis l'extérieur, pour 82 % des vulnérabilités. Mais 92,5 % d'entre elles, dans le Top 50, ont fait l'objet d'un correctif disponible le jour de leur divulgation. Reste que, sur l'ensemble de l'éventail applicatif connu sur le parc installé de Flexera, la situation a de quoi préoccuper : 81 % des vulnérabilités font l'objet d'un correctif le jour où elles sont rendues publiques, mais seulement 82 % des vulnérabilités font l'objet d'un patch 30 jours plus tard. D'où la conclusion de Flexera : « si un correctif n'est pas disponible le premier jour, l'éditeur n'accorde pas de priorité à corriger la vulnérabilité »

Mais moins qu'aux éditeurs, il semble que ce soit aux utilisateurs et/ou aux administrateurs qu'il convienne aujourd'hui de jeter la pierre. Car 39 % des Google Chrome déployés ne sont pas à jour de correctifs. Et il en va de même pour 41 % des Firefox, ou encore 27 % des Opera. A noter que seuls

Dans ce guide

6 % des Internet Explorer observés par Flexera chez ses clients ne sont pas à jour de correctifs. La situation des lecteurs PDF est pire : Adobe Reader domine de la tête et des épaules avec une part de marché de 40 % sur le parc considéré. Mais dans 75 % des cas, il n'est pas à jour de correctifs. Foxit Reader, en seconde position, n'est pas mieux traité : il n'est à jour de correctifs que dans 38 % des cas.

Dans ce guide

Bug Bounty : un moyen de démocratiser la recherche de vulnérabilités

Valéry Marchive, Rédacteur en chef adjoint

De plus en plus d'entreprises exposant des services sur Internet sont confrontées à des internautes plus ou moins bienveillants qui relèvent des vulnérabilités dans leurs services et les en informent. Souvent en demandant au passage une rétribution « quand ce n'est plus radical. Parfois, on n'est pas loin du racket », explique Yann Filliat, manager au sein de la practice cybersécurité et confiance numérique Wavestone, en s'appuyant sur l'expérience de ses clients.

De l'autre côté, certains grands acteurs des technologies de l'information, comme Facebook ou Google, ont également ouvert leurs propres programmes de chasse aux bugs, dits *Bug bounty*. Apple les a d'ailleurs récemment rejoints. Entre les deux, des plateformes ont émergé, comme Yogosha en France " qui vient de remporter le Grand Prix de l'Innovation de la Ville de Paris ", pour amener les entreprises à cette pratique de recherche de vulnérabilités où seules celles qui sont effectivement découvertes ouvrent droit à rémunération. Le tout en profitant d'un panel de chercheurs potentiellement très large.

Mais voilà, cela ne va pas sans interrogations. Et Yann Filliat de relever notamment des inquiétudes sur la probité des chercheurs impliqués : « le découvreur d'une vulnérabilité ne sera-t-il pas tenté d'aller la vendre sur le *Dark Web* pour en retirer plus ? » voire, « travaille-t-il depuis un poste suffisamment sûr pour que le fruit de ses recherches ne soit pas détourné ? » Mais aussi : « je vais proposer une récompense, mais sera-t-elle suffisamment élevée pour effectivement attirer les chercheurs ? »

Pour répondre à cela, Wavestone a donc lancé une nouvelle offre. Si elle est dite de Bug Bounty, elle rappelle pour beaucoup les services classiques de recherche de vulnérabilités : seuls les experts du cabinet de conseil interviennent " 40 auditeurs et spécialistes du test d'intrusion, des collaborateurs de Wavestone ", le tout dans le cadre d'une relation étroite entre le client et son fournisseur, en profitant d'une prestation réalisée dans le cadre d'un environnement certifié ISO 27001.

Alors quelle différence par rapport à une prestation de test d'intrusion classique, facturée au forfait sur la base d'un nombre de jours ? Le paiement à la faille, d'une part, mais également une prestation ouverte sur une période déterminée par le client et pouvant s'étendre sur plusieurs mois. De quoi également s'adapter à l'adoption croissante des méthodes agiles, où réaliser des tests de manière ponctuelle s'avère incohérent avec la logique de développement en continu. « Ce qui change aussi pas mal de choses chez

nous », précise Gérôme Billois, directeur de la practice cybersécurité et confiance numérique de Wavestone.

En fait, avec cette nouvelle offre, Wavestone s'adresse à une nouvelle population d'entreprises : « le Bug Bounty fonctionne bien avec les entreprises déjà très matures. Car si l'on y soumet une application ou un service qui n'a pas déjà été audité et développé en intégrant la dimension sécurité, le nombre de vulnérabilités remontée peut être considérable », explique Gérôme Billois. Et le coût aussi, par rapport à une prestation de test d'intrusion facturée au forfait. Dès lors, le Bug Bounty privé proposé ici semble surtout s'adresser aux grands comptes les plus matures, mais également soucieux d'une certaine discrétion.

Un ticket d'entrée, de l'ordre d'un millier d'euros, sera facturé aux clients de l'offre, ne serait-ce, explique Yann Filliat, que pour « pouvoir déclencher les assurances » liées au contrat de prestation, et passer le cap des services achats. Mais une seconde formule sera proposée, avec un prix de base plus élevé “ quelques milliers d'euros “ en contrepartie d'un prix à la faille découverte plus faible. Selon le niveau de criticité, le tarif peut alors évoluer de quelques centaines d'euros à plusieurs milliers d'euros pour les vulnérabilités les plus sérieuses.

Dans ce guide

Fuites de la CIA : entre menace et chance pour la cybersécurité

Valéry Marchive, Rédacteur en chef adjoint

Wikileaks vient de commencer à distiller une vaste quantité de documents plus que sensibles dérobés à la CIA, dite « Vault 7 » : la première série rendue publique ce mardi 7 mars porte sur près de 8800 documents et fichiers venus « d'un réseau isolé de haute sécurité du centre de renseignement cyber de la CIA, à Langley ». Et ce ne serait qu'un début : selon Wikileaks, « la CIA a récemment perdu le contrôle de la majorité de son arsenal de piratage, dont des logiciels malveillants, des virus, des chevaux de Troie, des exploits ˜zero day' militarisés, des systèmes de contrôle à distance de logiciels malveillants, et la documentation associée ».

