Livre blanc

La sécurité des APIs et du DevOps au cœur de la transformation numérique

Paul Fisher
Research Director

Juin 2017

CXP Group
BARC · le CXP · PAC

denyall
a Rohde&Schwarz Cybersecurity company

INTRODUCTION

En Europe, rares sont les décideurs qui n'ont pas encore pris conscience de la nécessité de transformer leurs activités et de passer aux applications numériques. Une organisation digitalisée est capable de réagir plus vite aux changements rapides qui transforment les conditions du marché. Elle est également à même d'utiliser plus efficacement les données pour accélérer le lancement des nouveaux produits et de s'adapter en fonction du retour des clients, tout en améliorant l'efficacité des infrastructures informatiques en place.

Avec la diffusion rapide des capteurs et des objets connectés, les acteurs économiques peuvent surveiller en temps réel les niveaux d'inventaire d'un magasin, ou anticiper des ruptures d'approvisionnement sur des articles en forte demande. Les données sont au cœur de la transformation numérique, et les applications basées sur les APIs permettent d'interpréter les schémas de données, les parcours clients et les transactions numériques, ou encore d'analyser les flux de données au sein même de l'organisation.

Bien que la transformation numérique soit considérée comme bénéfique pour de nombreuses entreprises, celles-ci font face à un nouveau défi, puisqu'elles doivent désormais sécuriser cette nouvelle architecture informatique, les applications et les opérations qui se mettent en place.

Par le passé, de trop nombreuses organisations ne se sont souciées de la sécurité informatique qu'après avoir « greffé » la technologie sur les systèmes existants, sans que celle-ci ne soit vraiment compatible avec les applications et le matériel déjà utilisés. La situation se complique d'autant plus lorsque des couches de sécurité supplémentaires y sont ajoutées, souvent en provenance de fournisseurs différents.

La transformation numérique offre aux entreprises une nouvelle opportunité : celle de se protéger correctement dès le départ et de créer un environnement intégré sécurisé. Les chefs d'entreprise doivent toutefois réfléchir différemment aux types d'outils et d'applications de sécurité requis.

Le nouveau modèle technologique utilisé par les organisations se compose de plus en plus d'applications mobiles et en ligne basées sur des APIs. Les limites et les barrières traditionnelles s'effritent peu à peu à mesure que les ressources d'entreprise sont mises directement à la disposition des clients et des partenaires externes par le biais des navigateurs web.

Les applications cloud et web sont de plus en plus souvent acquises ou conçues par des acteurs non traditionnels, comme les équipes DevOps opérant au sein des équipes opérationnelles ou des groupes de projets. On observe également un développement des communications machine-to-machine (M2M), qui remplace l'intervention humaine dans les transactions commerciales. Les technologies en amont des applications mobiles sont, elles aussi, en train d'être automatisées. Dans un cas comme dans l'autre, pour éviter que les données soient exposées à un risque quelconque, leur sécurisation s'impose.

La transformation numérique offre aux entreprises une opportunité nouvelle : celle de se protéger correctement dès le départ et de créer un environnement intégré sécurisé.

Mais la transformation numérique et l'accès aux ressources dans le cloud permettent maintenant d'introduire des changements rapides et de créer des produits innovants. Les ressources des réseaux et la capacité des serveurs peuvent être augmentés sur-le-champ, mais les applications de sécurité traditionnelles ne sont pas toujours conçues pour s'adapter aux changements incessants apportés aux données et au réseau.

Les nouvelles méthodes de travail sont de plus en plus prisées des CxO, qui considèrent la flexibilité et la transformation numérique comme des outils indispensables à l'amélioration de la rentabilité, de la compétitivité et de l'innovation.

Ce document examine les défis liés à la création d'un environnement sécurisé au sein duquel la transformation numérique, basée sur les APIs, peut s'opérer pleinement et délivrer les bénéfices concurrentiels qu'elle promet. Ce travail présente également les solutions que les entreprises doivent mettre en place afin d'atteindre cet objectif.

LES VULNÉRABILITÉS LOGICIELLES SONT UN DANGER POUR LES OPÉRATIONS NUMÉRIQUES

De nombreuses organisations utilisent des APIs afin de créer des applications mobiles exploitant leurs services web, basées sur des standards afin de réutiliser au mieux leur infrastructure informatique existante.

