E-book

Sécurité de la supply chain : **Comment éviter « l'effet papillon » ?**

Ce rapport de WithSecure™ explique comment repenser la sécurité de votre supply chain pour éviter « l'effet papillon ». Cet effet peut être résumé ainsi : de petites erreurs ou de légères négligences peuvent avoir des conséquences catastrophiques. Les cadres dirigeants l'apprennent souvent à leurs dépens et leurs récits sont souvent éloquents.

Pour ce rapport, WithSecure™ a interviewé les RSSI de plusieurs entreprises numériques, physiques et hybrides. Nous nous sommes également entretenus avec des experts et consultants en sécurité. Certains témoignages sont explicitement cités entre guillemets, d'autres non, mais chaque entretien a apporté un éclairage précieux. Les interviews avec les professionnels externes respectent les règles de la Chatham House.

Sommaire

Introduction
Les risques liés à la supply chain

La « supply chain » : l'un des termes commerciaux les plus trompeurs du 21ème siècle.

Une « chaîne » correspond, en théorie, à une suite linéaire d'éléments uniformes. Il peut donc être tentant de se représenter la « supply chain » selon une approche classique : entrée des matières premières, sortie des produits finis, conteneurs sur les navires puis des boîtes dans des camions. Les supply chains d'aujourd'hui sont pourtant bien différentes. Rien n'est jamais linéaire, rien n'est jamais uniforme.

Dans une économie numérique en réseau, même les chaînes d'approvisionnement traditionnelles observent rarement une structure simple : « début, milieu, fin ».

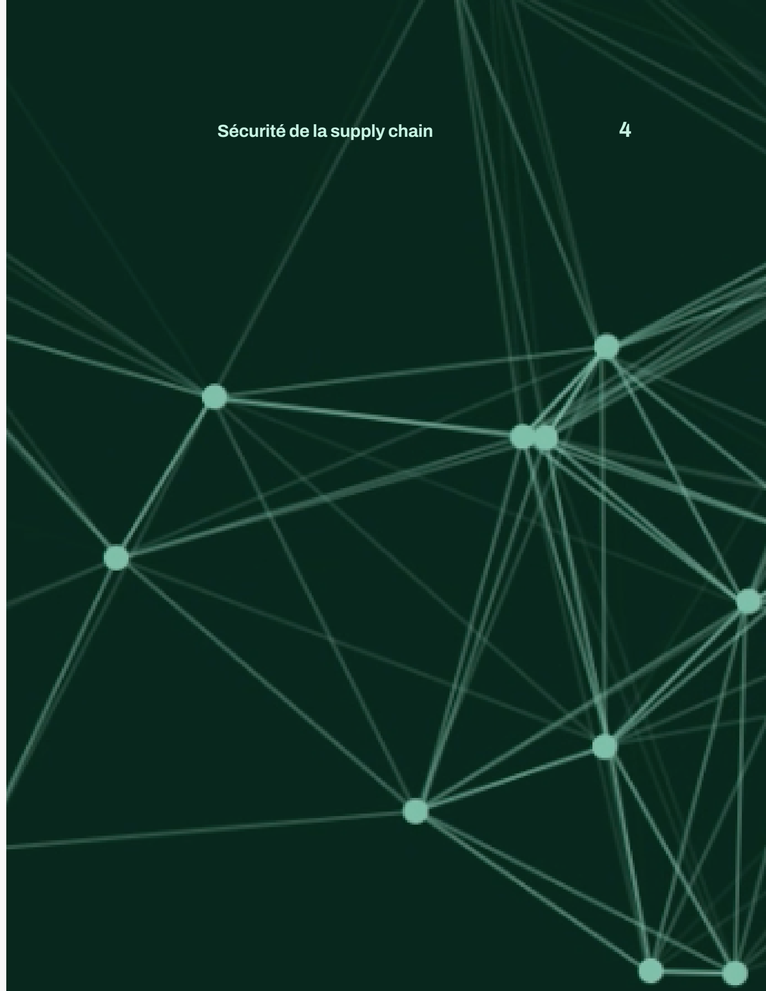
Du fait de la transformation numérique, les supply chains ne sont plus de simples lignes de dominos : elles ressemblent davantage à de gigantesques réseaux, où tout est interconnecté.

La danse des dominos

L'analogie des dominos supposait aussi des entreprises de même taille, de même forme. Ce n'est plus le cas aujourd'hui : désormais, une même entreprise peut désormais collaborer avec des organisations de toutes tailles, depuis les multinationales jusqu'aux petites start-ups. Ces organisations fournissent tout type de biens, de matériaux ou de services, aussi bien en amont qu'en aval de la supply chain.

Les pirates informatiques l'ont bien compris. Cybercriminels, « hacktivistes », hackers opportunistes et États-nations hostiles s'intéressent donc tout particulièrement aux supply chains. En ciblant ces écosystèmes d'approvisionnement tentaculaires, ils peuvent amplifier l'impact de leurs attaques, voire même cibler des secteurs tout entiers.

La supply chain constitue pour eux un filon particulièrement rentable.



Enjeux technologiques

Les risques DevOps

Les équipes informatiques et DevOps utilisent souvent des référentiels de code, notamment open-source. Elles réutilisent ainsi des composants fiables qui ont été codés et validés par un réseau mondial de confrères spécialistes. Ces référentiels sont aujourd'hui ciblés par les pirates informatiques, tout comme les plateformes cloud, les services managés et les utilitaires les plus courants.

Selon la recherche WithSecure™, les attaques ciblant des applications spécifiques ont atteint un pic en 2017. Les attaques contre des logiciels utilitaires ont atteint leur paroxysme l'année suivante. Les attaques ciblant les référentiels de code populaires, quant à elles, ont explosé en 2020, et augmentent chaque année. Il est important de considérer tous ces incidents comme des attaques particulières, ciblant les rapports de collaboration et de confiance.

Le principe de confiance mutuelle

Montrez-vous particulièrement vigilants concernant les composants logiciels de votre supply chain numérique. WithSecure™ vous invite à toujours sélectionner des fournisseurs particulièrement attentifs à leur propre sécurité, en particulier lorsqu'il s'agit de petites entreprises ou d'entrepreneurs individuels.

Posez les questions suivantes :

- Quelles sont les autorisations et politiques mises en place par ces fournisseurs ?
- Quelles sont les données personnelles identifiables et informations de propriété intellectuelle confiées par votre entreprise à ce fournisseur ?
- Ce fournisseur utilise-t-il sa cyberprotection comme argument de vente vérifiable pour eux ?
- Dispose-t-il d'équipes de sécurité propres ou de consultants en sécurité ?
- Propose-t-il des programmes de bug bounty, pour récompenser les experts qui identifient de nouvelles vulnérabilités et de nouveaux exploits ?

N'oubliez pas que votre entreprise s'inscrit dans un réseau d'approvisionnement interconnecté : vous déployez ou distribuez peut-être le code de certains de vos fournisseurs via vos propres produits. Vous transmettez donc leurs failles potentielles à vos utilisateurs et clients.

Posez-vous donc également les questions suivantes :

- Avez-vous identifié tous les composants open-source intégrés à vos produits ?
- Êtes-vous certain que le code provenant de sources externes est sécurisé ?
- La correction des vulnérabilités constitue-t-elle une priorité pour votre entreprise ?
- Votre processus de modélisation des menaces prend-il en compte votre responsabilité en tant que fournisseur ?

Pour faire simple : à quel point êtes-vous un facteur de risque pour vos partenaires ?

L'effet papillon

Pour décrire l'écosystème actuel des cybermenaces, il existe des analogies plus pertinentes que celles des dominos. WithSecure™ préfère ainsi évoquer « l'effet papillon », qui reflète bien mieux la réalité quotidienne des entreprises, à une heure où les systèmes sont tous interdépendants, et interconnectés.

L'effet papillon est souvent ramené à une idée simple : de petites actions (ou inactions) peuvent avoir des conséquences considérables au fil du temps. Dans ce rapport, nous vous présenterons ce concept plus en détail. Nous vous expliquerons ensuite quels enseignements en tirer pour sécuriser votre supply chain.

Mais, avant cela, procédons à un rapide état des lieux.

