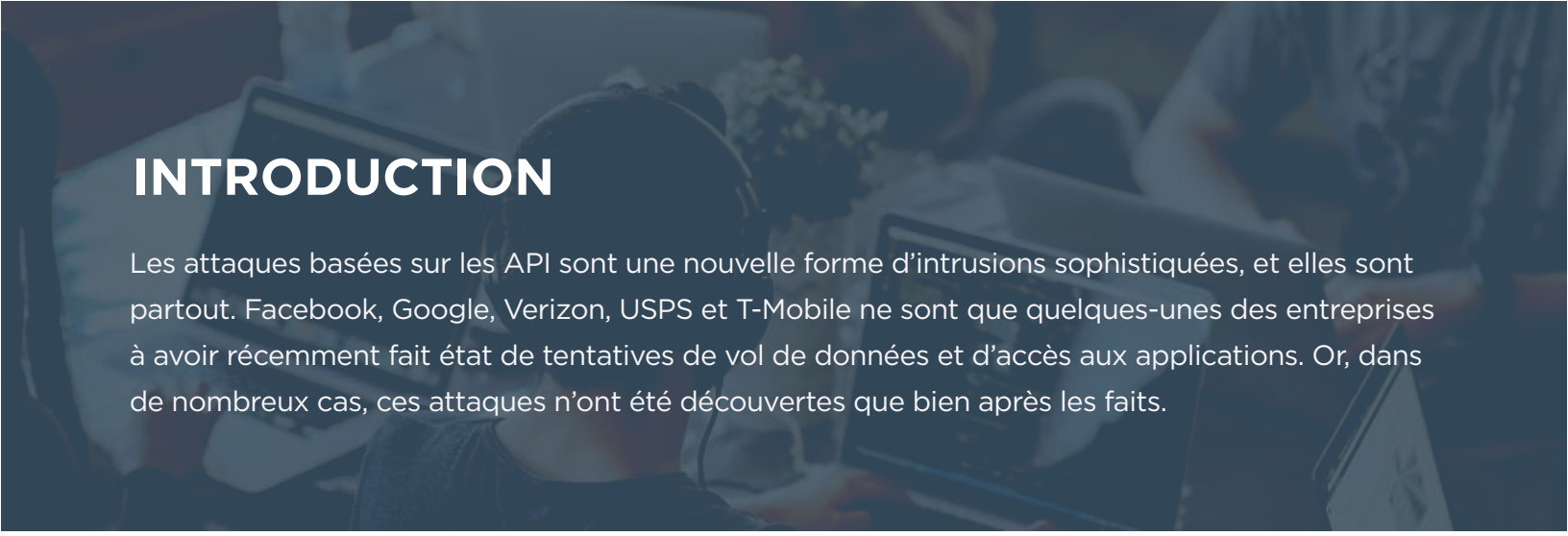
TOP 12 DES POINTS À RESPECTER EN MATIÈRE DE DEVOPS ET DE SÉCURITÉ IT POUR PROTÉGER LES API



INTRODUCTION

Les attaques basées sur les API sont une nouvelle forme d'intrusions sophistiquées, et elles sont partout. Facebook, Google, Verizon, USPS et T-Mobile ne sont que quelques-unes des entreprises à avoir récemment fait état de tentatives de vol de données et d'accès aux applications. Or, dans de nombreux cas, ces attaques n'ont été découvertes que bien après les faits.

L'une des principales raisons de cette rapide propagation, c'est qu'en général, il n'y a pas grand-chose qui sépare un pirate d'une API. Les malfaiteurs exploitent habituellement une vulnérabilité découverte en procédant à l'ingénierie inverse de l'API et en s'appuyant sur des procédures largement automatisées. Aucune solution fondée sur des signatures ou des règles n'est en mesure de déceler ces attaques, et il n'existe aucun moyen simple de tester le grand nombre de possibilités exploitables.

Pour combattre ces attaques, il ne suffit pas de contrôler les accès. Il ne s'agit pas non plus simplement de contrer des tentatives d'injection SQL ou d'attaques XSS. Il faut empêcher que soit pratiquée l'ingénierie inverse des API, qui montre aux pirates comment accéder facilement aux données et aux applications. Il faut protéger les API contre les individus qui se connectent avec des identifiants volés. Il faut déjouer les vols de données et d'informations confidentielles, et empêcher les hackers de paralyser des API par des attaques DDoS ciblées à faible volume, minutieusement réglées.

VOICI 12 BONNES PRATIQUES INDISPENSABLES POUR PROTÉGER VOS INFRASTRUCTURES D'API CONTRE LES CYBERATTAQUES.

1

Composez une équipe chargée de rechercher, d'identifier et de déployer des solutions et processus qui englobent les besoins de sécurisation spécifiques de vos API.

