Devolutions

SolarWinds et Solorigate : ce qui est arrivé, pourquoi c'est important et la suite des choses

IL Y A TELLEMENT DE VIOLATIONS DE DONNÉES CES TEMPS-CI

Il y a tellement de violations de données ces temps-ci qu'elles semblent toutes se transformer en un cycle sans fin de cyberdestruction. Il n'y a pas si longtemps, on était choqués par les histoires de cyberattaques. Vous vous souvenez de Target et Sony? Maintenant, on voit ça comme des évènements très prévisibles – comme une autre journée chaude dans une canicule ou une journée glaciale au milieu d'une vague de froid extrême.

De temps en temps, toutefois, il y a une cyberattaque qui capte l'attention du monde entier en raison de sa portée, de sa gravité, de sa taille et de sa singularité. Vous l'aurez deviné, **l'attaque qui coche toutes ces cases, c'est Solorigate.**

À propos de l'attaque

SolarWinds est une compagnie basée aux États-Unis qui développe des logiciels qui aident les grandes entreprises et les agences gouvernementales à gérer leurs réseaux, systèmes et infrastructures informatiques. L'un des produits de l'entreprise est SolarWinds Orion, une plateforme évolutive de surveillance et de gestion d'infrastructure. La bonne nouvelle est que de nombreuses entreprises utilisent ce produit pour simplifier leur administration informatique pour les environnements sur site, hybrides et SaaS. La mauvaise nouvelle, c'est que les pirates ont identifié et exploité une faiblesse – et ont élaboré ce qui est maintenant connu comme le piratage le plus sophistiqué de l'histoire.

En septembre 2019, des pirates ont infiltré les serveurs de SolarWinds et ont inséré du code malveillant dans le fichier **SolarWinds.Orion.Core.BusinessLayer.dll**, qui était une bibliothèque de codes appartenant à la plateforme Orion. En mars 2020, dans le cadre d'une mise à jour logicielle, cette DLL compromise a été distribuée (via une plateforme automatique) à environ 18 000 clients de la chaîne d'approvisionnement de SolarWinds à travers le monde. Ç'a créé une porte dérobée que les chercheurs en sécurité de Microsoft ont surnommée « Solorigate ». La porte dérobée est également appelée « SUNBURST », qui est le nom donné par les chercheurs en sécurité de FireEye qui l'ont découverte.

Une fois la porte dérobée établie, les pirates ont commencé à voler des informations d'identification et à se déplacer latéralement pour chercher des actifs et des comptes de grande valeur. L'attaque a persisté pendant plus de six mois. Elle a finalement été découverte par les chercheurs de FireEye en décembre 2020.

Ce qui change la donne avec Solorigate, c'est que les pirates ont utilisé la chaîne d'approvisionnement de SolarWinds pour infiltrer des victimes très médiatisées, qui (jusqu'à présent) comprennent :

- Le Pentagone
- Le département de la Sécurité intérieure
- Le département d'État
- Le département de l'Énergie
- L'administration nationale de la sécurité nucléaire
- Le trésor américain
- Microsoft
- Cisco
- Intel
- Deloitte

- *California Department of State Hospitals*
- L'Université Kent State
- FireEye
- Palo Alto Networks
- Mimecast (ça vient d'être annoncé fin janvier 2021 et ça aurait affecté 10 % des 36 000 clients de Mimecast – cliquez ici pour en apprendre plus).

Qui est à blâmer?

Il y a des spéculations selon lesquelles le gouvernement russe est derrière Solorigate. En janvier 2021, Kaspersky a publié une analyse qui suggère une similitude entre Solorigate et une autre porte dérobée appelée Kazur, qui a été liée au groupe *Turla Advanced Persistent Threat* (APT) basé en Russie. Ces allégations doivent encore être prouvées et il faut connaître les faits avant de tirer des conclusions. Cependant, on sait que le but de Solorigate était de générer de l'intelligence sur une longue période. Cette cyberattaque de type surveillance est généralement parrainée par les gouvernements.

Il est également important de noter qu'à l'heure actuelle, il n'y a aucune preuve que l'attaque était liée à une négligence chez SolarWinds. Rappelons quand même qu'une enquête est en cours et que plus de détails seront révélés dans les mois à venir.

