Date de publication :
7 février 2020
Auteur :
Alan Rodger

Une politique pérenne de mise à jour : essentielle pour une sécurité robuste, une réduction des risques et une réponse adaptée aux enjeux de conformité.

Face à une hausse de la complexité et des niveaux de menace, les clients ont besoin d'un support à toute épreuve

OMDIA

Résumé

En bref

Dans de nombreux secteurs, l'augmentation des investissements en transformation numérique montre que les logiciels sont plus que jamais essentiels à la valeur et à la réputation des entreprises. Dans le même temps, des facteurs tels que la complexité accrue induite par les nouvelles possibilités technologiques (notamment la prévalence plus grande des chaînes d'approvisionnement numériques), la très forte croissance des menaces et l'environnement concurrentiel (qui entraîne des mises à jour de logiciels plus fréquentes de la part des fournisseurs pour introduire de nouvelles fonctionnalités) sont autant d'éléments qui accélèrent l'adoption des logiciels et les cycles de changement au sein des organisations d'utilisateurs. Il en résulte un parc logiciel dont la surface d'attaque est nettement plus importante et sur laquelle, les acteurs malveillants se focalisent de plus en plus pour en découvrir les faiblesses et ainsi pouvoir les exploiter.

Si de nombreuses solutions de sécurité peuvent être mises en œuvre pour intégrer des éléments de protection ponctuels, l'application en temps voulu des logiciels correctifs proposés par les éditeurs est la base indispensable pour éviter le risque lié à la présence de vulnérabilités de sécurité non corrigées. La gestion des risques et de la conformité sont de plus en plus proches des pratiques de protection des logiciels du fait de la tendance à la numérisation. Les menaces restant sans réponse en raison de vulnérabilités non corrigées constituent de ce fait de véritables problèmes métiers.

Omdia estime que de nombreuses organisations ont besoin de gagner en maturité et de mieux comprendre la valeur d'une gestion proactive de la charge de travail et du cycle de vie des correctifs. Cela nécessite un véritable engagement pour établir une fenêtre de déploiement de correctifs de sécurité dans le cadre d'une maintenance programmée prioritaire. Le déploiement de correctifs constituant un point clé essentiel, la gouvernance informatique est le reflet de ce besoin de maturité et doit passer uniquement par l'obtention de correctifs auprès de l'éditeur d'origine.

Vision d'Omdia

Les clients passent souvent par un processus rigoureux d'examen et de vérification avant d'investir dans des logiciels d'entreprise, et ce à juste titre, étant donné l'ampleur et le coût de la plupart des projets. Il est toutefois toujours surprenant que certains clients ne fassent pas preuve de la même précaution lorsqu'il s'agit de sécuriser correctement leurs investissements logiciels par l'application de correctifs et une maintenance en continu des logiciels, mesure nécessaire pour conserver tout le potentiel de valeur du logiciel. L'approche de la gouvernance informatique dans toute organisation doit se prémunir très fortement de toute tendance à « acheter puis oublier » tout élément du parc logiciel, car

cela peut ouvrir des failles dans la protection de l'entreprise et favoriser les risques et les problèmes de conformité qui sont à l'origine de graves problèmes métiers.

Assurer la mise à jour corrective et la maintenance des logiciels de manière régulière doit être un impératif pour chaque entreprise. Cet impératif doit être appliqué rigoureusement par une Direction engagée dans l'élaboration des plans de maintenance et dans la maturité nécessaire à la culture de l'organisation, si l'on veut garantir une application de correctifs régulière et réussie. Une maintenance régulière de la sécurité permet aux clients de créer une culture de la conformité dans laquelle ils peuvent avoir l'assurance de respecter les réglementations et les procédures de conformité du secteur. L'incapacité à bien appliquer des correctifs logiciels et à assurer une bonne maintenance met en danger les résultats d'une société et sa réputation d'entreprise fiable et responsable. La culture d'entreprise, en plus de renforcer ces raisons essentielles pour l'entreprise de s'engager à appliquer des correctifs, se doit de surmonter toute crainte que ces correctifs puissent être éventuellement responsables d'entraîner des défaillances. Bien au contraire, la réalité est que l'absence d'application de correctifs constitue un risque bien plus important.