Diriger, c'est savoir reconnaître le problème en amont, orienter vers les bonnes techniques de sécurisation d'API et mettre en œuvre des solutions capables de suivre l'activité des API et de bloquer les menaces.

2

Testez la sécurité des API et des référentiels de données.

Et, ce faisant, « pensez comme un pirate. » Assurez-vous que le développeur d'API est impliqué dans les tests d'intrusion, car il saura bien reconnaître les éventuels points faibles et vulnérabilités. Exemple : dans la faille de LocationSmart, la sécurité des API a été contournée en modifiant simplement le type de charge utile.

3

Restez fidèle à une logique de sécurité tout au long du développement.

Il est recommandé de familiariser les équipes DevOps avec la sécurisation des API et de rappeler régulièrement aux développeurs la nécessité de soumettre toute tentative d'accès aux données à une autorisation dans les règles de l'art, entre autres bonnes pratiques.

4

Réalisez des scans, des tests et une surveillances automatisés de la sécurité.

Il est important de tester le code face aux vulnérabilités telles que celles définies par exemple dans le Top 10 de l'OWASP avant de passer à la production. Sans cela, des vecteurs d'attaque faciles à éliminer, comme une authentification faible ou des erreurs de configuration au niveau de la gestion et de la sécurité des sessions, pourraient exposer des données sensibles.

5

Déployez un système d'authentification et d'autorisation fort à tous les niveaux.

Lorsqu'elles sont adaptées, des mesures de sécurité telles que l'authentification multifacteur, l'authentification et l'autorisation en continu, et une validation correcte des jetons/cookies font déjà du bon travail.

6

Utilisez le contrôle de flux et le chiffrement TLS en permanence.

Cela prévient les attaques DoS et permet la transmission sécurisée de données entre différentes parties. Elles ne pourront pas être interceptées ni écoutées ou altérées.

7 Empêchez les serveurs d'applications d'envoyer des messages d'erreur contenant des traces du système.

Les hackers sont doués pour provoquer des erreurs lorsqu'ils sondent des API, dans l'espoir de recevoir un message d'erreur comportant des traces de débogage avec adresses IP, noms du système, etc.

8 N'enregistrez JAMAIS les noms d'API internes dans un DNS public.

Le mieux est de conserver tous les noms d'API en interne et de leur faire correspondre des noms externes qui seront utilisés pour les serveurs DNS. Cette pratique a également l'avantage de vous permettre de modifier les noms internes d'API sans avoir à modifier les entrées dans le DNS.

9 Suivez TOUTES les API.

Il existe des outils qui permettent de découvrir automatiquement les API. Qu'elles soient en production, utilisées pour les tests ou conservées à des fins de rétrocompatibilité, aucune n'est oubliée. Toutes les API doivent être surveillées par votre équipe de sécurité.

10 Effectuez des examens périodiques de l'activité des API afin d'identifier les anomalies.

Vous devez posséder une visibilité totale sur chaque tentative d'accès et chaque session, de manière à connaître parfaitement l'activité de vos API. Le manque de visibilité explique en partie pourquoi tant de failles n'ont été découvertes qu'au bout de plusieurs mois de vol ininterrompu de données.

11 Traitez toutes les API comme si elles étaient tournées vers l'extérieur.

Les API internes donc, mais aussi celles qui sont en laboratoire, car elles peuvent être à l'origine de fuites de données. Ces API sont souvent oubliées par les développeurs une fois déployées, et parfois même, les équipes DevOps ou de sécurité ne sont jamais informées de leur présence. Toutes les API doivent être protégées et sécurisées de manière uniforme, et leur activité doit être suivie à l'aide d'une piste d'audit afin d'identifier les comportements anormaux.

12 Misez sur les nouvelles technologies pour que votre entreprise ait une chance de s'en sortir.

Les malfaiteurs s'appuient sur l'intelligence artificielle pour infiltrer vos systèmes. Votre entreprise doit voir plus loin que les outils traditionnels et trouver de nouveaux moyens de déceler et stopper des attaques sur les API avant qu'elles n'aient un impact. Par exemple, PingIntelligence pour les API applique des modèles d'intelligence artificielle permettant d'inspecter en continu toute l'activité des API et d'établir des rapports en conséquence. Parallèlement, il détecte et stoppe les attaques qui se servent des API pour compromettre les données et les applications.

Aujourd'hui, l'une des plus grandes menaces consiste à ignorer la nécessité de faire davantage pour sécuriser vos API. Pour en savoir plus sur la manière de protéger vos API contre les cyberattaques et les fuites de données, téléchargez le rapport des analystes « Gartner: How to Build an Effective API Security Strategy »