Supply chain, confiance et cyber attaques

Didier Danet

Supply chain, confiance et cyber attaques.

Didier Danet

Chercheur associé a GEODE, Université Paris 8

Présentation à l'European Cyber Week, Rennes 21 novembre 2024

Introduction

La mondialisation et la digitalisation des chaînes d'approvisionnement (supply chains) ont transformé les dynamiques industrielles et commerciales, créant des écosystèmes hyperconnectés. Cette interconnexion, bien qu'essentielle à l'efficacité et à la compétitivité, expose les supply chains à des **cyberattaques** de plus en plus fréquentes et sophistiquées. Ces menaces, en plus d'affecter les performances opérationnelles, mettent en péril un facteur intangible mais fondamental : la **confiance**.

La confiance, moteur de collaboration et de résilience, se trouve fragilisée par les failles de sécurité et les intrusions malveillantes. Cela soulève trois questions essentielles :

1. Pourquoi les supply chains sont-elles particulièrement vulnérables aux cyberattaques ?
2. Comment les cyberattaques affectent-elles la confiance, tant en interne qu'en externe ?
3. Quelles politiques ou stratégies permettent de préserver ou de restaurer cette confiance dans un environnement de menaces croissantes ?

En s'appuyant sur des exemples concrets et des perspectives théoriques, cette analyse explore ces questions, mettant en lumière des solutions à la fois pratiques et innovantes.

Partie 1 : Les vulnérabilités des supply chains face aux cyberattaques

1.1. Complexité et interdépendance : des vulnérabilités structurelles

Les supply chains modernes sont des réseaux complexes reliant plusieurs acteurs, souvent répartis à l'échelle mondiale. Cette interdépendance crée une **surface d'attaque étendue**, où une faille dans un seul maillon peut compromettre l'ensemble de la chaîne.

Exemple : L'affaire SolarWinds (2020) a révélé comment une intrusion dans un fournisseur de logiciels tiers a compromis des centaines d'organisations, des agences gouvernementales aux grandes entreprises.

SolarWinds : l'exemple type de l'attaque contre la supply chain

Contexte de l'attaque
La cyberattaque SolarWinds, révélée en décembre 2020, est l'une des plus importantes attaques de supply chain jamais enregistrées. Les attaquants ont compromis le logiciel de gestion Orion, développé par l'entreprise SolarWinds, en insérant un code malveillant dans une mise à jour logicielle légitime. Environ 18 000 organisations, parmi lesquelles des agences gouvernementales américaines, des multinationales, et des infrastructures critiques, ont téléchargé la mise à jour infectée, permettant aux attaquants d'accéder à leurs systèmes.

Une attaque sur la supply chain
L'attaque a ciblé un maillon crucial de la supply chain numérique : le fournisseur de logiciels tiers. En compromettant SolarWinds, les attaquants ont utilisé la confiance inhérente aux mises à jour logicielles pour pénétrer les systèmes de ses clients. Une fois infiltrés, ils ont déployé des outils de surveillance avancés pour voler des données sensibles, notamment dans les domaines de la défense, de l'énergie et des technologies.

Impacts sur l'ensemble de la supply chain

1. ***Propagation systémique** : L'attaque a mis en évidence le risque d'effet domino, où une faille dans un acteur tiers peut compromettre une chaîne entière de partenaires. Cela a affecté des entreprises privées comme Microsoft, Cisco, et FireEye, ainsi que des agences américaines stratégiques (Département du Trésor, Commerce, et Énergie).*
2. ***Perte de confiance** : Les organisations touchées ont vu leur crédibilité et la sécurité de leurs systèmes remises en cause. Cela a généré des coûts financiers importants, des retards dans les projets critiques et des impacts sur leur réputation.*
3. ***Ressources mobilisées** : Des mois d'efforts ont été nécessaires pour détecter et neutraliser les intrusions. La complexité de l'attaque a mis en évidence des failles dans la détection et la réponse aux cyberincidents.*