Les APIs sont souvent considérées comme le « Lego » de l'internet. Selon les estimations, quelque 9 millions de développeurs travaille sur des APIs privées, et environ 1 million sur des APIs publiques.[1]

L'utilisation d'APIs a contribué de manière notable à la croissance et au succès des plateformes de réseaux sociaux ; Facebook, en particulier, a grandement profité d'APIs ouvertes compatibles avec sa plateforme. Ses APIs ont permis à des milliers d'applications externes et d'organisations de s'intégrer à Facebook et d'exploiter les données de ses utilisateurs.

Les entreprises appliquent actuellement le même modèle. Cependant, à mesure que le nombre d'APIs et d'applications web augmente sous l'effet de la transformation numérique, le risque d'avoir des failles au niveau des codes et des vulnérabilités exploitables par les pirates informatiques, devient lui aussi de plus en plus élevé.

Ce risque s'accroît d'autant plus que les équipes DevOps conçoivent davantage d'applications en réponse aux besoins des équipes opérationnelles. La pression est telle que ces groupes produisent souvent de nouvelles applications qui seront peut-être publiées avant même d'avoir fait l'objet d'un contrôle-qualité complet et conforme aux protocoles en vigueur.

L'une des difficultés liées à la création d'applications sécurisées au sein d'une organisation, en incluant les applications web, est que la sécurité est trop souvent considérée comme la responsabilité des

[1] **https://techcrunch.com/2016/05/21/the-rise-of-apis/**

rédacteurs et des responsables de l'application des codes. Les organisations attendent souvent de ces derniers qu'ils vérifient eux-mêmes la qualité de leur travail. Par conséquent, certaines erreurs ont tendance à ne pas être détectées à mesure que l'échéance approche.

Le problème des APIs est notamment qu'elles peuvent dévoiler le fonctionnement d'une application – ce que les pirates peuvent exploiter si cela n'est pas dissimulé dès le départ. Parallèlement, à mesure que les APIs gagnent en complexité pour s'adapter à l'ère numérique et être toujours plus performantes, elles envoient davantage de requêtes dans les protocoles web et à d'autres applications ; la surface d'attaque s'élargit elle aussi et expose les failles et vulnérabilités à de plus nombreux utilisateurs finaux. Si les APIs ne sont pas protégées, les pirates ont en théorie la possibilité de s'attaquer à une myriade d'autres applications auxquelles les APIs vulnérables donnent accès.

Les vulnérabilités des APIs peuvent entraîner de sérieuses violations de données. En janvier 2014, environ quatre millions d'utilisateurs de Snapchat ont été touchés par une attaque au cours de laquelle des numéros de téléphone et des identifiants ont été dérobés de la plateforme.

Les pirates ne ciblent plus une seule et même application ; ils peuvent viser d'un seul coup de nombreux services par l'intermédiaire des APIs. Il y a donc beaucoup plus de risques qu'ils parviennent à accéder à des données sensibles ou à caractère personnel.

Les équipes DevOps cherchent avant tout à créer des applications intelligentes destinées à des utilisateurs internes ou externes à l'organisation. Elles ne réfléchissent pas forcément à la manière dont les applications web et mobiles et les APIs dont elles dépendent, fonctionneront lorsque les applications seront en service et que des utilisateurs non fiables y accéderont.

Mais sommes-nous en droit d'exiger que les DevOps accordent plus d'attention à ces questions de sécurité que ne devraient le faire eux-mêmes les utilisateurs finaux au moment d'ouvrir et d'utiliser ces mêmes applications ? À l'ère numérique, les utilisateurs finaux s'attendent aussi à ce que tout se fasse le plus rapidement possible.

COMMENT LES APPLICATIONS VULNÉRABLES PEUVENT ÊTRE INFILTRÉES ET EXPLOITÉES

Les pirates et les cybercriminels attaquent les APIs et les applications web de différentes façons lesquelles, si elles s'avèrent efficaces, peuvent entraîner des pertes de données, des dommages ou la disparition de services web, ainsi que l'injection de logiciels malveillants tels qu'un ransomware.

