Hygiène informatique en matière de sécurité : le premier niveau de défense

Version 1.3
Publication : mai 2021

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Note de l'auteur

Le contenu de ce rapport a été élaboré sans aucune forme de partenariat commercial. Il s'inspire du contenu publié sur le blog de Securosis, mais il a fait l'objet d'améliorations, de révisions et de modifications par des professionnels.

Je remercie tout particulièrement Chris Pepper pour sa relecture et son expertise.

Droits d'auteur

Hygiène informatique en matière de sécurité

Table des matières

En quoi l’hygiène informatique en matière de sécurité est-elle essentielle à la protection ?

En tant que professionnels de la sécurité, nous constatons avec dépit que les mêmes problèmes et erreurs se répètent depuis des dizaines d'années, un peu comme si nous nous trouvions dans le film « Un jour sans fin ». Au quotidien, nous détectons et réparons les erreurs commises par des utilisateurs ou des administrateurs, nous gérons la dernière attaque en date et nous remplissons les rapports de conformité. Il ne s'écoule pas un jour sans qu'il faille tout recommencer. Toutefois, il faut reconnaître que la lutte contre les pirates informatiques est un combat asymétrique.
Il suffit aux pirates de bien s'y prendre une seule fois pour parvenir à pénétrer dans votre écosystème. Les défenseurs doivent quant à eux être irréprochables à chaque instant. Une seule erreur de leur part peut s'avérer fatale et permettre aux pirates de s'engouffrer dans la brèche. C'est injuste, mais c'est ainsi.

Le conseil le plus élémentaire que nous donnons à tous ceux qui établissent un programme de sécurité est de bien maîtriser les fondamentaux. Nous espérons que vous vous souvenez de la base : visibilité de chaque ressource, configuration de sécurité robuste et attitude attentive à l’égard de ces ressources ainsi que la mise à jour rapide et efficace des systèmes lorsque les fournisseurs publient des correctifs. La plupart des professionnels sont conscients de l’importance de ces points fondamentaux mais préfèrent passer leurs journées à disséquer le nouveau malware, perdre plusieurs jours à traquer les menaces présentes dans leur écosystème ou juste espérer béatement que rien ne leur arrivera. Les fondamentaux ont beau être

Le conseil le plus élémentaire que nous donnons à tous ceux qui établissent un programme de sécurité est de bien maîtriser le fondamentaux.

ennuyeux, force est de constater qu'ils sont efficaces. Certes, ils ne permettent pas d'éviter toutes les attaques, mais ils pourront en repousser une grande partie. Ce n'est pas un hasard s'ils sont devenus des fondamentaux. Nous ne manquerons pas de le souligner dans ce document. Nous ne pouvons bien entendu pas éliminer tous les risques, mais il est de notre devoir de compliquer la tâche aux acteurs mal intentionnés. Nous devons colmater les brèches les plus évidentes pour éviter que des adversaires insignifiants tels que des programmeurs du dimanche ou des pirates en herbe compromettent votre système d’information. Si vous compliquez la tâche de ces adversaires, il est probable que ces derniers échoueront, déclencheront un mécanisme de détection des intrusions ou laisseront des preuves qui pourront être utilisées contre eux lors d'une enquête.

Florilège de catastrophes

Parmi les milliers d'incidents de sécurité enregistrés ces dernières années, un bon nombre résultait de problèmes de configuration, de failles de sécurité connues qui n'avaient pas été corrigées ou des correctifs de fournisseurs qui n'avaient pas été installés. Examinons trois incidents pour nous faire une idée des conséquences d'une mauvaise hygiène informatique.

- **Microsoft Exchange :** il s'agit de la dernière attaque en date d'un acteur majeur. Les pirates ont réussi à obtenir un accès complet à des serveurs Exchange sur site. Une vague d'attaques de demande de rançon s'en est suivie, soulignant la nécessité de maintenir ces composants critiques à jour.