Mesures gouvernementales
L'attaque a déclenché une réponse rapide des gouvernements, en particulier des États-Unis, pour renforcer la résilience des supply chains :

- ***Ordres exécutifs** : En mai 2021, le président américain Joe Biden a signé un ordre exécutif visant à renforcer la cybersécurité des infrastructures critiques, incluant des exigences accrues pour les fournisseurs tiers.*
- ***Partenariats public-privé** : Des collaborations renforcées entre les gouvernements et les entreprises technologiques ont été mises en place pour améliorer le partage d'informations sur les menaces.*
- ***Normes de sécurité** : De nouvelles réglementations ont été proposées pour imposer des standards de cybersécurité plus stricts aux fournisseurs technologiques et intégrer des audits réguliers.*
- ***Investissements** : Des programmes fédéraux ont été initiés pour moderniser les systèmes technologiques et réduire la dépendance à des fournisseurs étrangers.*

Conclusion
L'attaque SolarWinds a été un signal d'alarme mondial sur les vulnérabilités des supply chains numériques. Elle a montré que la cybersécurité doit être une priorité stratégique, non seulement pour les entreprises, mais aussi pour les gouvernements. En réponse, des initiatives réglementaires et technologiques visent à renforcer la résilience des supply chains, bien que des défis subsistent pour standardiser et étendre ces efforts à l'échelle internationale.

Les vulnérabilités structurelles sont de différentes natures :

- **Etendue parfois incertaine de la supply chain** : les parties prenantes d'une supply chain X sont elles mêmes souvent insérées dans des chaînes distinctes que l'entreprise qui contrôle X

ne connaît pas entièrement. Il en résulte une surface d'attaque étendue même si la remontée de la chaîne peut alors prendre un certain temps.

- **Manque d'harmonisation des normes de sécurité** : Les standards varient d'un pays à l'autre, et les PME manquent souvent des ressources nécessaires (humaines, techniques, budgétaires) pour atteindre des niveaux de sécurité élevés.
- **Complexité des flux de données** : Les systèmes de gestion logistique (ERP, IoT, etc.) sont interconnectés, augmentant les points d'entrée pour les attaquants.
- **Insuffisance des mécanismes de supervision** : La surveillance en temps réel des chaînes d'approvisionnement est difficile à mettre en place, notamment dans des environnements multinationaux.
- **Moindre résistance au déploiement de l'intrus** : une fois l'intrus dans la supply chain, il bénéficie du climat de confiance qui y règne et peut conduire son déploiement en abusant du fait que la confiance, si elle n'exclut pas le contrôle, peut en adoucir les modalités.

Il n'est donc pas toujours évident de discerner dans cet ensemble de possibilités les voies et moyens mis en œuvre par les attaquants. Le laconisme compréhensible des victimes concernées n'aide évidemment pas à la pleine information des tiers.

Le cas Boulanger

En novembre 2024, l'enseigne Boulanger a été victime d'une cyberattaque ayant entraîné une fuite de données personnelles. Les informations concernées incluent les noms, prénoms, adresses postales, adresses e-mail et numéros de téléphone des clients. Aucune donnée bancaire n'aurait été compromise selon l'entreprise.

Cette attaque, reconnue par Boulanger, a touché plusieurs centaines de milliers de clients, bien que le pirate prétende avoir dérobé des données concernant plus de 27 millions de personnes, sans fournir de preuves concrètes. Les données provenaient possiblement des bases de données utilisées pour gérer les livraisons, impliquant potentiellement un prestataire externe. Boulanger a affirmé que ses sites et applications mobiles fonctionnent normalement avec des mesures de sécurité renforcées.