Les attaques visant les paramètres sont conçues afin d'intercepter et de manipuler les termes qu'un utilisateur final pourrait saisir dans un navigateur web. Il suffirait par exemple qu'un utilisateur introduise

l'adresse légitime du site de sa banque pour que le navigateur compromis ouvre un faux site prêt à enregistrer ses véritables identifiants et mot de passes.

Les pirates cherchent habituellement à exploiter les failles dans la gestion de l'identité, de l'authentification, de l'autorisation et du suivi des sessions, qui leur permettent de tromper les applications web et d'obtenir ainsi l'accès aux serveurs et aux données sensibles.

L'attaque de l'homme du milieu, ou « man-in-the-middle » en anglais, intercepte de véritables interactions entre les utilisateurs et dérobe toutes les données qu'ils échangent. Une fois le dispositif établi, les pirates peuvent se cacher et continuer à espionner les communications.

Les criminels peuvent également utiliser des commandes SQL dans des champs de recherche, des formulaires d'identification ou la barre d'adresses afin de contourner les barrières de sécurité intégrées aux applications web et accéder ainsi à des bases de données en ligne, des applications et d'autres sites web. Ils peuvent également y accéder à l'aide de l'API JSON ou du payload XML.

Les attaques cross-site scripting (XSS) sont menées à l'aide d'un code malveillant « injecté » dans un site web via une application web contenant une faille. Il s'agit d'un type d'attaque fréquent, mais aussi efficace, car bon nombre d'applications web ne sont pas testées afin d'éviter que ce genre de script malveillant soit ajouté par des personnes externes mal intentionnées. Une fois dans le système, les pirates ont le contrôle du site web. Ils peuvent ainsi tromper les utilisateurs et les inciter à leur communiquer des informations personnelles, voire s'introduire dans leur ordinateur.

Si un site web comporte une vulnérabilité XSS, un pirate peut alors rédiger un code qui s'exécutera lorsque d'autres utilisateurs ouvriront le site en question. Ces nouveaux utilisateurs se retrouveront alors dans l'environnement malveillant créé par le pirate.

Toutes ces attaques deviendront possibles en exploitant les failles des APIs et des applications web qui n'ont pas été sécurisées.

LE FACTEUR HUMAIN

Nous nous sommes jusqu'à présent intéressés aux défis techniques liés à la protection des applications web contre les attaques des cybercriminels et à la création d'APIs plus sécurisées en vue de limiter ces risques dès le départ.

Cependant, les utilisateurs finaux et les clients ignorent en grande partie ce qui se passe derrière l'écran de l'ordinateur ou du smartphone. À leurs yeux, les applications web sont un outil qui leur permet d'effectuer leur travail ou de correspondre avec les entreprises le plus rapidement et le plus efficacement possible. Quoi qu'il en soit, leur rapport à la technologie et aux applications évolue rapidement.

Les réseaux sociaux et les applications mobiles ont profondément transformé la manière dont les utilisateurs finaux interagissent avec les données et les applications. Pour de nombreuses personnes en dessous de la trentaine, le monde est déjà numérique à 100 %. et elles ne connaissent aucune autre façon de travailler ou de s'adonner à des activités de loisirs.

Elles s'attendent à avoir instantanément accès à des services haut de gamme et se montrent versatiles dans leurs choix. Elles acceptent de transmettre des données à caractère personnel à des entreprises sur internet afin d'accéder gratuitement à des services, soit par naïveté, soit par ignorance, et ne sont souvent pas informées ou conscientes des risques de sécurité auxquels elles s'exposent ainsi, tels que les attaques par ransomware ou les vols de données.

Les employés agissent de la même façon au sein de leur entreprise et de leur environnement de travail, tandis que des applications comme WhatsApp brouillent peu à peu les frontières qui séparent la sphère professionnelle de la sphère privée, puisque ses utilisateurs partagent sur une seule et même application ou plateforme, des données relatives à ces deux univers.

Les utilisateurs finaux apprécient la facilité et la rapidité des applications web et mobiles, mais les caractéristiques propres à la plupart des échanges numériques les exposent aux risques que nous avons déjà évoqués. Les fuites de données sensibles via les applications sont le plus grand risque que court une organisation. Cependant, le modèle dans le cadre duquel nous devons sécuriser l'informatique et les organisations a profondément changé.