Cartographier l'entreprise

Désormais, le périmètre informatique de votre entreprise s'étend désormais bien au-delà de votre siège social : il concerne désormais les plateformes cloud, les services partagés, le travail à distance, etc. Ce processus s'est accéléré durant la pandémie. Ces évolutions ont rendu nécessaire l'installation de système de détection et de défense au niveau des endpoints.

Voilà pourquoi certains professionnels de la sécurité affirment aujourd'hui que le concept de périmètre à proprement parler est mort et enterré. Ce n'est pas réellement le cas. Il est vrai que les périmètres sont devenus beaucoup plus difficiles à cartographier et à quantifier, mais pour lutter efficacement contre les cybermenaces externes et internes, vous devez préalablement définir votre périmètre. Si vous n'avez pas identifié vos différents actifs, comment pouvez-vous les sécuriser et détecter les attaques ?

D'après l'indice IBM X-Force Threat Intelligence 2021, l'exploitation des vulnérabilités est devenue le vecteur d'attaque favori des pirates informatiques - devant le phishing - en raison notamment des possibilités d'automatisation. Ce phénomène explique sans doute en partie l'envolée des attaques sur les référentiels de codes, et doit inviter les entreprises à bien identifier les actifs constitutifs de leur périmètre.

Bonne nouvelle : la gestion de la surface d'attaque externe (EASM) permet désormais de cartographier et de gérer le périmètre avant que toute faille ne puisse être exploitée. WithSecure™ a publié une série de recommandations à ce sujet, et nous vous suggérons d'envisager le déploiement de systèmes EASM.

« L'EDR [Endpoint Detection and Response] a pour mission d'identifier les vecteurs d'attaque potentiels. Ce type de solution vous permet de détecter et de répondre à une attaque de la supply chain le plus rapidement possible. En cas d'incident, l'EDR peut faire toute la différence et sauver votre activité : cette technologie vous donne le temps de rattraper votre retard face au pirate informatique. »

Jordan LaRose, Director of Consulting & Incident Response, WithSecure™

Les employés

Chaque employé possède son propre réseau de contacts. Et chacun de ces contacts peut être synonyme de dangers. Il peut suffire d'un code malveillant dans un e-mail ou d'un regard indiscret sur un téléphone pour compromettre votre entreprise toute entière, et plus encore. L'effet papillon commence là.

Il est essentiel de mener une formation sur la cybersécurité et d'appliquer des politiques rigoureuses, mais le risque d'erreur humaine demeure. Vous devez donc mettre en place un niveau de sécurité supplémentaire au niveau des endpoints, notamment lorsque vos employés travaillent à distance.

La sécurité de la supply chain ne se résume pas à un processus linéaire simple. Il s'agit plutôt d'un mélange complexe de risques, d'interconnexions et d'interdépendances, le tout agrémenté de la notion de responsabilité personnelle.

Voyons tout cela plus en détail.

L'interdépendance

Dans l'ancien modèle de la supply chain linéaire, vos fournisseurs étaient en amont, et vos clients en aval.

Tous interagissent désormais avec nous dans un monde multicanal. Vos clients vous font confiance pour assurer la sécurité de leurs données. En cas d'attaque réussie sur votre entreprise, ils risquent de payer un lourd tribut. À l'inverse, une attaque contre l'un de vos clients - une entreprise qui achète vos produits ou services, par exemple - peut aussi avoir des répercussions plus complexes sur votre entreprise.

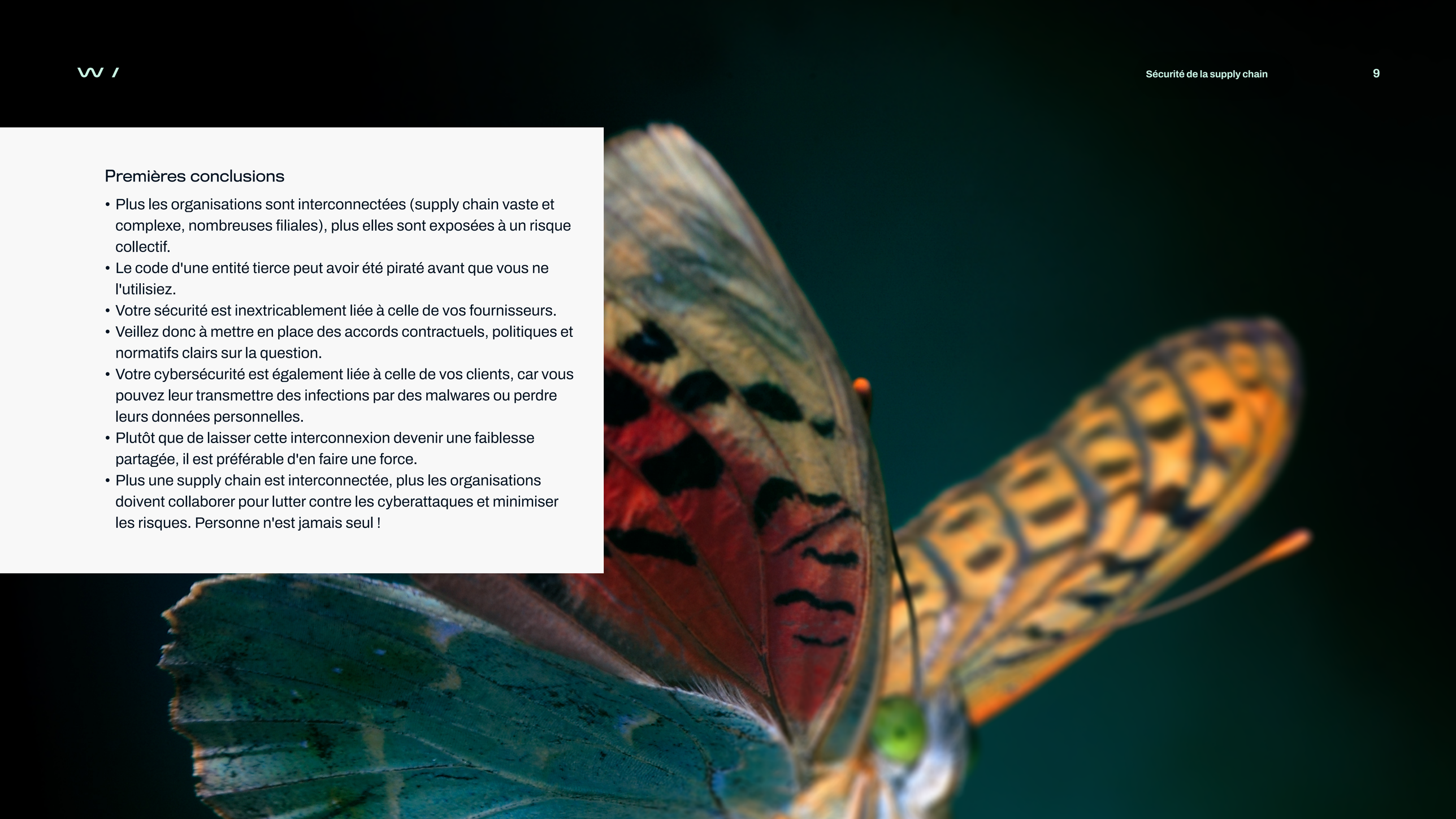
Du point de vue de la cybersécurité, dans les supply chains actuelles, nous sommes clairement devenus interdépendants les uns des autres.

Une intrusion informatique peut provenir de n'importe quelle partie de votre écosystème et se propager dans n'importe quelle direction, avec des répercussions croissantes à mesure que le risque est transmis.

Une fois encore, c'est l'effet papillon.

Premières conclusions

- Plus les organisations sont interconnectées (supply chain vaste et complexe, nombreuses filiales), plus elles sont exposées à un risque collectif.
- Le code d'une entité tierce peut avoir été piraté avant que vous ne l'utilisiez.
- Votre sécurité est inextricablement liée à celle de vos fournisseurs.
- Veillez donc à mettre en place des accords contractuels, politiques et normatifs clairs sur la question.
- Votre cybersécurité est également liée à celle de vos clients, car vous pouvez leur transmettre des infections par des malwares ou perdre leurs données personnelles.
- Plutôt que de laisser cette interconnexion devenir une faiblesse partagée, il est préférable d'en faire une force.
- Plus une supply chain est interconnectée, plus les organisations doivent collaborer pour lutter contre les cyberattaques et minimiser les risques. Personne n'est jamais seul !