Les détails exacts de la méthode utilisée par les cybercriminels pour infiltrer le système d'information de Boulanger n'ont pas été divulgués par l'entreprise. Cependant, quelques indices permettent d'esquisser des hypothèses :

1. ***Accès via un prestataire externe** : Des informations indiquent que les données volées provenaient de bases de données utilisées pour la gestion des livraisons, potentiellement hébergées ou gérées par un sous-traitant. Cela pourrait suggérer une faille dans la chaîne logistique ou chez un partenaire tiers, confirmant le constat que la sécurité renforcée mise en place par les grands acteurs de la supply chain peuvent être contournées par l'attaque sur des maillons moins sécurisés.*
2. ***Exploitation de failles techniques** : Les attaques de ce type reposent souvent sur des vulnérabilités dans les systèmes informatiques, comme des logiciels obsolètes ou mal configurés, des accès administratifs mal protégés, ou des erreurs humaines, comme des mots de passe faibles. La faille pourrait alors être indistinctement présente chez le chef de file de la chaîne comme chez ses parties prenantes.*

3. ***Techniques de phishing*** *: Bien qu'aucun détail spécifique ne mentionne cela, il est fréquent que les pirates utilisent des campagnes de phishing pour récupérer des informations d'identification permettant l'accès initial. Cette dimension humaine de la cyber sécurité est d'autant plus critique que les innovations profitent tout autant aux attaques contre les personnes (perfectionnement du social engineering) que contre les systèmes techniques.*

1.2. Nature évolutive des menaces

L'année 2024 a malheureusement été riche en cas d'étude des attaques de la supply chain. En se limitant aux tout derniers mois et au seul périmètre national, les exemples ne manque pas de fuites de grands volumes de données détenues par des enseignes connues (Auchan, Boulanger, Cultura, Sofinco, Truffaut, Free…) résultant d'intrusion réalisées par le truchement d'outils ou de prestataires externes, notamment de fournisseurs de services informatiques. Qu'en sera-t-il en 2025 ? Il ne semble guère difficile de prédire que cette tendance ne va pas s'inverser pour de multiples raisons :

Les tendances propres de la criminalité dans l'espace numérique : l'activité cyber criminelle ne connaît pas de ralentissement. Les outils dont disposent les cyber criminels se perfectionnent et facilitent les manœuvres trompeuses, notamment la production de faux documents, voire de fausses conversation ou réunions en visio-conférence. Le coût de ces outils baisse drastiquement quand ils ne sont pas purement et simplement libres d'accès. Certains groupes offrent de concevoir et de conduire des attaques pour le compte d'autrui. En bref, le coût d'accès à des opérations criminelles est aujourd'hui à la portée de tous (ou presque)

La contrepartie de l'innovation dans la cyber sécurité : le secteur IT foisonne d'innovations ou de changements de toutes sortes. C'est évidemment une dynamique qui procure des avantages mais dont la contrepartie ne doit pas être ignorée. Le cas des nouvelles approches Zero-Trust ou Data Centric Security est particulièrement intéressant à cet égard. Leur plus-value en termes de sécurité est indéniable. Pour autant, ces transformations impliquent une adaptation des acteurs à de nouveaux outils, voire à une nouvelle approche de la cyber sécurité. La transition d'un modèle à l'autre demande des ressources dont tous les acteurs ne disposent pas et elle supposera une phase d'apprentissage pendant laquelle des erreurs seront commises. Il n'est guère difficile de comprendre que cette phase de transition sera une aubaine pour les cyber criminels.

Arnaque au président et deepfake.

En janvier 2024, une entreprise multinationale basée à Hong Kong a été victime d'une fraude sophistiquée mobilisant de manière inédite une vidéo fabriquée de toute pièce (Deepfake). Des cybercriminels ont usurpé l'identité du directeur financier de l'entreprise, basé au Royaume-Uni, en créant une vidéo falsifiée pour une visioconférence. Lors de cet échange, les escrocs ont convaincu un employé du service financier de transférer environ 26 millions de dollars sur des comptes bancaires désignés.

La fraude a exploité des vidéos et des audios accessibles en ligne pour générer une imitation réaliste de la voix et de l'apparence du cadre supérieur. Au départ, l'employé avait soupçonné un possible hameçonnage après avoir reçu des messages demandant des transactions secrètes. Cependant, la visioconférence truquée, montrant ce qu'il croyait être ses supérieurs légitimes, l'a convaincu de procéder aux transferts. Ce n'est que plusieurs jours plus tard que l'arnaque a été découverte, lorsque l'employé a contacté le siège pour obtenir des clarifications.