Il existe aussi certains enjeux liés à la protection de la vie privée qui doivent être pris en considération. Facebook est souvent critiqué pour la quantité de données personnelles auxquelles les applications tierces peuvent accéder grâce à ses APIs (bien que tous les utilisateurs acceptent le partage de données lorsqu'ils s'inscrivent). Bien souvent, ces APIs se sont révélées vulnérables aux piratages.

Au sein des organisations, il se peut que les APIs soient également utilisées afin de permettre un accès vers et depuis des applications. Les informations du client ou d'autres données sensibles risquent d'être partagées illégalement, divulguées ou volées, car ces APIs auront peut-être été développées fortuitement dans l'organisation et qu'elles n'auront sans doute pas été testées correctement.

En bonne pratique, la sécurité doit être intégrée dans les applications au niveau du code, mais si cela n'est pas possible, les failles doivent être identifiées et supprimées automatiquement des applications web et cloud, avant qu'elles ne puissent être exploitées.

Le Règlement Général sur la Protection des Données (GDPR en anglais) de l'UE vient encore compliquer la donne, puisque les entreprises sont désormais entièrement responsables des données personnelles qui sont traitées et hébergées sur les serveurs, dans les centres de données et sur les réseaux. Les organisations qui ont recours à des APIs doivent également s'assurer que les données circulant d'une API à une autre sont sécurisées et permettent de respecter la réglementation, par exemple, on doit être en mesure de vérifier par exemple, que les données concernent une personne âgée de plus de 13 ans.

Ces mesures de sécurité et ces fonctionnalités doivent être inhérentes aux APIs et aux applications web, faute de quoi l'organisation sera jugée non conforme et passible d'amendes. Il y a aussi des implications pour les établissements financiers, qui sont tenus de respecter les obligations d'identification des clients finaux dans le cadre de la réglementation antifraude et anti-blanchiment.

A défaut de disposer d'APIs impénétrables, nous devons alors trouver de meilleurs moyens de défendre nos organisations contre les vulnérabilités engendrées par le processus DevOps.

COMMENT LES BONNES SOLUTIONS PEUVENT ATTÉNUER LE RISQUE DE VULNÉRABILITÉS DES APIS

Bon nombre d'outils de sécurité existants sont incapables de fonctionner à la vitesse requise par les organisations numériques. Ils ne peuvent pas fonctionner s'ils sont utilisés par plusieurs équipes de DevOps qui travaillent sur des projets différents. De même, il est pratiquement impossible de surveiller les données dans le cloud ou les données liées aux activités des employés et des clients, et d'empêcher les cyberattaques de se produire.

Cependant, bien qu'aucune entreprise ou organisation ne puisse espérer rester à l'abri de toute cyberattaque, il existe un certain nombre de méthodes permettant d'en réduire le risque de manière significative, et de limiter le plus possible leur impact.

Alors que le nombre et la gravité des menaces augmentent, la procédure de gestion des correctifs est trop lente, compliquée et obsolète. Les scanneurs de vulnérabilités génèrent souvent des faux positifs et se concentrent sur des ressources non critiques. Ils sont donc inefficaces et distraient l'attention des nouvelles architectures numériques et des applications web potentiellement vulnérables.

La nouvelle génération d'outils de gestion des vulnérabilités permet d'identifier les ressources-clés à travers l'organisation et priorise les vulnérabilités selon leur degré de criticité. Bon nombre des scanneurs de vulnérabilités classiques négligent ces nouvelles ressources, qui

caractérisent pourtant la structure numérique naissante. Celles-ci incluent les applications web, les APIs et les nouveaux services numériques, sans oublier les analyses traditionnelles des systèmes d'exploitation, des réseaux et des services de bases de données.

Un pare-feu est essentiel à la sécurité de n'importe quelle organisation. Cela étant, pour une organisation moderne, un pare-feu applicatif est tout aussi crucial. Ce dernier devrait être capable de gérer toutes les tâches liées à la sécurisation des services web, de la validation des schémas à l'authentification des agents, la signature des messages et le chiffrement des données.