Transformation numérique : simplifier ou complexifier ?

Dans un tel contexte, les contrats, les accords de niveau de service et les indicateurs de performance-clés deviennent essentiels. Soyez également attentifs aux stratégies visant à normaliser votre infrastructure informatique sur une seule plateforme technologique : une telle mesure simplifiera, certes, votre infrastructure, mais elle risque d'aggraver l'impact des attaques menées via la supply chain.

Les programmes de transformation numérique consistent souvent à favoriser le cloud dans une optique de consolidation et de simplification. Mais ces programmes peuvent avoir des répercussions inattendues sur la sécurité de la supply chain.

En lieu et place, vous pouvez combiner plusieurs systèmes best-of-breed. Pour les pirates informatiques, il sera plus difficile de mener des attaques d'ampleur sur ce type d'infrastructure. Malheureusement, une telle approche peut aussi créer un parc informatique beaucoup plus difficile à gérer.

« La complexité n'est pas toujours synonyme d'un risque accru. Parfois, la diversification des charges de travail peut aider à maintenir un service critique en état de fonctionnement. »

Jordan LaRose, Director of Consulting & Incident Response, WithSecure™

Vos choix en la matière vous appartiennent mais vous ne pourrez malheureusement pas influer sur les choix de vos partenaires. Seules quelques multinationales de premier plan et certaines plateformes technologiques mondiales disposent du poids nécessaire pour imposer à d'autres leurs propres standards. De tels rapports de force ne sont même pas profitables en soi, puisqu'ils peuvent nuire à la capacité d'innovation de vos partenaires.

« Si vous rationnalisez en appliquant un ensemble de normes ou en réduisant les coûts, il se peut que vous rendiez votre infrastructure plus vulnérable du point de vue de la sécurité. Il est très difficile pour les pirates informatiques de paralyser une entreprise si celle-ci est répartie sur 1 000 bits différents. Mais si elle est intégrée sur une seule plateforme, alors ils n'auront qu'une seule cible à atteindre. »

« Dans tout processus de transformation numérique, certains secteurs de l'entreprise doivent rester cloisonnés. Mais plutôt que de donner la priorité à la sécurité, les entreprises préfèrent mettre en avant le budget ou la transformation numérique elle-même… Les responsables de la transformation numérique ont souvent tendance à arriver de nulle part, à mener leur transformation, puis à laisser le problème de la sécurité à quelqu'un d'autre. »

Jordan LaRose, Director of Consulting & Incident Response, WithSecure™

L'effet papillon et ce qu'il suppose

Éviter l'effet papillon doit donc être une priorité pour les entreprises. Comment doivent-elles procéder ? À quoi les responsables de la sécurité doivent-il prêter attention ? Pour répondre à ces questions, il faut revenir aux origines de ce concept.

En 1952, l'auteur américain Ray Bradbury décrit, dans sa nouvelle *A Sound of Thunder*, le concept d'effet papillon. Le terme lui-même sera inventé par la suite.

L'histoire décrit un groupe de voyageurs temporels se rendant dans un passé préhistorique. Pour échapper à un dinosaure, l'un des voyageurs s'écarte du chemin que son équipe doit suivre et marche accidentellement sur un papillon. De retour à l'époque actuelle, tous constatent que le monde a connu des changements majeurs, à l'impact catastrophique.

La première leçon est claire : une petite erreur, même apparemment innocente, peut avoir des conséquences désastreuses. Dans l'histoire, cette action a des répercussions sur toute l'Histoire du monde, avec un effet exponentiel au fil du temps, à mesure que les conséquences s'accumulent.
.
Cette idée d'interdépendance dans les systèmes fermés a été proposée en 1800 lorsque le philosophe Johann Gotlieb Fichte a remarqué que de déplacer un seul grain de sable « engendrait un changement dans toutes les parties d'un ensemble non-mesurable ». Aujourd'hui, nous pensons en termes d'écosystème technologique : de petites actions ont des effets sur l'ensemble du système.

Dans les années 1960, le météorologue Edward Norton Lorenz popularise le concept en suggérant que le simple battement d'ailes d'une mouette peut, à terme, déclencher une tempête. En 1972, il reprend sa métaphore, cette fois avec l'idée qu'un seul battement d'ailes de papillon peut engendrer un ouragan.

Cette image puissante est restée dans les esprits. Pour autant, la version originale proposée par Ray Bradbury revêt un caractère plus instructif. Les entreprises d'aujourd'hui peuvent même en tirer de précieux enseignements. Dans cette nouvelle, les voyageurs temporels eux-mêmes tirent quelques leçons de leur mésaventure.

Les voici.

Effet papillon - Cinq leçons à retenir

1.

Les explorateurs sont dans l'incapacité de remonter jusqu'au moment où l'erreur a été commise. Ils ne peuvent donc pas la corriger. Ils doivent accepter les conséquences de cet incident et vivre dans ce monde qui n'est plus le même.

Pensez aux dommages durables d'une attaque de la supply chain sur vos finances et sur votre réputation. N'oubliez pas : les réseaux sociaux ont bonne mémoire !

2.

L'effet papillon a été provoqué par un individu qui a renoncé, un bref instant, à rester avec le reste de son équipe.

Pensez à cet employé qui oublie les protocoles de sécurité durant une seconde, clique sur un lien apparemment sans danger, et compromet l'ensemble du système. Dans un tel scénario, la sécurité des endpoints créerait une couche de protection supplémentaire.

Face à l'augmentation des ransomwares, du cryptojacking (utilisation à distance des ressources informatiques d'autrui pour extraire de la crypto-monnaie) et des autres malwares, vous devez miser sur le travail d'équipe. Les supply chains actuelles exigent plus de vigilance, et une collaboration constante.

3.

Une passerelle sécurisée avait été créée pour les voyageurs temporels. Elle flottait au-dessus d'une forêt vierge dangereuse, peuplée de dinosaures mangeurs d'hommes. L'explorateur temporel a ignoré la règle d'or à laquelle toute l'équipe avait accepté de se plier, à savoir : ne jamais quitter cette passerelle.

Vos employés travaillent ensemble et avancent sur un même chemin, à travers une forêt jonchée de dangers communs. Le degré de protection de votre entreprise dépend de votre maillon le plus faible.

Veillez à appliquer efficacement votre politique de sécurité. Les « monstres » ne constituent pas toujours la vraie menace.

4.

Le voyageur était tellement effrayé par les tyrannosaures qu'il n'a pas vu le papillon.

Les monstres les plus impressionnants ne sont pas les seuls dangers. Une chose apparemment inoffensive - comme un papillon ou une vulnérabilité - peut avoir des conséquences très sérieuses.

N'oubliez pas : les insectes ont survécu aux dinosaures.

5.

Une fois de retour au quartier général, les voyageurs temporels retrouvent le papillon sur la semelle de la chaussure du voyageur, dans un monde bouleversé.

Peut-être avez-vous déjà, par le passé, fait preuve d'imprudence sur le chemin du numérique. Sans le vouloir vous avez fait entrer un pirate informatique, qui a pu accéder à des systèmes critiques. Le message est on ne peut plus clair : ne soyez pas ce voyageur imprudent !

« Certaines attaques actuelles résultent de contrôles de base insuffisants. Pour les pirates informatiques, ces attaques sont souvent faciles à exécuter. Les entreprises tendent à implémenter des mesures sophistiquées mais elles en oublient l'essentiel. Si vous négligez la sécurité de base, vous rendez service aux pirates en leur simplifiant la tâche. »

Directeur des risques informatiques EMEA, banque multinationale

Une analogie efficace pour la sécurité

Il existe un parallèle évident entre cette histoire et la sécurité des supply chains actuelles.

Les tyrannosaures sont aujourd'hui incarnés par les groupes de pirates informatiques, les criminels organisés et les États hostiles. Dans la jungle technologique d'internet, se cachent désormais les attaques de phishing, les malwares, les ransomwares, les chevaux de Troie et autres vols de données.

