SOPHOS
Cybersecurity evolved.

Réduire les risques d'attaque de la supply chain : Guide des bonnes pratiques

Les cyberattaques de la supply chain se sont fait connaître du grand public en décembre 2020 avec le cas de la société de surveillance informatique SolarWinds, mais elles sont loin d'être un phénomène nouveau. En réalité, et c'est un constat inquiétant, presque une victime de ransomware sur dix (9 %) rapporte que l'attaque s'est immiscée par le biais d'un fournisseur tiers de confiance, selon une enquête Sophos réalisée en 2020 auprès de 5 000 responsables informatiques dans 26 pays[1].

Mais qu'entend-on exactement par « attaque de la supply chain », et quel est son fonctionnement ? Et plus important encore, que pouvez-vous faire pour protéger votre organisation des conséquences d'une attaque de la supply chain ?

Ce document examine toutes ces questions et apporte des réponses.

1 L'état des ransomwares 2020 – Sophos, 2020

Un livre blanc Sophos. Avril 2021

Qu'entend-on par « attaque de la supply chain » ?

Souvent, les organisations font appel à un prestataire externe pour gérer tout ou partie d'une activité ou fonction spécifique, comme leur infrastructure informatique. Si le fait d'autoriser ces sous-traitants à se connecter à votre réseau présente des avantages pour vous (en libérant des ressources en interne par exemple), cela introduit des risques de sécurité, notamment une vulnérabilité aux attaques de la supply chain

Dans une attaque de la supply chain, plutôt que de vous infiltrer directement, les attaquants exploitent les accès que vous avez déjà autorisés à vos fournisseurs tiers. À partir du moment où ils parviennent à s'introduire dans votre environnement, ils peuvent lancer toutes sortes d'activités malveillantes.

Le risque d'une attaque de la supply chain existe donc dès lors que vous avez un sous-traitant — et un seul suffit — connecté à votre réseau. En moyenne, les petites et moyennes entreprises déclarent avoir au moins trois fournisseurs autorisés à se connecter à leurs systèmes.[2] Sécuriser ces fournisseurs connectés génère d'importants défis et une charge de travail accrue pour les équipes informatiques. Pour corser le problème, les attaques de la supply chain sont difficilement détectables et il est compliqué de s'en protéger, car l'attaque peut se produire à n'importe quel niveau de la chaine d'approvisionnement.

Types de fournisseurs tiers

Les prestataires de services professionnels et de services informatiques sont les deux principaux types de fournisseurs pouvant se connecter au réseau d'une organisation.

Services professionnels

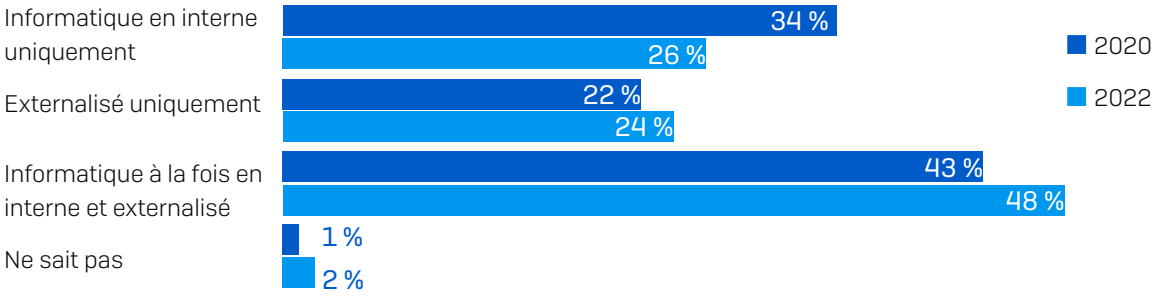
Les services professionnels sont souvent sollicités pour gérer de manière indépendante des fonctions commerciales (ou des parties de celles-ci) lorsque les entreprises ne disposent pas en interne des compétences et des connaissances spécialisées requises. Prenons l'exemple d'un cabinet d'expertise comptable qui pourra accéder à des données financières sensibles (via un logiciel) pour fournir à son client les analyses et les informations pour lesquelles il a été engagé. Comme vous pouvez l'imaginer, une cyberattaque réussie contre une telle organisation pourrait être dévastatrice pour son portefeuille de clients.

