Rapport

Analyse d'une attaque de la supply chain via Salesforce

Comment prévenir les attaques de la supply chain menées via les intégrations tierces Salesforce ?

Sommaire

1. Introduction
Les risques liés à la supply chain numérique

Les entreprises d'aujourd'hui ont désormais accès à un vaste réseau de fournisseurs numériques. Grâce aux connexions internet haut-débit et au développement du cloud, elles peuvent facilement externaliser, pour développer plus efficacement leur activité.
Les solutions logicielles spécialisées sont désormais accessibles via des modèles SaaS. Les entreprises peuvent aussi acquérir des composants et des plug-ins pour personnaliser leur propre infrastructure.

La supply chain numérique offre une flexibilité inédite et une liberté inégalée. Elle permet aux entreprises de se doter rapidement de nouvelles capacités, pour accéder à de nouvelles opportunités. Mais il existe un prix à payer : une exposition accrue aux cyber-risques.

Face à un réseau constitué de milliers de maillons mobiles, il devient extrêmement difficile d'assurer une visibilité suffisante et d'identifier les vulnérabilités potentielles.

Les pirates informatiques cherchent à tirer profit de cet état de fait. En attaquant les connexions tierces, comme celles des fournisseurs de SaaS ou des développeurs de plug-ins logiciels, ils cherchent à contourner les défenses de sécurité des entreprises qu'ils ciblent, pour frapper en plein cœur de leur réseau. La connexion obtenue peut être exploitée pour déployer des malwares (comme des ransomwares ciblés hautement destructeurs), pour exfiltrer des données stratégiques ou pour établir un command-and-control.

Gartner® a classé les risques de la supply chain parmi les grandes préoccupations 2022 en matière de gestion des risques. « D'ici 2025, 45 % des organisations à travers le monde auront subi des attaques de leur supply chain logicielle, soit trois fois plus qu'en 2021 »[1].

D'après les estimations, les attaques de la supply chain ont d'ores-et-déjà triplé en 2021. Certaines des plus grandes violations de données de l'année dernière sont liées à des attaques de la supply chain.

1. Communiqué de presse de Gartner, « Top Trends in Cybersecurity 2022 », publié le 18 février 2022.

Par les analystes : Peter Firstbrook, Sam Olyaei, Pete Shoard, Katell Thielemann, Mary Ruddy,Felix Gaehtgens, Richard Addiscott, William Candrick. GARTNER est une marque déposée et une marque de service de Gartner, Inc. et/ou de ses sociétés affiliées aux États-Unis et dans le monde, et est utilisée ici avec autorisation. Tous droits réservés.

Log4Shell

Cet exploit très médiatisé a affecté la célèbre bibliothèque java Apache Log4j 2 utilisée pour enregistrer les messages d'erreur. La vulnérabilité, baptisée CVE-2021-44228, permettait aux pirates informatiques de contrôler à distance les appareils exécutant certaines versions de Log4j 2 par le biais de messages textes. La faille a été identifiée et rapidement corrigée en décembre 2021, mais elle existait peut-être depuis 2013. D'après les estimations, près de la moitié des organisations à travers le monde auraient pu être ciblées par cette vulnérabilité à un moment donné.

Okta

En mars 2022, le fournisseur d'authentification multifactorielle sécurisée Okta a annoncé avoir subi, en janvier, une importante violation de sécurité ayant affecté des centaines de clients. L'attaque, qui a débuté par le piratage d'un sous-traitant d'Okta, a montré comment les connexions tierces peuvent être ciblées et exploitées. Le groupe de pirates, connu sous le nom de Lapsus$, a pu s'infiltrer sur les réseaux des clients et accéder à leurs données via un outil de bureau à distance.

Office 365

Les pirates informatiques ciblent de plus en plus l'environnement étendu d'Office 365 dans le cadre de leurs attaques de phishing ciblées. Les victimes reçoivent un e-mail les invitant à se connecter à leur compte 365 et à vérifier une nouvelle application. À l'Inverse des attaques de phishing traditionnelles, cet e-mail renvoie vers la véritable page de connexion Office 365 de l'utilisateur. La menace se situe au niveau de l'application à vérifier : elle permet au hacker d'accéder aux fichiers et aux e-mails de l'utilisateur. Comme elle se trouve déjà dans l'environnement concerné, l'application malveillante peut contourner l'authentification multifactorielle (AMF).