Cette attaque, l'une des premières de ce type à Hong Kong, donne un bon exemple des dangers induits par l'utilisation de l'intelligence artificielle dans les escroqueries. Les autorités locales ont ouvert une enquête et procédé à des arrestations liées à des utilisations frauduleuses similaires de deepfakes dans la région.

Le contexte géopolitique : La dégradation de l'environnement international encourage certains Etats (comme la Chine, la Corée du Nord ou l'Iran) à multiplier les actions offensives dans l'espace numérique pour renforcer leurs positions par l'espionnage, le sabotage ou la désinformation. La guerre en Ukraine est, à cet égard, un moteur important de l'insécurité dans le cyberespace. Les attaques menées par la Russie ne s'embarrassent guère du contrôle de leur impact et les effets de bord peuvent être particulièrement important, y compris pour les acteurs économiques européens (cf Les dommages provoqués aux éoliennes allemandes suite à l'attaque contre Viasat) La mise en œuvre d'outils nouveaux (comme certains wipers) peut également s'avérer très nocive puisqu'elle alimente la panoplie des groupes cybercriminels lesquels peuvent les récupérer et les adapter à leurs besoins. Enfin, certains groupes cyber criminels qui ont coopéré aux opérations offensives de la Russie ont consommé des ressources techniques, humaines et financières qu'ils doivent reconstituer. Ils le feront en redoublant d'attaques contre les intérêts européens ou américains, base du « deal » implicite qu'ils peuvent avoir avec les autorités russes. Surtout, l'aggravation de ces tensions géopolitiques pourrait favoriser une multiplication d'opérations hybrides visant à porter atteinte à des intérêts commerciaux à travers une combinaison d'opérations numériques (ransomwares, wipers, désinformation par exemple) mais aussi d'opérations de sabotage très concrètes. Des incendies criminels se sont multipliés en Pologne durant l'été, des colis piégés ont explosé dans des avions de DHL en Allemagne ou en Angleterre, des câbles sous-marins ont été coupés en mer Baltique. On peut imaginer que ces actions hybrides sont destinées à désorganiser, ralentir ou paralyser certaines filières essentielles pour la vie quotidienne des populations.

Partie 2 : Les impacts des cyberattaques sur la confiance

2.1. Confiance interne : relations entre les parties prenantes

La confiance est essentielle à la fluidité des échanges entre les acteurs de la supply chain. La confiance n'est pas qu'une simple inclination morale entre des parties prenantes bienveillantes. Elle est un véritable actif économique immatériel. Elle réduit l'incertitude, favorise la collaboration par le partage d'information et limite les coûts de transaction en ce qu'elle instaure une norme attendue de comportement, en particulier un bridage de l'opportunisme contractuel. Cet actif économique est donc une des sources d'efficacité économique et opérationnelle au sein d'une supply chain. Mais, cet actif est fragile. Au-delà du fait qu'une cyber attaque peut interrompre les opérations industrielles et commerciales, elle peut avoir des effets plus directs sur l'actif « confiance » :

- **La perte de données stratégiques** : Le fait que des données soient effacées, chiffrées et volées par un attaquant va affecter la coopération entre partenaires. Un climat de suspicion va presque nécessairement se développer à l'encontre du maillon par lequel l'intrusion a eu lieu. Elle va se propager à celui qui gérait les données et dont les mesures de protection n'étaient peut-être pas suffisantes… La confiance qui facilitait les échanges est perdue et, avec elle, l'avantage en termes de coûts de transaction. La défiance est particulièrement contagieuse lorsque la victime de l'attaque, craignant les effets négatifs de sa révélation, s'efforce d'empêcher qu'elle ne soit connue ou en minimise l'importance.