Fournisseurs de services informatiques

Les fournisseurs de services informatiques sont des sociétés externes chargées de gérer l'infrastructure informatique ou la sécurité informatique d'une entreprise. Souvent connus sous le nom de fournisseurs de services managés (MSP) ou de fournisseurs de services de sécurité managés (MSSP), ils sont fréquemment visés par les attaques de la supply chain.

Ce sont des cibles particulièrement intéressantes, car elles détiennent les clés d'un grand nombre de clients. D'ici 2022, 72 % des organisations externaliseront leur sécurité informatique[3], c'est pourquoi la posture de sécurité de ces prestataires est d'une importance capitale pour la vôtre.

Comment la sécurité informatique est assurée : Aujourd'hui et d'ici 2022



2,3 Cybersécurité : le défi humain – Sophos, 2020

Types d'attaques contre la supply chain

Si les attaques de la supply chain diffèrent en termes de mode opératoire, les principes et la finalité pour les attaquants sont souvent les mêmes : infiltrer un fournisseur tiers de confiance et exploiter son accès pour implanter un malware, voler des données de propriété intellectuelle ou espionner les communications internes.

Attaques par phishing

Les emails de phishing constituent l'un des vecteurs d'attaque les plus couramment utilisés par les attaquants de la supply chain. L'objectif des attaquants est d'accéder au réseau des fournisseurs tiers ciblés et de le compromettre, puis de l'utiliser comme tremplin pour infiltrer les systèmes de leurs clients.

Mise à jour logicielle compromise

Dans des attaques plus sophistiquées de la supply chain, les hackers s'infiltrent dans l'infrastructure d'une société ou d'un distributeur de logiciels et insèrent un code malveillant dans les packs de mise à jour des logiciels. Le prestataire distribue ensuite ces mises à jour à ses clients, en les infectant à son insu. Comme vous vous en doutez, les conséquences peuvent être catastrophiques, surtout si l'organisation possède une clientèle importante. L'attaque SolarWinds de décembre 2020 est un parfait exemple de ce type d'attaque.

Étude de cas d'une attaque de la supply chain : SolarWinds

Fin 2020, on a découvert que la supply chain de la société de gestion informatique SolarWinds avait été compromise. Cette cyberattaque, qui a mis en lumière la vulnérabilité de la sécurité de la supply chain, a fait la Une des journaux dans le monde entier. On estime à plus de 18 000 le nombre de clients ayant été touchés.

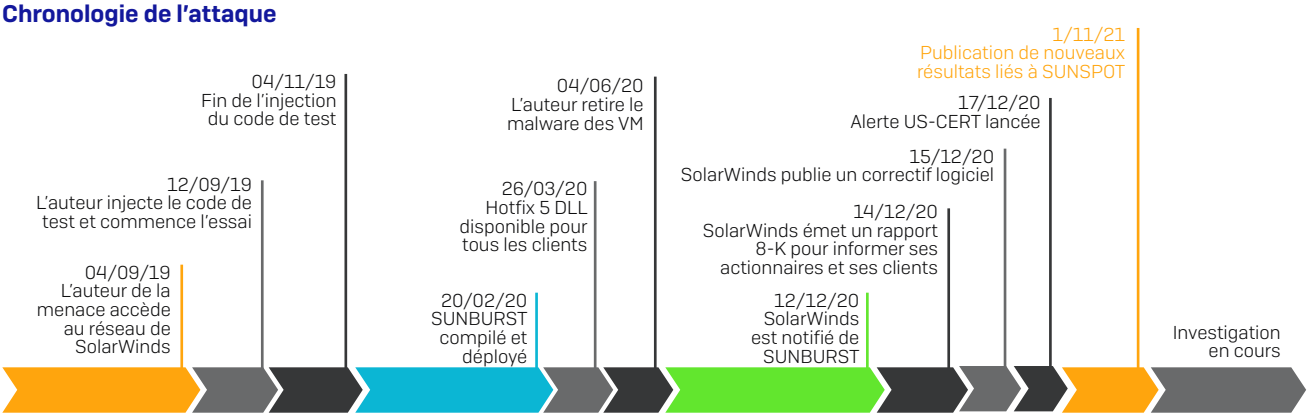
Il est à noter que, à la date de publication de ce document (avril 2021), l'enquête sur l'attaque de SolarWinds est toujours en cours et les conclusions peuvent changer.

Comment les attaquants ont-ils procédé ?