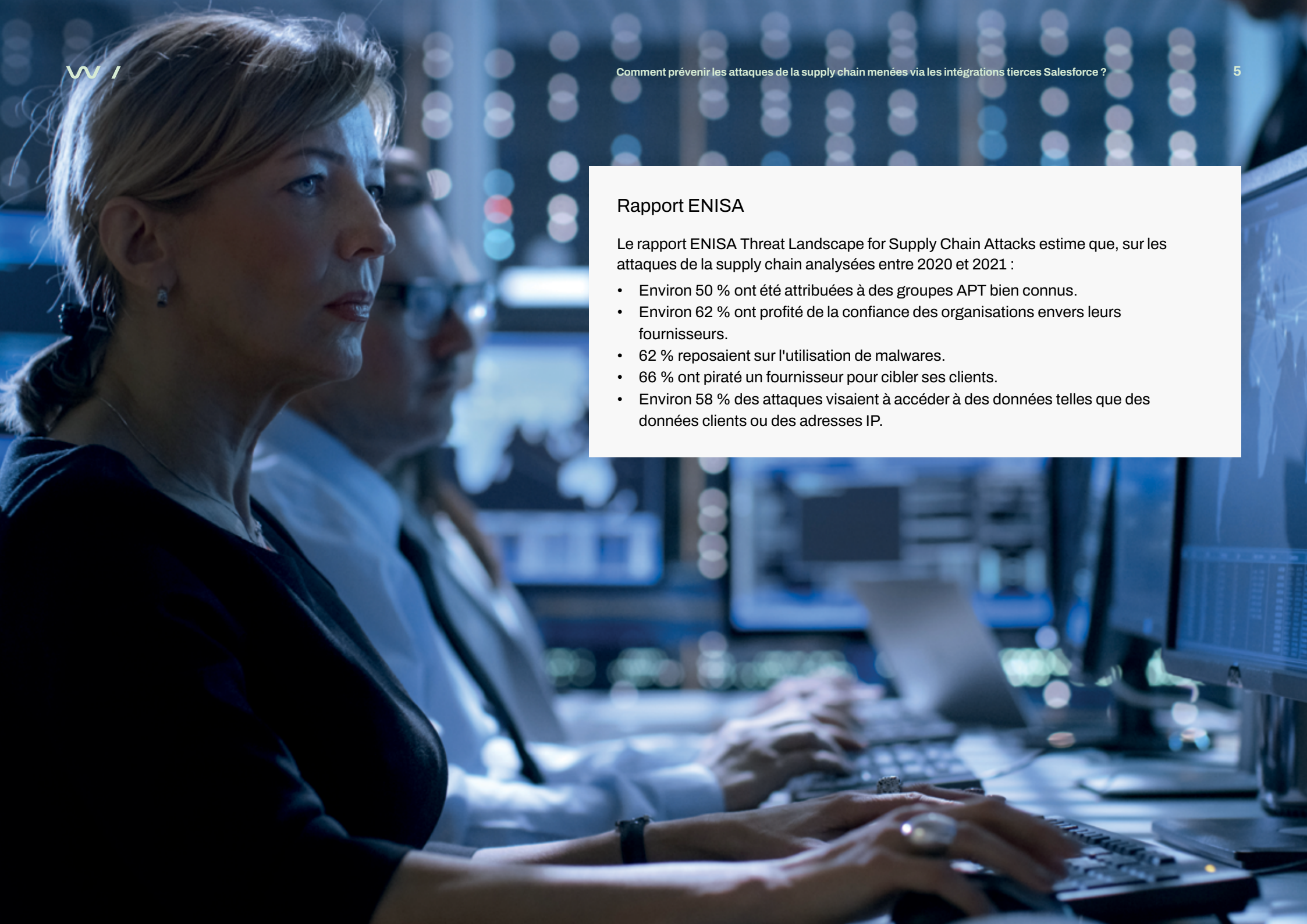
SolarWinds

Bien qu'elle se soit produite en 2020, l'attaque SolarWinds reste l'exemple le plus notoire d'une attaque de la supply chain numérique. Largement soupçonnée d'être le fait de hackers soutenus par la Russie, cette attaque sophistiquée, menée sur plusieurs fronts, a ciblé la solution Orion de Solar-Winds. Les pirates informatiques ont secrètement injecté un code malveillant dans une mise à jour du logiciel, ce qui leur a permis d'accéder aux réseaux de milliers d'utilisateurs, dont des organismes gouvernementaux tels que le Trésor américain et le ministère américain de la Justice.

Ces attaques montrent pourquoi toutes les organisations doivent prendre au sérieux les risques liés à la supply chain numérique. Une seule application corrompue peut affecter des milliers d'organisations dans le monde. Les entreprises doivent comprendre l'ampleur du danger et s'efforcer de mettre à niveau leur sécurité pour que celle-ci puisse faire face à l'augmentation des interconnexions numériques.

Tout service ayant fait l'objet d'une initiative de transformation numérique ou d'intégration de logiciels tiers est vulnérable aux attaques de la supply chain. Et plus la fonction commerciale de ce service est importante, plus les risques sont élevés.

Plus de 150 000 organisations dans le monde utilisent le système CRM Salesforce. À ce titre, Salesforce est l'un des environnements logiciels les plus exposés aux attaques de la supply chain. Bien que l'infrastructure de Salesforce n'ait encore été impliquée dans aucun incident majeur, des attaques réussies ne sont pas à exclure à l'avenir.



Rapport ENISA

Le rapport ENISA Threat Landscape for Supply Chain Attacks estime que, sur les attaques de la supply chain analysées entre 2020 et 2021 :

- Environ 50 % ont été attribuées à des groupes APT bien connus.
- Environ 62 % ont profité de la confiance des organisations envers leurs fournisseurs.
- 62 % reposaient sur l'utilisation de malwares.
- 66 % ont piraté un fournisseur pour cibler ses clients.
- Environ 58 % des attaques visaient à accéder à des données telles que des données clients ou des adresses IP.

2. Les intégrations tierces, sources de nouvelles menaces pour Salesforce

La plateforme Salesforce joue un rôle-clé dans le quotidien de nombreuses organisations. Elle sert de socle à leur stratégie d'expérience numérique et de gestion de la clientèle. Pour utiliser Salesforce le plus efficacement possible, les entreprises cherchent à personnaliser et à configurer leur environnement selon leurs besoins opérationnels spécifiques.