- **Augmenter les tensions internes** : La découverte d'une intrusion qui date souvent de plusieurs mois fait de certaines parties prenantes, de certains outils ou de certains systèmes des pestiférés. Peut-on encore accorder du crédit à ce prestataire qui nous a livré un logiciel défaillant ? Faut-il encore laisser les mises à jour se faire automatiquement ? Ne faut-il pas songer à remplacer ce maillon de la chaîne qui est aux prises avec des difficultés importantes de remise en route de son activité et qui pourrait nous contaminer une deuxième fois ou ralentir l'ensemble de la chaîne par un retour à des procédures manuelles ?

2.2. Confiance externe : perception des parties tierces

La dimension externe de la confiance vise la perception de l'intrusion par l'ensemble des acteurs qui traitent avec la supply chain : clients finals, investisseurs ou régulateurs. Une gestion de crise mal conçue et mal conduite peut :

- **Détériorer l'image de marque :** la révélation d'une cyberattaque contre une suply chain pilotée par une enseigne connue soulève presque inévitablement l'attention des médias. Les attaques récentes contre Free ou le groupe Mulliez ont fait l'objet de nombreux articles ou reportages, suscitant une certaine inquiétude des clients concernés par le vol des données. La tendance générale des entreprises touchées et de leurs communiquants étant généralement de minimiser les conséquences de l'intrusion combinée avec des messages conseillant de surveiller attentivement les opérations bancaires des personnes dont les données ont été volées constitue à cet égard un puissant moteur de défiance.

- **Provoquer des sanctions juridiques ou administratives :** La protection des infrastructures, des équipements et des données traitées par les grands opérateurs fait l'objet de nombreuses mesures réglementaires visant à éviter les attaques ou à en réduire l'impact. Lorsque des fuites massives de données interviennent ou que la sécurité des opérations d'une supply chain est mise en cause, la victime s'expose à des procédures réglementaires ou judiciaires. Elle doit alors faire face à des demandes d'explication, voire des enquêtes qui, là encore, ne vont pas restaurer son crédit auprès de l'ensemble de ses partenaires.

- **Réduire la confiance des actionnaires** : Last but not least, une cyber attaque peut avoir un effet négatif sur la valeur boursière de la victime et lui faire perdre une partie de son crédit auprès de ses actionnaires. Il lui sera alors plus difficile et plus coûteux d'obtenir les financements propres dont elle pourrait avoir besoin pour son développement futur.

Les sanctions en cas de manquement aux règles de protection des données.

La protection des données fait l'objet de dispositions légales et réglementaires (notamment celles issues du RGPD) mises en application par la CNIL.

À l'issue de contrôle ou de plaintes, en cas de méconnaissance des dispositions du RGPD ou de la loi de la part des responsables de traitement et des sous-traitants, la formation restreinte de la CNIL ou son président peuvent prononcer des sanctions à l'égard des responsables de traitements qui ne respecteraient pas ces textes.

***Concernant la procédure ordinaire**, avec le RGPD (règlement général sur la protection des données), **le montant des sanctions pécuniaires peut s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial**. Ces sanctions peuvent être rendues publiques.*

Lorsque des manquements au RGPD ou à la loi sont portés à sa connaissance, la formation restreinte de la CNIL peut :

- *prononcer un rappel à l'ordre ;*
- *enjoindre de mettre le traitement en conformité, y compris sous astreinte ;*
- *limiter temporairement ou définitivement un traitement ;*
- *suspendre les flux de données ;*
- *ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte ;*
- *prononcer une amende administrative.*

***Concernant la procédure simplifiée**, la loi Informatique et Libertés prévoit des sanctions moins nombreuses et moins sévères que celles encourues dans la procédure ordinaire. Ces sanctions ne peuvent par ailleurs jamais être rendues publiques.*

Dans ce cadre, le président de la formation restreinte peut :

- *prononcer un rappel à l'ordre ;*
- *enjoindre de mettre le traitement en conformité, y compris sous astreinte d'un montant maximal de 100 € par jour de retard ;*
- *prononcer une amende administrative d'un montant maximal de 20 000 €.*[1]

Comme toutes les normes de ce type, les dispositions sanctionnant les manquements à la protection des données peuvent être jugées trop timides au regard de l'importance de la protection des données. Quant à leur effectivité, c'est-à-dire leur application réelle, là aussi, des débats peuvent exister quant à la manière dont le régulateur appréhende les faits et détermine la sanction.