- **Equifax :** cette société n'a pas appliqué les correctifs disponibles à des serveurs Apache Struts vulnérables qui étaient accessibles depuis le réseau Internet. Les pirates en ont profité pour exécuter du code à distance. Pourtant, Apache avait publié un correctif, mais Equifax ne l'avait pas installé sur tous ses systèmes. Pire encore, leur équipe des opérations avait lancé la vérification de la présence de systèmes non mis à jour et n'en avait trouvé aucun, alors même que certain de leurs systèmes étaient encore vulnérables. Ce cas d'école en matière d'hygiène informatique a eu pour conséquence le vol de données personnelles de centaines de milliers d'utilisateurs. Equifax a dû, *in fine*, payer des centaines de millions de dollars de dommages et intérêts. Voilà une journée peu enviable.

- **Citrix :** lorsqu'une mise à jour est publiée pour un composant technologique important, il faut l'installer. En effet, les pirates ne se privent pas de réaliser de la rétro-ingénierie sur les correctifs pour identifier les vulnérabilités qu'ils comblent. La situation s'est avérée particulièrement problématique lors du piratage de Citrix au début de l'année 2020, car des pirates qui pouvaient rechercher de manière automatisée les périphériques vulnérables l'ont effectivement fait.. Les solutions d'atténuation de la menace initialement proposées par Citrix, qui n'avait pas encore publié de correctif, n'étaient pas fiables et n'ont par ailleurs pas été appliquées par un grand nombre de leurs clients, exposants ainsi de nombreuses entreprises et administrations.. Qui plus est, le code d'exploitation a largement été diffusé, ce qui a contribué à l'ampleur de l'incident. Une fois que Citrix a publié des correctifs, les clients les ont rapidement adoptés, ce qui a en grande partie mis fin à l'attaque. Les correctifs fonctionnent, mais encore faut-il les installer.

Nous n'aimons pas montrer du doigt des entreprises qui ont connu des problèmes de sécurité, mais nous nous devons d'apprendre de leurs erreurs. En outre, l'hygiène en matière d'infrastructure ne cesse de se complexifier. L'attaque menée contre SolarWinds à la fin de l'année 2020 illustre un cas où il n'a pas été suffisant de faire ce qui devait l'être, puisque l'installation d'un correctif a permis aux pirates d'obtenir un accès au système. Si vous examinez seulement cette situation, il se peut que vous vous demandiez à quoi peuvent bien servir les correctifs.

Si tel est le cas, il semblerait que vous n'ayez pas tiré tous les enseignements de cette histoire. En effet, précédemment, nous vous indiquions qu'il était impossible d'éliminer tous les risques.

Des attaques de l’écosystème peuvent se produire, et vous ne pouvez vraiment pas faire grand-chose à leur sujet mis à part vous concentrer sur la détection et la surveillance. Toutefois, si vous omettez d'installer un correctif sur un composant, vous laissez vos systèmes à la merci de tous les pirates qui savent comment exploiter la vulnérabilité.

Pourquoi vous n'avez pas le choix

Supposons que, malgré tous les inconvénients listés ci-dessus, vous rechigniez toujours à adopter une bonne hygiène informatique en matière d'infrastructure. Soyez à l'écoute de votre auditeur, plutôt que de nous. Il trouvera (et remontera) toutes sortes de lacunes si vous ne maintenez pas une configuration robuste de vos systèmes et si vous n'y installez pas les correctifs. Soulignons quelques obligations réglementaires qui devraient vous inciter à installer les correctifs.

- **PCI :** les conditions 2, 6 et 11 abordent les correctifs.
- **ISO 27001 :** le point A.12.6.1 traite de la correction des vulnérabilités (installation de correctifs).
- **L'article 25 du RGPD sur** « la protection des données dès la conception et la protection des données par défaut » ainsi que l'article 32 sur « la sécurité du traitement » abordent la nécessité de disposer de systèmes qui protègent les données des clients et indiquent que des systèmes qui ne sont pas à jour ne peuvent pas protéger lesdites données.

> Nous n'aimons pas montrer du doigt des entreprises qui ont connu des problèmes de sécurité, mais nous devons apprendre de leurs erreurs.

- **NIST SP 800-53 R3 :** les points sur la gestion de la configuration (CM), l'évaluation des risques (RA) et l'intégrité des systèmes et de l'information (SI) soulignent la nécessité d'installer les correctifs pour les infrastructures.