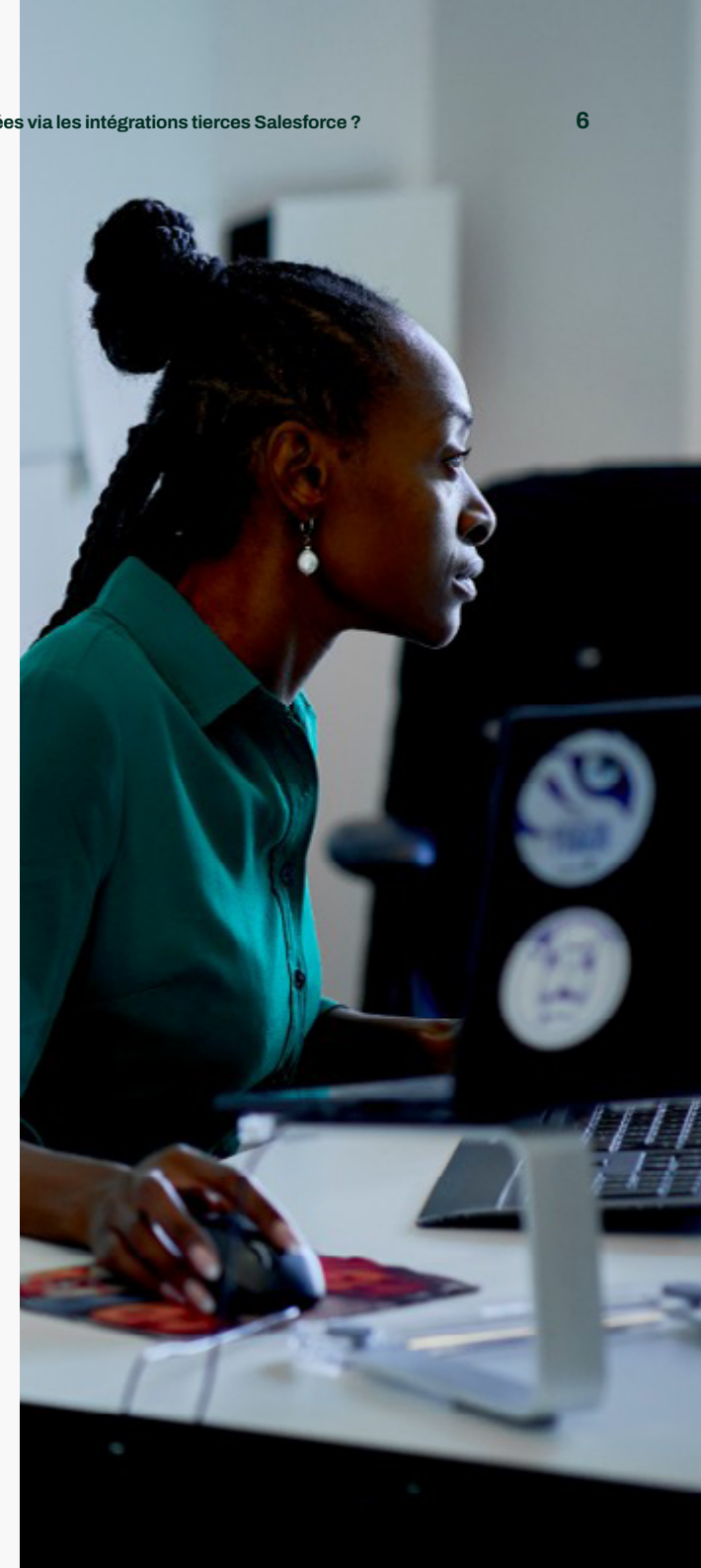
La plateforme Salesforce peut être fortement personnalisée et enrichie avec des applications, des composants et des services cloud tiers. Salesforce AppExchange, la boutique d'applications officielle de la plateforme, propose plus de 3 400 applications. Les entreprises peuvent également connecter leurs environnements Salesforce à des systèmes ou applications externes via des API SOAP ou REST. Ces systèmes peuvent être hébergés dans différents environnements cloud et utiliser de nombreux logiciels propriétaires ou open-source. Salesforce prend également en charge l'intégration traditionnelle par e-mail ou par formulaire web.

Les entreprises sont assurées de trouver une intégration tierce pour toutes les options et extensions qu'elles souhaitent appliquer à leur environnement Salesforce. Toutefois, chaque nouvel ajout accroît l'exposition de l'entreprise au risque d'attaque de la supply chain.

Les menaces potentielles sont nombreuses :

Les fausses applications

Dans le pire des cas, les ressources tierces peuvent avoir été créées spécifiquement comme vecteurs d'attaque. Les groupes criminels organisés téléchargent des applications légitimes et réalisent une rétro-ingénierie pour créer des clones corrompus, qui renferment des codes malveillants. Ils les mettent ensuite à disposition pour téléchargement. Bien qu'aucun cas n'ait été signalé dans l'AppExchange de Salesforce, ce problème est de plus en plus courant dans Android, Google et d'autres sources. Les exigences de vérification strictes de Salesforce font de l'AppExchange une source raisonnablement sûre, mais cela ne vaut pas pour les nombreuses autres ressources logicielles en ligne. Il est également difficile de contrôler ce que fait une application après son installation, ce qui laisse la possibilité d'utiliser des applications déjà validées à des fins malveillantes.



Logiciels piratés

Dans ce cas de figure, les cybercriminels peuvent chercher à exploiter la supply chain numérique en ciblant le fournisseur de logiciels lui-même. Les attaques de SolarWinds et Kaseya en constituent les meilleurs exemples. Les pirates informatiques utilisent des applications légitimes et préalablement approuvées comme vecteur d'attaque, de manière à contourner un grand nombre de mécanismes traditionnels de sécurité. Ce type d'attaque, qui nécessite des moyens importants, est souvent le fait de groupes organisés qui cherchent à cibler des grandes organisations ou à frapper un grand nombre de victimes via des vecteurs sophistiqués comme les ransomwares. Les utilisateurs individuels de Salesforce ne constituent pas des cibles de choix pour ces attaques mais Salesforce et ses intégrateurs de premier plan peuvent, eux, être visés.

Code vulnérable

Les vulnérabilités logicielles sont omniprésentes. 19 733 d'entre elles ont été signalées en 2021. Un chiffre record. Ainsi, même sans l'intervention de hackers, un actif numérique peut introduire des cyber-risques. Même l'application la mieux testée contiendra inévitablement au moins quelques vulnérabilités.