Partie 3 : Stratégies pour préserver ou restaurer la confiance

Au sein d'une supply chain, l'impact d'une attaque est démultipliée puisque la désorganisation et la méfiance s'étendent à l'ensemble des maillons de cette chaîne. Il est donc peut être encore plus important de protéger la chaîne contre des attaques qui ont vocation à se multiplier. Cette mise en sécurité comporte de nombreux aspects, certains très matériels (Comment sensibiliser les différents maillons de la chaîne à la nécessité de sécuriser leurs systèmes automatisés ? Comment rédiger une fiche d'incident ?...) Elle comporte également une dimension organisationnelle, technique… La troisième partie de la présentation se consacre pour sa part à la « philosophie » de la cybersécurité ou, pour le dire autrement, à l'esprit dans lequel est abordée la politique et la mise en œuvre des mesures de protection de la supply chain. En simplifiant à l'extrême, deux grandes approches peuvent se rencontrer, la première que l'on qualifiera de « rétributive » et la seconde d' »exploratoire ».

3.1. Approche rétributive : une solution dissuasive mais d'une efficacité limitée

[1] https://www.cnil.fr/fr/definition/sanction

La logique rétributive repose sur un cadre strict de sanctions pour les acteurs jugés négligents. L'objectif poursuivi par le pilote de la supply chain est d'imposer à tous les membres de la chaîne un alignement de leurs mesures de sécurité sur un standard jugé propre à empêcher l'intrusion d'attaquants au sein de la chaîne. Cette approche prend la forme de :

- **Contrats renforcés** : Définissant des obligations de faire ou de ne pas faire ; elle définit des responsabilités et des sanctions claires pouvant trouver leur sources dans les normes juridiques en vigueur ou dans des normes contractuelles qui les complètent. Cette approche relève du même esprit que les politiques de qualité menées, par exemple, par les enseignes de la grande distribution et qui imposent, au nom de la transparence et de leur propre responsabilité en matière de traçage des produits, des règles particulièrement détaillées à leurs fournisseurs avec un dispositif de contrôle que l'on pourrait qualifier de très intrusif.
- **Punition des manquements** : En cas d'intrusion, la victime est considérée comme fautive. Elle est soupçonnée de n'avoir pas respecté à la lettre les termes du contrat de cybersécurité, ce qui est souvent vrai si, par exemple, la charte de cybersécurité impose un devoir de vigilance à l'égard de l'ouverture des pièces jointes dans les courriers électronique. Dans ce cas, la victime s'expose à des punitions pouvant aller de sanctions contractuelles jusqu'à des sanctions judiciaires civiles ou pénales.

Cette méthode qui domine largement dans la conception des politiques de cybersécurité des supply chains, présente deux grandes séries d'inconvénients :