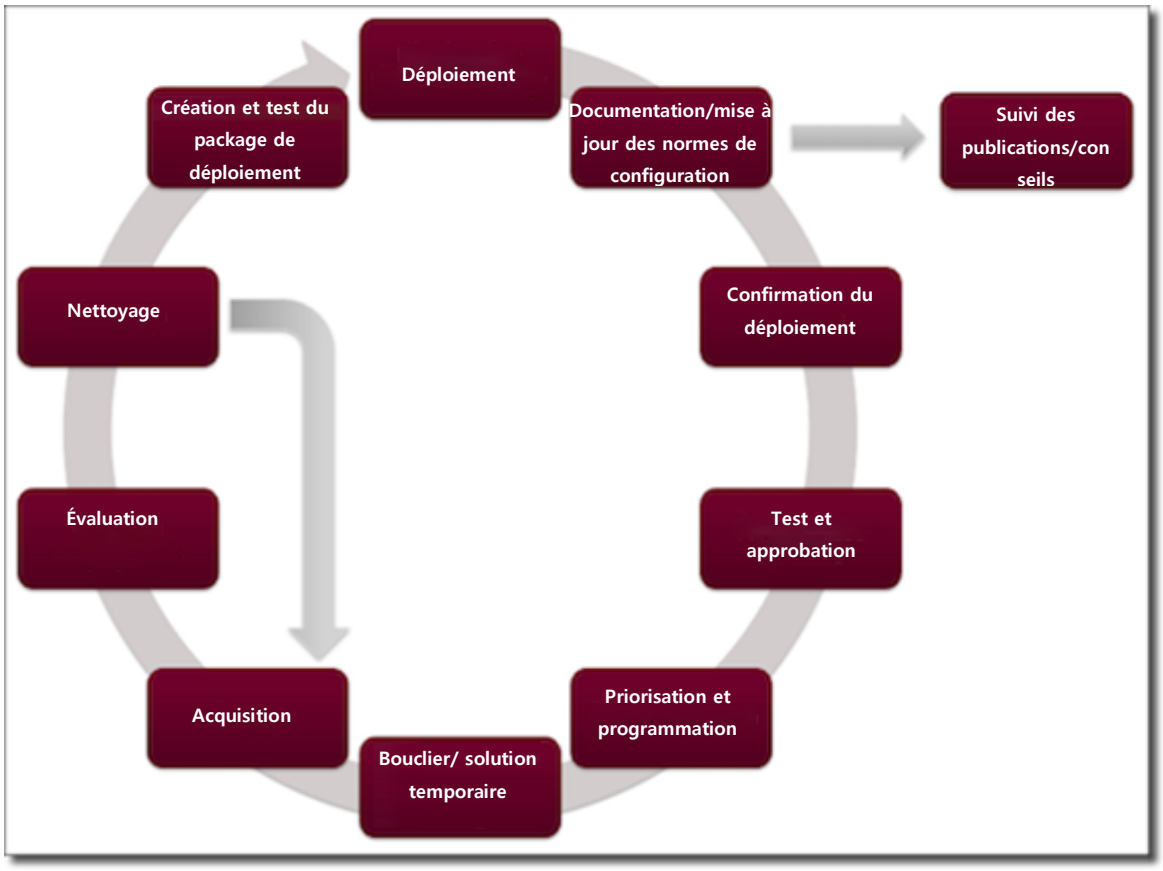
Il semblerait donc que vous n'ayez pas vraiment le choix. Qu'en pensez-vous ?

Corriger les vulnérabilités

Comme nous l'indiquions précédemment, le conseil le plus élémentaire que nous puissions donner en matière de sécurité est de se préoccuper en priorité des fondamentaux. Ces fondamentaux ne vous protégeront pas des pirates déterminés et bien financés, mais ils combleront les brèches les plus simples dans lesquelles la majorité des pirates chercheront à s'introduire.

Comme si cela ne suffisait pas, la marge d'erreur dont vous disposez aujourd'hui est quasiment nulle, car les pirates ont automatisé la reconnaissance de nombreuses attaques. Dès lors, si le moindre composant de votre écosystème reste vulnérable, ils le trouveront. Ils disposent de bots et de scripts qui cherchent constamment les maillons faibles.