Ainsi, une seule application, un seul composant tiers non-sécurisé peut suffire à ouvrir la voie à une intrusion informatique.

Un environnement complexe, avec des centaines d'applications et de plug-ins supplémentaires, devient donc vite extrêmement difficile à gérer. Dans une telle fourmilière, même les meilleurs administrateurs ont des difficultés à assurer une gestion efficace.

Les plateformes d'infrastructure as-a-service (IaaS) plus complexes, comme AWS, nécessitent de mobiliser d'emblée les équipes informatiques, réseau et sécurité. Les administrateurs système et les équipes chargées de l'infrastructure sont de plus en plus conscients des défis liés à la sécurisation de ces environnements. Pour autant, Salesforce est souvent considéré comme une plateforme autonome et autosécurisée et ne bénéficie pas de la même attention.

La menace interne

Comme tout environnement numérique, Salesforce peut devenir très vulnérable lorsqu'il n'a pas été correctement configuré.

Lorsque les applications sont mal configurées et que les contrôles d'accès sont insuffisants, il devient beaucoup plus facile pour des hackers de s'infiltrer. Les pirates informatiques sont d'ailleurs passés maîtres dans l'art de repérer les comptes utilisateurs mal sécurisés et les applications utilisant des paramètres par défaut.

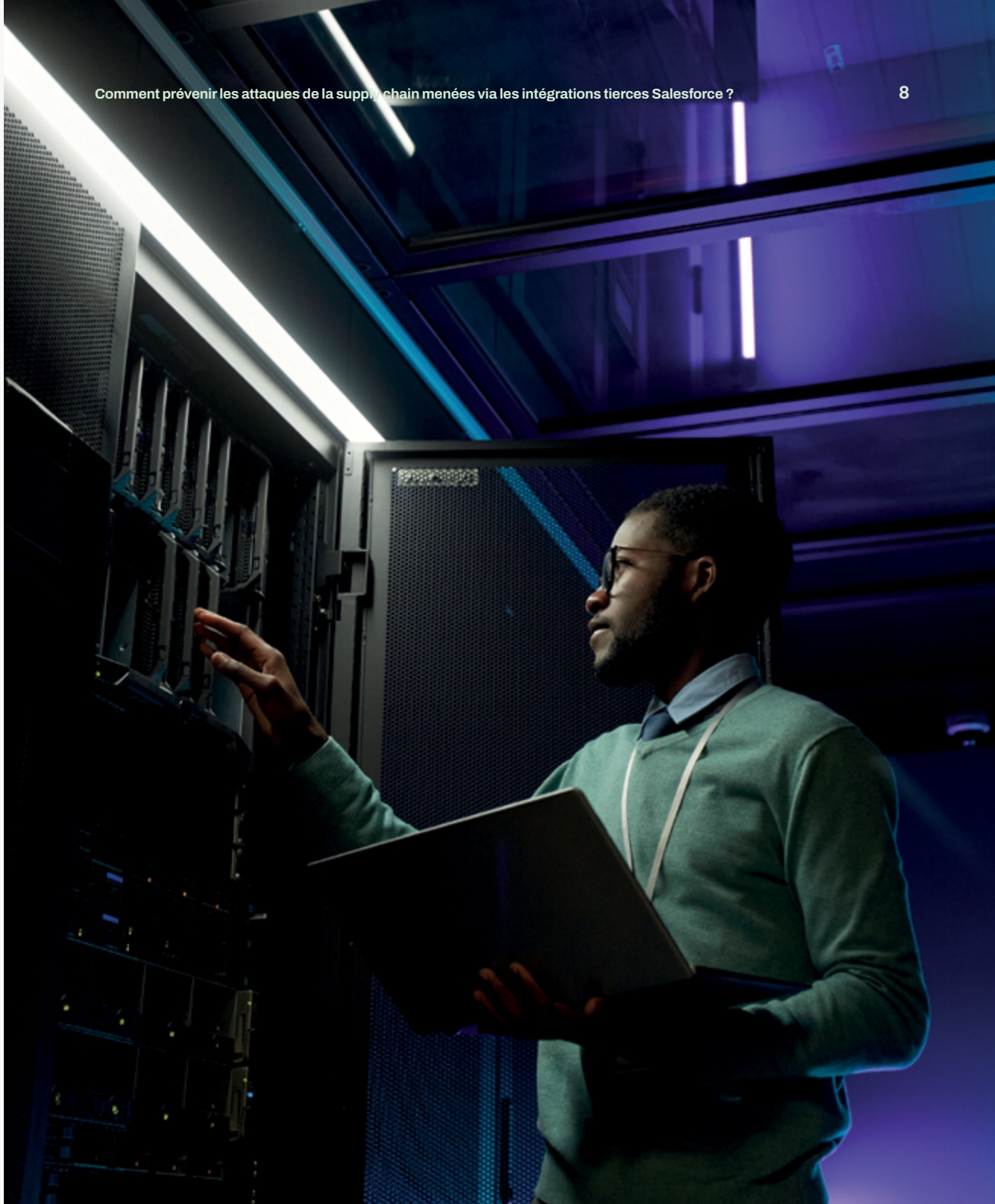
Il s'agit là d'un risque majeur, qui existe même sans l'introduction d'applications et de composants tiers. Les grandes organisations sont particulièrement concernées : du fait du manque de coordination entre les différents bureaux et services, leur environnement abrite souvent des applications et des plug-ins redondants pour les mêmes taches. Les petites entreprises, quant à elles, disposent d'un fonctionnement plus simple et rationnalisé, mais elles sont plus susceptibles d'ajouter de nouveaux composants à l'improviste, sans les mesures de précaution qui s'imposent.