Un autre géant aux pieds d'argile

Comme la NSA avant elle, l'agence centrale américaine du renseignement apparaît aujourd'hui bien plus vulnérable qu'elle ne le souhaiterait probablement. De rappeler, au passage, le côté illusoire de l'isolation physique des systèmes informatiques en matière de sécurisation. Fin 2015, Lexsi (passé depuis dans le giron d'Orange Business Services) soulignait

d'ailleurs que l'absence d'antivirus actif et à jour sur les postes de travail et serveurs des systèmes industriels en *airgap* avait « engendré, pour 50 % des cas, la présence du ver Conficker sur des postes de supervision industrielle ».

Matthew Ravden, vice-président de Balabit, ne manque de souligner « l'ironie » de la situation pour une agence capable de pirater un très large éventail de systèmes informatiques mais pas « de détecter un accès inhabituel à l'un de ses serveurs ou une exfiltration de données ». Pour lui, c'est bien simples, « les leçons tirées de l'affaire Snowden n'ont pas été suivies, et une meilleure technologie de surveillance et d'analyse et nécessaire pour empêcher de telles fuites de se produire ».

Et l'ironie semble d'autant plus grande que la CIA apparaît disposer, dans son arsenal rendu public, de logiciels malveillants dédiés aux systèmes sans connectivité extérieure, isolés en *airgap*.

Une menace renforcée pour tous

Pour Julian Assange, cette fuite massive de cyberarmes souligne le risque « extrême de prolifération » induit par leur seul développement. Mais il n'est pas seul à penser ainsi. Déjà en mars 2014, Art Coviello, alors président exécutif de RSA, appelait au bannissement de cyberarmes dont « personne ne tire avantage », disait-il alors. Mais déjà en 2010, Eugène Kaspersky ne

disait pas autre chose, soulignant que tout logiciel espion d'état « finira par tomber dans les mains de cybercriminels ». Mais l'inverse est vrai aussi : la CIA ne s'est pas privée de réutiliser, pour son arsenal, des composants malveillants connus.

Reste que le développement de tels logiciels malveillants et mouchards n'est pas une surprise. Les autorités françaises peuvent disposer de leurs propres logiciels espions depuis 2011. Mais comme le relèvent les équipes de ProtonMail dans un billet de blog, le chiffrement de bout-en-bout s'est généralisé depuis les révélations sur les activités de la NSA, poussant les services de renseignement du monde entier à « se concentrer sur la production de logiciels malveillants pour attaquer les appareils des utilisateurs finaux ».

Avant peut-être un effet salvateur

L'étendu de l'arsenal de la CIA dévoilé par Wikileaks a de quoi impressionner. Sans surprise, on y trouve des composants malicieux pour Android, iOS, Windows, macOS, Solaris, FreeBSD, mais aussi les téléviseurs connectés Samsung, ou encore des voitures connectées. Mais les documents dévoilés par Wikileaks font également apparaître des travaux portant sur des matériels réseau de différents équipementiers, sur des distributions Linux CentOS, Debian et Ubuntu, les serveurs Exchange, ou encore les logiciels de protection contre les logiciels malveillants.

Dans ce guide

Dans un premier temps, les vulnérabilités divulguées et non déjà corrigées sont susceptibles de renforcer la menace sur l'ensemble des utilisateurs de matériels et de logiciels concernés. Mais les industriels sont déjà sur le qui-vive. Apple assure ainsi que nombre des vulnérabilités décrites dans les documents dévoilées par Wikileaks ont déjà été corrigées, au moins dans sa dernière version d'iOS, tandis que Microsoft et Samsung ont indiqué s'être mis au travail.

Mais ce n'est pas la première fois qu'une trousse à outils de piratage se retrouve dans la nature. Les italiens de Hacking Team en avaient fait l'expérience en juillet 2015, dénonçant un piratage générant une « situation extrêmement dangereuse ». Reste que les éditeurs concernés par les vulnérabilités exploitées par Hacking Team n'ont pas manqué de réagir. Et rapidement, les correctifs ont été distribués, contribuant à améliorer, dans son ensemble, la sécurité informatique. A charge à chacun, ensuite, de les installer. A condition de pouvoir y accéder comme cela peut être hélas souvent problématique dans l'univers Android.

IIS 6.0 : une vulnérabilité corrigée par micro-correctif tiers

Valéry Marchive, Rédacteur en chef adjoint

C'est fin 2015, après deux ans de développement en secret, qu'Acros Security a présenté 0patch, une solution de déploiement de micro-rustines accessible en bêta gratuite depuis le mois de juillet 2016. Et le serveur Web de Windows, IIS, vient de lui offrir une occasion de faire sa promotion.

De fait, depuis fin mars, GitHub héberge le démonstrateur, écrit en Python, de l'exploitation d'une faille affectant IIS 6.0 sur Windows Server 2003 R2. Celle-ci permet de forcer l'exécution de code arbitraire à distance, et serait exploitée depuis l'été dernier.

Las, comme le souligne l'équipe de 0patch, le support étendu de ce système d'exploitation serveur est arrivé à son terme il y a bientôt deux ans. Sauf décision exceptionnelle, il apparaît peu probable que Microsoft décide de proposer un correctif pour cette vulnérabilité.

Mais voilà, il faut encore compter, selon le moteur de recherche spécialisé Shodan, avec plus de 600 000 serveurs IIS 6.0 accessibles publiquement sur Internet. Mais tous ne sont pas concernés : il faut qu'ils s'exécutent sur

Windows Server 2003 et que la fonctionnalité WebDAV soit activée. Cela concernerait « environ 10 % » d'entre eux.