Ce que les organisations doivent faire

Les organisations ne peuvent pas arrêter soudainement d'utiliser des logiciels, des produits et des applications tiers basés sur le nuage, parce que ces solutions sont intégrées à l'infrastructure de l'organisation. Et on ne parle pas seulement des grandes entreprises et des agences gouvernementales. Les PME dépendent fortement, et dans certains cas exclusivement, des offres SaaS tierces. Donc, la seule chose à faire est d'atténuer le risque. **Pour y arriver, on recommande d'adopter les stratégies suivantes :**

1. Effectuer une évaluation rigoureuse des fournisseurs

Lorsque les entreprises évaluent un fournisseur, elles se concentrent évidemment sur des éléments comme l'offre, l'assistance technique, la mise en œuvre, la tarification, etc. Sauf qu'il y a un autre aspect critique qui doit faire partie du processus : la conformité.

Les entreprises doivent faire une évaluation des risques de sécurité de chaque fournisseur par rapport à sa chaîne d'approvisionnement. Dans un article sur le site TechRepublic.com, Nick Fuchs, directeur principal de l'infrastructure, de la sécurité, du soutien et des contrôles à la clinique Springfield, conseille aux organisations de se poser les questions suivantes :

- Le fournisseur teste-t-il régulièrement sa force de résilience en matière de cybersécurité et fournit-il des preuves de la dernière analyse du code source et/ou de la pénétration des applications?
- Le fournisseur a-t-il mis en place des pare-feux d'application ou une segmentation du réseau pour restreindre l'accès aux programmes d'application ou au code source?
- Le fournisseur se conforme-t-il aux politiques et/ou réglementations pertinentes (par exemple, SOC 2, RGPD, CCPA, NIST, COBIT, ISO-27001/2) et peut-il fournir la preuve d'une certification à jour?
- Le fournisseur a-t-il un programme de sensibilisation des employés à la cybersécurité?

Les réponses à ces questions critiques réduiront considérablement l'exposition aux risques en identifiant les fournisseurs (et leurs logiciels, produits, applications, etc. associés) qui devraient être évités.

Cependant, il faut reconnaître que même avec une évaluation rigoureuse des fournisseurs, les attaques de la chaîne d'approvisionnement (comme Solorigate) sont généralement discrètes et collectent des données pendant de longues périodes. Comme l'a souligné TechTarget : « Souvent, les équipes de sécurité n'identifient pas ces aiguilles dans la botte de foin tant que les pirates ne passent pas aux étapes suivantes. C'est pourquoi, en ce qui concerne les risques liés à la chaîne d'approvisionnement, la recherche proactive des menaces est vraiment l'art d'explorer tout dans votre réseau auquel vous ne faites pas totalement confiance. »

2. Adopter la sécurité Confiance zéro

L'architecture Confiance zéro utilise la microsegmentation du réseau pour rapprocher le plus possible le périmètre des applications privilégiées et des surfaces protégées. Avec une telle sécurité, même si les pirates informatiques réussissent à compromettre un appareil, ils ne « toucheront pas le jackpot » et ne se déplaceront pas latéralement sur le réseau. Voici une liste des bonnes pratiques par rapport à l'approche Confiance zéro :

- Ajouter des technologies infonuagiques pour remplacer les services et systèmes hérités non authentifiés.
- Concevoir une architecture Confiance zéro en fonction de la manière dont les données se déplacent sur le réseau et dont les utilisateurs et les applications accèdent aux informations sensibles.
- Vérifier la confiance lors de l'accès à toute ressource réseau à l'aide de l'authentification multifacteur en temps réel.
- Organiser les utilisateurs par groupe/rôle pour prendre en charge les stratégies d'appareil.

- Utiliser le déprovisionnement automatique, ainsi que la capacité d'effacer, de verrouiller et de désinscrire les appareils volés ou perdus.
- Mettre régulièrement à jour les droits des utilisateurs finaux en fonction des modifications apportées aux rôles/tâches et des modifications des politiques de sécurité ou des exigences de conformité en vigueur.
- Former les utilisateurs finaux pour qu'ils participent à la solution dans le nouvel environnement de Confiance zéro (ça fait partie du « programme de sensibilisation à la sécurité des employés » que Nick Fuchs conseille plus haut).

