sosafe

Attaques de la chaîne d'approvisionnement

Comment protéger votre entreprise de cette menace

Imaginez : vous êtes à court de carburant et vous allez jusqu'à la station la plus proche pour faire le plein... Mais vous découvrez qu'elle est en rupture de stock. C'est exactement ce qu'il s'est passé en Allemagne, en février 2022, lorsque la société de logistique Marquard & Bahls a été victime d'une « attaque de la chaîne d'approvisionnement » qui s'est soldée par une demande de rançon. Cette société était également chargée de l'approvisionnement en matières premières des stations-service et des sociétés comme Shell. À cause de cette cyberattaque, ils ont été dans l'impossibilité de remplir les citernes de carburant. Cet exemple illustre bien pourquoi la sécurité de l'information doit être une priorité tout au long de la chaîne d'approvisionnement. En effet, les conséquences et les retombées financières peuvent être désastreuses pour toutes les parties impliquées, des prestataires de services et fournisseurs aux consommateurs.

Les attaques de ce type ne ciblent pas les entreprises en elles-mêmes mais plutôt leurs chaînes d'approvisionnement. Les cybercriminels exploitent les failles de la chaîne d'approvisionnement pour s'infiltrer dans les systèmes ou infecter le réseau d'une société avec un logiciel malveillant. Ainsi, dans l'exemple cité plus haut, la cyberattaque a fini par affecter la chaîne logistique physique et par provoquer des ruptures d'approvisionnement.

Ces dernières années, les attaques de ce type n'ont cessé de se multiplier au point de se hisser parmi les principales tendances actuelles dans le domaine des rançongiciels. Les assurances Allianz ont ainsi noté, dans leur « Cyber Report 2021 » une hausse constante des attaques de la chaîne d'approvisionnement. Selon une autre enquête, menée par le fournisseur en cybersécurité Anchore, plus de 3 sociétés sur 5 ont été victimes d'une attaque de la chaîne d'approvisionnement en 2021. Le tout dernier « ThreatLabz Report 2022 » parvient à la même conclusion et explique l'une des principales raisons de cette augmentation : « En s'immisçant dans les relations commerciales que leurs victimes potentielles entretiennent avec des fournisseurs dignes de confiance, les pirates réussissent à impacter des douzaines de sociétés en même temps, y compris des organisations dotées de solides systèmes de sécurité qui les protègent des attaques externes. »

Généralement, ces attaques ne ciblent pas premièrement les systèmes technologiques à proprement parler, mais plutôt les gens : selon le « Data Breach Investigations Report 2022 » de Verizon, 82 % des cyberincidents et des compromissions de données impliquent le facteur humain. Les attaques commencent en effet souvent par des méthodes d'ingénierie sociale sophistiquées comme des e-mails de spear phishing. La manipulation psychologique y joue toujours un rôle clé. Le récent « Rapport concernant le paysage des menaces dans le cadre des attaques de la chaîne d'approvisionnement » de l'Agence de l'Union européenne pour la cybersécurité (ENISA) cite un certain nombre d'autres vecteurs potentiels de l'ingénierie sociale, tels que le vishing (technique d'arnaque vocale visant à duper les victimes) et le typosquattage (ciblant les internautes qui saisissent une URL incorrecte dans leur navigateur Web).

Dans ce paysage de menaces cyber, une chose est sûre : pour être efficaces, les mesures de prévention doivent être axées sur le facteur humain, puisque ce sont les employés qui ont le rôle principal dans la prévention contre les cyberattaques, y compris contre les attaques de la chaîne d'approvisionnement. Tout système de sécurité cohérent devrait inclure une équipe dûment formée. Poursuivez votre lecture pour en savoir plus sur les causes et les conséquences éventuelles des attaques de la chaîne d'approvisionnement, sur les méthodes de prédilection des cybercriminels et sur la façon dont vos employés peuvent identifier les risques suffisamment tôt pour prendre les bonnes décisions.