Bien entendu, comme toute autre discipline de gestion informatique, l'opération de mise à jour doit faire l'objet d'un contrôle rigoureux. Un des éléments clés du succès d'un programme de déploiement de correctifs est l'utilisation de sources fiables d'information sur les correctifs, et de ne pas faire confiance à des sources de mauvaises qualités telles que les conseils qu'on trouve partout sur le web. Une autre faiblesse à éviter est l'engagement de prestataires de services tiers sans l'assurance que leurs processus et leurs compétences intègrent toute la rigueur nécessaire pour n'utiliser que des sources de contenu sur les correctifs dignes de confiance. Une mauvaise gouvernance de ces relations est susceptible d'avoir comme conséquences l'augmentation des coûts pour l'organisation cliente ainsi que des problèmes de risque et de conformité. De plus, les organisations ne doivent pas se fier à des mesures de mitigation non éprouvées ou à des changements de configuration non vérifiés pour se passer de certains correctifs.

Messages clés

- Le maintien de la sécurité des logiciels tout au long de leur cycle de vie est une responsabilité essentielle.
- La mise à jour corrective est une pierre angulaire de la gouvernance informatique et permet de soutenir les responsabilités de conformité.
- Le risque n'est évité que si les correctifs sont obtenus auprès de sources fiables.

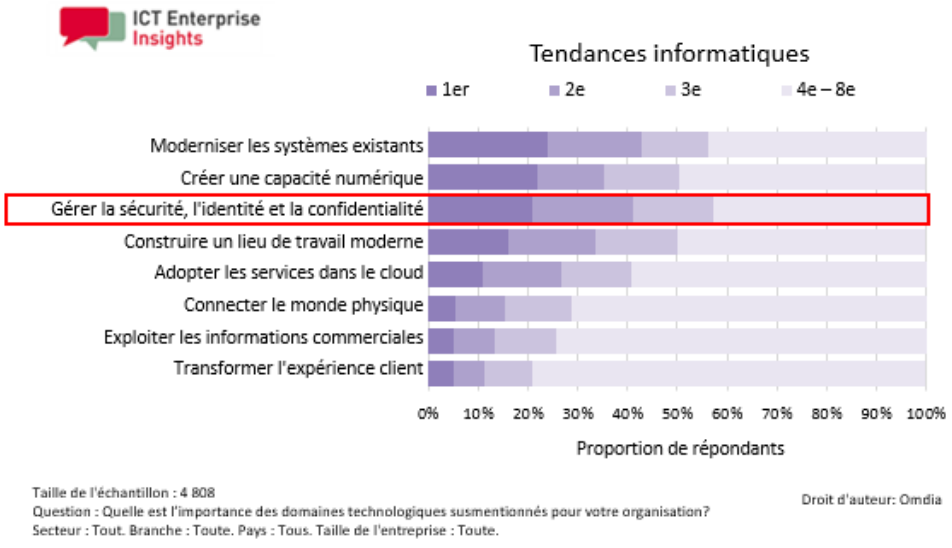
Le maintien de la sécurité des logiciels tout au long de leur cycle de vie est une responsabilité essentielle

De nombreuses entreprises clientes tentent de transformer leur écosystème informatique afin de suivre le rythme accéléré du changement sur leurs marchés et dans leurs activités en tirant parti des possibilités technologiques telles que le cloud, la mobilité et l'analytique. En général, il faut constamment trouver un équilibre entre l'investissement dans des initiatives de transformation numérique (tirer parti d'applications et de processus métiers

nouveaux et améliorés) et la nécessité de s'assurer que l'évolution de l'environnement fonctionne de manière fiable avec une sécurité à toute épreuve. L'éventail de composants de l'infrastructure informatique qui doivent être sécurisés s'étend, non seulement en englobant le « socle » traditionnel, depuis les systèmes d'exploitation jusqu'au matériel, en passant par les bases de données, le middleware et les applications, sans oublier les services basés sur le cloud et d'autres services tiers. En dehors des frontières traditionnelles de l'informatique, toute présence d'une entreprise dans les environnements mobiles des consommateurs doit passer par une protection de sécurité intégrée, parce que, qu'ils le veuillent ou non, les utilisateurs mobiles sont enclins à prendre des mesures susceptibles de mettre l'appareil en situation de péril face aux menaces.