Les prochains pare-feux réseau et pare-feux applicatifs devront être combinés afin de gérer de manière centralisée l'ensemble des applications web et des communications entre services, au sein d'un réseau d'entreprise et avec le monde extérieur. Ils devront aussi bloquer les attaques et les demandes de données en provenance d'agents non fiables. Le pare-feu applicatif détectera les pirates qui tentent d'exploiter les failles ou les vulnérabilités des APIs utilisées par les applications. Il pourrait s'agir d'attaques « man-in-the-middle » ou par déni de service conçues pour paralyser une organisation et ses services web.

Pour éviter les erreurs récurrentes et les faux positifs, l'organisation doit impérativement disposer de gestionnaires de vulnérabilités et de pare-feu applicatifs capables d'apprendre et de coopérer entre eux afin de valider les transactions web légitimes.

En même temps, les exigences des organisations numériques en matière de rapidité et d'agilité doivent également être prises en compte par les applications de sécurité, de manière à ce que les utilisateurs puissent continuer à accéder normalement aux applications. Ceci est d'une importance vitale pour les organisations qui utilisent des APIs et les applications web pour transformer leurs activités.

Enfin, si les fonctions peuvent commencer à être entièrement automatisées via les applications M2M (« machine-to-machine ») qui, comme nous l'indiquions précédemment, doivent être protégées, le facteur humain reste le maillon le plus faible de la sécurité pour n'importe quelle organisation.

Dès lors, il est souhaitable que l'organisation ait la capacité de surveiller l'activité des utilisateurs en temps réel, afin d'ajuster sa réaction en fonction de l'évolution de leur comportement ou de leur interaction avec l'application ou avec les données. La technologie doit pouvoir signaler ce type de comportement et permettre à l'organisation de déterminer si l'activité ou l'application est, ou non, anormale.

CONCLUSION

Pour prospérer à l'ère du numérique, les entreprises doivent arbitrer entre la création d'un environnement de travail agile pour les employés et les clients, et la maintenance des exigences de sécurité à travers les infrastructures existantes, le Cloud, les réseaux et applications.

En attendant que les APIs et les applications web et mobiles puissent être créées sans la moindre vulnérabilité, ce qui est improbable, la demande de services destinés à protéger les entreprises auraient dûment augmentée.

Les entreprises devront réévaluer leurs politiques et leurs systèmes de sécurité si elles souhaitent continuer à bénéficier de l'agilité qu'offrent les solutions basées sur les APIs, en local, mais aussi, et de plus en plus, dans le cloud.

A court terme, la solution pour remédier au problème des APIs corrompues ou mal programmées, consiste à améliorer la qualité des scanneurs et des outils de gestion des vulnérabilités pouvant être appliqués au sein de l'entreprise et étendus aux solutions dans le cloud, Amazon Web Services, Azure ou autres, et même aux achats informatiques fantômes (shadow IT).

Les systèmes de protection des applications web devraient également être disponibles sous la forme de services aux entreprises qui n'ont soit pas le budget nécessaire pour des solutions sur site, soit souhaitent externaliser cette activité.

Vu la fragilité ambiante des APIs internes, il sera alors important d'étudier méticuleusement de tels services avant de faire un choix. Le service doit être capable de détecter la totalité des attaques basées sur les vulnérabilités et d'en protéger parfaitement les processus.

Les entreprises continueront à mettre une pression importante sur les équipes DevOps, afin qu'elles conçoivent et produisent rapidement des applications et des APIs pour contribuer à la réalisation des objectifs.

Alors que l'économie de l'Internet et les programmes de transformation numérique accélèrent le développement, il devient essentiel de concevoir une couche de sécurité ultra-fiable, qui se composerait notamment des pare-feux applicatifs et des scanneurs de vulnérabilités, capables de gérer les vulnérabilités des APIs et des applications web.

Il se peut que dans un avenir proche, le législateur introduise des réglementations obligeant les organisations à démontrer la fiabilité et la sécurité de leurs codes pour pouvoir opérer en toute légalité.