Comment fonctionnent les attaques de la chaîne d'approvisionnement

Ces attaques utilisent toujours la chaîne d'approvisionnement comme porte d'entrée pour accéder au réseau de la société. Les secteurs dans lesquels la chaîne d'approvisionnement joue un rôle majeur pour fournir à l'entreprise des biens et des services essentiels sont particulièrement vulnérables : la logistique, l'industrie pharmaceutique, l'alimentaire, l'énergie et la technologie, par exemple. Selon l'ENISA, les prestataires d'infogérance constituent également des cibles lucratives pour les cybercriminels. En effet, leur chaîne d'approvisionnement logicielle peut servir de point d'accès à des réseaux de sociétés, avec des répercussions dévastatrices (voir le cas de Kaseya, page 7). Il existe d'autres types de cybercrimes susceptibles d'affecter la chaîne d'approvisionnement, mais ce sont généralement les conséquences d'une attaque, non les causes.

Une attaque de la chaîne d'approvisionnement suit généralement un schéma bien défini : les attaquants commencent par rechercher des points faibles dans la chaîne d'approvisionnement d'une société, par exemple des prestataires de services qui n'ont pas spécialement de critères élevés en matière de sécurité de l'information.

Ils exploitent alors les failles techniques dans les systèmes du prestataire de services pour accéder à leur véritable cible. Il leur suffit d'un seul point faible pour s'infiltrer. Dans un premier temps, l'infiltration du réseau n'est pas visible : en réalité, il s'écoule souvent des semaines, des mois, voire des années avant que le piratage ne soit découvert.

Ayant constaté que le taux de réussite des attaques ciblant le facteur humain était incroyablement élevé, les cybercriminels s'en prennent souvent aux collaborateurs du fournisseur ou du prestataire de services au moyen, notamment, d'e-mails de phishing, de fausses applications et de faux sites Internet. Ces attaques d'ingénierie sociale visent à tromper les gens en les poussant à prendre des risques qu'ils n'auraient jamais pris autrement. Lorsque les victimes sont tombées dans le piège, la moitié du travail est faite. Les pirates peuvent ensuite se faire passer pour les prestataires de services et envoyer de faux e-mails ou des demandes de mises à jour contenant des virus. La société ciblée n'a guère de raisons de se méfier. Un manque de préparation et une faible réactivité peuvent alors contribuer à la réussite des cybercriminels.

Les modes d'attaque les plus fréquents

Les cybercriminels modifient constamment leurs méthodes et leurs techniques. Il est donc essentiel que les sociétés se tiennent informées des dernières évolutions en la matière pour pouvoir identifier leurs faiblesses et les pallier le plus tôt possible. Il existe différents types d'attaques de la chaîne d'approvisionnement : par exemple, un logiciel peut être infecté par du code malveillant ou des mises à jour, les attaques peuvent cibler les gros équipements ou les machines utilisés dans la chaîne d'approvisionnement ou introduire des modifications dans le code de démarrage du firmware.

Les méthodes ci-dessous sont, à l'heure actuelle, les plus efficaces pour permettre aux pirates d'accéder aux réseaux de leurs victimes :

Infection par un logiciel malveillant

La plupart des attaques de la chaîne d'approvisionnement commencent par un logiciel malveillant. Les cybercriminels l'introduisent dans les systèmes d'une société pour qu'il contamine peu à peu toute la chaîne d'approvisionnement. Il existe différents types de logiciels malveillants qui jouent sur différents processus. Par exemple, les logiciels espions surveillent les activités des collaborateurs pour trouver leurs informations de connexion confidentielles. Les rançongiciels sont utilisés pour collecter et crypter des données que les cybercriminels prennent en otage jusqu'à ce que leurs victimes payent une rançon. Les portes dérobées et les chevaux de Troie permettent de contrôler des programmes à distance et peuvent également servir de tremplin à une attaque de la chaîne d'approvisionnement. Tous ces logiciels malveillants ont un point commun : ils exploitent des failles de sécurité ou d'autres points faibles techniques.

Exploitation des vulnérabilités d'un logiciel

Aucun logiciel n'est parfait. Les concepteurs ont beau tester leurs produits sous toutes les coutures, la garantie de sécurité absolue n'existe pas. Les cybercriminels traquent toute faiblesse qu'ils pourront exploiter avec leurs outils. Souvent, il leur suffit de failles temporaires pour mener des attaques zero-day, telles que des manipulations ou des mises à jour. L'Agence américaine de cybersécurité et de sécurité des infrastructures (United States Cybersecurity & Infrastructure Security Agency - CISA) a compilé une liste de vulnérabilités fréquentes, comprenant notamment celles exploitées pour l'exécution de code à distance, ou pour la gestion des autorisations et la lecture des données.