L'équipe 0patch s'est donc penchée sur l'analyse de la vulnérabilité pour identifier le processus affecté, mais également les éléments de code - compilé - responsables de vulnérabilité. Et de proposer un « micro-correctif ». L'occasion de montrer une nouvelle fois comment fonctionne l'outil et à quel point il s'avère léger.

Ce n'est toutefois pas la première que l'équipe 0patch a l'occasion de présenter le fonctionnement de son agent. L'an passé, elle a proposé des micro-correctifs pour Adobe Reader, Foxit Reader, l'extension de navigateur Web de WebEx, mais aussi Windows et IE 11 - en l'absence de lot de correctifs de Microsoft en février dernier - ¦ jusqu'à l'agent 0patch lui-même. Ce dernier est d'ailleurs en cours de développement pour Linux.

De son côté, Trend Micro propose des règles permettant, avec ses produits, de bloquer les attaques tentant d'exploitation la vulnérabilité d'IIS 6.0 avec WebDAV. C'est également le cas de SonicWall, de F5 Networks, ou encore de Qualys pour son pare-feu applicatif, entre autres. Une règle pour Snort a également été soumise.

Solutions du marché

Aperçu du système de gestion de vulnérabilités Saint 8 Security Suite

Ed Tittel, contributeur LeMagIT

Depuis que Saint a lancé son premier scanner de vulnérabilités en 1998, il a considérablement étendu son éventail fonctionnel. L'éditeur a également ajouté un outil de test d'intrusion, le SaintExploit, et un service Cloud.

La Saint 8 Security Suite est un produit logiciel de gestion des vulnérabilités vendu sous la forme d'une appliance virtuelle. Saint commercialise également une version portable allégée ainsi q'une appliance physique préconfigurée à installer en rack : les SaintBox. L'appliance virtuelle est toutefois l'option de déploiement privilégiée des clients de Saint. SaintCloud est un service en ligne assurant l'analyse de cibles externes. Mais il est également capable d'administrer les instances de la suite déployées en local.

Dans ce guide

Fonctionnalités

Comme d'autres produits comparables, la Saint Security Suite analyse systèmes d'exploitation, systèmes de gestion de bases de données et applications Web pour détecter d'éventuelles vulnérabilités. Elle vise aussi bien les cibles internes qu'externes et peut être configurée avec plusieurs sondes distinctes selon une architecture distribuée.

La suite se configure et d'administre via une interface Web, et à l'aide d'assistants. Le déploiement en est ainsi simplifié et accéléré. Les bases de données de vulnérabilités sont mises à jour régulièrement.

La Saint Security Suite et le service SaintCloud intègrent recherches de vulnérabilités et test d'intrusion, mais également analyse de configuration. Le tout assorti d'un système de gestion de tickets de niveau entreprise.

Les résultats d'analyse peuvent être exporter vers le système de gestion des informations et des événements de sécurité QRadar d'IBM. Saint est également compatible avec Cisco FireSight Management Center " hérité de Sourcefire " pour permettre analyse et corrélation.

Dans ce guide

Comme il fonctionne

L'interface Web d'administration permet de gérer une ou plusieurs sondes déployées dans l'environnement. L'interface est facile à utiliser et largement personnalisable. Elle permet d'identifier rapidement les 10 vulnérabilités les sévères observées, les dix hôtes les plus vulnérables, mais également de dégager des tendances en matière de gestion des vulnérabilités ainsi que de produire des analyses. La suite de Saint permet de hiérarchiser les vulnérabilités avec flexibilité : l'utilisateur n'est pas confiné dans les classiques options « élevé-moyen-bas ».

Ainsi, un utilisateur peut associer des vulnérabilités à des codes de sévérité spécifiques à son domaine d'activité, comme ceux définis par le standard PCI DSS, ou les notes numériques du CVSS. L'utilisateur peut basculer entre plusieurs tableaux de bord et sélectionner des jeux de données différents pour vérifier sa conformité avec différentes réglementations. Des rapports standards sont fournis, mais il est possible de créer des rapports personnalisés.

Toutefois, les rapports et les évaluations de Saint se conforment au protocole 1.2 d'automatisation des contenus de sécurité du NIST américain. Ses outils sont validés comme scanner de configuration authentifié et pour les contenus CVE.

Prix, licences et support

Une licence pour petit réseau (classe C) est facturée moins de 5 000 $ pour une appliance virtuelle. Les appliances physiques sont proposées à partir de 995 $ pour la mini, et 2 600 $ pour la version rack. Un numéro de licence valide est requis pour la configuration de l'appliance.

Le support client est inclus gratuitement dans le cadre de la licence pour la Saint 8 Security Suite, de même que la maintenance des appliances physiques. Un support de base, avec un délai de réponse de 4h, est accessible via le portail client en ligne durant les heures ouvrées. Un support avancé 24/7 est proposé moyennant surcoût.

Le portail client de Saint fournit une documentation complète, ainsi que des vidéos pédagogiques. Il est également possible de suivre des formations de deux à quatre heures en ligne, recouvrant installation et configuration. Celles-ci peuvent être personnalisées selon les besoins de l'utilisateur.

A noter qu'il est possible de demander une démonstration en ligne ou une licence de test gratuite pour essayer les produits Saint dans son propre environnement.

Dans ce guide

Aperçu du scanner de vulnérabilités Tenable Nessus

Ed Tittel, contributeur LeMagIT

Tenable se spécialise dans la surveillance et l'évaluation en continue des vulnérabilités. Sa gamme de produits inclut Nessus Cloud, une offre en mode SaaS ; Nessus Manager, une appliance locale, physique ou virtuelle, de gestion des vulnérabilités ; Nessus Professionnal, un logiciel à exécuter sur un poste client ; et Nessus Home, une version gratuite destinée au grand public.