En résumé, les pirates ont réussi à insérer un code malveillant dans Orion, la plateforme de gestion et de surveillance des infrastructures de SolarWinds. Ce code malveillant a ensuite été envoyé involontairement aux clients à travers une mise à jour logicielle classique. Environ 18 000 clients (dont bon nombre d'entreprises du classement Fortune 500 et d'agences gouvernementales américaines) auraient installé ces mises à jour, devenant ainsi vulnérables aux attaques.

Fait inquiétant, SolarWinds aurait soupçonné des indices d'actes criminels dès septembre 2019, comme le montre la chronologie ci-dessous. Ces soupçons suggèrent d'une part que le coup était calculé et d'autre part, que les auteurs de la menace ont fait preuve d'une extrême prudence, cherchant à dissimuler au maximum leur intrusion. Vous pouvez lire l'analyse approfondie de Sophos sur la façon dont le variant du malware Sunburst a échappé aux défenses de sécurité ici.

Chronologie de l'attaque



Tous les événements, dates et heures sont approximatifs et sujets à modification, en attendant la fin de l'enquête

SolarWinds - https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

Quel a été l'impact de l'attaque ?

Le succès de l'attaque, baptisée Sunburst, a donné aux auteurs un accès étendu aux systèmes d'information des entreprises et des organismes gouvernementaux ciblés. De grandes quantités de données ont été volées (dont le volume reste à déterminer) et l'on craint que les attaquants n'aient profité de ces accès pour introduire d'autres portes dérobées, qui n'ont pour l'heure pas encore été découvertes.

Mais ce qu'il faut vraiment retenir de cette attaque mondiale, c'est le manque évident de préparation des entreprises en matière de défense contre les attaques de la supply chain.

Des packages empoisonnés

Un type d'attaque de la supply chain moins courant, mais qui devrait se répandre à l'avenir, est ce que nous avons appelé les « packages empoisonnés ». À mesure que l'utilisation du Cloud, de Docker et des méthodologies de développement agiles s'intensifie, le recours à des composants prêts à l'emploi permettant de raccourcir le cycle de vie du développement se multiplie également. Les cybercriminels ont commencé à piéger certains conteneurs, bibliothèques et autres ressources couramment utilisés, dans l'espoir d'être intégrés dans votre produit final.

Recommandations pour se protéger contre ces attaques

Étant donné la complexité et la nature des attaques de la supply chain, la technologie seule ne suffit pas pour les empêcher. Les bonnes pratiques suivantes ont pour but de vous permettre de minimiser le risque associé à une attaque de la supply chain.

1. Passez d'une approche réactive à une approche proactive de la cybersécurité

SolarWinds a été le signal d'alarme pour de nombreuses entreprises à travers le monde. Lorsqu'une attaque devient évidente, il est souvent trop tard. Au moment où un criminel lance une charge utile, il a déjà eu accès à votre réseau pendant plusieurs jours et a peut-être déjà volé des données critiques. Il faut donc adopter une nouvelle stratégie : partez du principe que vous êtes compromis et traquez les menaces avant qu'il ne soit trop tard. Il existe des technologies et des services qui étayent cette approche, nous y reviendrons plus loin.

2. Surveillez les premiers signes de compromission

Lors des investigations menées par l'équipe Sophos Managed Threat Response (MTR), deux signes avant-coureurs semblent se démarquer. D'une part, l'utilisation d'identifiants pour l'accès à distance et des tâches administratives en dehors des heures de travail ; d'autre part, l'utilisation abusive d'outils d'administration système pour surveiller et exfiltrer des données volées en dehors du réseau.

L'expression « Living Off the Land » (LOL) est souvent utilisée pour désigner cette technique qui consiste à utiliser des comptes légitimes et vos propres outils pour obtenir et maintenir une persistance. La détection de ces comportements exige de la vigilance et des compétences, et un analyste qualifié en opérations de sécurité est capable de les identifier rapidement et de vous alerter avant que les dégâts n'aient lieu. Deux solutions s'offrent donc à vous : soit vous investissez dans la technologie et la formation requises pour surveiller ces signaux en interne, soit vous faites appel à un prestataire de services de détection et de réponse managés (MDR) pour le faire à votre place.