Pour réduire les risques, Salesforce a pris certaines mesures visant à mettre en évidence les mauvaises configurations de partage. Salesforce Optimizer, une application Lightning Experience, permet notamment d'effectuer des contrôles réguliers et de mettre en évidence tout problème potentiel concernant les utilisateurs invités. Des mises à jour sont aussi venues modifier les paramètres par défaut, pour les rendre plus sûrs.

3. Déroulement d'une attaque de la supply chain via Salesforce

Du fait de sa popularité et de sa complexité, la plateforme Salesforce peut être ciblée par différents types d'attaques de la supply chain numérique.

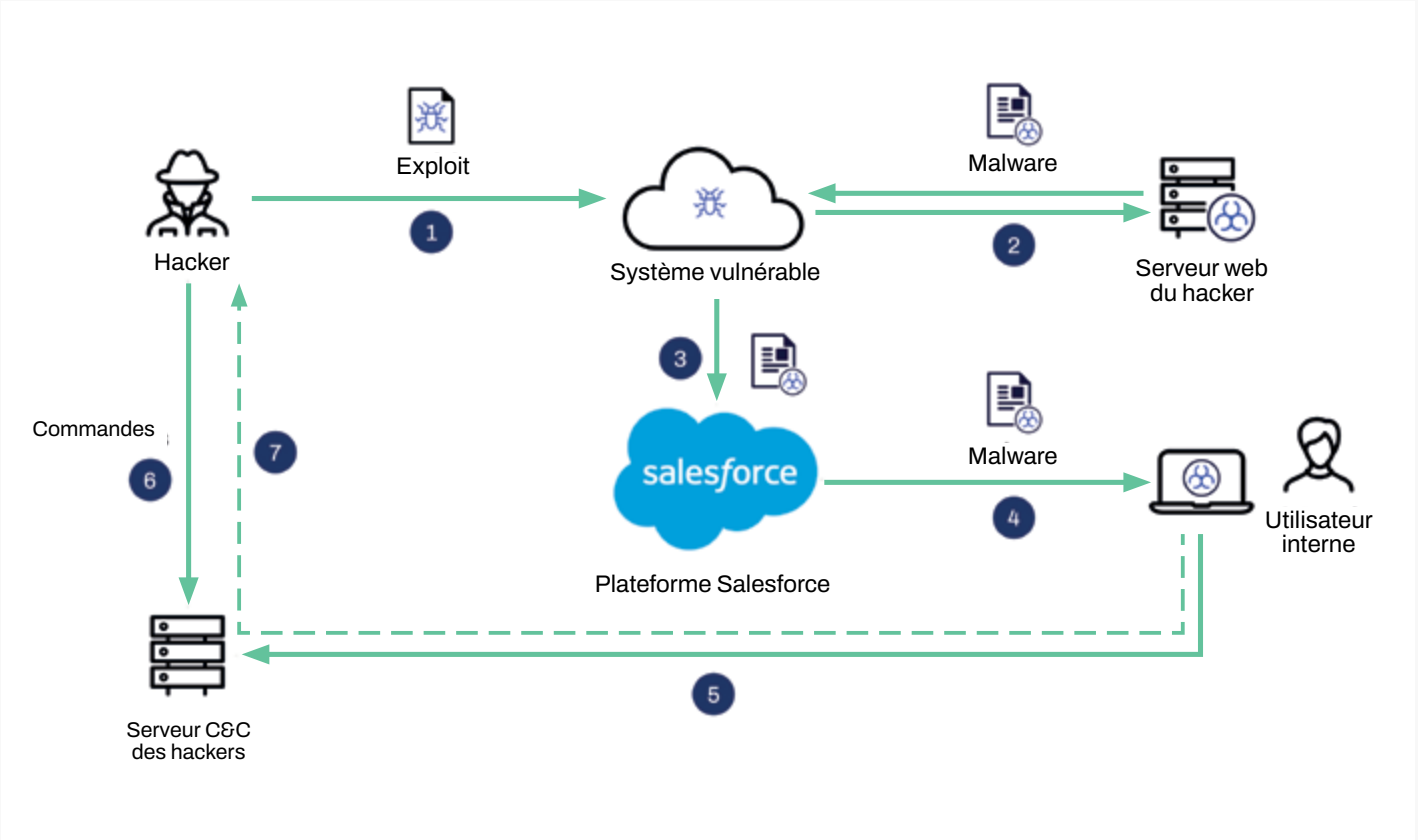
Voici deux exemples de scénarios d'attaque.



Scénario 1 : Système tiers vulnérable

Ici, le pirate informatique identifie une vulnérabilité dans une application logicielle intégrée à Salesforce, par exemple un outil qui récupère des données à des fins d'analyse. Il décide d'exploiter cette vulnérabilité pour établir un accès distant au système. L'application vulnérable est connectée à Salesforce via une API. Or, les API se voient généralement attribuer un niveau de confiance plus élevé que les utilisateurs. Le hacker peut donc accéder au système avec une certaine facilité.

Il peut alors chercher à voler ou à endommager des données dans Salesforce, ou bien utiliser la plateforme pour aller plus loin. Il peut, par exemple, diffuser des documents et URL malveillants au sein de l'environnement Salesforce en question. Des utilisateurs peu méfiants (des employés, des clients et d'autres contacts) risquent alors de cliquer et de les télécharger. Le hacker pourra alors exploiter leur accès au système pour poursuivre son attaque sur le reste de l'infrastructure informatique de l'entreprise.