Dans ce monde où l'informatique hybride et cloud tend à s'imposer, les hackers mettent tout en œuvre pour que leurs attaques passent inaperçues. Certains génèrent un trafic malveillant conçu pour ressembler à du trafic réseau normal ; d'autres s'attaquent à des outils et à des bibliothèques de codes considérés comme fiables.

La détection dans le cloud

Les cybercriminels opportunistes cherchent à exploiter des fonctionnalités normales et des systèmes mal configurés : ils veulent être le papillon sous la semelle de votre chaussure, pour s'introduire dans votre siège social.

La détection des menaces devient donc essentielle pour sécuriser la supply chain. Dans les nouveaux environnements hybrides, les données télémétriques exclusivement basées sur les endpoints perdent en pertinence, à mesure que s'impose la « télémétrie des actions ».

Ces actions concernent le plan de contrôle de vos plateformes cloud. Elles concernent le réseau d'API qui permet à un administrateur de créer, modifier ou détruire des ressources ou des données dans un environnement cloud.

Les hackers les plus aguerris utilisent de plus en plus les API pour atteindre leurs objectifs : ils créent de nouveaux comptes d'utilisateurs, modifient les autorisations sur des comptes existants ou accordent un accès à certaines ressources depuis des sites externes. Ces activités créent un trafic qui peut sembler légitime à un œil non-averti ou non-expert.

En d'autres termes, les pirates informatiques ne vont pas toujours rugir comme le font les tyrannosaures (même s'ils peuvent effectivement le faire, comme dans le cadre d'attaques par déni de service distribué (DDOS) ou en piratant le portail de votre entreprise). Souvent, ils vont préférer s'introduire discrètement sur votre réseau, comme un papillon sous une chaussure.

Des centaines de millions de lignes de code malveillant flottent dans la forêt dense de nos infrastructures hybrides et interconnectées. Elles veulent paraître innocentes et sans danger. Elles cherchent même à être attrayantes, pour que vous les laissiez entrer dans l'entreprise.

Les attaques de la supply chain : cas concrets

La fiction est une chose. Mais qu'en est-il de la réalité ? De telles attaques ont-elles réellement lieu ? Sans aucun doute. Au cours des dix dernières années, au moins 200 campagnes d'attaques ciblant la supply chain ont été répertoriées. Elles ont touché les réseaux d'innombrables fournisseurs et de millions de clients. Elles ont aussi eu un impact notable sur les relations entre fournisseurs, acheteurs et clients, et ont entamé la confiance en certaines entreprises ou en certaines institutions.

Plusieurs de ces attaques ont, par ailleurs, fait l'objet d'une large couverture médiatique :

SolarWinds

En 2020, des pirates informatiques ont compromis le système Orion du fournisseur de technologies américain SolarWinds. Ils ont procédé en injectant un code malveillant dans un logiciel utilisé par 33 000 entreprises et organismes du secteur public.

Le code infecté a été envoyé via des mises à jour logicielles standard à au moins 18 000 clients. SolarWinds est ainsi devenu, malgré lui, un vecteur d'attaque. Le piratage n'a été détecté qu'en 2021.

Pendant toute cette période, les pirates informatiques ont pu utiliser leurs exploits pour accéder aux systèmes internes des clients de SolarWinds, et aux données privées qui s'y trouvaient. Ils pouvaient espionner ces systèmes, et même installer d'autres logiciels malveillants.

Parmi les victimes de cette attaque, figurait le gouvernement fédéral américain avec sa supply chain, l'une des plus importantes et les plus sécurisées au monde. Certains organismes stratégiques pour la sécurité américaine ont été touchés, notamment le Pentagone, le Département de la sécurité intérieure et l'Administration nationale de la sécurité nucléaire, sans oublier plusieurs universités.

Les attaques ont également concerné le secteur privé, avec les géants Microsoft, Intel et Cisco. Via ces multinationales, les pirates informatiques ont pu compromettre encore plus de systèmes et de supply chains. Ils ont pu frapper en plein cœur de l'infrastructure cloud des entreprises.

Tout comme dans le récit de Ray Bradbury, il a suffi d'un papillon, d'un seul incident, pour changer le monde.

Kaseya

En 2021, le collectif de pirates REvil, affilié à la Russie, a mené une attaque contre le logiciel édité par Kaseya, un fournisseur de services de gestion technique. REvil a exploité deux vulnérabilités pour s'infiltrer sur les réseaux de plus de 50 fournisseurs de services managés (MSP). Chacun de ces fournisseurs se trouvait au centre de réseaux complexes d'approvisionnement. Plus de 1500 organisations ont ainsi été infectées par un ransomware.

Tout comme dans le cas de SolarWinds, cette attaque s'est propagée à travers les supply chains numériques. Elle exploitait la confiance des clients pour accéder à leurs systèmes critiques.

Ne négligez pas la gestion des vulnérabilités, qui vous permet de disposer d'une visibilité accrue sur votre surface d'attaque.

Log4j

Cette attaque, menée fin 2021 contre l'utilitaire de journalisation gratuit et open source Apache Log4j a permis aux pirates informatiques d'exécuter du code à distance (une attaque RCE).

Log4j a été téléchargé plusieurs millions de fois. Il s'agit de l'un des outils les plus couramment utilisés pour enregistrer et collecter des données sur les utilisateurs et leur comportement en ligne. Cet outil constituait donc, rétrospectivement, une cible évidente pour les pirates informatiques.

Voilà pourquoi il est si important d'adopter le point de vue du pirate informatique, de « penser comme lui », même dans le cas de menaces inconnues. Demandez-vous de quoi un hacker pourrait se servir pour compromettre vos systèmes. Réalisez un exercice de détection des menaces en Red teaming, pour modéliser les schémas d'attaque possibles. Ou bien utilisez un modèle de Purple teaming, en combinant des tactiques offensives (Red) et défensives (Blue).

L'attaque Log4j a impliqué des ransomwares, du cryptojacking et de nombreux autres incidents. Ses répercussions à plus long terme restent inconnues. Il s'agit peut-être de la plus grande attaque de la supply chain à ce jour. Sur le MITRE, son score de risque atteint 10/10.

NotPetya

Pour autant, l'attaque ayant eu le plus grand impact financier à ce jour reste celle du malware NotPetya, survenue en 2017. Cette attaque ciblait l'application ukrainienne de déclaration d'impôts ME Doc.

L'utilisation de ME Doc était obligatoire pour chaque entreprise déclarant ses impôts en Ukraine : à l'époque, plus de 400 000 entreprises étaient concernées. L'attaque, qui se propageait via des mises à jour, a coûté aux entreprises un montant estimé à 10 milliards de dollars, principalement en dommages collatéraux.

De plus en plus de pays numérisent les transactions fiscales entre les citoyens, les entreprises et le gouvernement. Au Royaume-Uni, par exemple, les utilisateurs doivent désormais effectuer certaines déclarations d'impôts via un logiciel dédié. Dans ce pays, 99 % des entreprises sont des PME. Une attaque réussie sur la fiscalité des PME aurait donc un impact catastrophique, et rapporterait gros aux criminels.

« Certaines attaques actuelles résultent de contrôles de base insuffisants. Pour les pirates informatiques, ces attaques sont souvent faciles à exécuter. Les entreprises tendent à implémenter des mesures sophistiquées mais elles en oublient l'essentiel. Si vous négligez la sécurité de base, vous rendez service aux pirates en leur simplifiant la tâche. »

Directeur des risques informatiques EMEA, banque multinationale

Attaques contre les logiciels utilitaires

D'autres campagnes de piratage réussies contre les supply chain ont ciblé des logiciels utilitaires.

L'application Codecov de code-testing a notamment été prise pour cible : les pirates informatiques avaient collecté des identifiants utilisateurs via des scripts. Ils avaient ainsi pu obtenir un accès privilégié aux référentiels Git pendant plus de deux mois, jusqu'à ce que l'intrusion soit finalement découverte.

Cela montre à quel point, désormais, les attaques de la supply chain se veulent discrètes. Plus semblables au papillon qu'au tyrannosaure, elles volent des identifiants pour imiter le trafic réseau normal et peuvent passer inaperçues pendant de longues périodes.