Cela étant dit, vous ne lisez probablement pas ce document pour entendre parler des difficultés liées à la sécurité. Abordons donc la manière de résoudre les problèmes.



Colmater rapidement et complètement les brèches

Les fournisseurs publient des mises à jour et des correctifs pour les vulnérabilités découvertes dans leurs produits. Les clients appliquent ensuite ces correctifs dans leurs systèmes afin qu'ils restent à jour et sécurisés. Les correctifs rythment le travail de notre secteur depuis longtemps. Chez Securosis, nous étudions les correctifs depuis presque aussi longtemps. Nous vous invitons à faire un bond dans le temps et à consulter notre travail précurseur sur les correctifs dans le Project Quant.

L'illustration ci-dessus présente en détails le processus d'application de correctifs que nous avons défini en 2009. Pour être efficace, l'application des correctifs doit suivre un processus fiable et systématique. Nous insistons spécifiquement sur l'importance des étapes de test et d'approbation, afin d'éviter les inconvénients que pourrait poser l'application d'un correctif tel que l'arrêt d'un composant

Cela étant, un cycle complet du processus d'application de correctifs peut prendre entre quelques jours et un mois. De nombreuses grandes entreprises prévoient l'application des correctifs dans un délai d'un mois. Toutefois, dans la réalité, il n'est parfois pas possible d'attendre plusieurs semaines avant d'appliquer un correctif si la faille de sécurité de grande ampleur est activement exploitée. Il faut disposer d'un processus d'application de correctifs de haute priorité pour les vulnérabilités qui présentent un risque très élevé. Il est essentiel d'établir et de convenir de critères pour déclencher l'application prioritaire de correctifs (hors cycle) ainsi que que quelles sont les étapes du processus normal qui pourront être ignorées.

Vous pouvez également utiliser un correctif virtuel temporaire, une mesure qui vise à protéger vos systèmes contre l'exploitation d'une vulnérabilité non corrigée en repérant la signature de l'attaque. Les correctifs virtuels ne peuvent être mis en place que si le schéma de l'attaque a été clairement identifié, sans quoi il est impossible d'établir une signature. Il faut toutefois noter qu'une signature ne constitue qu'une protection de surface souvent inadéquate contre les attaques. En revanche, le déploiement de correctifs virtuels présente l'avantage de pouvoir être rapide. Cependant, étant donné que les informations sur les nouvelles vulnérabilités à haut risque sont souvent maigres et vagues, il s'avère difficile, voire impossible, de s'assurer que ces solutions de fortune ciblent le schéma identifiable optimal et que l'attaque ne prennent pas une forme différente afin de changer de signature. En fin de compte, c'est la capacité du fournisseur à proposer un correctif virtuel temporaire à même d'identifier le plus précisément possible le schéma de l'attaque qui en déterminera l'efficacité. Si le correctif est trop permissif, il laissera un trop grand nombre de pirates exploiter la faille qu'il est censé protéger. Par contre, si le fournisseur ne cible pas assez précisément le schéma de l'attaque, le correctif risque de bloquer des transactions légitimes. En outre, il est toujours nécessaire d'effectuer de nombreux tests pour vérifier que tout fonctionne, ce qui ne vous fera pas économiser beaucoup de temps par rapport à l'application de correctifs. Voilà beaucoup d'éléments à prendre en compte, mais les risques en présence sont bien réels.

L'un des autres inconvénients des correctifs virtuels temporaires est que tout le trafic destiné aux composants vulnérables doit passer par le point d'inspection ou le dispositif exécutant la logique

d'atténuation. Si le trafic peut atteindre directement les composants vulnérables, le correctif virtuel temporaire ne sert à rien. Par exemple, si un correctif virtuel est déployé sur un dispositif de sécurité contrôlant le périmètre de vos systèmes afin de protéger une base de données, une personne disposant d'un accès interne et direct à la base de données peut contourner le correctif pour s'introduire dans la base de données vulnérable. Dans ce contexte, une « personne disposant d'un accès interne » peut simplement être une personne mal intentionnée qui s'est introduite à l'intérieur du périmètre ou qui dispose des informations d'identification d'un administrateur.