Le fondateur et analyste principal de KuppingerCole Analysts, Martin Kuppinger, conseille fortement aux organisations d'étendre la Confiance zéro au-delà des réseaux et des systèmes de sécurité et de l'appliquer à tous les types de logiciels. Pour ce faire, M. Kuppinger conseille cinq mesures pour assurer continuellement la sécurité des logiciels :

- Mettre en place des pratiques de conception et de codage sécurisées, y compris des principes modernes de tests de logiciels.
- Suivre et analyser le code réutilisé comme les bibliothèques open source, pour savoir où il est utilisé, quelle version est utilisée, s'il existe des vulnérabilités et des correctifs connus, et quelles pratiques de codage sont utilisées par ceux qui fournissent le code.
- Effectuer une analyse de code statique et dynamique pour détecter les problèmes de sécurité dans le code. Cette analyse devrait également être étendue à des domaines comme la conception d'API.
- Intégrer tous les contrôles organisationnels dans un système de gestion de la sécurité de l'information (SMSI) complet avec des contrôles clairement définis et appliqués.
- Développer l'analyse opérationnelle pour inclure la télémétrie de sécurité et la criminalistique, parce que ça peut aider à détecter les anomalies dans les logiciels.

Comme le conseille M. Kuppinger : « La Confiance zéro doit être étendue et couvrir la sécurité des logiciels, pour les logiciels en tous genres (intégrés, COTS, SaaS) et indépendamment du fait qu'ils soient développés à l'interne ou à l'externe. "Ne faites pas confiance. Vérifiez." C'est aussi essentiel pour les logiciels que pour l'identité, les appareils ou les réseaux. »

3. Appliquer le principe du moindre privilège (POLP)

Une enquête récente d'ESG a révélé que les privilèges trop permissifs sont les vecteurs d'attaque les plus courants contre les applications basées sur le nuage. Pour diminuer les risques, toutes les organisations devraient mettre en place le POLP. C'est une approche selon laquelle les utilisateurs finaux ne bénéficient que de l'accès dont ils ont besoin pour effectuer leur travail – rien de plus.

4. Auditer et surveiller les comptes privilégiés

Les comptes privilégiés représentent l'une des plus grandes surfaces d'attaque et, à ce titre, les organisations doivent atténuer les menaces et les risques de deux manières. Premièrement, les organisations doivent auditer tous les comptes et déterminer ceux qui nécessitent réellement un accès privilégié et ceux qui n'en nécessitent pas. La recherche a révélé que 88 % des organisations avec plus d'un million de dossiers n'ont pas les limites d'accès appropriées, et 58 % des entreprises ont plus de 100 000 dossiers accessibles à tous les employés.

Deuxièmement, les organisations doivent surveiller toutes les sessions privilégiées pour identifier de manière proactive les comportements suspects et analyser ce qui pourrait suggérer des vols d'informations d'identification. Comme Solorigate l'a démontré, les pirates informatiques qui ciblent les chaînes d'approvisionnement font tout en leur possible pour cacher leurs traces et éviter d'être détectés. La surveillance des sessions privilégiées peut révéler des indices subtils qui mènent à un crime majeur.

Pour atteindre ces deux objectifs – c'est-à-dire l'audit et la surveillance des comptes privilégiés – les organisations doivent utiliser une solution PAM robuste, qui isole l'utilisation de comptes privilégiés et réduit le risque d'utilisation abusive. De cette manière, chaque système a son propre compte. Si un système particulier est compromis, les pirates ne pourront pas l'exploiter ou en profiter pour obtenir des accès ailleurs. Une solution PAM prend également en charge l'authentification à deux facteurs, le contrôle d'accès basé sur les rôles, la journalisation et la création de rapports, et l'injection des identifiants (pour que les utilisateurs finaux n'aient jamais besoin de voir les mots de passe).

5. Adopter une approche de défense en profondeur

La défense en profondeur ajoute plusieurs contrôles diversifiés dans un environnement, ce qui crée plusieurs couches de sécurité. Un pirate doit se frayer un chemin jusqu'au cœur, comme dans un oignon. C'est un moyen de ralentir autant que possible les attaques en utilisant une variété de défenses complexes entre les réseaux et les systèmes.

6. Mettre en place la séparation des tâches

La séparation des tâches (Segregation of Duties en anglais ou SoD) est une politique qui interdit à une seule personne d'être responsable de l'exécution de tâches contradictoires. Le but, comme souligné dans le cadre ISO/IEC 27001, est de réduire les opportunités de manipulation non autorisée ou non intentionnelle ou d'utilisation

abusive des actifs de l'organisation. Fondamentalement, lorsque plusieurs personnes sont impliquées dans des tâches sensibles, il y a moins de chances que quelqu'un essaie d'enfreindre les règles ou que des erreurs ne soient pas détectées.