Citons, à titre d'exemple, l'attaque menée par le groupe Lapsus$ en janvier 2022 contre le service d'authentification du groupe Okta. Okta compte parmi ses clients un large panel de sociétés et d'organes gouvernementaux. Les attaquants ont réussi à tirer parti d'une vulnérabilité chez l'un de ses prestataires de services, Sitel : à l'aide d'un logiciel de maintenance à distance, ils se sont connectés à l'ordinateur portable d'un employé, mais ne l'ont révélé au public que deux mois plus tard. Ce cas illustre bien que les hackers peuvent rester longtemps dans des systèmes tiers et propager leurs logiciels malveillants très rapidement – et à large échelle – dans toute la chaîne d'approvisionnement.

Ingénierie sociale

Les cybercriminels s'ingénient à mettre le facteur humain à rude épreuve. Selon l'Agence nationale de la sécurité des systèmes d'informations (ANSSI), l'ingénierie sociale est une « manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes ». Les victimes en viennent à révéler des informations confidentielles, à désactiver des fonctions de sécurité ou sont poussées, par ruse, à installer des logiciels malveillants. Les attaques d'ingénierie sociale peuvent prendre différentes formes, telles que le phishing (l'utilisation d'e-mails ou de sites Internet falsifiés qui demandent aux utilisateurs de réaliser certaines actions) ou le smishing (le phishing par texto ou via d'autres types de messageries). Les utilisateurs sont souvent moins prudents lorsqu'ils reçoivent des messages de smishing et tendent à y répondre plus rapidement qu'aux e-mails. Ainsi, en juillet 2022, des pirates ont tenté de pousser la présidente de la Banque centrale européenne, Christine Lagarde, à révéler son code de confirmation pour WhatsApp. Pour ce faire, ils ont utilisé le véritable numéro de téléphone d'Angela Merkel, ancienne chancelière d'Allemagne, mais personne ne sait comment ils se le sont procuré. Prise de soupçons, Christine Lagarde avait appelé Angela Merkel pour vérifier qu'elle était à l'origine du message et avait ainsi éventé le piège.

Attaque par force brute

Les cybercriminels ont aussi recours aux attaques par force brute pour accéder à des données sensibles telles que les informations de connexion internes qui leur permettront de pénétrer dans les systèmes de la société. Ces attaques sont basées sur une procédure par tâtonnement : les cybercriminels testent un large éventail de possibilités pour deviner le mot de passe d'un employé. Les hackers se servent alors d'outils qui essaient automatiquement toutes les combinaisons possibles. Lorsqu'ils sont parvenus à cracker la bonne combinaison, les pirates peuvent infecter plus facilement les systèmes de la société avec un logiciel malveillant.

Les grandes attaques de la chaîne d'approvisionnement de ces dernières années

Pour mieux comprendre le fonctionnement de ces attaques de la chaîne d'approvisionnement, penchons-nous sur des exemples récents:

Une mise à jour aux conséquences désastreuses

En 2021, une faille dans le code du logiciel de Kaseya a eu de graves conséquences pour cette société informatique américaine. Profitant d'une attaque zero-day, les attaquants ont réussi à contourner le processus d'authentification et à accéder au moteur de script interne. Ils ont ensuite envoyé, à tous les clients, une mise à jour qui a installé un rançongiciel sur leurs ordinateurs. Or, la plupart des clients étaient des fournisseurs d'infogérance au service de nombreuses autres entreprises.

La société a communiqué ouvertement sur l'incident, fait appel à une équipe d'experts et publié peu à peu des mises à jour et des correctifs pour ses clients. Selon TechTarget, l'incident avait, au départ, l'apparence d'une mise à jour inoffensive pour un logiciel développé par un prestataire fiable. Il a affecté pas moins de 60 fournisseurs d'infogérance et 1 500 de leurs clients. Les hackers ont créé des mises à jour malveillantes qui semblaient vraiment provenir de Kaseya, ce qui prouve, de manière inquiétante, qu'ils ont su acquérir une solide connaissance de la société avant de perpétrer leurs attaques.