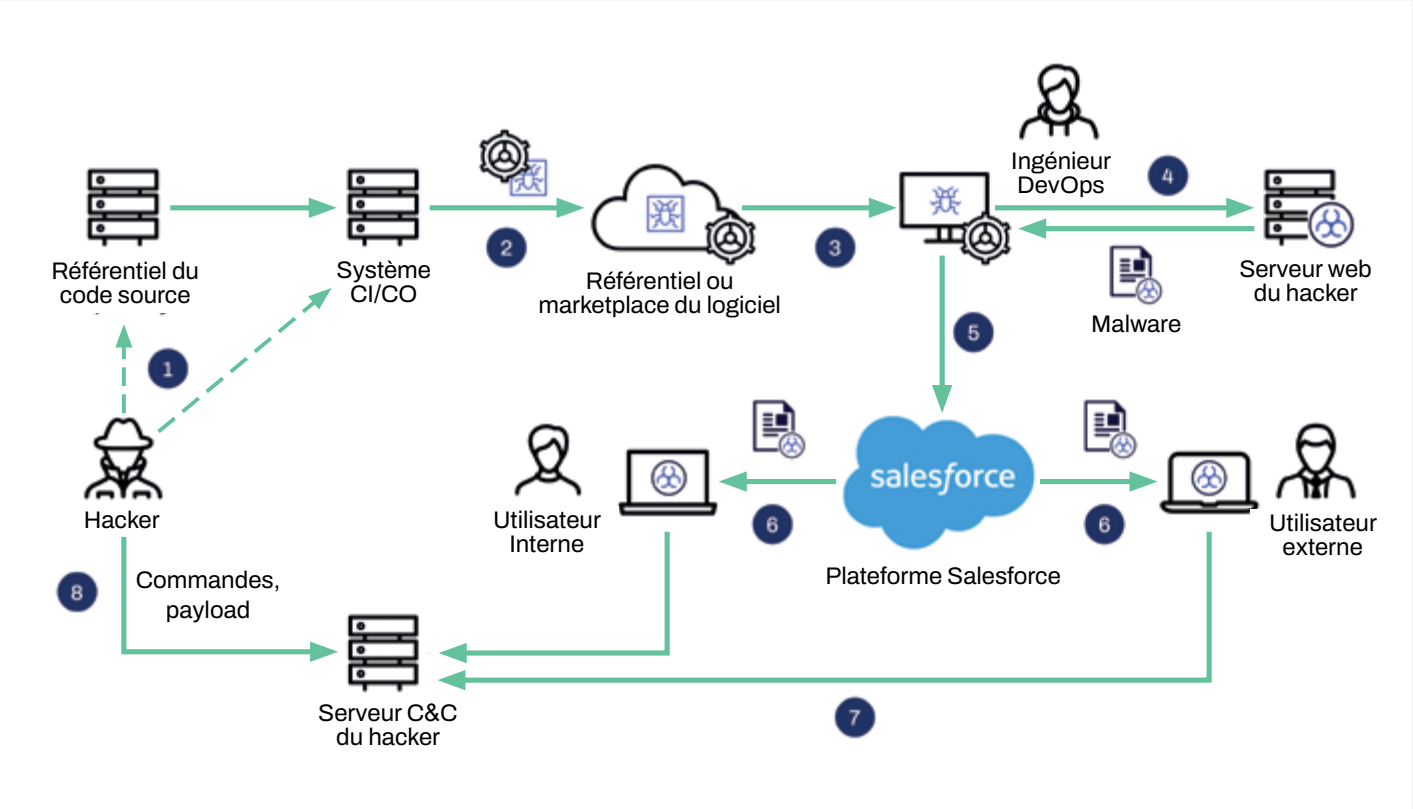
1. Le pirate informatique exploite la vulnérabilité dans le système cloud (ou on-prem) tiers connecté à Salesforce.
2. Il exécute le code d'exploitation pour accéder au système vulnérable et y télécharger le malware à partir du serveur web.
3. Il « injecte » le malware dans la plateforme Salesforce. Le malware est, par exemple, intégré à un message Chatter ou uploadé dans la bibliothèque commune de fichiers.
4. Un utilisateur interne télécharge un fichier contenant le malware et l'ouvre sur son appareil. Il ne remarque rien d'anormal.
5. Le malware se connecte au serveur de commande et de contrôle (C&C) hébergé par le pirate informatique.
6. Le pirate informatique découvre que le malware a réussi à se connecter au serveur C&C. Il interagit avec le malware en envoyant des commandes ou des payloads supplémentaires.
7. Il exfiltre des données sensibles de l'ordinateur de l'utilisateur interne et/ou de Salesforce.

Scénario 2 : Outils de développement corrompus

Dans ce scénario, le hacker cible d'abord le référentiel de code source ou le système CI/CD d'un fournisseur logiciel pour introduire un code malveillant dans son produit. L'accès initial au système peut se faire de plusieurs manières. La tactique la plus courante consiste à utiliser une attaque de phishing pour obtenir des identifiants utilisateurs, comme cela a été le cas dans l'attaque SolarWinds.

L'application ou le composant corrompu est ensuite intégré à l'environnement Salesforce : le hacker peut alors s'en servir pour infecter d'autres utilisateurs et endpoints. Il peut alors atteindre tous ses objectifs malveillants. Le processus peut même être répété si le hacker choisit d'utiliser l'organisation ciblée pour mener son attaque plus en avant dans la supply chain.

Soit le pirate informatique accède directement à l'instance Salesforce, soit il met en place une porte dérobée et attend que l'intégrateur ait par la suite un accès de production. Les développeurs ont tendance à faire aveuglément confiance à la sécurité de leurs outils, surtout s'ils proviennent d'un fournisseur connu. Pourtant, comme en témoigne l'attaque de SolarWinds, même un fournisseur de confiance peut être source de danger s'il est la cible de cybercriminels organisés.