La SoD est utilisée depuis de nombreuses décennies dans la comptabilité, la gestion des risques et l'administration financière. Cependant, ces dernières années, le concept s'est déplacé dans le domaine de la cybersécurité pour :

- Prévenir les conflits d'intérêts (réels ou apparents), les actes fautifs, la fraude, les abus et la construction de « silos » secrets autour des activités.
- Détecter les défaillances de contrôle comme les failles de sécurité, le vol d'informations et le contournement des contrôles de sécurité.
- Empêcher les erreurs occasionnées par des employés qui portent « trop de chapeaux ».

Conseils de notre Chef de la sécurité, Martin Lemay :

S'il y a une leçon à tirer de l'incident de SolarWinds, c'est que peu importe le partenaire dans la chaîne d'approvisionnement, votre organisation doit prendre en compte les risques de sécurité. Cette préoccupation doit être aussi forte que les considérations de disponibilité.

C'est en effet nécessaire de prendre en considération l'aspect « violation de données » lors de l'évaluation des risques liés à l'utilisation d'un nouveau produit ou service. Ça permet de s'assurer que la sécurité déployée autour de ces offres est proportionnelle à l'exposition au risque. Et si un bon processus de gestion des fournisseurs peut prévenir les risques liés à un fournisseur moins mature en matière de sécurité, ce n'est certainement pas une solution à toute épreuve.

En fait, même après avoir mis en application toutes les stratégies ci-dessus – qui devraient être considérées comme des incontournables et non comme des options – votre organisation peut encore être exposée à certains risques résiduels et ne pas avoir l'assurance à 100 % que vous souhaitez. Est-ce que ça signifie que la partie est déjà terminée et que les pirates ont gagné? Non, et voici pourquoi :

J'entends souvent des gens affirmer que si Microsoft et le gouvernement américain ne peuvent pas empêcher une menace comme Solorigate, alors quel espoir ont les petites organisations? Est-il inutile d'investir de l'argent et du temps sur des contrôles que même les plus grandes organisations (et les plus riches) ne peuvent pas contrer à 100 %? À ces personnes, je demande : « Laissez-vous votre voiture déverrouillée simplement parce qu'un voleur pourrait casser une vitre ? »

Ce que je veux dire, c'est que certains efforts pour réduire la probabilité ou l'impact d'une attaque valent la peine, étant donné les conséquences potentielles de l'intervention et de la récupération après un incident. Le problème n'est

pas nécessairement de perdre la voiture, mais tout ce qui est associé à cette perte. Cette déclaration ne s'applique pas uniquement aux risques liés à la chaîne d'approvisionnement, mais à tout risque. Peut-être que les rançongiciels sont plus importants que la chaîne d'approvisionnement pour votre organisation, et c'est correct, mais demander la transparence à un fournisseur ou à un service, C'EST GRATUIT – tout comme verrouiller une voiture quand on la stationne au centre d'achats.

Après avoir examiné les risques liés à la chaîne d'approvisionnement, votre organisation pourrait être surprise de découvrir comment certains contrôles ne sont pas SI coûteux et longs à utiliser.

Conclusion

Bien qu'il reste encore de nombreuses questions sans réponse, une chose est sûre: il y aura beaucoup plus d'attaques de la chaîne d'approvisionnement en 2021 et dans les années à venir. Les pirates sont connus pour arriver avec de nouveaux stratagèmes. Et, malheureusement, l'attaque de Solorigate a été un énorme succès. Ça a non seulement compromis certaines des plus grandes organisations du monde, mais elle a persisté pendant sept mois avant d'être détectée – et même dans ce cas, la découverte a été faite par une entreprise privée de cybersécurité (FireEye) et non par le US Cyber Command, qui admet qu'il a été « pris de court » par l'attaque.

La mise en œuvre des stratégies ci-dessus éliminera-t-elle la menace d'une attaque de la chaîne d'approvisionnement? Non, parce que c'est impossible. Sauf qu'elle atténuera considérablement les risques et peut également limiter la durée et la gravité d'une attaque. Toutes les organisations sont donc invitées à faire du renforcement de leur cybersécurité – pas seulement pour les attaques de la chaîne d'approvisionnement, mais pour toutes les menaces – leur priorité absolue. Comme le dit le vieil adage : « Une once de prévention vaut une livre de guérison! »