Un logiciel malveillant intégré

Le logiciel de gestion informatique du fournisseur américain SolarWinds a été infecté en 2020. Si l'attaque n'a été découverte qu'en décembre, les hackers avaient déjà accès, depuis le mois de mars, à de nombreux systèmes de serveur Windows utilisés par le logiciel Orion de SolarWinds. Ils y étaient parvenus en installant un logiciel malveillant dans le produit, probablement grâce à une négligence au niveau de la gestion des mots de passe. Les attaquants ont ainsi eu beaucoup de temps pour explorer les systèmes et voler des données.

Ce cas a fait beaucoup de vagues car l'attaque a touché de grosses sociétés comme Microsoft, ainsi que des agences gouvernementales telles que le US Treasury Department (département du Trésor des États-Unis) et le Department of Commerce (département du commerce). Le fournisseur lui-même a estimé que 18 000 entreprises, organes gouvernementaux et sociétés avaient été contaminés par les mises à jour.

Un cheval de Troie à l'origine de pertes de plusieurs millions

NotPetya est une variante du cheval de Troie de cryptage Petya qui circule depuis 2016. En exploitant des vulnérabilités connues du système d'exploitation Windows, il a réussi à infiltrer des réseaux entiers pour crypter ou supprimer les systèmes infectés.

Parmi les principales victimes de NotPetya, on compte l'ancienne filiale de FedEx, TNT Express, et la compagnie de transport maritime Maersk, qui ont toutes deux signalé des pertes de près de 300 millions de dollars suite à cette attaque. La vulnérabilité a été corrigée ultérieurement dans la plupart des systèmes.

Une attaque de phishing qui provoque l'indisponibilité de sites

On suppose que l'attaque contre Count + Care, en Allemagne, a commencé lorsqu'un employé a cliqué sur une pièce jointe contaminée dans un e-mail de phishing. Count + Care est une entreprise informatique au service de nombreuses sociétés, dans différents secteurs d'activité. À ce titre, l'entreprise est un maillon de leur chaîne d'approvisionnement. L'attaque s'est poursuivie en affectant le fournisseur d'énergie Entega à Darmstadt, les services municipaux de Mayence ainsi que les transports publics de la ville. Les services s'en sont trouvés limités et les sites Internet n'étaient plus disponibles.

Pénurie de gaz sur la côte est des États-Unis

Un mot de passe non sécurisé a suffi pour permettre aux cybercriminels de s'en prendre au Colonial Pipeline. Le PDG Joseph Blount a annoncé, lors d'une conférence de presse, que les attaquants avaient pu mettre la main sur un mot de passe insuffisamment protégé. On ne sait pas s'ils se le sont procuré par ingénierie sociale ou par force brute, mais l'absence d'authentification multifacteur leur a permis d'accéder à distance au compte VPN d'un employé, ainsi qu'à de nombreux systèmes internes et aux données de l'exploitant de l'oléoduc. Cette attaque a provoqué une perturbation de la chaîne d'approvisionnement et des pénuries de gaz de plusieurs semaines sur la côte est des États-Unis.

Quand le rançongiciel s'en prend aussi aux clients

Les collaborateurs de la plateforme américaine de gestion des ressources humaines Kronos ont remarqué une activité inhabituelle sur leur système en décembre 2021. Malheureusement, c'était déjà trop tard : la société venait d'être victime d'un rançongiciel. L'attaque a non seulement affecté Kronos, mais aussi ses clients. Plusieurs des sociétés qui utilisaient la plateforme pour l'enregistrement comptable de leurs salaires ont été impactées. Au bout de quelques semaines, le logiciel a cessé de fonctionner normalement et de nombreux employés ont été payés en retard. On n'a jamais su précisément comment le rançongiciel avait réussi à infiltrer la plateforme Kronos, mais les analyses d'autres cyberattaques ont montré que les cybercriminels exploitent de plus en plus les points faibles des entreprises. Souvent, les collaborateurs ne savent pas vraiment comment éviter ces risques.