3. Faites un audit de votre supply chain.

Cela peut sembler évident, mais prendre le temps de répertorier l'ensemble des organisations avec lesquelles vous êtes en relation peut s'avérer inestimable. Il y en a probablement plus que vous ne le pensez. En faisant cet exercice, vous pourrez rapidement identifier les maillons faibles (par exemple, les sociétés les plus propices à la cybercriminalité) et prendre des mesures supplémentaires pour atténuer les risques associés. Vous serez certainement en relation avec des fournisseurs tiers, par exemple :

- **Prestataires de services informatiques**
  - MSP/MSSP
  - Fournisseurs de Cloud
- **Services professionnels**
  - Finance
  - Juridique
  - Sécurité
  - Service d'entretien
- **Fournisseurs**
  - Matériaux
  - Services
  - Main-d'œuvre
  - Logistique

Une fois que vous aurez inventorié les prestataires avec lesquels vous travaillez, vous pourrez évaluer le type d'accès réseau dont ils disposent et les informations auxquelles ils peuvent accéder en utilisant leurs identifiants. Si leurs privilèges d'accès sont largement surévalués, il est temps de verrouiller cet accès et de le limiter aux seules données nécessaires. Commencez par les prestataires dont l'accès à vos données est le moins essentiel, puis ainsi de suite par ordre croissant.

4. Évaluez la posture de sécurité de vos fournisseurs et partenaires commerciaux

Il existe plusieurs approches évaluer la posture de sécurité de vos fournisseurs. Pour les grands prestataires de services, les opérateurs de Cloud et les sociétés de traitement des paiements, nous vous conseillons de vérifier leurs types de certifications et les audits auxquels ils sont soumis.

Par exemple, une société de traitement des paiements doit être en conformité avec la norme PCI DSS. Si elle est soumise à la norme PCI DSS niveau 1 ou 2, vous devriez lui demander son rapport de conformité (RoC) délivré par leur QSA/ISA (Qualified Security Assessor/Internal Security Assessor). Vous devriez examiner ces rapports RoC tous les trimestres pour être bien sûr que la société répond bien à vos exigences.

Une autre certification répandue pour valider les audits est la SOC 2/2+/3 relative aux fournisseurs de services Cloud. Les audits SOC évaluent les contrôles de sécurité et les mesures d'atténuation couvrant cinq principes de confiance : la confidentialité, la sécurité, la disponibilité, l'intégrité du traitement et le respect de la vie privée.

Tout comme pour votre propre sécurité, aucun nombre d'audits ne constitue une véritable garantie en soi, mais ils montrent néanmoins que le prestataire prend la sécurité et la conformité au sérieux. Les rapports de tests de pénétration, la conformité au RGPD, la fréquence des failles ou des violations de données antérieures sont d'autres informations utiles à prendre en compte ou à demander le cas échéant.

5. Passez constamment en revue votre propre hygiène informatique

Si la posture de vos prestataires est déterminante pour vous protéger contre les attaques de la supply chain, ne négligez pas votre propre « hygiène » en matière de cybersécurité. De nombreuses organisations n'en font pas cas, soit parce qu'elles ne savent pas par où commencer, soit parce qu'elles pensent ne pas être assez importantes pour faire l'objet d'une compromission. Vos pratiques de cybersécurité peuvent faire toute la différence entre un léger désagrément et une fuite de données de grande envergure.

Activez l'authentification multifacteur (MFA)

Dans les attaques de la supply chain, la technique la plus employée est l'utilisation d'un accès volé, mais autorisé. Trop souvent, les prestataires de services se voient attribuer des identifiants leur donnant les mêmes droits et privilèges que les employés de l'entreprise.

Cela signifie qu'ils ne sont pas soumis à l'authentification multifacteur (MFA), ce qui permet aux pirates d'exploiter les identifiants volés lors des attaques de phishing mais aussi leur réutilisation non autorisée par leur personnel. Et comme la plupart des organisations utilisent l'authentification unique (SSO), ces identifiants peuvent être exploités pour accéder à toutes sortes de systèmes qui ne sont pas nécessaires dans le cadre de la mission qui leur est confiée, ce qui accroît les risques d'intrusions malveillantes, qu'elles soient internes ou externes.

Passez en revue l'accès des fournisseurs et les privilèges des applications

Une autre erreur courante consiste à fournir un VPN, un RDP ou un autre moyen d'accès à distance en libre accès à des prestataires pour leur permettre de gérer les solutions. Par libre accès, nous entendons l'accès à l'ensemble du réseau au lieu de segmenter et de restreindre les outils d'accès à distance nécessaires.