- **Elle réduit mais ne fait pas disparaître les intrusions dans la chaîne :** les supply chains présentent des vulnérabilités spécifiques qui jouent incontestablement en faveur des attaquants. Imposer l'alignement de tous les maillons sur des standards de sécurité qu'ils atteindront et maintiendront difficilement compte tenu des ressources dont ils disposent est donc largement illusoire. Aucune supply chain ne peut se dire exempte de tout risque d'intrusion du fait d'une charte de cybersécurité, fût elle d'une impitoyable sévérité.
- **Surtout, la logique rétributive a un effet délétère en cas d'intrusion :** lorsqu'une intrusion s'est produite, tout l'effort de la supply chain doit tendre vers la lutte contre la menace. Les questions sont nombreuses et difficiles : depuis quand l'intrusion a-t-elle eu lieu ? Jusqu'où l'attaquant s'est-il déployé ? Qu'a-t-il modifié dans le système ? Quelles données a-t-il volé ? … La réponse à ces questions supposerait une coopération pleine et entière de tous les acteurs de la chaîne. Mais, à cause de la logique rétributive, le premier concerné, celui qui dispose des informations les plus précieuses, c'est-à-dire la victime de l'intrusion, se mure dans le silence ou la dénégation car il se sait en position d'accusé. La logique rétributive fait de lui un coupable dont la seule préoccupation est, dès lors, d'échapper à toute responsabilité et à toute sanction. Ceux qui luttent contre l'attaque se retrouvent alors dans la peau du détective qui doit confondre le coupable pour résoudre l'affaire. Il va sans dire que cette enquête policière fait perdre un temps précieux, qu'elle ne rassemble l'information utile que par bribes successives, qu'elle exige des procédures susceptibles de valoir comme preuve en cas de litige judiciaire, qu'elle décuple la méfiance au sein de la chaîne…

Le bilan de la logique rétributive est donc pour le moins mauvais : elle ne permet pas de construire une barrière sécuritaire impénétrable (même si elle incite par la peur à adopter des comportements responsables ou à mettre en place des dispositifs utiles) et elle génère immanquablement une absence de coopération de la victime en cas d'intrusion. Or, sans cette coopération, l'attaquant bénéficie d'un avantage précieux qu'il peut exploiter pour parfaire ses opérations au sein de la chaîne.

3.2. Approche exploratoire : un modèle collaboratif

Une cyber sécurité fondée sur une logique exploratoire ne consiste pas à prendre l'entier contrepied de la logique rétributive. Elle n'écarte pas l'idée d'imposer certaines normes communes pour renforcer la sécurité de l'ensemble de la chaîne. Mais, elle s'en distingue radicalement sur un point : l'absence de sanctions à l'encontre de la victime.

La logique exploratoire ne se donne pas pour objectif le « zéro intrusion ». Elle part du principe que tout système automatisé interconnecté à travers l'espace numérique est susceptible d'être attaqué et pénétré. Certains systèmes sont mieux protégés que d'autres mais, dans le cas de supply chains étendues et impliquant un certain nombre d'acteurs hétérogènes, l'intrusion d'un groupe cyber criminel doté de moyens quasi étatiques est toujours possible. Le problème est donc moins de rendre la supply chain totalement impénétrable que de favoriser une réaction rapide et appropriée pour limiter les dommages et bouter l'attaquant hors de la chaîne. Les principaux points d'une approche exploratoire sont alors les suivants :

- **La mise en place de normes adaptées aux ressources des parties prenantes :** là où l'approche rétributive tend à imposer des normes homogènes pour aligner l'ensemble des maillons de la chaîne sur une même exigence, l'approche exploratoire peut se contenter de normes plus souples, mobilisant d'ailleurs l'atout de la confiance pour laisser chaque acteur tendre vers un idéal sécuritaire tout en sachant que les contraintes qui pèsent sur lui ne lui permettront pas de l'atteindre dans toutes ses dimensions. La confiance qui règne au sein de la chaîne doit permettre que 'instauration de normes souples soit interprétée par chaque maillon comme une obligation à satisfaire de bonne foi et au mieux de ce qu'il est possible de faire. La chaîne n'est donc pas victime d'une illusion d'invulnérabilité ; elle se sait plus ou moins fragile à tel endroit (et peut d'ailleurs demander à ce que ces sources de fragilité soient répertoriées et partagées)
- **Le principe de non punition :** le but de l'approche exploratoire est tout entier tourné vers la coopération des acteurs en cas d'intrusion, en premier lieu la coopération pleine, entière et immédiate de la victime. Puisque la crainte des sanctions mure la victime dans le silence et la dénégation, l'approche exploratoire renverse le principe et stipule que la victime d'une attaque informatique ne sera pas l'objet de sanctions du fait de l'intrusion. Ce principe est assortie de certaines conditions pour qu'il ne soit pas une incitation à l'irresponsabilité. La première condition tient à l'attitude de la victime. En cas d'intrusion, elle doit faire remonter immédiatement toute l'information qui est en sa possession de sorte que les services compétents puissent agir rapidement et sans avoir à conduire une enquête de police sur les circonstances, les causes ou les effets de l'attaque. Si la victime ne se montre pas diligente ou cache volontairement certains éléments, par exemple la violation d'une obligation stipulée par la charte de cybersécurité, le principe de non punition est écarté. La seconde condition tient à la faute éventuelle de la victime. Toute faute n'est pas excusable, en particulier s'il s'agit d'une faute lourde, voire d'une faute volontaire, la victime étant alors complice intentionnel de l'attaquant ou ayant elle-même conduit une attaque. Une interprétation casuistique sera alors nécessaire dans certains cas mais une jurisprudence existe et l'interprétation n'est pas forcément si difficile qu'elle suffise à écarter l'approche exploratoire.