Tout manque de protection au sein de l'infrastructure informatique dans sa globalité peut causer des temps d'arrêt qui peuvent avoir des répercussions sur l'ensemble de l'entreprise et, dans certaines circonstances, donner lieu à des failles de sécurité susceptibles d'entraîner des violations des réglementations du secteur et des procédures de conformité. Dans ce contexte, il n'est pas surprenant que les réponses à la dernière enquête annuelle d'Omdia aient montré que la gestion de la sécurité, de l'identité et de la confidentialité figurait plus que toute autre catégorie dans le choix des trois tendances informatiques les plus importantes pour les organisations (voir graphique 1).

Graphique 1 : La gestion de la sécurité, de l'identité et de la confidentialité est considérée comme la plus importante des trois grandes tendances



Source : Omdia ICT Enterprise Insights 2019/20

Le secteur des technologies de l'information étant lui-même de plus en plus interconnecté (par exemple, par le biais de partenariats technologiques) pour soutenir la numérisation, la cadence des mises à jour logicielles est désormais beaucoup plus rapide que ce à quoi les clients ont été habitués par le passé. Alors que les clients bénéficient de la concurrence plus vive que jamais des fournisseurs de nouvelles fonctions et fonctionnalités, leur parc informatique représente une surface d'attaque plus large qui peut être soumise à un éventail lui aussi plus large de menaces provenant d'acteurs malveillants. Les principaux

fournisseurs s'engagent de plus en plus à répondre aux menaces en publiant des correctifs pour les vulnérabilités de cybersécurité connues : une organisation qui met à jour son parc logiciel avec les correctifs mis à disposition par les fournisseurs adopte le principal moyen de protection contre les menaces liées aux logiciels, et ce, dans les meilleurs délais. Les nouvelles versions et les correctifs peuvent également exiger des clients qu'ils reviennent à une version antérieure aux correctifs pour certains éléments de leur « socle » (par exemple, middleware, système d'exploitation ou base de données) pour remplir les conditions de support. De plus, la chaîne de dépendances liées à la protection entre les composants du socle demande une attention permanente. Par exemple, certaines mises à jour de micrologiciels Intel sont connues pour nécessiter des correctifs correspondants aux couches de système d'exploitation et de virtualisation, et pour les anciens types de processeurs, l'atténuation des problèmes de processeur nécessite la désactivation de certaines fonctions (hyperthreading) si les charges de travail exécutées ne sont pas fiables.

Il n'est pas difficile de comprendre pourquoi la sécurité est une priorité pour tous les types d'entreprises quand on regarde ce qu'un incident ou une faille de sécurité peut avoir comme conséquences pour l'activité et la réputation d'une entreprise. Les nouveaux cas de failles et de piratages de sécurité au sein des multinationales sont plus fréquents que jamais, avec des signalements de vols de données de cartes de crédit, d'informations personnelles, de dossiers médicaux, etc. (par exemple, les incidents impliquant Equifax et CapitalOne). On observe déjà des exemples d'augmentation des sanctions liées à la conformité en raison de procédures inadéquates d'application de correctifs. Cela pourrait se reproduire à mesure que les règlements et la législation deviennent plus stricts (par exemple, 4 % du chiffre d'affaires mondial pour la non-conformité liée à une violation dans le cadre du RGPD). Au-delà des conséquences financières directes, ces événements entraînent généralement une perte de revenus et ternissent la réputation de l'entreprise concernée, avec de potentielles pertes d'activité et de fidélité des clients dont il est difficile de se remettre. La plupart des entreprises reconnaissent la nécessité de se protéger autant que possible des menaces potentielles de cybersécurité, mais elles doivent également comprendre que ces menaces peuvent provenir non seulement de pirates informatiques externes, mais aussi de l'incapacité à maintenir une protection de sécurité interne à jour dans l'ensemble du socle informatique.