Tous les outils d'accès à distance doivent mettre en place une authentification multifactorielle et être limités à des hôtes ou systèmes uniques. Lorsqu'un accès supplémentaire est requis, il est recommandé d'utiliser des « jump servers » pour réduire les risques et offrir des options supplémentaires de surveillance et de journalisation.

Le fait d'autoriser par défaut toutes les applications signées par le certificat logiciel d'un fournisseur expose également les entreprises aux attaques de la supply chain. Nous avons vu à plusieurs reprises des certificats volés et utilisés abusivement pour signer des malwares. Les outils de sécurité doivent tout inspecter, sans exception.

Surveillez de manière proactive les bulletins de sécurité des fournisseurs

Surveillez les bulletins de sécurité de tous vos fournisseurs pour pouvoir déployer rapidement des correctifs et des mesures d'atténuation lorsque des vulnérabilités apparaissent, et tenez-vous au courant de leur actualité. Si une crise arrive suite à un incident, vous ne serez peut-être pas en tête de la liste des entreprises à prévenir. Cela peut vous permettre de verrouiller l'accès puis de vérifier si vous êtes impacté par leur situation.

Passez en revue votre police d'assurance cybersécurité (si vous en avez une)

Enfin, si vous avez une assurance cybersécurité, vérifiez si elle couvre les pertes liées aux tierces parties et comment faire jouer la police, le cas échéant. Vérifiez auprès de vos fournisseurs que votre couverture s'aligne sur leur couverture.

Facilitateur en matière de technologie et de service

Comme nous l'avons vu, se défendre contre les attaques de la supply chain est complexe de par leur nature. Une bonne pratique consiste davantage à maîtriser les risques qui leur sont associés et d'atténuer les dégâts. Heureusement, il existe des technologies et des services qui sont idéalement placés pour prendre en charge cette gestion des risques.

Chasse aux menaces (Threat Hunting)

Nous avons mentionné la nécessité d'adopter une approche proactive de la cybersécurité afin de bien se protéger des attaques de la supply chain. L'une des techniques clés de cette approche consiste à mettre en place une chasse aux menaces.

Endpoint Detection and Response (EDR)

La technologie EDR est un élément clé de la chasse aux menaces. Habituellement intégrée aux plateformes de protection Endpoint, l'EDR associe la surveillance continue en temps réel et la protection des données sur les terminaux avec des capacités de réponse et d'analyse automatisées. Cela permet aux équipes de sécurité d'identifier rapidement les menaces et d'y remédier.

Sophos Intercept X Endpoint comprend une puissante fonctionnalité EDR. Sophos EDR est la première solution conçue à la fois pour les analystes de sécurité et les administrateurs informatiques, qui offre les outils nécessaires pour poser des questions détaillées lorsque vous devez traquer les menaces et renforcer l'hygiène de vos opérations de sécurité. Elle vous permet d'effectuer des requêtes SQL puissantes, prêtes à l'emploi et personnalisables qui vous donnent les informations dont vous avez besoin pour prendre des décisions éclairées.

De plus, la fonction d'identification automatique des menaces de Sophos EDR vous permet d'identifier automatiquement les activités suspectes, de prioriser les indicateurs de menaces et de rechercher rapidement les menaces potentielles sur vos terminaux et vos serveurs.

En savoir plus sur les fonctionnalités EDR de Sophos

Services MDR (Managed Detection and Response)

Les cybermenaces les plus ravageuses, tel le piratage de SolarWinds, impliquent généralement des attaques menées par des humains. Si la technologie, en particulier les outils de chasse aux menaces tels que l'EDR, joue un rôle important, il est indispensable de faire appel à des experts. Pour arrêter des attaques menées par des humains, il faut une chasse aux menaces menée des humains. Les directeurs informatiques le savent bien, puisque 48 % d'entre eux prévoient d'intégrer ces pratiques au cours de l'année prochaine[4].

Une des façons d'y parvenir consiste à utiliser un service MDR (Managed Detection and Response). Le service Managed Threat Response (MTR) de Sophos va au-delà de la simple notification des menaces. Il met à la disposition de votre service informatique une équipe dédiée d'experts en cybersécurité qui travaille 24 heures sur 24 pour traquer, valider et corriger les menaces et incidents potentiels de manière proactive.