Il est aussi nécessaire d'avoir une vision claire des mesures à prendre quand un schéma d'attaque a été identifié. Si vous arrêtez toutes les connexions, les autres utilisateurs du même pool de connexions seront touchés ou l'application pourrait présenter des comportements inattendus.

Si vous rencontrez des vulnérabilités de haute importance et que vous ne pouvez pas appliquer immédiatement le correctif, soit parce qu'il n'est pas encore disponible, soit en raison d'un temps d'arrêt ou d'autres problèmes de maintenance que son installation engendrerait, un correctif virtuel temporaire peut constituer une bonne alternative à court terme. Toutefois, il ne faut pas perdre de vue que vous n'aurez alors pas réparé le composant ; le correctif virtuel ne fait que cacher le problème. Avec 30 ans d'expérience à notre actif, nous pouvons vous dire avec certitude qu'il est vain d'espérer que les pirates ne trouveront pas vos systèmes vulnérables.

Étant donné la facilité avec laquelle les acteurs mal intentionnés peuvent modifier la signature de leurs attaques pour ne pas se faire repérer et pour échapper aux correctifs virtuels temporaires, force est de constater qu'il est impossible d'obtenir une signature de détection parfaite et qu'il est difficile de s'assurer que tout le trafic passe par un point d'inspection. L'application des correctifs des fournisseurs reste la seule solution viable à long terme. Et en parlant de solutions à long terme...

Tirer pleinement parti des responsabilités partagées

L'un des aspects les plus remarquable de la révolution du cloud est qu'elle permet de remplacer certains composants d'infrastructure par des services de plate-forme (PaaS). Nous y avions déjà fait allusion précédemment. À présent, étudions comment la responsabilité partagée peut améliorer votre hygiène informatique en matière d'infrastructure.

Avant tout, la responsabilité partagée est essentielle pour le cloud. Chaque fournisseur de cloud assume des responsabilités spécifiques. Les utilisateurs du cloud, c'est-à-dire vous, ont également des responsabilités concernant la sécurité. Cette combinaison forme la responsabilité partagée.

La répartition précise des responsabilités dépend du service et du modèle de livraison (SaaS ou PaaS), mais, dans tous les cas, le recours à un service PaaS en vue de remplacer un composant d'infrastructure vous permet de ne plus avoir à vous en occuper. Vous ne devez alors plus vous soucier de son évolution ou de sa maintenance, notamment au travers des correctifs de sécurité. Il va sans dire que vous serez certainement attristés à l'idée de ne plus devoir passer des nuits blanches et des week-ends loin de votre famille à installer des correctifs urgents sur des serveurs et des bases de données.

En fin de compte, en transférant une partie de vos responsabilités à un fournisseur de services, vous réduisez à la fois votre surface d'attaque et opérationnelle, ce qui est une bonne chose.
À long terme, l'utilisation stratégique des services PaaS est l'un des meilleurs moyens de réduire les risques pour votre pile technique.

En fin de compte, en transférant une partie de vos responsabilités à un fournisseur de services, vous réduisez à la fois votre surface d'attaque et opérationnelle, ce qui est une bonne chose. À long terme, l'utilisation stratégique des services PaaS est l'un des meilleurs moyens de réduire

les risques pour votre socle technique. En effet, un fournisseur de services peut encore commettre des erreurs, mais le risque est considérablement moindre. Les prestataires de services doivent préserver leur réputation et leur image de marque. Pour ce faire, ils consacrent des ressources considérables afin d’adresser leurs vulnérabilités et d’assurer la sécurité de leurs clients.

L’écosystème

S'il y a bien un enseignement que nous avons tiré de l'incident de sécurité de SolarWinds et de l'attaque de Target (2013), qui ont commencé par l'exploitation d'une faille de sécurité présente chez un prestataire tiers, c'est que les responsabilités en matière d'hygiène informatique ne se cantonnent pas à votre environnement. Comme indiqué ci-dessus, vous n'êtes peut-être pas responsables de la maintenance des composants de l'infrastructure de vos fournisseurs et partenaires, mais vous avez le devoir d'endiguer les conséquences de leurs faiblesses sur votre environnement.