Tous ces exemples illustrent l'importance de bien former les équipes pour qu'elles soient capables de discerner d'éventuelles anomalies dans le système et de réaliser rapidement qu'il s'agit de cyberattaques. Seule une solide culture de la cybersécurité peut protéger les entreprises de telles menaces.

Le rôle d'une formation de sensibilisation pour prévenir les attaques de la chaîne d'approvisionnement

Ces attaques montrent que les failles de sécurité et les vulnérabilités de tout ordre peuvent avoir de graves conséquences pour les entreprises. Malgré les nombreux systèmes de sécurité sophistiqués que nous utilisons, ou peut-être à cause d'eux, les cybercriminels s'acharnent de plus en plus sur les personnes pour tenter de forcer l'accès aux systèmes. Après tout, les gens restent sensibles à la manipulation psychologique. Il est donc important d'intégrer davantage les collaborateurs dans des stratégies de cybersécurité globales afin de réduire les risques d'attaque de la chaîne d'approvisionnement ou de toute autre cyberattaque. C'est bien connu : « un homme averti en vaut deux ». Il faut donc informer et sensibiliser les employés aux méthodes des pirates informatiques. Un simple diaporama d'explications ne suffit pas. En effet, les connaissances théoriques sont rarement mises en pratique et s'oublient rapidement. Pour communiquer un savoir qui se traduise de manière active par des réflexes de vigilance, il faut de la pratique. C'est ce que proposent les formations modernes de sensibilisation à la cybersécurité : des exercices pratiques, des cours faciles à comprendre et des simulations réalistes. L'accent doit toujours être mis sur les besoins de l'apprenant. L'enseignement de comportements vigilants et le développement d'une solide culture de la sécurité passent par quatre piliers incontournables : le contexte, la connaissance, la motivation et les réflexes.

Il faut évaluer le niveau de départ des collaborateurs : que savent-ils sur le sujet ? Quelles sont leurs responsabilités ? Quelles ressources utilisent-t-ils dans le cadre de leur travail ? Leur apprentissage doit ensuite se fonder sur ces quatre piliers. La psychologie cognitive a permis de mettre au point des méthodes qui ancrent profondément les connaissances apprises dans la mémoire des collaborateurs et les motivent à poursuivre leurs efforts. Par exemple, à l'aide de rappels automatisés : ceux-ci encouragent les employés à apprendre en intégrant, par exemple, des modules pédagogiques dans les processus de routine pour favoriser constamment des résultats sur le long terme. La gamification est également une méthode efficace : le recours à des aspects ludiques comme la compétition facilite l'apprentissage. Ainsi, lorsque les collaborateurs apprennent ce qu'ils doivent faire en cas d'urgence dans le cadre de simulations, ils sauront comment réagir si de tels incidents se produisent en situation réelle. Ces mesures systématiques et cette formation personnalisée permettent une réduction des risques cyber allant jusqu'à 90 %. Grâce à elles, toute l'entreprise progresse à pas de géant dans ses objectifs de cybersécurité.

Autres types de mesures de protection efficaces

Il existe d'autres méthodes pour se protéger des attaques de la chaîne d'approvisionnement :

SIEM : C'est le sigle de Security Information and Event Management ou gestion des informations et des événements de sécurité, en français. Il s'agit de systèmes qui surveillent en permanence l'intégralité du réseau informatique et l'analysent. Ces outils, comme d'autres, sont indispensables pour permettre aux organismes travaillant sur une infrastructure critique, tels que les fournisseurs d'énergie ou les hôpitaux, de détecter les éventuelles menaces le plus tôt possible. Ils sont capables d'identifier toute activité suspecte et de tirer la sonnette d'alarme.

Permissions raisonnables et restrictives : Les concepts d'architecture dédiés à la sécurité comme Zero Trust sont vraiment performants dans ce domaine. Ces systèmes ne font confiance à aucun périphérique, aucun utilisateur ni aucun logiciel dans un réseau. Il faut également mettre en place des processus d'authentification complets qui n'accordent l'accès aux données sensibles qu'aux personnes ayant l'autorisation de les consulter. Toutefois, d'autres concepts moins poussés, comme ceux qui nécessitent une double authentification, peuvent également contribuer à la protection contre des accès non autorisés.