Les cybercriminels ciblent généralement les bibliothèques utilisées pour des produits largement utilisés. Il est donc essentiel d'organiser des exercices de sécurité pour les Red teams et les Purple teams, afin de mettre en évidence les chemins que les hackers peuvent emprunter pour se faufiler au sein de vos réseaux d'approvisionnement sans être repérés.

Attaques hardware

Bien que relativement rares, certaines attaques ciblent la supply chain physique en implantant des portes dérobées dans des composants matériels.

WithSecure™ connaît par exemple une société de micro-puces ayant identifié une porte dérobée imprimée dans le micrologiciel de chaque puce graphique qu'elle avait commercialisée. La porte dérobée a finalement été identifiée et effacée de la bibliothèque.

Le fabricant de puces a découvert que des pirates informatiques avaient compromis un environnement web de développement intégré (IDE). Ils avaient ainsi pu accéder à un compte développeur, écrire la porte dérobée et l'uploader dans le dépôt de code central.

Le coût caché des attaques contre la supply chain

Les attaques de la supply chain peuvent donc avoir des effets majeurs, clairement quantifiables. Dans d'autres cas, les organisations subissent des dommages quelque peu différents.

Lorsqu'une entreprise de la supply chain est en proie à une intrusion ou à un incident, toutes les autres doivent vérifier leur réseau pour savoir si elles sont concernées par l'attaque. Souvent, ce n'est pas le cas, mais des équipes ont dû être mobilisées pour s'en assurer.

Les attaques de la supply chain sont insidieuses : elles consomment du temps, de l'argent, des compétences et des ressources. Elles détournent ainsi les entreprises de leurs objectifs commerciaux stratégiques. Notre première étude de cas est là pour en témoigner.

Études de cas et recommandations

Étude de cas : un commerçant hybride

Notre première étude de cas concerne un grand groupe européen de distribution. Il s'agit de l'un des deux grands distributeurs diversifiés de son pays. Il s'appuie sur un réseau de magasins physiques et en ligne pour proposer une gamme complète de produits, y compris alimentaires, à un pays dont la population est relativement réduite.

Chaque magasin est une coopérative indépendante et reverse ses bénéfices aux clients qui en sont propriétaires. Chaque point de vente est libre d'agir de manière autonome, tout en reconnaissant l'autorité de l'entité centrale. Le groupe possède également une branche bancaire coopérative prospère, ainsi que des stations-service. Il assure également ses propres opérations logistiques.

Le réseau d'approvisionnement de ce distributeur est atypique et hybride. Il ne ressemble pas à celui d'une entreprise traditionnelle. Le groupe compte plus de 800 fournisseurs informatiques, dont 150 livrent des services ou des outils critiques. Parmi ces fournisseurs, figurent les grandes plateformes cloud ainsi que de petits fournisseurs locaux et des développeurs indépendants.

L'intégration et ses limites

La supply chain du groupe est donc vaste et, à certains égards, bien intégrée. Pour l'essentiel, il s'agit d'une entité très souple composée d'organisations et de sociétés privées de toutes tailles, qui travaillent ensemble avec des objectifs communs.

La coopération est donc essentielle pour faire fonctionner l'ensemble du système. Le fait que les clients soient également propriétaires de chaque point de vente - plutôt qu'un investisseur étranger ou un milliardaire - incite le groupe à rester sécurisé dans l'intérêt de tous.

Malgré cela, certaines coopératives individuelles font cavalier seul sur des décisions-clés, comme les choix technologiques. Elles en ont légalement le droit. Au moment de sécuriser la supply chain, respecter les principes communs n'est pas toujours évident.

Le professionnel chargé de la sécurité de l'information pour la maison mère, explique :

« Du point de vue de la sécurité de l'information, nous insistons toujours sur le fait que les coopératives individuelles ne doivent pas prendre de décisions en matière de risques, sur quelque sujet que ce soit. »

Du fait de la composition et de la structure inhabituelle de ce groupe, le vol de données clients ne constitue pas une préoccupation majeure pour la maison mère. La population du pays concerné est plus petite que certaines capitales, et la base de clients du groupe représente un peu moins de la moitié de cette population.

Autant dire que les pirates informatiques du pays pourraient facilement trouver les mêmes informations par ailleurs. Des hackers n'auraient peu d'intérêt à pirater ce distributeur, à moins qu'ils opèrent pour le compte d'un État hostile et souhaitent déstabiliser le pays.

Les attaques par force brute

Parmi les attaques ciblant la supply chain de cette entreprise, les attaques DDoS ont été les plus fréquentes. Nous ne pouvons donc pas écarter la possibilité que des puissances étatiques hostiles, même peu qualifiées, cherchent à perpétrer des attaques par force brute contre des produits de marque couramment consommés.

Ce grand groupe de distribution a-t-il été la victime collatérale d'attaques comme celles de SolarWinds, Kaseya ou Log4j ? L'Infosec Manager reconnaît que le groupe a effectivement été touché, mais de manière indirecte :

« Nous avons certes été affectés… mais pas directement. Nous avons dû passer des centaines d'heures à enquêter sur l'impact éventuel de ces attaques sur notre structure. Log4j et Log4Shell ont constitué des sources de préoccupation majeures. Nous n'avons pas détecté d'intrusion mais nous avons consacré un temps considérable aux enquêtes, aux opérations d'urgence et à des réunions de crise. »

Avant d'ajouter :

« Nous avons apporté beaucoup de changements suite à ces enquêtes. Ce n'était donc pas juste une perte de temps. L'attaque de SolarWinds, n'a pas eu d'impact majeur sur nous, mais nous avons passé un temps considérable à enquêter suite à cet incident. »

Du temps investi, mais pas de temps perdu

L'investigation pro-active peut s'avérer frustrante : elle implique de passer des heures à rechercher des vulnérabilités qui n'existent pas. Pour autant, ce processus est essentiel. Il permet aux équipes de sécurité de renforcer leurs systèmes centraux, et de mieux déterminer où les menaces pourraient un jour survenir.

Quelles autres leçons le groupe a-t-il tiré de ces exercices critiques ?

« Des vulnérabilités majeures apparaissent tous les trois ou quatre ans, mais on en revient toujours aux contrôles de sécurité de base. »

« Si vous disposez d'un système de gestion des vulnérabilités, d'une CMDB (base de données de gestion des configurations stockant des informations-clés sur votre parc hardware et logiciel) et d'une bonne gestion de la supply chain, vous êtes parés : lorsqu'une vulnérabilité comme Log4j apparaîtra, il vous sera beaucoup plus facile d'enquêter. »

Conclusion : vous devez connaître votre périmètre, et identifier les actifs déployés en son sein. Parfois, malheureusement, vous vous heurterez aux autres professionnels de votre entreprise.

« Lorsque vous parlez aux dirigeants et que vous leur dites : " Notre CMDB n'est pas à jour, il manque environ 30 % des données ", ils vous répondront : "Nous reconnaissons que c'est un problème important, mais pour l'instant nous avons d'autres priorités". »

« Puis, tout à coup, vous devez enquêter sur un problème comme Log4j, qui nécessite d'avoir toutes les données pour mener une analyse poussée. Tout à coup, le manque de données devient un problème majeur. »

Étude de cas : Conglomérat de médias international

Que faire si votre entreprise est une société parapluie pour des milliers d'entités commerciales ? Comment procéder lorsque vous êtes l'élément central d'un réseau de supply chain particulièrement vaste, qui compte des dizaines de milliers de partenaires... voire plus de 130 000 selon certaines estimations ?

C'est le défi auquel est confronté ce géant des médias et des communications. Le Security and Assurance Manager de ce géant du Fortune 500 reconnaît l'ampleur du problème : la société se heurte, comme dans la nouvelle de Ray Bradbury, à une forêt menaçante, renfermant de nombreux dangers... mais cette fois, les dangers peuvent se cacher au sein même de l'entreprise :

« Dans une organisation normale, il existe une équipe de gestion des risques fournisseurs. Cette équipe identifie tous les fournisseurs, ainsi que tous les produits utilisés. Elle peut ensuite mettre en place un système de surveillance des menaces pour les fournisseurs-clés.