Comment ça ? Pour le dire plus clairement, si un de vos partenaires commerciaux externes est compromis et qu'un attaquant en profite pour s'introduire dans votre environnement et commence à y faire des ravages, vous serez tenus pour responsable. Vous pourrez, bien sûr, faire valoir que votre partenaire était responsable de la protection de son environnement et qu'il a échoué dans cette mission. Mais cela ne vous sera d'aucune utilité lorsque vous devrez expliquer pourquoi votre programme d'atténuation des risques tiers n'était pas suffisant devant le comité d'audit de votre organisation.

Il est légitime de vouloir tirer parti du modèle de responsabilité partagée pour obtenir un soutien opérationnel et réduire votre surface d'attaque, mais il est tout aussi nécessaire d'allouer des ressources supplémentaires à la gestion des risques afin de comprendre l'importance des risques et donc de choisir les mesures correctives appropriées.

Succès et cohérence

Il convient de rappeler que les différentes mesures d'hygiène de sécurité pour les infrastructures ne sont en aucun cas incompatibles. Un correctif élimine la vulnérabilité d'un composant, mais dans certains cas un correctif virtuel temporaire peut à court terme réduire un risque immédiat. La meilleure solution à long terme demeure toujours d'appliquer les correctifs distribués directement par les fournisseurs et parfois de passer à un service de PaaS. Vous devrez déterminer la meilleure approche au cas par cas, en pesant le pour et le contre en fonction des risques, des éléments à votre disposition et de votre capacité à remanier l'application.

Obtenir des résultats rapidement

Corriger des vulnérabilités d'importance élevée est une situation particulièrement fréquente. C'est la manière dont vous gérez ces situations qui détermine généralement comment les autres perçoivent les capacités et les compétences de votre équipe de sécurité. Prenons l'exemple d'une petite entreprise proposant des services financiers, telle qu'une banque régionale. Ses équipes utilisent une application client/serveur locale pour gérer les données des prêts des clients et recourent largement à des procédures stockées pour le traitement en back-end. L'équipe chargée du développement de l'application met régulièrement à jour l'interface web, tandis que le back-end reste en grande partie inchangé. Cette situation est fréquente : on ne touche pas à ce qui fonctionne. Qui plus est, l'application semble moderne pour les clients, qui utilisent l'interface web, et le back-end fonctionne correctement. Toutefois, l'équipe reçoit régulièrement des messages des fournisseurs les alertant au sujet de vulnérabilités d'importance élevée qui touchent la base de données du back-end et les avertissant de la publication imminente d'un correctif. L'équipe de sécurité doit donc trouver la manière la plus sûre et la plus efficace de faire face à cette situation.

Corriger des vulnérabilités d'importance élevée est une situation particulièrement fréquente. C'est la manière dont vous gérez ces situations qui détermine généralement comment les autres perçoivent les capacités et les compétences de votre équipe de sécurité.

La première étape de notre processus consiste en une analyse des risques. Si une analyse rapide des données relatives aux menaces nous apprend que des informations sur une faille de sécurité exploitable circulent, nous devons réagir. Le temps nous est compté. Ensuite, il faut évaluer l'importance de l'application. Dans l'exemple qui nous occupe, il s'agit d'un système contenant des données sur les prêts des clients. Ces dernières sont

essentielles pour l'entreprise et sont soumises à des obligations réglementaires. Étant donné que l'application est généralement utilisée pendant les heures de bureau, les correctifs peuvent être appliqués en dehors de ce créneau.

Dans ce cas, un correctif rapide est nécessaire, parce que des informations sur la faille de sécurité circulent et parce que les chercheurs en sécurité ont indiqué que des requêtes pouvaient permettre aux pirates d'accéder à la base de données. L'équipe de sécurité installe un correctif virtuel temporaire qui utilise un système de prévention des intrusions (IPS) sur le périmètre du système pour examiner les requêtes et bloquer les plus dangereuses d'entre elles. Les paramètres des attaques sont souvent trop larges pour que l'IPS puisse les bloquer, mais, dans le cas qui nous occupe, le correctif temporaire fonctionne.