À PROPOS DE DENYALL

DenyAll, une entreprise de Rohde & Schwarz Cybersecurity, DenyAll assiste les organisations dans leur transformation numérique, en s'assurant que les interactions avec les utilisateurs sont sécurisées et se déroulent parfaitement. Les services cloud et les équipements de DenyAll simplifient le travail des équipes de sécurité et DevOps chargées de la mise en place d'un environnement numérique sûr, et ce, tout au long du cycle de développement logiciel. Ils les aident à identifier les vulnérabilités, à les classer par priorité et à y remédier. Ils simplifient et renforcent l'accès des utilisateurs aux applications, où qu'ils se trouvent, quel que soit l'endroit où sont déployées ces applications. Ils bloquent également les attaques ciblant les applications web, les APIs et les services web qui soutiennent les applications mobiles, en évaluant le comportement des utilisateurs dans leur contexte afin d'y répondre de manière adéquate. Avec les outils de sécurité applicative de nouvelle génération de DenyAll, vos utilisateurs profitent d'une expérience numérique parfaitement sécurisée.

Pour plus d'informations

https://www.denyall.com
https://www.cloudprotector.com

Suivez-nous sur Twitter @DenyAllSecurity

A PROPOS DE PAC

Fondé en 1976, Pierre Audoin Consultants (PAC) fait partie du CXP Group, le premier cabinet européen indépendant d'analyse et de conseil dans le domaine des logiciels, des services informatiques et de la transformation numérique.

Il offre à ses clients un service complet d'assistance pour l'évaluation, la sélection et l'optimisation de solutions logicielles, l'évaluation et la sélection des ESN et les accompagne dans l'optimisation de leur stratégie de sourcing et dans leurs projets d'investissements. Ainsi, le CXP Group accompagne DSI et directions fonctionnelles dans leur transformation numérique.

Enfin, le Groupe CXP aide les éditeurs et les ESN à optimiser leur stratégie et leur go-to-market à travers des analyses quantitatives et qualitatives ainsi que des prestations de conseil opérationnel et stratégique. Les organisations et les institutions publiques se réfèrent également à nos études pour développer leurs politiques informatiques.

Capitalisant sur 40 ans d'expérience, implanté dans 8 pays (et 17 bureaux dans le monde), fort de 140 collaborateurs, le CXP Group apporte chaque année son expertise à plus de 1 500 DSI et directions fonctionnelles de grands comptes et entreprises du mid-market et à ses fournisseurs. Le CXP Group est composé de 3 filiales : le CXP, BARC (Business Application Research Center) et Pierre Audoin Consultants (PAC).

Pour plus d'information : www.pac-online.com

Suivez-nous sur Twitter @PAC_FR

PAC - CXP Group
8, avenue des ternes
75017 Paris
Tel. : +33 (0)1 53 05 05 53
info-france@pac-online.com
www.pac-online.com

GLOSSAIRE

Interface de programmation applicative (APIs – Application Programming Interface)

Considérées comme les « Lego » des environnements en ligne des entreprises, les APIs constituent un ensemble de conditions permettant à des applications de communiquer et de s'échanger des données. Elles sont publiquement disponibles dans le cas de certaines plateformes, comme Salesforce.com, ou écrites en interne pour des applications aussi diverses que variées.

Applications web

N'importe quelle application web peut être vulnérable aux attaques, soit directement, soit indirectement via des clients infectés. Cependant, les cibles sont souvent des applications de messagerie en ligne, des frontaux d'ERP et des portails d'infrastructure collaborative vu qu'ils offrent un accès direct aux données critiques de l'entreprise.

Pare-feu applicatif

Un pare-feu applicatif est installé devant un serveur web. Il filtre les attaques, transforme les demandes et les réponses, accélère le trafic de données, oblige le chiffrement des données sensibles et effectue des authentifications à la place du serveur.

Scanneur de vulnérabilités

Un scanneur de vulnérabilités effectue des tests de sécurité actifs sur des ressources ou sur l'ensemble d'une infrastructure informatique, y compris les infrastructures cloud distantes. Cette analyse permet d'identifier les failles potentielles (au niveau des applications, des systèmes et des réseaux).

DevOps

Terme désignant le processus intégré entre le développement logiciel et la mise en production informatique Utilisé de plus en plus pour décrire les équipes de programmeurs et de développeurs d'APIs qui travaillent en interne à un rythme élevé (selon les méthodes de développement « agile ») afin de faciliter la transformation numérique.

Amazon Web Services (AWS)

Amazon Web Services est la plus grande plateforme de services cloud au monde. Elle propose aux entreprises de toutes tailles une offre de services « sur étagère » : puissance de calcul, stockage de bases de données, fourniture de contenu, etc.

CXP Group

BARC · Ie CXP · PAC