Caractéristiques

La gamme de produits Nessus est l'une des complètes dans le domaine de la gestion des vulnérabilités. Elle est fortement représentée sur le marché depuis des années. Outre l'infrastructure pour la recherche et l'analyse automatisées de vulnérabilités, Nessus couvre les applications Web, les environnements Cloud et les terminaux mobiles. La gamme de scanners de vulnérabilités Nessus assure aussi détection de logiciels malveillants, audit de systèmes industriels Scada et embarqués, ainsi qu'audit de configuration et vérification de conformité.

Le moteur d'analyse Nessus utilise des plug-ins pour détecter de nouvelles vulnérabilités. Tenable pousse des extensions contenant les plus récentes informations sur les systèmes de ses clients moins de 24 heures après qu'une vulnérabilité a été rendue publique. Et comme les vulnérabilités apparaissent quasiment tous les jours, les clients reçoivent des flux quotidiens pour rester à jour.

Les outils Nessus n'intègrent pas de capacités de test d'intrusion, mais les administrateurs peuvent intégrer les résultats avec des outils de *pentest* populaires tels que Metasploit, Core Impact et Immunity Canvas, afin d'en savoir plus sur le risque réel d'exploitation.

Administration

Les administrateurs de Nessus Cloud et Nessus Manager peuvent déployer des agents pour les points de terminaison. Ceux-ci permettent des analyses hors ligne ; les résultats sont collectés lorsque l'appareil visé se reconnecte au réseau. Les agents permettent également de détecter la présence éventuelle de logiciels malveillants.

Nessus Cloud et Nessus Manager s'intègrent facilement avec CyberArk pour la gestion des accès, et avec les outils de gestion de correctifs tels que ceux de Dell, IBM, Microsoft et Red Hat, ou encore les systèmes de gestion des terminaux mobiles (MDM) signés AirWatch, MobileIron, et Microsoft,

entre autres. Tous les produits de recherche de vulnérabilités Nessus s'appuient sur une API REST.

L'interface de la console et du tableau de bord sont conçus pour être faciles à utiliser, permettant aux utilisateurs de créer des règles en l'espace de quelques clics. Les administrateurs peuvent exécuter tout un éventail de rapports pré-configurés ou les personnalisés pour leur environnement, et configurer l'outil pour l'envoi de notifications ciblées par e-mail.

Prix, licences et support

Les produits Nessus sont proposés avec une souscription à l'année, qu'il est possible d'obtenir en direct ou via un partenaire commercial de Tennable. Nessus Cloud et Nessus Manager sont commercialisés suivant le nombre d'hôtes ou d'agents, au même prix chacun : 128 hôtes ou agents coûte 2920 $, voire 4745 $ pour le double. Au-delà, il convient de consulter un représentant commercial de Tennable pour obtenir un prix sur-mesure. Chaque souscription couvre un an de mises à jour logicielles et des renseignements sur les vulnérabilités.

Le logiciel Nessus Professional est également disponible en souscription annuelle, au prix de 2190 $. Ce qui inclut les mises à jour quotidiennes pour une seule sonde Nessus, des fichiers téléchargeables d'audit et de conformité, les mises à jour de logiciels, et une appliance virtuelle.

Dans ce guide

Le support est disponible 24h/24 et 7j/7, par téléphone, e-mail ou dialogue en ligne. Le portail de support de Tenable intègre par ailleurs une base de connaissance et la documentation des produits, ainsi qu'un outil de gestion de tickets de demande de support.

Tenable lance une plateforme d'administration des vulnérabilités en mode Cloud

Rob Wright, Site Editor

Tenable Network Security a profité de la conférence RSA, le mois dernier, pour dévoiler une nouvelle plateforme de gestion des vulnérabilités proposée en mode cloud. Baptisée Tenable.io, cette plateforme propose API et kit de développement logiciel permettant d'exporter et d'importer des données de vulnérabilités. La plateforme inclut le balayage des applications Web et des fonctions de surveillance de la sécurité des conteneurs. Elle intègre un algorithme de suivi des actifs qui permet de suivre non seulement les équipements physiques, mais aussi les machines virtuelles et les instances cloud.

« Nous cherchons à être le hub de la sécurité de l'information pour l'industrie », explique Cris Thomas, responsa ble de la stratégie de sécurité chez Tenable : « il était important pour nous de construire un écosystème qui fonctionne de manière cohérente pour tout le monde ».

Cris Thomas indique que Tenable.io s'appuie sur le portefeuille produits existant de l'éditeur, dont les sondes Nessus de recherche de vulnérabilités

et d'analyse de configuration. Toutefois, la plateforme de gestion des vulnérabilités a été en grande partie construite à partir de rien, comme une offre cloud totalement nouvelle. Par exemple, Tenable.io propose un contrat de niveau de service avec une garantie de disponibilité comparable aux SLA d'autres fournisseurs de services cloud importants.

La plateforme peut s'intégrer aux workflows ITSM de plusieurs autres fournisseurs de solutions de sécurité et fournisseurs de technologies pour systèmes d'information, notamment Amazon Web Services, CyberArk et ForeScout. Le programme Tenable Technology Integration Partner permet à d'autres sociétés de collaborer avec Tenable et de construire des intégrations avec la plateforme tenable.io.

« Nous l'avons conçue pour qu'elle soit facile à utiliser », souligne Cris Thomas : « vous pouvez exporter les données et les injecter dans d'autres produits, si vous le souhaitez. Nous préférons évidemment que vous l'utilisiez avec les produits Tenable, mais nous supportons à peu près n'importe quel produit ».

Cris Thomas admet que la gestion des vulnérabilités n'a pas été le domaine le plus actif de la sécurité au cours de ces dernières années et qu'elle est souvent négligée par de nombreuses entreprises. Mais il estime qu'une meilleure gestion des vulnérabilités est cruciale pour réduire la surface d'attaque. Selon lui, plus le nombre d'entreprises participant à tenable.io sera élevé, plus la plateforme pourra générer des données de vulnérabilités

précieuses pour les participants. « L'un des problèmes qui rend ce genre de choses difficile, c'est d'atteindre une masse critique. Mais nous avons près de 2 500 clients qui utilisent déjà des produits qui constituent la base de tenable.io ».