L'équipe décide aussi par précaution d'augmenter la surveillance de la base de données pour les alerter de toute activité interne visant à contourner le correctif virtuel temporaire. Un mécanisme de surveillance supplémentaire détectera les pirates qui chercheraient à contourner l'application en utilisant un composant déjà compromis en vue d'effectuer les requêtes dangereuses directement sur la base de données.

Ensuite, l'équipe des opérations installera le correctif du fournisseur lors du prochain créneau de maintenance. Le correctif virtuel temporaire a permis à l'équipe de gagner un peu de temps pour tester le correctif du fournisseur afin de s'assurer qu'il ne perturbe pas l'application. Le test du correctif du fournisseur montre qu'il n'a pas d'impact négatif. L'équipe des opérations l'installe donc avec succès lors de la période de maintenance suivante.

Finalement, elle procède à un examen stratégique du processus afin de recenser les améliorations à apporter la prochaine fois. L'application sera remaniée et migrée dans le cloud de la banque, mais il faudra attendre 24 mois avant que le projet ne commence. Serait-il utile d'augmenter la priorité ? Probablement pas, car, même si la prochaine vulnérabilité ne peut être atténuée à l'aide d'un correctif virtuel temporaire, le correctif peut être réalisé au travers d'une mise à jour d'urgence en dehors des heures de bureau sans impact significatif sur la disponibilité des applications. Lorsque le remaniement de l'application commencera, les équipes envisageront de migrer dans un premier temps certaines procédures stockées vers un serveur d'applications, puis de migrer les données vers un PaaS pour réduire la surface d'attaque et opérationnelle de l'application. Ils doivent également examiner si une offre commerciale SaaS pourrait remplacer l'application dans son ensemble.

Alignement organisationnel

Le scénario présenté ci-dessus montre comment toutes les mesures d'hygiène informatique en matière d'infrastructure peuvent être combinées pour atténuer le risque élevé de vulnérabilité d'une base de données. Plusieurs équipes ont participé à ce processus. Tout a commencé quand la sécurité a identifié le problème, a examiné les mesures correctives et a décidé d'utiliser un correctif virtuel temporaire ainsi qu'un mécanisme de surveillance supplémentaire. L'équipe des opérations informatiques a joué un rôle essentiel en testant les correctifs du fournisseur et en les installant. L'équipe d'architecture envisagera de remanier l'application ou de la migrer vers une offre SaaS.

Pour collaborer efficacement, toutes ces équipes doivent s'aligner et collaborer afin de parvenir au résultat souhaité, à savoir garantir la disponibilité des applications sans perdre de données. Toutefois, il faut souligner qu'une autre équipe a un rôle crucial à jouer pour faciliter le processus: le service financier. En effet, il finance des éléments tels qu'un dispositif installé sur le périmètre en attendant une solution plus stable et un contrat de support/maintenance pour garantir l'accès aux correctifs, en particulier pour les anciennes applications qui sont facilement oubliées. Aussi essentielles que les compétences techniques puissent être pour maintenir l'infrastructure au premier plan, il est tout aussi important de s'assurer que les techniciens disposent des ressources nécessaires pour faire leur travail.

Si vous avez des questions sur ce sujet ou si vous souhaitez discuter de votre situation en particulier, n'hésitez pas à nous envoyer un message à l'adresse info@securosis.com.

À propos de l'analyste

Mike Rothman, Analyste et Président

Les perspectives audacieuses et le style irrévérencieux de M. Rothman sont d'une valeur inestimable pour les entreprises au moment de déterminer quelles stratégies seront efficaces pour leur adaptation à l'évolution des pratiques en matière de sécurité. M. Rothman est spécialiste des aspects les plus attrayants de la sécurité, tels que la protection des réseaux et des terminaux, la gestion de la sécurité et la conformité.
Fort de vingt années dans le secteur de la sécurité ou dans des domaines connexes, il connaît tous les secrets du métier.

Au début de sa carrière de programmeur et de consultant en réseau, M. Rothman a été analyste pour le groupe META avant de créer SHYM Technology. Ensuite, il a occupé des postes de cadre à CipherTrust et TruSecure. En 2006, M. Rothman a lancé Security Incite afin de faire entendre une voix raisonnable dans un secteur de la sécurité surmédiatisé, mais aux résultats décevants. Après un bref passage comme Vice-président senior de la stratégie à eIQnetworks, M. Rothman a rejoint Securosis avec un cynisme nouveau quant à l'état de la sécurité.