« Mais rien de tout cela n'est possible dans un environnement comme le nôtre, qui réunit des milliers d'entreprises, chacune comptant d'une vingtaine à plusieurs milliers d'employés. Nous ne disposons pas d'une fonction centralisée et efficace de la supply chain, contrairement à la majorité des grandes organisations traditionnelles. »

« À la place, nous définissons les grandes lignes de la politique de sécurité, et nous disposons d'une équipe chargée de la conformité. Je fixe les normes en matière de conformité, en disant : " Voici les politiques que nous attendons des entreprises individuelles ". Et ces entreprises, à leur tour, opèrent en s'appuyant sur leurs propres équipes de gestion des risques et des fournisseurs. »

Un rôle à assumer

Cependant, même une mission de surveillance aussi large doit être gérée de manière stricte. Les politiques doivent être rigoureusement appliquées et contrôlées… car lorsqu'une filiale est ciblée par un pirate informatique, c'est la holding qui en porte la responsabilité du point de vue de la loi, de la réglementation, de la réputation et des investisseurs.

L'Assurance team a-t-elle mené des actions concrètes en matière de sécurité ? A-t-elle pu déjouer les attaques en aval de la supply chain ? La réponse est oui :

« L'une de nos entreprises menait des contrôles satisfaisants à l'égard de ses fournisseurs mais un jour, elle demandait à une start-up de prendre en charge une tâche dangereuse. Il s'agissait d'utiliser un système qui – s'il n'était pas correctement géré et sécurisé – pouvait mettre toute l'entreprise en danger. Mon équipe est intervenue et a dit : "Non, ce n'est pas acceptable." »

À ne pas faire

La transformation numérique était au cœur de cette problématique, explique-t-il :

« Les entreprises que nous regroupons au sein de notre société gèrent leurs propres instances de plateformes cloud, mais il y avait un projet visant à regrouper plusieurs d'entre elles au sein d'une instance unique. Cette consolidation devait permettre d'harmoniser les paramètres de configuration pour une vingtaine d'instances cloud. Une start-up disait être en mesure de procéder à cette opération. »

« Puis j'ai vu apparaître sur cette plateforme des comptes de services qui avaient des droits d'administrateur généraux, mais dont l'authentification multifactorielle n'était pas activée. Cela a tout de suite tiré la sonnette d'alarme. »

« La technologie utilisée par la start-up n'était pas en cause ; elle aurait pu faire l'affaire. Mais j'ai tout de suite vu que l'outil disposait de droits d'administration généraux sur plusieurs instances d'une importante plateforme cloud. Si cet outil avait été piraté, le hacker aurait obtenu un contrôle total sur toutes les instances cloud concernées. »

Un autre paramètre entrait en jeu :

« Non seulement je n'avais aucune confiance en la capacité d'une si petite start-up à sécuriser correctement son système, mais en plus elle n'avait pas d'argent en banque. En d'autres termes, elle n'aurait pas eu de quoi payer les indemnités juridiques en cas de problème. Pour autant, le service informatique n'avait pas conscience du risque fournisseur. Nous avons donc dû intervenir. »

Autre secteur : Les objets connectés

Ces dernières années, les équipements connectés (IoT) et les équipements connectés industriels (IIoT) ont fait l'objet d'attaques répétées via des malwares, ransomwares et cryptojackers. Il arrive que ces attaques soient menées via des frappes chirurgicales sur des cibles faciles, dans des secteurs comme la santé, ou dans les administrations nationales et locales.

Malgré la multiplication des initiatives visant à « sécuriser dès la conception », de nombreux appareils dits intelligents sont encore commercialisés trop rapidement, et leurs contrôles de sécurité sont insuffisants. Par ailleurs, les utilisateurs oublient souvent de modifier les identifiants et mots de passe par défaut… Ces identifiants d'usine peuvent pourtant être utilisés par les pirates informatiques.

Lorsqu'ils ne sont pas sécurisés, les appareils intelligents de type caméra, radiateur, ventilateur, voire même ampoule électrique, peuvent offrir aux hackers des voies d'accès secrètes aux systèmes d'une entreprise et à sa supply chain. Et une telle intrusion peut déboucher sur des vols de données colossaux.

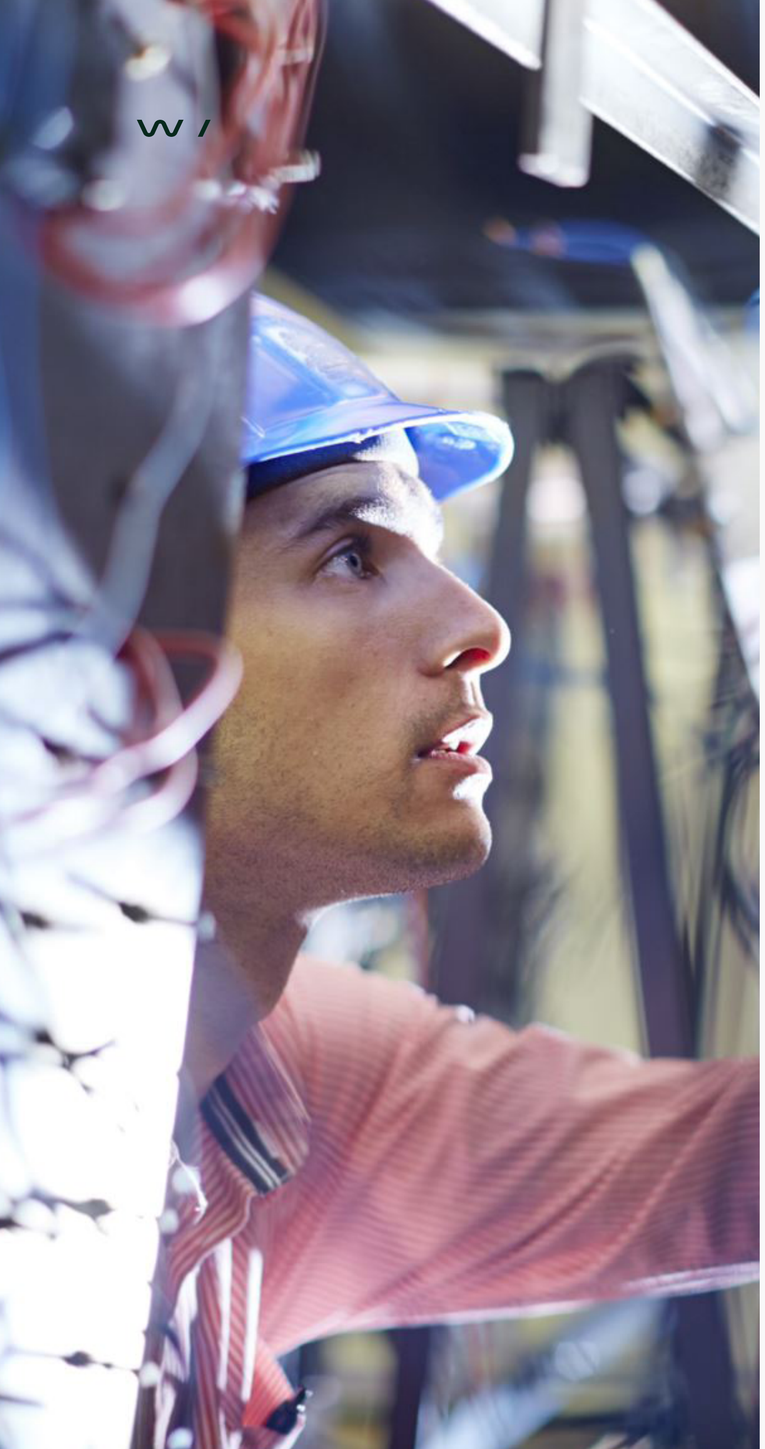
De multiples fournisseurs dans un seul produit

N'oubliez pas : pour fabriquer un produit donné, une entreprise peut mobiliser un réseau complexe de fournisseurs. Il peut s'agir des fabricants du hardware, du micrologiciel, du système d'exploitation, d'applications autonomes ou d'autres composants électroniques.

Il peut aussi exister des affiliations de partenaires pour la collecte de données, le marketing, la recherche et la publicité. Ces partenariats peuvent être invisibles pour l'utilisateur, et même pour les autres partenaires.