Dans ce guide

Barracuda Networks veut automatiser la correction des vulnérabilités Web

Valéry Marchive, Rédacteur en chef adjoint

Barracuda Networks vient d'annoncer le lancement d'un service destiné aux utilisateurs de ses pare-feu applicatifs (WAF) et visant à fournir une actualisation régulière des règles de protection en fonction des vulnérabilités éventuelles détectées.

Baptisé Vulnerability Remediation Service (VRS), ce service permet de lancer des opérations de recherche de vulnérabilités, à la demande ou de manière planifiée, sur les applications Web censées être protégées par ses WAF. Dans un communiqué, Barracuda Networks explique vouloir, avec ce service Cloud, « rendre plus somple, pour les organisations de toutes tailles, le déploiement de règles de sécurité complètes pour applications Web avec un minimum de surcharge administrative ». Et d'adresser en particulier les besoins des approches DevOps.

Début décembre, l'équipementier avait fait un premier pas dans cette direction, en annonçant un partenariat avec High-Tech Bridge pour proposer sa technologie ImmuniWeb aux utilisateurs de ses WAF. La plateforme ImmuniWeb s'appuie sur l'apprentissage automatique pour améliorer la

détection des vulnérabilités sur les applications Web. Les données des rapports d'analyse peuvent être exportées au format XML pour créer de nouvelles règles de WAF.

Avec cette approche, Barracuda apparaît surtout combler son retard face des Imperva et F5 qui ont déjà noué des partenariats avec des spécialistes de la recherche de vulnérabilités dans les applications Web tels que WhiteHat et Qualys, notamment. Ce dernier propose d'ailleurs depuis le printemps 2015 des capacités de *patching* virtuel en intégrant les résultats de son service de recherche de vulnérabilités dans les applications Web à son propre pare-feu applicatif Web.

Dans ce guide

DenyAll fait évoluer son offre en pensant aux DevOps

Valéry Marchive, Rédacteur en chef adjoint

Bien que l'on l'imagine mal effectuée au pied lever, l'annonce sonne presque comme une réponse à celle, toute récente, du rachat de Veracode par CA Technologies. De fait, DenyAll s'adresse également aux équipes DevOps avec la nouvelle version 6.3 de son pare-feu pour applications Web (WAF) et ses modules associés, Vulnerability Manager 6.5 et son service Cloud Protector.

Dans un communiqué, le Français relève ainsi que « l'intégration et la livraison en continu deviennent une pratique courante pour les entreprises qui investissent dans la transformation numérique ». Pour les aider à traiter en continu la sécurisation de leurs applications Web, DenyAll a ajouté plusieurs fonctions à ses outils.

Et cela commence par un mécanisme de clonage des configurations WAF : « la configuration des tunnels est synchronisée automatiquement lorsqu'un équilibreur de charge est positionné devant le WAF. L'API d'orchestration permet d'automatiser d'autres tâches répétitives comme celle-ci ». A cela s'ajoute une fonction d'apprentissage automatique des applications Web et

des API REST exposées, à partir des logs de développement ou de pré-production : de quoi « gagner du temps en reconnaissant automatiquement chemins, méthodes et paramètres ». En outre, la version 6.3 du WAF de DenyAll doit aider à réduire les taux de faux positifs.

Vulnerability Manager 6.5 peut lui interpréter les fichiers Swagger produits par les développeurs ou par le pare-feu applicatif pour rechercher automatiquement les vulnérabilités, modifier le fichier de description initial, et le renvoyer au WAF afin d'assurer le patching virtuel.

DenyAll WAF 6.3 propose aussi un tableau de bord personnalisable d'analyse du trafic applicatif. Il est basé sur Elastic Search et Kibana ; une approche somme toute logique, la pile ELK ne manquant pas d'adeptes en matière de supervision de la sécurité. Cloud Protector propose également un tableau de bord personnalisable basé sur ELK, mais il est enrichit de fonctions de réseau de distribution de contenus (CDN).

Le groupe allemand Rohde & Schwarz a récemment annoncé le rachat de DenyAll, élargissant ainsi une offre combinant jusque là UTM, protection du terminal, sécurisation des accès Web, et chiffrement du stockage Cloud.

Dans ce guide

CA Technologies s'offre un spécialiste de la sécurité applicative

Valéry Marchive, Rédacteur en chef adjoint

CA Technologies vient d'annoncer le rachat de Veracode pour 614 M$ en numéraire. Dans un communiqué, l'éditeur explique que cette opération doit lui permettre de se renforcer sur le marché des DevOps en intégrant la sécurité. Les fameux DevSecOps. Et cela même alors que l'intégration de la sécurité dans les approches DevOps apparaît toujours difficile, comme le relevait encore Gartner à l'automne dernier. Avec Veracode, CA entend faire le lien ses offres de sécurité et de DevOps tout en renforçant ses activités SaaS.

Veracode propose une plateforme Cloud d'analyse de sécurité des applications, avec analyse statique de code compilé (Java, C/C#, Objective-C, notamment), analyse de composants logiciels, analyse dynamique, mais également découverte automatique des applications Web exposées publiquement et réputation des applications mobiles. Sa plateforme peut s'intégrer par API dans les chaînes de développement agile et de déploiement continu, ainsi qu'avec les pare-feu applicatifs pour accélérer la remédiation des vulnérabilités éventuellement découvertes.

Pour son offre, Veracode a récemment été classé par les leaders du test de sécurité applicative par Gartner, aux côtés d'IBM et de HPE. Selon le cabinet, ses clients saluent tout particulièrement la facilité d'utilisation de la plateforme.