L'application des correctifs est une pierre angulaire de la gouvernance informatique et permet de soutenir les responsabilités de conformité

Les entreprises d'aujourd'hui ne peuvent tout simplement pas se permettre de se passer d'un programme rigoureux de sécurité et de maintenance des logiciels, d'autant plus que les menaces externes sont constantes et de plus en plus élaborées, nécessitant une vigilance et une maintenance permanentes. Pour avoir un profil de sécurité rigoureux, les entreprises doivent travailler en étroite collaboration avec leurs éditeurs de logiciels, car ce sont eux qui ont le plus d'expérience et d'expertise en matière de correctifs, de support et de sécurisation de leurs propres produits.

Les entreprises de toutes tailles et de tous secteurs doivent s'associer à un éditeur de confiance pour mettre en place des procédures visant à maintenir leur sécurité logicielle à jour et à remédier aux vulnérabilités potentielles. Les vulnérabilités logicielles non corrigées, les vulnérabilités logicielles peuvent permettre à des pirates informatiques malveillants ou à du personnel non autorisé de contourner les contrôles de sécurité, ce qui peut entraîner directement des vols, des fraudes et des pertes financières immédiates, sans parler du préjudice porté à la marque de l'entreprise. Au-delà de ces pertes, les entreprises qui ne parviennent pas à maintenir la sécurité de leurs logiciels s'exposent à d'éventuelles amendes pour avoir enfreint les réglementations et les procédures de conformité imposées par le gouvernement ou le secteur, d'autant plus que ces conséquences deviennent de plus en plus coûteuses à mesure que les incidents de sécurité gagnent en fréquence et en gravité.

Aux États-Unis, les organismes de réglementation gouvernementaux ont pris l'habitude d'imposer de lourdes amendes suite à des violations de la sécurité et des données, ce qui coûte des millions de dollars aux entreprises de divers secteurs. En fait, les failles de sécurité et leurs conséquences sont devenues si fréquentes que la Federal Trade Commission (FTC) a publié des directives détaillées sur la manière dont les entreprises doivent aborder la sécurité informatique sur l'ensemble de leur socle. Pour citer un exemple, la FTC a publié *Start with Security* : *A Guide for Business*, (Commencer par la sécurité, un guide pour les entreprises) une compilation des 10 principaux enseignements à tirer des amendes et des règlements amiables qu'elles ont adoptés dans des cas de violations passées, comme le montre le tableau 1.

Tableau 1 : Recommandations de la FTC en matière de sécurité informatique
Commencer par la sécurité
Contrôler l'accès aux données de manière judicieuse
Exiger des mots de passe et une authentification sécurisés
Stocker les informations personnelles sensibles en toute sécurité et les protéger pendant leur transmission
Cloisonner et surveiller votre réseau
Sécuriser l'accès distant à votre réseau
Appliquer de bonnes pratiques de sécurité lors du développement de nouveaux produits
S'assurer que vos prestataires de services mettent en œuvre des mesures de sécurité raisonnables
Mettre en place des procédures pour maintenir votre sécurité à jour et remédier aux vulnérabilités qui pourraient survenir
Sécuriser les supports papier et physiques et les appareils

Source : *Federal Trade Commission*

Bien que certaines parties de ce guide soient assez intuitives, certains enseignements méritent d'être examinés de plus près dans l'optique d'une mise à jour et d'un support appropriés du produit. Lorsqu'elle évoque les bonnes pratiques de sécurité dans le développement de produits, la FTC fait référence aux entreprises qui ont été citées et condamnées à une amende pour ne pas avoir suivi les directives de sécurité des plateformes de produits informatiques.

S'agissant des procédures de sécurité visant à remédier aux vulnérabilités, la FTC recommande précisément de mettre à jour et de corriger les logiciels tiers, de tenir compte des éventuelles alertes de sécurité des éditeurs et d'y remédier immédiatement. Si elle ne le fait pas, une entreprise pourrait être soumise à un contrôle minutieux des organismes de régulation et d'autres parties, et se voir infliger une amende substantielle si un grave problème de sécurité devait survenir et si l'entreprise n'a pas respecté au préalable les politiques de conformité.