Les objets connectés posent de nombreux défis en matière de sécurité, de confiance et de transparence. À titre d'exemple, un rapport de la Consumers Association, publié en 2020, a révélé qu'un modèle de smart TV répandu avait envoyé des données concernant ses usagers à 700 adresses IP différentes en seulement 15 minutes. Un tel constat pose de nombreuses questions du point de vue de la protection des données.

Les RSSI doivent donc déterminer clairement à qui appartient chaque objet connecté dans l'entreprise. Ils doivent disposer d'une expertise suffisante, et rester toujours à la pointe du changement en matière de gouvernance, de comportement organisationnel, de systèmes et de processus.



Autre secteur : Industrie manufacturière

Sécuriser est encore plus difficile quand certains appareils utilisés n'ont jamais été conçus pour être exposés ou connectés à internet.

Certains secteurs sont à cet égard particulièrement vulnérables. Dans la santé, il est particulièrement difficile de moderniser, retirer ou remplacer certains appareils médicaux.

Dans l'industrie manufacturière, les systèmes de contrôle industriels (ICS) vieillissants posent eux aussi problème. Par ailleurs, dans ce secteur, les entreprises tendent à assimiler la sécurité aux technologies opérationnelles plutôt qu'aux technologies IT.

Veillez à développer des pratiques de sécurité de bout en bout, à commencer par la couche matérielle. Assurez une gestion rigoureuse de vos équipements connectés. Choisissez avec soin chaque appareil, et menez ensuite des contrôles proactifs.

Michael Weng, consultant en sécurité chez WithSecure™, explique :

« Mon travail consiste notamment à sensibiliser nos clients à la norme IEC 62443 [une norme internationale pour les systèmes industriels et systèmes de contrôle]. »

« Cette norme renvoie à un ensemble d'exigences que vous, en tant que propriétaire d'actifs, pouvez imposer aux fournisseurs ou aux intégrateurs lorsque vous bâtissez une infrastructure et utilisez leurs équipements. C'est un moyen pour vous de formuler vos exigences de sécurité, pour éviter d'être victime d'une attaque de la supply chain. »

« Les normes et la conformité ne constituent qu'une première étape. Il vous faut également contrôler le cycle de vie du développement logiciel : vous devez veiller à ce que le fournisseur y intègre la sécurité, pour minimiser les risques d'attaques de la supply chain. »

« Vous devez également mettre en place des contrôles et des stratégies pour vous assurer que votre certificat d'autorisation, d'utilisation et de distribution est sécurisé. Si ce n'est pas le cas, un pirate informatique pourrait en tirer profit. »

Les systèmes de contrôle

À une heure où les usines deviennent intelligentes, comment les responsables de la sécurité et des technologies opérationnelles peuvent-ils gérer des systèmes industriels qui n'ont pas été conçus pour internet ?

Weng explique :

« C'est un problème auquel nous sommes encore confrontés aujourd'hui. Ces appareils plus anciens n'ont jamais été conçus pour être intégrés à un réseau ou à internet. En tant que tels, ils représentent un danger évident. »

« Ils ne disposent pas de contrôles de cybersécurité suffisants. Ils ne sont pas efficacement protégés et mettent en danger le réseau et les autres systèmes. Ils deviennent un vecteur susceptible de permettre aux pirates informatiques de s'introduire sur les réseaux informatiques et sur les réseaux IoT. »

« Nous devons fermer ces points d'accès et réduire la surface d'attaque. Pour ce faire, il est possible de recourir à la technique de la « défense en profondeur ». Il s'agit de construire des couches de contrôle supplémentaires et des contre-mesures sur ces appareils. L'objectif est de mettre autant d'obstacles que possible sur le chemin d'un hacker potentiel. »

« Parfois, il faut se rendre à l'évidence et accepter le fait qu'il est nécessaire d'isoler ces systèmes d'internet et des autres systèmes informatiques de l'entreprise. »

Autre secteur : Les Services

Le secteur des services est crucial pour de nombreuses économies. Selon les chiffres du gouvernement britannique, les services représentent environ 81 % du PIB de la Grande-Bretagne et 82 % des emplois dans le pays.

La tendance est à la numérisation de ces services, notamment dans le secteur financier où les applications jouent un rôle croissant, tant pour les consommateurs que pour les entreprises. Les banques, mais aussi les services de paiement, la gestion de patrimoine et les investissements sont concernés par ces évolutions.

Durant la pandémie, les services mobiles ont littéralement explosé, au détriment des services en personne. Cette tendance a été boostée par un marché FinTech en plein essor aux États-Unis et au Royaume-Uni, et par des initiatives telles que l'Open Banking.

Étude de cas : Banque multinationale

Cette banque d'affaire américaine pèse plusieurs milliards de dollars. Elle propose des services de gestion des investissements et de gestion d'actifs. Ses principaux clients sont des institutions extrêmement bien financées et des particuliers très fortunés. Il s'agit donc d'une cible évidente pour les cybercriminels.

Pour le directeur des risques informatiques de la région EMEA de cette société, le numérique n'est pas le seul aspect de la sécurisation de la supply chain...

La sécurité repose aussi sur les individus :

« Dans le secteur financier, il est normal d'accorder la plus grande importance aux technologies et aux processus. Mais l'élément humain joue également un rôle essentiel. Ensemble, ces trois piliers (technologies, processus, personnes) forment le triangle de la sécurité. »

« La clé est la communication. Comment transmettre des informations critiques sur la sécurité à un groupe qui montre peu d'intérêt pour le sujet ? Il ne s'agit pas seulement de dire simplement "Tout va bien ? Si oui, passons à autre chose" ».

« Si vous ne disposez que de 15 minutes pour faire passer un message important sur la sécurité, il vous faut aller droit au but. C'est là que les responsables de la sécurité échouent souvent. C'est là que notre communication doit être plus pointue et plus pertinente. »

« Les professionnels de la sécurité aiment aller toujours plus loin dans le détail, mais il faut savoir cerner notre audience. Comment convaincre et dire : "C'est là que de l'argent et des ressources doivent être investis" ? Notre objectif n'est pas d'être alarmistes, mais d'expliquer la réalité de la situation. »

« Les responsables de la sécurité doivent apprendre à dire : "Nous faisons de notre mieux pour protéger l'organisation, nos partenaires, nos actionnaires, nos clients et nos employés. Parlons des menaces auxquelles nous faisons face. Quelles sont-elles ? Comment les affronter ?" »

« Il faut également leur dire : " Quelles sont les entreprises les plus lucratives avec lesquelles nous travaillons ? Quels produits génèrent le plus de profit ? En répondant à ces questions, nous saurons où se situent les menaces". »

Où la supply chain s'arrête-t-elle ?

D'autres problèmes se posent lorsque la supply chain devient trop axée sur la technologie, explique-t-il :

« Dans le secteur numérique, le concept de supply chain peut être assez flou. Exemple : vous utilisez peut-être Microsoft Teams. Microsoft fait théoriquement partie de la supply chain, de manière simple et directe. »

« Maintenant, prenez également en compte les services cloud hébergés par Microsoft. Du point de vue de la concentration des risques, l'empreinte de Microsoft devient nettement plus importante. Si Vladimir Poutine décidait soudainement de s'en prendre à Microsoft, vous auriez clairement un problème. »

L'externalisation

« La technologie est désormais extrêmement intégrée aux processus commerciaux et aux produits... si bien qu'il est devenu difficile de faire la différence entre un fournisseur et une entité si proche de l'entreprise qu'elle en devient presque un service à part entière. »

« Prenons un exemple. Partons du principe que le développement des produits est sous-traité à une maison de développement basée en Inde. Ils travaillent main dans la main avec l'entreprise, si bien qu'ils constituent une seule et même équipe : ils utilisent les mêmes adresses e-mails, et apporte la même valeur ajoutée. La distinction entre fournisseur, client et employé devient floue, ce qui nécessite une gestion prudente. »

« Nous n'avons pas encore résolu toutes ces questions. Prenons l'exemple d'un fournisseur, société de développement. Nous formulons des attentes et un contrat est signé. Mais comment pouvons-nous être certains que le produit développé pour nous restera sécurisé ? »

« Comment savoir qu'ils feront tout pour ne laisser aucune faille de sécurité dans les produits que nous vendons à nos clients ? Quelles garanties donnent-ils et comment leur demander des comptes ?»