1. Le pirate informatique examine le référentiel public du code source. Il recherche des identifiants pour le système CI/CD et parvient à y accéder.
2. Il « injecte » une payload spécialement conçue pour le paquet logiciel du système CI/CD et disponible dans le référentiel officiel ou sur la marketplace.
3. L'ingénieur DevOps se procure le paquet logiciel contenant la payload sur le référentiel/la marketplace et l'exécute sur son ordinateur.
4. La payload télécharge le malware à partir du serveur web du hacker.
5. L'ingénieur DevOps accède à Salesforce : le malware est uploadé dans Salesforce.
6. L'utilisateur interne et/ou externe télécharge le malware et l'ouvre sur son ordinateur.
7. Le malware se connecte au serveur de commande et de contrôle (C&C) du hacker.
8. Le hacker envoie des commandes et des payloads malveillantes supplémentaires à l'ordinateur de la victime.

4. Minimiser les risques d'attaque de la supply chain

La cybersécurité est un problème complexe, auquel il n'existe aucune solution miracle. Ce constat est particulièrement vrai pour un environnement cloud aussi vaste et complexe que Salesforce. Pour minimiser les risques d'attaques de la supply chain, vous devez adopter une approche à plusieurs niveaux, avec des solutions de sécurité efficaces, des processus pertinents et des politiques bien choisies. Voici les éléments-clés d'une stratégie efficace de sécurité pour Salesforce :

Gestion du portefeuille applicatif (APM)

Toutes les applications et tous les composants doivent faire l'objet d'une vérification approfondie avant d'être introduits dans votre environnement Salesforce. Vous devez répertorier toutes les vulnérabilités connues et dresser un historique des incidents qui ont impliqué l'actif en question ou son fournisseur. Vérifiez que tous ces problèmes ont bien été résolus. Une gestion efficace de votre portefeuille applicatif (APM) vous permettra de mener un inventaire des actifs existants et de contrôler les nouvelles applications. Assurez-vous également que tous vos partenaires fournisseurs aient mis en place un niveau de sécurité approprié pour minimiser les risques d'attaque de la supply chain. Ne négligez pas le risque de mises à jour renfermant accidentellement de nouvelles vulnérabilités.

Les entreprises présentant un profil de risque particulièrement élevé peuvent imposer des exigences de sécurité dans le cadre de leurs accords de niveau de service (SLA). Vu le climat géopolitique actuel, elles doivent également s'intéresser à l'origine géographique de leurs fournisseurs, au cas où ces derniers entretiendraient des rapports rapprochés avec certains États-nations.

Cartographie des risques et impact d'une attaque potentielle

Examiner l'actif lui-même ne suffit pas : vous devez procéder à un examen approfondi de sa place dans votre environnement Salesforce et évaluer l'impact d'une éventuelle intrusion. Vous devez tenir compte des caractéristiques de ce produit et de la manière dont il est connecté à Salesforce et à d'autres domaines de votre infrastructure informatique. Un nouvel actif apportera avec lui de nouveaux risques. C'est inévitable. Mais vous devez vous assurer que la balance bénéfices-risques reste favorable. Et vous devez intégrer ces nouveaux risques à votre stratégie de sécurité.

Une visibilité centralisée sur les actifs tiers

Pour les environnements Salesforce les plus vastes qui comprennent des centaines de composants externes, il est pratiquement impossible de tout contrôler. Pour autant, les administrateurs doivent s'efforcer de disposer de la plus grande visibilité possible pour réduire les angles morts susceptibles de provoquer des incidents graves.

Ils doivent agir par priorité. Il leur faut assurer contrôle et visibilité sur les composants-tiers les plus importants et les plus risqués, avant de s'intéresser ensuite aux éléments moins critiques. Des politiques structurées doivent ensuite être prévues pour l'introduction de nouveaux actifs : vous pourrez ainsi maintenir une visibilité suffisante et réduire les risques d'ajout d'applications redondantes au fil du temps.

Éliminer les mauvaises configurations et les problèmes d'accès

En plus d'examiner la supply chain, vous devez également évaluer vos propres processus internes. Des applications mal configurées et une mauvaise gestion des accès peuvent laisser la porte ouverte aux attaques, même avant l'introduction de composants tiers.

Les administrateurs doivent auditer leur environnement Salesforce pour s'assurer que les applications ont été correctement configurées, selon le niveau approprié de droits d'accès. Dans l'idéal, tous les actifs doivent être configurés avec le niveau d'accès le moins élevé possible ; et les capacités de partage doivent être désactivées, sauf en cas de besoin particulier.

Cette approche s'applique également aux utilisateurs de l'organisation. Les profils utilisateurs et les systèmes automatisés doivent tous être configurés selon l'approche du moindre privilège, pour ne leur conférer que les droits d'accès nécessaires à leur fonction. Cette règle est particulièrement importante pour l'administration du système, dans la mesure où les entreprises ont tendance à accorder par défaut des droits d'administration à tout utilisateur connecté au système.

Ces règles de bonnes pratiques permettent de réduire les risques d'intrusion. Elles minimisent aussi l'impact d'éventuelles attaques lorsqu'un utilisateur ou une application est effectivement corrompu.

Rappelez-vous qu'il ne s'agit pas d'une opération ponctuelle. Toutes les nouvelles fonctionnalités de Salesforce doivent être régulièrement examinées à la lumière des notes de publications fournies.

Les organisations disposant d'environnements très vastes doivent procéder régulièrement à des examens approfondis de leurs configurations système. Le service de conseil cloud de WithSecure peut fournir une expertise spécialisée pour qu'aucun aspect ne soit négligé.

Bloquer les contenus malveillants sur Salesforce

Les pirates informatiques recourent à diverses méthodes pour lancer leur attaque sur la supply chain même si, le plus souvent, ils se servent d'identifiants volés. Pour éviter les attaques de la supply chain basées sur le phishing, le vol d'identifiants et les malwares, vous devez adopter une approche holistique de la sécurité incluant la protection des endpoints, du réseau et du cloud.