Veracode a été fondé en 2006 par plusieurs experts en sécurité, dont Chris Wysopal et Christien Rioux, deux anciens de Symantec passés dans les années 90 par les L0pht Heavy Industries, ou encore Matthew Moynahan, désormais Pdg de Forcepoint. Depuis sa création, Veracode a levé un peu plus de 114 M$ en six tours de table. A l'automne dernier, certains observateurs anticipaient une entrée en bourse d'ici à 18 mois.

Dans ce guide

Conseils et Projets IT

Avec iKare, le CHU d'Amiens se dote d'une visibilité accrue sur les vulnérabilités

Valéry Marchive, Rédacteur en chef adjoint

Le centre hospitalier universitaire d'Amiens est, comme le reste du secteur médical, soumis à une exigeante réglementation en matière de protection des données personnelles. Julien Rousselle, qui en est le RSSI depuis 2004, soulignait, à l'occasion d'un séminaire Web à l'automne dernier, que celle-ci exige notamment la conduite régulière d'audits de vulnérabilité.

Mais voilà, s'ils répondent aux impératifs réglementaires, les audits réalisés une ou deux fois par an ne permettent pas de disposer « d'une visibilité au fil de l'eau ». Et c'est bien ce que recherchaient Julien Rousselle et ses équipes avec, en prime, un gain d'autonomie dans la réalisation des audits et dans le choix de leur périmètre. Pour le RSSI, la « visibilité en temps de tout ce qui peut être sujet à vulnérabilités » apparaît essentielle : souvent, les attaques réussies le sont aussi en raison de « vulnérabilités laissées sur les machines », non corrigées.

Une infrastructure auditée de l'intérieure comme de l'extérieur

La première force d'iKare s'est manifestée à ce stade : l'outil peut être téléchargé et essayé gratuitement sur 32 adresses IP. Si cela peut sembler peu, c'est toutefois suffisant pour mettre en place une première maquette. De quoi là apprécier une interface à la prise en main intuitive, selon le RSSI du CHU d'Amiens.

Après l'achat d'une licence, les équipes de Julien Rousselle ont donc pu mettre en place l'audit des serveurs du CHU " 400 machines, sur leurs adresses IP internes, mais également sur celles, publiques, exposées à l'extérieur. « La priorité va aux serveurs parce que c'est là que se trouvent les données médicales, les données sensibles ».

Mais ses efforts d'audit ne s'arrêtent pas là, parce « de plus en plus tout devient connecté en IP ». Et s'il ne s'agit d'auditer tout l'environnement, les équipes de la RSSI peuvent utiliser des échantillons d'un même matériel, l'auditer régulièrement, et, en cas en de vulnérabilité, entrer en contact avec son fournisseur.

Les couleurs d'un sapin de Noël

Si pour les démonstrations, tous les voyants peuvent avoir tendance à clignoter au vert, ce n'est pas le cas dans un environnement de production. Et comme le relève Julien Rousselle, « dès que l'on commence à auditer, on voit surtout tout ce qui ne vas pas ». Avec à la clé une question : par où commencer ? Et c'est probablement là que commence la partie la plus difficile du travail.

Certes, le niveau de criticité des vulnérabilités ou des équipements concernés peuvent aider à définir les priorités. Mais le plan d'action doit aussi être établi avec les référents métiers, applicatifs, serveurs ou encore équipements réseau, souligne le RSSI, insistant sur l'importance de l'organisation.

Et si des correctifs sont disponibles, encore faut-il commencer par les déployer dans un environnement de test, afin de les qualifier avant de pouvoir envisager une mise en production.

Julien Rousselle ne cache pas sa satisfaction vis-à-vis d'iKare : son achat a été immédiatement rentabilisé, grâce à un coût inférieur à celui d'un audit externe, et il dispose désormais d'une visibilité étendue sur son environnement.

Mais pas question, donc, d'y voir une solution *push-button* (comme d'aucuns diraient) miraculeuse : l'outil permet au RSSI de disposer de la cartographie nécessaire à la définition des priorités dans son plan d'action. Mais la distribution des correctifs n'a rien d'une étape triviale.

Dans ce guide

Comment composer avec les logiciels les plus vulnérables

Nick Lewis, contributeur LeMagIT

Le principe de Pareto est fréquemment cité. Selon lui, dans la plupart des situations, environ 80 % du bénéfice provient de 20 % de l'effort consenti. Cette règle peut également s'appliquer à certains aspects de la sécurité de l'information. Selon un récent rapport de Digital Shadows portant sur l'exploitation des vulnérabilités, trois logiciels - Adobe Flash Player, Java et Internet Explorer - représentent 62 des 76 vulnérabilités ciblées par les kits d'exploitation. Soit près de 82 %. La communauté de la sécurité commence à apprendre qu'utiliser des données peut être un moyen efficace de sécuriser les entreprises et de donner la priorité à l'hygiène de base en matière de sécurité de l'information. Le rapport de Digital Shadows montre l'intérêt qu'il y a à utiliser des données pour identifier les logiciels vulnérables.

Enseignements du rapport Digital Shadows

L'utilisation des données pour orienter les décisions de sécurité de l'information est cruciale. Les entreprises devraient utiliser des informations

tirées de recherches et de publications telles que le annuel de Verizon sur les incidents de sécurité et le rapport de Digital Shadows.

Ce dernier s'est penché sur 22 kits d'exploitation et s'est concentré sur les cinq kits les plus utilisés, corrélant les vulnérabilités exploitées par chacun pour déterminer les plus courantes. Il n'est toutefois pas certain que les données du rapport soient un échantillon représentatif de tous les systèmes.

Mais même avec ces réserves, les résultats donnent un aperçu de la manière de hiérarchiser son programme de sécurité de l'information. Une approche similaire peut être appliquée aux données d'incident recueillies dans son infrastructure pour déterminer où le système d'information est le plus fréquemment attaqué et concentrer là son attention.