4 Cybersécurité : le défi humain – Sophos, 2020

L'équipe Sophos MTR, composée de chasseurs de menaces et d'experts en réponse, va :

- Chasser de manière proactive et confirmer les menaces et incidents potentiels
- Utiliser toutes les informations disponibles pour déterminer l'ampleur et la criticité des menaces
- Prendre en compte le contexte professionnel approprié pour valider les menaces
- Lancer des actions pour intercepter, contenir et neutraliser les menaces
- Fournir des conseils pratiques pour remédier aux causes profondes des incidents récurrents

En savoir plus sur Sophos MTR

Évoluer vers une approche Zero Trust de la cybersécurité

Nous avons vu plus haut qu'il était important de revoir votre propre posture de sécurité, en activant notamment l'authentification MFA et en vérifiant régulièrement les privilèges des applications et accès. Cela est possible en adoptant une approche Zero Trust de la cybersécurité.

Le principe de Zero Trust se base sur la formule : « Ne faites confiance à rien, vérifiez tout » et se focalise sur la protection des ressources indépendamment de leur emplacement physique ou digital. Aucun fournisseur, produit ou technologie ne vous permettra d'atteindre un niveau de confiance zéro. Pour y parvenir, il faut profondément revoir la manière dont nous protégeons nos ressources en modifiant notre approche de la cybersécurité et en installant une diversité de solutions de sécurité. L'adoption d'une solution d'accès réseau Zero Trust ou ZTNA (Zero Trust Network Access) constitue néanmoins un tremplin vers ce modèle.

Comme son nom l'indique, le ZTNA est basé sur le principe de Zero Trust. Il permet aux utilisateurs d'accéder aux données en toute sécurité, où qu'ils soient, tout en offrant aux administrateurs des contrôles très granulaires.

La solution ZTNA consiste à vérifier l'utilisateur, généralement au moyen d'une authentification multifacteur et d'un fournisseur d'identité, puis à valider l'état et la conformité de l'appareil (en vérifiant s'il est bien répertorié, à jour, correctement protégé, si le chiffrement est activé, etc.) et enfin à utiliser ces informations pour prendre des décisions basées sur les politiques de sécurité et déterminer l'accès et les privilèges des applications importantes. Le ZTNA constitue une excellente alternative au VPN d'accès à distance, car il permet de contrôler qui accède à quoi, et ce de manière très précise. C'est un paramètre essentiel pour se protéger des attaques de la supply chain qui s'articulent autour de l'accès des fournisseurs à vos systèmes.

Sophos ZTNA, notre nouvelle solution d'accès réseau managée est disponible depuis mi-2021. Elle protège toutes les applications en réseau hébergées sur votre réseau local, dans le Cloud public ou tout autre site d'hébergement. Elle couvre tout, de l'accès RDP aux partages de fichiers en réseau aux applications comme Jira, Wiki, les référentiels de code source, les applications de support et de dossiers, et au-delà.

En savoir plus sur Sophos ZTNA

Conclusion

Compte tenu de leur complexité, il est quasiment impossible d'empêcher une attaque de la supply chain de se produire. Mais en suivant les recommandations de ce document, vous pourrez réduire les risques d'en être victime et éviter qu'une attaque ait un impact significatif sur votre entreprise. En résumé :

1. Passez d'une approche réactive à une approche proactive de la cybersécurité
2. Surveillez les premiers signes de compromission
3. Auditez votre supply chain
4. Évaluez la posture de sécurité de vos fournisseurs et partenaires commerciaux
5. Passez constamment en revue votre propre hygiène en matière d'opérations de cybersécurité

En outre, envisagez l'adoption de technologies et de services tels que l'EDR, le MTR et le ZTNA pour soutenir vos objectifs de sécurité de la supply chain.

Le contexte mondial des cybermenaces a évolué, et la compromission de la supply chain est un risque pouvant affecter toutes les organisations, grandes et petites. En fait, nous faisons tous partie d'une chaine et sommes donc tous des cibles potentielles. C'est pourquoi minimiser les risques liés à la supply chain des fournisseurs est devenu crucial aujourd'hui.

Pour en savoir plus sur les solutions et l'expertise de Sophos en matière de cybersécurité, rendez-vous sur le site Sophos.fr.

Sophos fournit des solutions de cybersécurité de pointe aux entreprises de toutes tailles, les protégeant en temps réel contre les menaces avancées telles que les malwares, les ransomwares et le phishing. Grâce à des fonctionnalités Next-Gen éprouvées, les données de votre entreprise sont sécurisées efficacement par des produits alimentés par l'intelligence artificielle et le Machine Learning.

2021-04-14 (SB-NP)

SOPHOS