Un certain nombre d'autres règlements et normes comportent des dispositions relatives aux correctifs, notamment

- L'exigence 6.2 de la norme PCI DSS qui stipule qu'un évaluateur examine les stratégies et les procédures des organisations pour vérifier qu'il existe un processus établi de gestion des correctifs
- La section 12 de la norme ISO/IEC 27001, qui stipule que les vulnérabilités techniques doivent être corrigées et que des règles doivent être mises en place pour l'installation des logiciels par les utilisateurs.

Dans ce contexte, les entreprises indiquent de plus en plus souvent à Omdia que la sécurité et la conformité vont de pair lorsqu'elles envisagent de déployer des logiciels et que ces deux éléments jouent un rôle de plus en plus important dans l'ensemble du support et de la maintenance informatiques. Pour de nombreux régimes de conformité, il est essentiel de conserver des documents prouvant que les mesures prises (tant au niveau politique qu'opérationnel) répondent aux exigences de conformité. L'automatisation de la mise à jour corrective est susceptible de constituer le moyen le plus efficace de répondre à ces exigences de compte rendu à l'avenir, tout en garantissant l'efficacité et en évitant l'impact de l'augmentation de la demande de ressources liée à l'ampleur prise par les exigences en matière de correctifs.

La plupart des règlements sont soit basés sur les transactions (par exemple, dans les services financiers et bancaires), soit sur la gestion des données (par exemple, la confidentialité des données et le stockage des dossiers dans le domaine des soins de santé), soit les deux. Chez Omdia, nous recommandons régulièrement aux entreprises, quel que soit le secteur d'activité dans lequel elles opèrent, de créer une base et une culture de conformité solides fondements de leurs déploiements informatiques et logiciels existants, surtout si elles espèrent un jour mener des projets de transformation numérique qui amèneront leurs logiciels à une position plus critique en soutien à toutes sortes de processus. Nous estimons qu'un tel fondement ne peut exister sans des services réguliers de mise à jour corrective et de maintenance des logiciels, de préférence automatisés et évolutifs, qui permettent aux DSI et aux responsables informatiques de se concentrer sur d'autres initiatives. Pour ce faire, il est logique qu'une entreprise travaille avec ses éditeurs de logiciels – les entreprises qui créent, mettent à jour, corrigent et assurent le support de leurs produits sur une base régulière – afin d'atteindre cet objectif. Pour les produits plus

anciens, il est possible de passer à une version plus récente et entièrement prise en charge du logiciel de l'éditeur, à savoir une version conçue pour traiter les menaces de sécurité actuelles, et non celles datant de cinq ou dix ans.

Le risque n'est évité que si les correctifs sont obtenus auprès de sources fiables

Certaines entreprises ne procèdent à l'application des correctifs et à la maintenance de leurs logiciels qu'en cas de dégradation des performances, des fonctionnalités ou de la fiabilité, ou lorsqu'une menace pour la sécurité qui fait la une des journaux les oblige à voir quelles sont les failles de sécurité potentielles à combler. Parfois, dans ces circonstances, elles peuvent avoir recours à des sources d'information informelles telles que des sites web de conseil pour rechercher des solutions et, éventuellement, trouver des correctifs. Il peut s'agir d'une grave erreur qui entraîne immédiatement des risques si le correctif s'avère être malveillant ou s'il introduit une erreur technique. Compte tenu des problèmes de sécurité et de conformité actuels et de la fréquence accrue des cas de violations de la sécurité et des tentatives de piratage, de nombreuses entreprises ont décidé qu'elles devaient adopter une approche plus formelle, avec une surveillance, une application des correctifs et une maintenance régulières des logiciels comme fonctions essentielles de leurs opérations informatiques. L'envergure de ce type d'approche est bien adaptée aux besoins de conformité et de gouvernance et intègre une vision de haut niveau du « cycle de vie » des vulnérabilités et des correctifs. Cela contraste avec certaines solutions ponctuelles (par exemple, les pare-feu de base de données et les applications web proxy) qui prétendent contrer les vulnérabilités mais qui sont en fait limitées dans leur portée fonctionnelle et ne fournit en aucune façon une approche fondée vers le risque alignée sur les opérations.