Comment gérer ces vulnérabilités

L'option la plus évidente pour les entreprises consiste à désinstaller les logiciels les plus vulnérables afin de réduire la surface d'attaque. Toute entreprise qui utilise encore le logiciel non sécurisé doit avoir une bonne raison de le faire. Si les utilisateurs ont besoin d'une certaine fonctionnalité, comme la possibilité de lire des fichiers PDF, certains lecteurs PDF présentent peut-être moins de risques que d'autres. Tout logiciel alternatif devrait être évalué de manière critique pour déterminer s'il peut être utilisé de manière sûre afin de minimiser le risque.

Dans ce guide

L'étape suivante consiste à s'assurer que l'on dispose de systèmes de gestion des vulnérabilités et des correctifs. Sans eux, il sera difficile d'appliquer de nouveaux contrôles ou de modifier la façon dont les résultats sont hiérarchisés. Un scanner de vulnérabilités ou un système de gestion des correctifs peut effectuer une analyse authentifiée d'un hôte de l'infrastructure, y compris les systèmes virtualisés et mobiles, pour identifier ceux qui exécutent des logiciels vulnérables. La surveillance du trafic réseau peut également aider à cela.

Une fois qu'un système a été identifié comme nécessitant un correctif, celui-ci doit être testé et poussé vers le système cible. Et la version non sécurisée du logiciel doit être supprimée. Si un correctif ou une mise à jour sort pour Adobe Flash Player, Java d'Oracle ou Internet Explorer, il devrait être appliqué au plus tôt, en priorité devant d'autres logiciels, afin de réduire le risque.

Si une entreprise a besoin d'utiliser une version non sécurisée du logiciel, il convient de faire pression sur son éditeur pour obtenir un correctif. Il peut aussi être envisagé d'exécuter ce logiciel vulnérable dans un environnement virtualisé ou un bac à sable. Cela peut ajouter un niveau de complexité, mais cette approche permet de confiner un éventuel attaquant qui réussirait à tirer profit des vulnérabilités. Les entreprises peuvent également veiller à ce que leur surface d'attaque soit réduite au minimum en utilisant des systèmes configurés de manière sécurisée.

Des outils tels que Qualys BrowserCheck permettent de voir quelles extensions non sûres de navigateurs Web sont installées. Personal Software Inspector de Flexera permet quant à lui d'identifier les mises à jour nécessaires et d'automatiser leur installation.

Conclusion

Malheureusement, en matière de sécurité informatique, il n'est pas possible de choisir de ne bloquer que 80 % des attaques au prix de 20 % de l'effort. Mais il est possible d'utiliser des ressources limitées de manière plus efficace pour mieux protéger son entreprise. En veillant à ce se concentrer sur les risques les plus élevés identifiés, des protections efficaces peuvent être mises en Å“uvre à grande échelle pour limiter le risque réel au niveau des hôtes de l'infrastructure.

Dans ce guide

Comment gérer les correctifs de sécurité avec les administrateurs systèmes ?

Mike O. Villegas, contributeur LeMagIT

L'un des points les plus préoccupants de la posture de sécurité des entreprises touche à gestion des vulnérabilités. C'est du moins l'un des enseignements de l'étude annuelle de Symantec sur les menaces de sécurité. En particulier, selon celle-ci, depuis trois ans, plus de 75 % des sites Web analysés par l'éditeur sont affectés par des vulnérabilités non corrigées. Que devraient faire les RSSI pour accorder une importance plus grande à la gestion des correctifs ? Peuvent-ils travailler avec les administrateurs de systèmes pour traiter le problème, et si oui comment ?

L'application des correctifs est une mesure préventive qui protège les systèmes contre les accès non autorisés, les logiciels malveillants, ou encore les erreurs susceptibles d'affecter les processus normaux. Les produits tels que Microsoft Office, les antivirus, les équipements réseau, les serveurs, les grands systèmes ou les postes de travail ont tous besoin de correctifs de sécurité, de rustines temporaires ou de mises à jour. Ces dernières sont différentes des correctifs, mais il reste important de les évoquer parce qu'elles n'apportent pas que des améliorations fonctionnelles, mais également éliminent erreurs et potentielles vulnérabilités. La gestion

des correctifs de sécurité peut être automatisée, mais beaucoup d'organisations choisissent d'appliquer les correctifs de manière sélective en raison de contraintes de temps ou de disponibilité des systèmes. Là, il s'agit généralement d'appliquer les correctifs manuellement au cours de périodes d'indisponibilité planifiées.

Certaines organisations font preuve de diligence dans l'application des correctifs, mais d'autres attendent parfois plusieurs mois. La plupart des organisations fournissent toutefois tous les efforts nécessaires pour déployer les correctifs dans les 30 jours qui suivent leur diffusion. Mais il reste néanmoins un nombre significatif d'entreprises qui ne considèrent pas l'application des correctifs comme une priorité avant que les vulnérabilités correspondantes ne soient effectivement exploitées et ne conduisent à des indisponibilités ou à des brèches. Ou alors jusqu'à le déploiement soit nécessaire pour maintenir la conformité avec des standards tels que PCI DSS. Les scanners de vulnérabilités sont des outils utiles pour identifier les correctifs les plus critiques et en améliorer la gestion.

L'application des correctifs de sécurité peut et devrait être assurée par les administrateurs système. Mais les équipes de sécurité peuvent être chargées de la veille en matière de correctifs critiques. Elles peuvent également demander à ce que les correctifs soient testés et appliqués dans le délai standard de 30 jours. En l'absence d'automatisation de l'application

des correctifs, leur déploiement devrait suivre les procédures de contrôle du changement en place.

Pour renforcer leurs processus de gestion des correctifs, les RSSI peuvent engager plusieurs initiatives. Et cela commence par la définition d'une politique de gestion des vulnérabilités et des correctifs précisant les rôles et responsabilités de chacun, les sources d'identification des vulnérabilités, et celles d'identification des correctifs nécessaires. Un comité de gestion des correctifs peut également être installé, avec les équipes d'administration et celles chargées de l'identification des vulnérabilités, pour assurer que les correctifs requis ou les actions de remédiation nécessaires sont bien hiérarchisés et appliqués.