WithSecure propose une gamme de solutions pour vous aider à prévenir, détecter et répondre aux cyberattaques actuelles.

Mais vous devez aussi tenir compte du fait que la plateforme Salesforce elle-même peut être exploitée comme vecteur d'attaque. Salesforce permet d'uploader et de télécharger des contenus. Cette fonctionnalité possède de multiples applications : elle permet, par exemple, aux clients des compagnies d'assurance d'uploader leurs documents d'indemnisation et leurs justificatifs d'identité, et aux cabinets de recrutement d'envoyer et de recevoir des fiches de poste.

Malgré son caractère essentiel, cette fonctionnalité peut également être exploitée par les pirates informatiques pour uploader des fichiers et des URL malveillants. Cette approche représente, pour eux, une alternative efficace au phishing par e-mail. Ils se servent en effet de l'environnement Salesforce corrompu pour partager des contenus malveillants avec les utilisateurs et clients.

Bien que la plateforme Salesforce soit responsable de la protection des données dans son environnement, elle ne contrôle pas les uploads et les téléchargements : cette responsabilité incombe à l'entreprise.

WithSecure Cloud Protection for Salesforce permet de bloquer efficacement cette voie d'attaque. Cette solution, leader sur le marché, est conçue pour déjouer les attaques menées via des URL et des fichiers malveillants uploadés vers Salesforce par les hackers et les utilisateurs situés hors du périmètre de cybersécurité de l'entreprise.

Cette solution analyse en temps réel tout le contenu uploadé et téléchargé, pour identifier et bloquer tous les contenus malveillants grâce aux renseignements sur les menaces les plus récents fournis par WithSecure. Cloud Protection for Salesforce a été développé en coopération avec Salesforce pour fournir une protection robuste, sans impacter l'expérience utilisateur.

Un plan de réponse efficace

Vous devez comprendre qu'une intrusion informatique constitue plus qu'une simple éventualité : vous y serez confronté tôt ou tard ; ce n'est qu'une question de temps.

Même les organisations dotées de stratégies de sécurité bien établies et bien financées peuvent être victimes d'un pirate informatique suffisamment compétent et déterminé.

Il vous faut donc vous préparer à réagir en cas d'attaque de la supply chain ciblant Salesforce. Vous devez mettre en place un plan efficace de réponse aux incidents et de remédiation afin d'identifier et de bloquer rapidement les menaces, pour rétablir, le plus rapidement possible, un fonctionnement normal.

Salesforce Shield propose la journalisation détaillée et le chiffrement par champ. Ces fonctionnalités peuvent vous permettre de renforcer votre monitoring des activités, ce qui peut être utile pour détecter et analyser les incidents.

Il vous faut aussi pouvoir traquer la source de l'intrusion, et éliminer toute menace persistante dans votre environnement, comme les malwares cachés et les programmes de commande et de contrôle. Pour ce faire, la méthode la plus rentable consiste à travailler avec un partenaire spécialisé.

Préparez-vous également à minimiser l'impact des attaques potentielles ciblant votre environnement Salesforce : une attaque pourrait en effet entraîner l'arrêt de l'ensemble de votre CRM. Pensez donc à effectuer des sauvegardes régulières du système et à implémenter des méthodes de communication alternatives pour maintenir votre activité durant la gestion de crise.

5. Prendre une longueur d'avance sur ces attaques

- Pour déjouer les systèmes de protection mis en place par les entreprises, les pirates informatiques cherchent en permanence de nouvelles voies d'attaque. Dans ce contexte, la supply chain est de plus en plus à risque.
- Les environnements Salesforce étendus sont vulnérables. Les entreprises doivent donc prendre les précautions qui s'imposent.
- Elles doivent se préparer dès maintenant, avant d'être la cible d'une attaque.

Les pirates informatiques ne cessent d'explorer de nouvelles pistes pour contourner vos systèmes de protection. La supply chain, désormais incontournable, leur offre une nouvelle voie d'attaque.

Plus votre supply chain se développe, plus les risques augmentent. Vous devez donc veiller à actualiser en continu vos capacités de monitoring et de contrôle sur votre supply chain étendue. Ces efforts de sécurisation doivent impérativement prendre en compte Salesforce : il s'agit à la fois d'un système CRM crucial et d'un environnement qui peut abriter des centaines d'éléments tiers différents.

Il appartient à Salesforce de sécuriser sa propre infrastructure mais les utilisateurs restent responsables des composants et contenus uploadés. Cette approche est connue sous le nom de responsabilité partagée.

Des incidents très médiatisés comme ceux de SolarWinds, Kaseya et Log4J ont fait la une des médias. Ils contribuent à sensibiliser aux risques de la supply chain. Pour le moment, Salesforce n'a pas encore été utilisé dans ces attaques. Prenez contact avec notre équipe dès maintenant pour savoir comment WithSecure peut vous aider à sécuriser cette voie d'attaque avant qu'il ne soit trop tard.

Qui sommes-nous ?

WithSecure™ est le partenaire européen de référence en matière de cybersécurité depuis plus de 30 ans. Nous accompagnons les fournisseurs de services informatiques, les MSSP et des multinationales, qui nous font confiance, à travers des modèles commerciaux flexibles et adaptés au marché. Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir le bon fonctionnement de leurs activités. Notre protection basée sur l'IA sécurise les endpoints et protège les environnement cloud. Nos outils intelligents de détection et de réponse sont pilotés par des experts qui identifient les risques, assurent une recherche proactive des menaces et neutralisent les attaques en temps réel. Un service de consulting expert est également disponible pour les entreprises qui souhaitent renforcer leur résilience.

WithSecure™, anciennement F-Secure Corporation, a été fondée en 1988 et est cotée au NASDAQ OMX Helsinki Ltd.

WITH secure