Il est important d'appliquer le même niveau de précaution lorsque l'on s'appuie sur une relation de services de tiers pour la fourniture d'un support logiciel. Une définition inappropriée des exigences pourrait permettre à un fournisseur de services de tirer son épingle du jeu en mettant en œuvre des « solutions de contournement » sous forme de solutions partielles aux vulnérabilités pour clore les tickets de support. En plus de constituer un risque potentiel en raison de leur provenance inadéquate, ces dernières sont susceptibles d'entraîner une augmentation des coûts d'investissements en raison de l'éloignement des futures évolutions du logiciel, un facteur introduisant des coûts de régression à un stade ultérieur. Les éditeurs de services doivent en fin de compte démontrer qu'ils agissent en tant que partenaire des clients et de leurs fournisseurs de logiciels pour les besoins d'application de correctifs et de maintenance, et ils doivent répondre à trois critères importants :

- **Être un fournisseur de confiance.** Un fournisseur fiable et éprouvé possède des connaissances et une expertise en matière de sécurisation des données et des environnements informatiques d'entreprise, ainsi qu'une longue expérience de la sécurité et de l'assistance aux entreprises.

- **Avoir une expertise en matière de sécurité.** Un fournisseur doit avoir l'expérience de la sécurisation de l'ensemble du socle du système d'information, allant de l'infrastructure, aux bases de données et aux applications, et l'expertise pour fournir des ressources de support proactives et en temps réel à chaque fois que cela est nécessaire.

- **Proposer des offres complètes.** Un fournisseur doit proposer une suite complète et intégrée d'offres de sécurité et de support en constante évolution et faisant l'objet d'une innovation continue. Il doit en plus être en mesure d'aider un client à établir une culture axée sur la sécurité et la conformité informatique.

Les clients avec lesquels Omdia s'entretient indiquent qu'Oracle s'efforce à consacrer un nombre important de ressources et faire preuve de ces caractéristiques dans ses offres de support du socle Oracle, car il reconnaît le rôle essentiel que les systèmes Oracle jouent dans de nombreuses organisations.

De plus, le support Oracle offre des fonctionnalités et un niveau de sécurité bien supérieurs aux offres de support tiers, non-Oracle. Ces fournisseurs tiers ne peuvent pas fournir de correctifs de sécurité, comme le souligne Oracle, car ils ne peuvent pas modifier le code source d'Oracle et ils ne connaissent pas les détails techniques des vulnérabilités qu'Oracle corrige. Les clients de ces fournisseurs de support tiers ne bénéficient pas non plus des efforts continus d'Oracle en matière d'assurance de la sécurité, car tous les correctifs et patches précédents font déjà partie de chaque version suivante du logiciel Oracle.

Un client de longue date d'Oracle, une importante société de câble et de communication basée dans le sud des États-Unis, possède un important parc de 450 serveurs Oracle, dont six systèmes Oracle Exadata. Ces systèmes sont utilisés pour héberger l'entrepôt de données de l'entreprise et constituent ainsi une épine dorsale essentielle pour tous les processus métiers internes et externes. En fait, le client a été l'un des premiers à adopter Oracle Exadata a été témoin de l'évolution des services de support Oracle au fil du temps.

Lors du déploiement initial d'Oracle Exadata, la montée en niveau des logiciels a nécessité une mise à jour assez longue des micrologiciels et de l'intégralité de la plateforme, car l'Exadata est un système conçu pour offrir les avantages d'une plateforme intégrée. Fort de ces expériences, Oracle a introduit le support de niveau Platinum pour Exadata en 2012. Ce niveau de support offre une plus grande visibilité du système back-end et comprend des éléments proactifs tels que la fonction « Phone Home » qui permet aux ingénieurs support Oracle, en collaboration avec l'équipe de support du client, de détecter les problèmes potentiels avant qu'ils ne deviennent critiques.