M. Rothman a publié The Pragmatic CSO <http://www.pragmaticcso.com/> en 2007 afin de présenter aux experts techniques en cybersécurité toutes les subtilités à maîtriser pour devenir un professionnel aguerri. Il est également titulaire d'un diplôme d'ingénierie très prestigieux en recherche opérationnelle et génie industriel de l'Université Cornell. Ses collaborateurs se réjouissent de constater que son diplôme ne lui est d'aucune utilité au quotidien.

À propos de Securosis

Securosis, LLC est une société indépendante de recherche et d'analyse dédiée au leadership éclairé, à l'objectivité et à la transparence. Nos analystes ont tous occupé des postes de direction et s'emploient désormais à fournir des services de conseil pragmatiques et de grande valeur. Voici quelques-uns de nos services :

- **Publication de recherches « de première main » :** nous publions gratuitement une grande partie de nos recherches sur notre blog et nous compilons les recherches sous forme de documents pouvant être distribués sur une base annuelle. Tous les documents et présentations que nous publions répondent à nos exigences strictes en matière d'objectivité et suivent notre politique garantissant une recherche totalement transparente.
- **Accélérateurs de projet de sécurité cloud :** Securosis Project Accelerators (SPA) sont des offres de conseil prêtes à l'emploi qui nous permettent d'apporter à vos déploiements cloud le résultat de nos recherches appliquées et notre expérience éprouvée sur le terrain. Ces programmes approfondis combinent des évaluations, des ateliers personnalisés et un support continu pour vous assurer que vos projets cloud sont plus sûrs et plus rapides. Ils sont conçus pour réduire de plusieurs mois ou années la durée de vos projets tout en intégrant des pratiques de sécurité cloud de pointe dans vos opérations existantes.
- **Formation sur la sécurité dans le cloud :** Notre équipe a créé le cours de formation Cloud Security Alliance CCSK et notre propre programme Advanced Cloud Security and Applied SecDevOps. Participez à l'un de nos cours publics ou faites-nous venir chez vous pour une expérience privée et personnalisée.
- **Services de conseil pour les fournisseurs :** nous offrons un certain nombre de services de conseil pour aider nos clients fournisseurs à commercialiser correctement le bon produit/service qui répondra aux besoins essentiels du marché. Securosis a la réputation de dire à ses clients ce qu'ils DOIVENT entendre, et non ce qu'ils veulent entendre. Notre collaboration avec nos clients commence généralement par une journée sur la stratégie et peut se poursuivre par un abonnement pour un soutien continu. Les services disponibles dans le cadre de nos services de conseil comprennent notamment l'analyse du marché et des produits ainsi que le développement de stratégies en la matière, un suivi pour la feuille de route des technologiques et les stratégies concurrentielles. Vous devez toutefois garder à l'esprit que nous maintenons nos exigences strictes en matière d'objectivité et de confidentialité dans toutes nos missions.
- **Recherche personnalisée, discours et conseils :** Vous avez besoin d'un rapport de recherche personnalisé sur une nouvelle technologie ou une question de sécurité ? Vous êtes à la recherche d'un conférencier expérimenté pour un événement interne ou public sur la sécurité ? Il vous faut un expert extérieur pour le processus de diligence raisonnable dans le cadre d'une fusion ou d'une acquisition ? Votre entreprise a besoin d'un expert pour évaluer sa stratégie de sécurité, identifier ses lacunes et élaborer une feuille de route ? Ces projets prédéfinis sont utiles lorsque vous avez besoin de plus d'une journée sur la stratégie, mais pas d'un contrat de conseil à long terme.

Nos clients sont aussi bien des start-up de pointe que des fournisseurs de technologies et des utilisateurs finaux renommés. Nous comptons parmi nos clients de grandes institutions financières, des investisseurs institutionnels, des entreprises de taille moyenne et de grands fournisseurs de sécurité. Pour plus d'informations sur Securosis, visitez notre site Web : <http://securosis.com/>.