Il est également conseillé de mettre à jour les outils d'administration qui assurent l'installation automatique des correctifs de sécurité sur les postes de travail, portables, et équipements des utilisateurs. Par ailleurs, souscrire à un service d'alerte fournira des informations sur les nouvelles vulnérabilités et les correctifs associés.

Enfin, si l'entreprise est soumise à PCI DSS, il convient de s'assurer de sa conformité avec la règle 6.2 du standard qui requiert que tous les composants et logiciels des systèmes profitent des correctifs de sécurité dans un délai d'un mois après leur diffusion.

Dans ce guide

La gestion des correctifs de sécurité peut être fastidieuse et donner l'impression de n'apporter que peu de bénéfices. Mais rester à jour des correctifs, c'est se protéger à titre préventif des principales vulnérabilités. Et si cela s'avère négligé, cela peut conduire à de coûteuses interruptions de service à l'issue d'une brèche ou d'une indisponibilité.

Dans ce guide

Patching automatique : ce que les entreprises devraient considérer

Kevin Beaver, contributeur LeMagIT

L'édition de 2016 de la conférence Black Hat, qui se déroulait la semaine dernière à Las Vegas, a été l'occasion d'une première : la finale du défi Cyber Grand Challenge (CGC), organisé par la Darpa, l'agence américaine chargée des projets de défense avancés, et opposant des hackers totalement cybernétiques, sans la moindre intervention humaine.

Le CGC était en préparation depuis plus de deux ans. Il visait à « tester les capacités d'une nouvelle génération de systèmes de cyberdéfense complètement automatisés », combinant « vitesse et échelle d'automatisation avec des capacités de raisonnement dépassant celles des experts humains ».

Il s'agit d'une évolution technologique fascinante qui, compte tenu des complexités associées aux environnements réseau actuels, pourrait aider à améliorer la sécurité informatique des entreprises de nombreuses manières. Mais est-ce que cela en valoir la peine ? Quels sont les effets secondaires et les risques associés à la correction automatique de vulnérabilités ? Si la technologie n'est pas encore accessible à grande échelle, elle mérite

Dans ce guide

l'attention des entreprises alors que leurs programmes de sécurité de l'information et les technologies associées avancent.

De nombreuses organisations pourraient déjà utiliser une forme de correction automatisée des vulnérabilités. Les failles logicielles seraient reconnues et les correctifs déployés pour assurer la résilience des systèmes face aux attaques, avec une intervention humaine minimale. Sur le papier, c'est très séduisant et l'on imagine directions et auditeurs très sensibles à la promesse. Mais le processus d'application de correctif n'est pas aussi clair et net. C'est même un processus complexe qui implique beaucoup de systèmes et d'acteurs, devant travailler de concert pour s'assurer d'un déploiement effectif des correctifs, de l'amélioration de la sécurité, et de la stabilité de l'environnement. Et cette dernière est sans aucun doute l'aspect le plus important pour la majorité des professionnels impliqués. Et comme tout le monde a eu l'occasion de l'apprendre, un mauvais correctif suffit à faire tomber un système autrement stable. Une approche qui finit par créer une situation dont beaucoup diraient qu'elle est pire pour l'entreprise que toute vulnérabilité censée être corrigée¦

Des équipes de sécurité surchargées cherchent sans le moindre doute à améliorer leur posture de sécurité, comme avec un système de correction de vulnérabilités automatisé. Mais certains points doivent être pris en compte : comment déterminer ce qui doit être corrigé en premier ? Comment s'assurer que les systèmes critiques ne soient pas *patchés* si le

risque est trop grand, tout en restant sécurisés ? Comment impliquer certains éditeurs ne supportant pas le *patching* afin d'éviter de faire reposer tout le risque sur l'entreprise ? Quels sont les plans de replis en cas d'incident de production suite à l'application du correctif ?

Les avancées en matière de qualité logicielle des systèmes d'exploitation et des applications modernes permettent de déployer les correctifs de manière semi-automatisée, au moins au niveau des postes de travail. Après tout, c'est là qu'il convient de concentrer une grande partie de ses efforts, en particulier avec des logiciels tiers tels que Java et Flash. Mais quid des serveurs, applications, bases de données et systèmes d'infrastructure réseau susceptibles de rester vulnérables à une attaque ? Comment les mises à jour sont-elles appliquées à ces systèmes ?

Et puis ces systèmes de correction de vulnérabilité automatisés en valent-ils le coût ? Peut-être que les avantages surpassent effectivement les inconvénients. Mais le CGC de la Darpa n'était qu'une expérimentation spécialisée, s'appuyant sur des logiciels spécialisés qui n'avaient pas été analysés précédemment. Difficile de savoir donc comment ces systèmes de correction automatique de vulnérabilité se comporteraient avec des logiciels commerciaux et des applications patrimoniales complexes.

Chaque situation est différente. La réalité est que, compte tenu des ressources limitées des équipes et du risque d'erreur humaine, la sécurité a besoin d'être automatisée là où elle peut l'être. Il est donc aujourd'hui temps

Dans ce guide

de se pencher sur la manière dont le processus de correction de vulnérabilités pourrait ou devrait être automatisé à l'avenir.

Dans ce guide

Accéder à plus de contenu exclusif PRO+

Vous avez accès à cet e-guide en tant que membre via notre offre PRO+ : une collection de publications gratuites et offres spéciales rassemblées pour vous par nos partenaires et sur tout notre réseau de sites internet.

L'offre PRO+ est gratuite et réservée aux membres du réseau de sites internet TechTarget.

Profitez de tous les avantages liés à votre abonnement sur: http://www.lemagit.fr/eproducts

Images; stock.adobe.com