Ce niveau de support amélioré offre également au client des capacités accrues en matière de déploiement de correctifs ; le client applique généralement des correctifs une ou deux fois par an en fonction des besoins et de la criticité (Le support Platinum prévoit quatre cycles de patchs par rack complet d'Oracle Exadata). Le client peut coordonner toute application de correctifs avec les ingénieurs du support Oracle afin d'assurer une bonne gestion des changements au sein des systèmes et de limiter toute perturbation pour l'entreprise, ses employés et ses propres clients.

Le client souligne qu'un déploiement de correctifs selon des cycles réguliers et une attention toute particulière sur la sécurité des systèmes d'information à l'échelle de l'entreprise permettent d'assurer que ses systèmes soient moins vulnérables et mieux sécurisés. Étant donné que l'Exadata alimente certains des systèmes les plus essentiels de ce client, une panne aurait un impact direct sur la capacité du service informatique en interne à respecter ses accords de niveau de service avec ses clients internes et externes (malgré la mise en place d'un stockage robuste, d'un plan de reprise après sinistre et de mesures de redondance). La collaboration avec le support Oracle de niveau Platinum permet au client de décharger une partie de son support interne sur les ingénieurs

support Oracle et de libérer ainsi ses équipes pour qu'ils se recentrent sur d'autres projets et initiatives. Le client s'attend à plus d'innovation au travers des procédures d'application de correctifs et de support Oracle avec des fonctionnalités encore plus automatisées. Oracle continue à travailler avec le client par le biais de réunions régulières et d'autres méthodes pour s'assurer du bon traitement de l'application des correctifs et du support du client.

Recommandations

- **Adopter tout changement de culture nécessaire pour que l'application de correctifs ne soit plus vue comme une option ou une considération purement opérationnelle ; veiller au contraire à ce qu'elle soit considérée comme un élément essentiel du bon fonctionnement de l'organisation.** Les organisations doivent comprendre que les décisions de réduire leur engagement à appliquer des correctifs de manière assidue peuvent avoir un impact négatif sur l'intégrité des logiciels et ne peuvent donc pas être envisagées uniquement dans un contexte opérationnel. Une application de correctifs inappropriée peut s'accompagner de vulnérabilités exploitables dans les logiciels de l'organisation, et tant que les correctifs ne sont pas déployés, le temps dont disposent les acteurs malveillants pour causer des pertes continue de s'allonger. Les implications qui en résultent en termes de sécurité, de conformité et de risques sont impossibles à résoudre sans l'application des correctifs nécessaires, et tout retard augmente la probabilité de coûts potentiels pour l'organisation.
  Au vu de ces éléments, les décisions relatives à la politique de mise à jour doivent être réexaminées dans un contexte métier large, et non pas seulement en tenant compte d'éléments tactiques et opérationnels tels que des licences supplémentaires ou des économies perçues en matière de support. Il faut éliminer les pratiques qui consistent notamment à avoir recours à des versions de logiciels non prises en charge, aux fonctions de support tiers mal gérées ou partiellement exécutées, ou encore à dépendre de sources de conseils de mauvaise qualité.

- **Bien que l'idéal soit d'appliquer des patchs sur tout ce qui est nécessaire, la priorisation doit se faire en fonction des risques.** Les environnements informatiques doivent être appréhendés du point de vue des risques, tant dans un contexte métier que technique. S'agissant du contexte métier, il doit tenir compte de la criticité relative des entreprises au niveau des services individuels, ce qui clarifie l'impact des risques au niveau de l'activité (par exemple, financier et lié à la réputation). Pour ce qui est du contexte technique, il doit prendre en compte les caractéristiques techniques des éléments constitutifs du service (par exemple, le système d'exploitation, la base de données, le matériel et les applications) et les difficultés éventuelles dues aux vulnérabilités particulières qui sont actives ainsi que leur exposition via le réseau à différents environnements de menaces (par exemple, si les ressources sont connectées à Internet).