La logique exploratoire est souvent critiquée par les responsables des systèmes d'information car elle semble encourager l'irresponsabilité des usagers du système que l'on soupçonne alors, du fait de l'absence de sanctions, de ne plus se préoccuper du tout des questions de sécurité et mettre en péril l'ensemble de la supply chain. Elle est également mal perçue par les juristes chargés de rédiger les

chartes de cyber sécurité car l'édiction de règles dépourvues de sanctions leur apparaît comme gage d'inefficacité. Mais, encore une fois, la confiance qui se développe entre les membres d'une supply chain constitue un garde-fou puissant contre les comportements opportunistes dévastateurs. L'intérêt bien compris d'une partie prenante de la chaîne est d'interpréter les obligations qui lui incombent dans le sens d'un intérêt général commun dont tous sont responsables. Si les normes de sécurité sont suffisamment élevées pour garantie une protection solide des systèmes de traitement automatisés mais suffisamment souples pour que chaque acteur puisse les appliquer de manière raisonnable dans la limite de ses propres moyens, la supply chain se saura vulnérable sur tel ou tel point. Mais, elle se met en situation de lutter le plus efficacement possible contre une attaque réussie.

La logique exploratoire apparaît donc intéressante, avec des **sanctions ciblées pour les fautes graves** et une coopération renforcée pour les incidents signalés rapidement.

Conclusion

Les supply chains sont confrontées à des défis croissants liés aux cyberattaques, compromettant non seulement leurs performances mais aussi la confiance entre les parties prenantes. Les nombreux exemples d'attaques réussies contre des supply chains impliquant pourtant des acteurs puissants et compétents (Auchan, Free, Sofinco…) montre pour autant qu'aucune supply chain ne peut se prétendre à l'abri d'une attaque réussie et d'une intrusion qui rebondit de partie prenante en partie prenante en abusant de la confiance qui forme l'atout essentiel de la supply chain.

Le problème principal de la cybersécurité dans les supply chains n'est donc pas de parer à toute attaque mais de lutter le plus efficacement possible en cas d'attaque réussie. A cet égard, la condition fondamentale pour lutter contre l'intrus est la détection la plus précoce possible de sa présence et la compréhension la plus fine possible de ce qu'il a pu faire pour pouvoir ensuite prendre les mesures propres à le neutraliser. Or, cette condition fondamentale repose sur la coopération pleine et entière de tous les acteurs de la supply chain, en premier lieu de la victime.

Une bonne politique de cyber sécurité dans une supply chain doit donc mettre en avant la confiance qui est son tout essentiel et poser par principe que la victime d'une attaque ne saurait subir de sanction, même en cas d'erreur simple, dès lors qu'elle coopère immédiatement et sans restriction à la lutte contre l'attaque. Cette approche heurte nos habitudes qui associent faute et sanction selon une logique rétributive. Mais, ces habitudes doivent changer si l'efficacité de la lutte contre les cyber attaques est à ce prix.