« Il ne s'agit pas seulement de confiance. Ne vous contentez pas de faire confiance : vérifiez. »

Solutions de collaboration

Du point de vue de la sécurité, comment collaborer au sein d'un tel écosystème de fournisseurs ? Sur quelles informations se baser ?

« Il existe désormais d'innombrables outils permettant de détecter les lacunes de sécurité en temps réel. Les entreprises peuvent notamment recourir à des tests d'intrusion tiers [pen-testing] ou à des programmes de bug bounty, qui invitent des hackers éthiques à pirater vos systèmes pour en déceler les faiblesses. »

« Il faut adopter une approche basée sur le risque : vous devez prioriser les risques, selon une approche par palier. La surveillance est importante, mais vous devez également pouvoir demander des comptes à vos fournisseurs : "Montrez-moi que vous faites cela correctement". »

L'aspect réglementaire

Il y a aussi le volet réglementaire, explique-t-il. Cet aspect revêt une importance toute particulière dans un secteur aussi réglementé que le secteur financier :

« Nous nous devons d'évoquer la résilience opérationnelle. Un régulateur sectoriel pourrait dire : "Nous pensons que vous êtes trop dépendant d'un seul fournisseur, vous devez minimiser les risques et répartir la charge de travail du cloud". Un tel changement est difficile à réaliser. Il faut toujours déployer de nouvelles ressources pour répondre aux différentes exigences. »

« Le message à retenir est que la sécurité ne constitue pas un simple ajout après-coup. Elle doit faire partie intégrante de tout ce que vous faites. Elle doit être intégrée dès la conception de chaque projet ; elle se répercutera sur la technologie et les outils. »

Étude de cas : Cabinet d'avocats international

Les cabinets juridiques internationaux évoluent dans des environnements comparables à ceux des services financiers. Leurs opérations sont toutefois davantage axées sur les personnes : les avocats conseillent et représentent leurs clients en face à face, tout en gérant des volumes considérables de données confidentielles, sous forme physique et numérique.

Ces informations doivent être protégées tout au long de la supply chain, et pas seulement à l'échelle de l'entreprise. Le RSSI d'un grand cabinet basé à Londres ajoute à ce propos :

« Nous envoyons des questionnaires sur la sécurité de l'information et sur la confidentialité des données à tous nos fournisseurs, qu'il s'agisse de nos fournisseurs d'infrastructure, SaaS, d'autres services cloud, mais aussi aux compagnies de taxi et aux fleuristes... Tout le monde est évalué ! »

« Nous examinons à la loupe la sécurité de notre compagnie de taxis. Ils détiennent les noms et adresses de nos collaborateurs. Ils les reconduisent chez eux et nous leur confions notre sécurité. Nous procédons notamment à des vérifications d'antécédents et à des recherches de casier judiciaire. »

Stratégies

« Bien sûr, nous exigeons certaines garanties de la part de nos fournisseurs. Nous attendons d'eux qu'ils appliquent certains contrôles techniques appropriés au regard du service qu'ils fournissent. Nous pouvons, par exemple, exiger l'utilisation du chiffrement. »

Comme nous l'avons déjà évoqué, les attaques ciblant les outils et applications de confiance sont de plus en plus fréquentes. Cette tendance complique clairement la donne, du point de vue des processus de vérification. Il ajoute :

« Nous disposons de délais très courts pour patcher les systèmes. S'il s'agit d'un système critique ou de haute priorité, il doit être patché immédiatement. »

« Nous rejetons également 80 % des e-mails que nous recevons, mais il existe certains éléments difficiles à identifier par les systèmes anti-malware. De rares e-mails de phishing parviennent donc encore à atteindre nos boîtes de réception, mais nous utilisons d'autres technologies sophistiquées, comme la technologie CDR (Content Disarm and Reconstruction) qui permet de créer une version propre de n'importe quel document. »

« Enfin, d'autres systèmes éliminent les liens web malveillants. Nous utilisons un service de pare-feu proxy qui intègre un système de protection contre les intrusions (IPS). Il vient s'ajouter au logiciel de détection et de réponse installé sur chaque endpoint. »

Miser sur la gouvernance

La gouvernance, explique-t-il, reste au cœur du métier de RSSI :

« Nous nous engageons à respecter la norme ISO 27001 [norme internationale de gestion de la sécurité basée sur les risques]. En plus de nos audits internes, nous procédons à des audits de certification pour valider les technologies et processus en place. »

« La norme ISO 27001 concerne autant l'aspect administratif que l'aspect technique. Elle concerne les politiques, les processus et la formation que nous dispensons à nos utilisateurs. »

« La formation joue un rôle important. Nous dispensons une formation obligatoire sur la sécurité de l'information et sur la protection de la vie privée à tous nos utilisateurs, une fois par an. Nous dispensons également une formation sur mesure sur la sécurité et sur la confidentialité à tous les services commerciaux et aux groupes collaboratifs. Nous diffusons de nombreuses recommandations et conseils. »

Conclusions

Vous et vos partenaires avancez, ensemble, dans un environnement rempli de dangers. Pour rester en sécurité, il vous faut travailler ensemble. Vous devez miser sur la collaboration, mettre en place des règles communes, signer des accords. Plutôt que de faire de l'interdépendance une faiblesse, vous devez en faire une force.

Ce n'est qu'en adoptant cette approche que vous pourrez éviter l'effet papillon. Mais… Pourquoi la jungle du numérique est-elle si dangereuse ?

Jordan LaRose, Director of Consulting and Incident Response chez WithSecure™, propose, pour finir, quelques réflexions sur la sécurisation des supply chains actuelles :

« Les entreprises sont de plus en plus distribuées. Elles ont donc plus de difficultés à imposer une segmentation adéquate et un accès réseau sécurisé. Sur le plan technologique, de nombreuses équipes se tournent vers des plateformes cloud et vers des solutions d'authentification plus faibles. »

« Concernant le pipeline de code, de plus en plus d'organisations utilisent des outils publics comme GitHub. Il est possible de le verrouiller, mais du point de vue de la sécurité opérationnelle, je dirais qu'il est peu sécurisé par défaut. Plutôt que d'utiliser une solution interne comme GitLab, les développeurs préfèrent GitHub car c'est un moyen plus facile d'uploader et de gérer le code entre eux. »

« Mais les solutions de ce type peuvent favoriser les cyberattaques. Les pirates informatiques ne se serviront pas nécessairement pas du serveur GitHub comme d'un vecteur d'attaque ; ils n'y implanteront pas nécessairement de porte dérobée, mais GitHub peut leur montrer à quoi ressemble le back-end d'un logiciel. »

« Ils obtiennent ainsi une réponse à la question : "Comment concevoir ma porte dérobée ? Où puis-je l'insérer pour qu'elle m'offre un accès au réseau, tout en restant incognito ?" »

« Ils peuvent aussi consulter la liste des développeurs qui ont accès au référentiel, afin d'identifier les individus à cibler une fois sur le réseau de l'entreprise. »

« Ils peuvent ensuite s'introduire sur l'ordinateur personnel de l'un d'entre eux. Ils n'auront alors besoin que d'une connexion à GitHub, et de là, tout le référentiel de code pourra être piraté. »

« C'est un peu la même chose avec le code open-source. Le problème n'est plus tant l'informatique distribuée que l'écosystème dense des supply chains actuelles. »

Pensez comme un pirate informatique. Travaillez en équipe. Collaborez. Pour éviter l'effet papillon, restez sur le chemin de la sécurité avec WithSecure™.

« Non ! Une si petite créature ! Un papillon ! » s'écria Eckels. Le papillon tomba sur le plancher. Cet être, aussi minuscule soit-il, pouvait bouleverser tous les équilibres. De petits dominos allaient tomber, puis de plus gros dominos et, pour finir, des dominos gigantesques... Eckels était bouleversé. Il ne pouvait plus rien y changer. Tuer un papillon, cela ne pouvait pas être si grave, n'est-ce pas ? »

– A Sound of Thunder, Ray Bradbury (1952)

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.

W / T H®
secure