- **Les informations de mise à jour doivent provenir de sources fiables, sinon leur utilisation constitue un risque.** La gouvernance de mise à jour doit indiquer quelles sont les sources de conseils sur les correctifs qui peuvent être considérées comme dignes de confiance. Par exemple, les éditeurs de logiciels sont la source d'informations faisant autorité sur la sécurité de leurs produits, tandis que l'Internet n'est pas une source fiable de conseils pour les correctifs. De plus, des sources telles que la Base de données nationale sur la vulnérabilité (NVD) et le Centre de coordination de

l'équipe d'intervention d'urgence informatique (CERT/CC) sont gérées et font autorité, alors que les outils logiciels génériques d'analyse des vulnérabilités peuvent être insuffisamment spécialisés pour fournir des informations fiables. Par exemple, ces outils peuvent ne pas reconnaître de manière suffisamment précise une version de logiciel (et, par conséquent, si un correctif a été appliqué), ce qui entraîne une inexactitude dans la notification des problèmes en cours et un effet « Garbage In, Garbage Out ». En tout état de cause, la création de rapports est le niveau le plus élevé de valeur que ces outils peuvent fournir, et les organisations sont toujours tenues d'évaluer et d'obtenir les correctifs nécessaires pour elles-mêmes. Les services de mise à jour externalisés sont une exception : dans ce cas, les accords de services doivent stipuler que seules les sources d'informations les plus fiables sur les correctifs peuvent être utilisées.

- **Les processus de mise à jour ne doivent pas être le maillon faible de la protection de l'organisation.** Les organisations doivent s'engager à appliquer des correctifs dans le cadre d'une maintenance de sécurité régulière et de leurs activités de maintenance récurrentes. L'application de correctifs est une mesure de protection proactive fondamentale et constitue un aspect essentiel de la bonne gouvernance de la sécurité informatique. L'absence de planification et de préparation des activités de maintenance périodique se traduira par des correctifs incomplets et, en fin de compte, par une dégradation de la posture de sécurité qui est directement liée aux préoccupations accrues des conseils d'administration en matière de sécurité.

Annexe

Lecture complémentaire

Federal Trade Commission (2015) Start With Security: A Guide for Business. Disponible sur <www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business> [Accès en janvier 2020]

Auteur

Alan Rodger, Analyste principal, Solutions d'infrastructure
alan.rodger@Omdia.com

Omdia Consulting

Omdia est une entreprise de données, de recherche et de conseil leader sur le marché, dont l'objectif est d'aider les fournisseurs de services numériques, les entreprises technologiques et les décideurs d'entreprise à prospérer dans l'économie numérique connectée.

Grâce à nos 150 analystes répartis dans le monde entier, nous offrons des analyses d'experts et une vision stratégique dans les secteurs des technologies de l'information, des télécommunications et des médias.

Nous créons un avantage commercial pour nos clients en leur fournissant des informations utiles pour soutenir la planification commerciale, le développement de produits et les initiatives de mise sur le marché.

En combinant de manière unique des données fiables, une analyse de marché et une expertise sectorielle verticale, nous sommes à même de favoriser la prise de décision en aidant nos clients à tirer profit des nouvelles technologies et à capitaliser sur des modèles métiers en évolution.

Omdia fait partie d'Informa Tech, une entreprise de services d'information B2B au service du secteur des technologies, des médias et des télécommunications. Le groupe Informa est coté à la Bourse de Londres.

Nous espérons que cette analyse vous aidera à prendre des décisions métiers éclairées et imaginatives. Si vous avez d'autres besoins, l'équipe de consultants d'Omdia peut aider votre entreprise à identifier les tendances et les opportunités futures. Veuillez nous contacter via :

https://www.omdia.com/contact/contact-us

consulting@Omdia.com

Avis de droit d'auteur et clause de non-responsabilité

L'ensemble des points de vue et/ou des avis exprimés dans ce produit par les auteurs ou les co-auteurs sont leurs points de vue et/ou avis personnels, et ne reflètent pas nécessairement les points de vue et/ou avis d'Informa Telecoms and Media Limited.