Analyse des chaînes d'approvisionnement de l'entreprise : Généralement, les relations des entreprises avec leurs fournisseurs, leurs prestataires de services et leurs clients se construisent au fil du temps. Mais rares sont les sociétés qui ont une vue d'ensemble complète de ces relations, et cela devient particulièrement difficile lorsqu'elles utilisent différents types de logiciels. Or, une telle vue d'ensemble peut s'avérer essentielle pour assurer la sécurité de toute l'équipe. En cas d'attaque, les sociétés seraient alors en mesure de déterminer rapidement les éventuelles conséquences.

Évaluation des prestataires de services et des partenaires : Avant d'entamer une relation avec un prestataire de services ou un fournisseur, il est essentiel de connaître son niveau de sécurité et de conformité afin de réduire les risques au niveau de la chaîne d'approvisionnement. Si votre réseau de partenaires dispose d'une solide infrastructure de sécurité, cela réduit les risques d'attaques de la chaîne d'approvisionnement. Vous pouvez, par exemple, vérifier qu'ils disposent des certifications (logicielles) requises et qu'ils répondent aux exigences légales comme celles du RGPD.

Solutions EDR : Les solutions techniques comme les outils de détection et réponse sur les terminaux permettent de détecter et de prévenir les attaques contre le système. Ils surveillent en permanence les terminaux d'un système, tels que les ordinateurs portables et les autres périphériques mobiles. Ce faisant, ils y traquent toute activité suspecte, détectent les menaces persistantes sophistiquées et peuvent mettre en place une contre-offensive à un stade précoce.

Améliorer la communication et la résistance : Il vaut mieux poser des questions que se contenter de faire ce qu'on vous a demandé (dans l'urgence). Or, une telle attitude nécessite une communication ouverte. La cyberrésilience aussi s'apprend. Même si un e-mail semble urgent, gardez votre sang-froid.

Des règles de sécurité claires pour le télétravail : Dans de nombreux secteurs, le télétravail ou le travail hybride sont devenus monnaie courante. L'instauration de règles claires et compréhensibles permet de limiter les risques d'attaque.

Pourquoi le facteur humain joue-t-il un rôle clé dans la protection des chaînes d'approvisionnement ?

Notre monde est en constante évolution et la cybercriminalité n'échappe pas à la règle. Les stratégies de sécurité de l'information doivent donc toujours rester à la page. À l'heure du travail hybride et de l'informatique sur le cloud, les mesures technologiques pures ne suffisent plus pour protéger les sociétés des cyberattaques et des assauts sophistiqués ciblant les chaînes d'approvisionnement (logicielles). Les entreprises devraient s'assurer d'avoir une vue d'ensemble complète sur les risques cyber, y compris ceux touchant leur réseau de partenaires, afin de pouvoir réagir rapidement. « Nul homme n'est une île » disait le poète John Donne et c'est la raison pour laquelle la « résilience humaine connectée » est de plus en plus importante : les attaques ne peuvent être efficacement prévenues que si tout le monde collabore.

Plus le temps passe, plus les cybercriminels ciblent les faiblesses humaines. Pour deux raisons : la première, c'est que la technologie de la sécurité a fait d'énormes progrès et qu'il est de plus en plus difficile de la contourner. La seconde, c'est que toutes les entreprises emploient des êtres humains. Ce sont eux le « passe-partout universel » pour accéder aux systèmes internes parce qu'ils sont sensibles à la manipulation psychologique. Il est donc capital d'investir dans la sensibilisation à la sécurité. C'est ce qui permettra aux entreprises de résister à des attaques qui pourraient leur coûter cher.

SoSafe aide les entreprises à développer leur culture de la sécurité et à réduire les risques cyber. Sa plateforme de sensibilisation, conforme au RGPD, diffuse du contenu de formation personnalisé inspiré de concepts psychologiques et propose des simulations d'attaques. Les collaborateurs apprennent ainsi à se protéger activement contre les menaces en ligne. Cette plateforme, évolutive et facile à implémenter, fournit des analyses détaillées permettant de mesurer le retour sur investissement et d'identifier tout point faible. SoSafe veille à ce que chacun sache se protéger.

sosafe

SoSafe GmbH
Lichtstrasse 25a
50825 Cologne

info@sosafe.de
www.sosafe-awareness.com
+49 221 65083800