Option Finance
Le premier hebdomadaire des décideurs financiers

PAYS :France
PAGE(S) :14;15;16
SURFACE :185 %
PERIODICITE :Hebdomadaire

RUBRIQUE :Innovation et transformation
DIFFUSION :(20000)
JOURNALISTE :Joffrey Marcellin

► 11 décembre 2023 - N°1730

Innovation & transformation

Nouvelles technologies

Image non disponible.
Restriction de l'éditeur

Alors que la cybermenace est toujours aussi prégnante, les hackers ciblent de plus en plus les petites et moyennes entreprises, avec à la clé un double bénéfice : non seulement les attaques atteignent plus souvent leurs cibles, souvent mal protégées, mais elles permettent également de viser les grands groupes par ricochet. Une menace face à laquelle les entreprises peuvent prendre un certain nombre de précautions.

Cybersécurité : gare au cheval de Troie !

Comment infecter simultanément les systèmes d'information de 1 500 entreprises dans le monde entier ? Un groupe de hackers a trouvé l'année dernière une solution « simple » : il leur a suffi d'infiltrer leur fournisseur commun à toutes de logiciels de gestion informatique, en l'occurrence l'américain Kaseya. Depuis la pratique a connu un grand succès et ne cesse de se développer. En effet, les cybermalveillants ayant de plus en plus de difficultés à s'introduire dans les systèmes d'information des grands groupes, de mieux en mieux protégés, ils tentent désormais de les atteindre via leur chaîne d'approvisionnement. Si ce phénomène n'est pas nouveau, il a pris une ampleur inédite ces derniers mois : les attaques de la chaîne d'approvisionnement, ou attaques « par ricochet », ont augmenté de 650 % l'année dernière, selon le dernier rapport du fournisseur de solutions de cybersécurité CheckPoint.

Et le processus est quasiment toujours le même. « Une fois introduits au sein de Kaseya, les hackers ont profité des accès privilégiés du fournisseur de logiciels auprès de ses clients pour poursuivre leurs actions malveillantes en s'introduisant chez ces derniers, en toute discrétion », indique Pauline Mendiela, référente sécurité IT pour le cabinet de conseil Finegan. Ce type d'attaques présente un avantage de taille pour les hackers. « Au lieu de s'attaquer à une seule organisation ciblée, une attaque cyber sur la chaîne d'approvisionnement leur donne la possibilité d'obtenir l'accès à de nombreuses entreprises pour exfiltrer silencieusement de grandes quantités de données à leur insu ou installer des logiciels malveillants », souligne Pauline Mendiela. Ils ont en outre des chances plus raisonnables de réussir leur offensive, dans la mesure où les entités visées dans ce type d'attaques, à savoir des PME ou des ETI, sont généralement moins bien protégées que les grands groupes.

Les attaques de la chaîne d'approvisionnement, ou attaques « par ricochet », ont augmenté de 650 % l'année dernière.

Les grands groupes toujours à portée des hackers

Cette tendance risque de profondément bouleverser la manière dont les grandes entreprises vont organiser leur stratégie de défense cyber, car il ne s'agit plus désormais de sécuriser son propre système informatique, mais bien de s'assurer du niveau de sécurité de l'ensemble de ses partenaires, prestataires et fournisseurs, beaucoup plus fragiles face à une menace cyber qui ne faiblit pas. « Les attaques sont plus sophistiquées qu'il y a quelques mois, estime Benoît Grunemwald, expert en cybersécurité chez l'éditeur d'antivirus ESET. Toutefois, les deux grandes catégories de menaces demeurent la vulnérabilité logicielle et l'hameçonnage. Ce dernier consiste à obtenir du destinataire d'un courriel d'apparence légitime qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services financiers, afin de lui dérober de l'argent. Certes, c'est toujours le

Option Finance
PAYS :France
PAGE(S) :14;15;16
SURFACE :185 %
PERIODICITE :Hebdomadaire
RUBRIQUE :Innovation et transformation
DIFFUSION :(20000)
JOURNALISTE :Joffrey Marcellin
► 11 décembre 2023 - N°1730

même mécanisme, mais l'intelligence artificielle rend ces menaces plus opérantes. Pour le phishing par exemple, les mails utilisés sont beaucoup plus réalistes et contextualisés qu'avant. Concernant la vulnérabilité logicielle, des IA développées pour assister les développeurs informatiques peuvent très bien être détournées de leur objet initial pour trouver des failles au sein des logiciels et les exploiter. »

Par ailleurs, si la menace s'accentue d'un point de vue qualitatif, elle s'intensifie également au niveau quantitatif. Le nombre d'attaque a augmenté de 38 % dans le monde en 2022, selon le dernier rapport du fournisseur de services de sécurité Checkpoint, à cause notamment de l'accessibilité accrue des logiciels malveillants, également appelés malware. « Bien souvent, aujourd'hui, ces logiciels malveillants sont vendus ou loués sur le darkweb avec toutes les ressources nécessaires pour lancer une attaque facilement, y compris lorsqu'on n'est pas un professionnel du cybercrime, souligne Julien Lopizzo, PDG de Semkel, cabinet d'intelligence économique spécialisé dans la cybersécurité. Ces programmes d'attaque "clé en main", plus connus sous le nom de "malware as a service", ou Maas, inondent aujourd'hui le darkweb, et font exploser le nombre potentiel de hackers. »

L'avènement des logiciels « clé en main »

Les flux financiers générés par les achats de Maas sur le darkweb ne font d'ailleurs qu'augmenter, selon les experts de l'éditeur de logiciel américano-néerlandais Elastic. Dans leur dernier « global threat report », basé sur un milliard d'incidents de marché recueillis à travers le monde entre janvier 2022 et janvier 2023, ils constatent l'avènement de ces outils d'attaque prêt à l'emploi. « 73 % des malwares sont aujourd'hui des Maas, ce qui veut dire que la grande majorité des attaques sont perpétrées via ces outils « clé en main », relève Yannick Fhima, directeur solutions architecture pour l'Europe du Sud chez Elastic.

« Le recours massif à l'externalisation est désormais considéré comme un grand risque pour les entreprises, car il s'accompagne souvent d'ouvertures de flux et d'accès. »

Pauline Mendiela, référente sécurité IT, Finegan

Au sein des Maas, cette accessibilité accrue des logiciels malveillants profite avant tout à la catégorie des ransomwares, ces programmes dont l'objet est de chiffrer les données de la victime afin de lui réclamer une rançon contre la clé de déchiffrement. « Aujourd'hui, les trois ransomwares les plus actifs (Sodinokibi, Hive, Blackcat) sont distribués par Raas, c'est-à-dire qu'ils sont vendus clé en main pour le hacker », indique Yannick Fhima. Ainsi, les cyberattaques peuvent désormais être initiées par des profils moins spécialisés, et des organisations mafieuses se sont engouffrées dans cette brèche. « Ce sont des équipes très organisées, souvent venues de l'Est, avec des financeurs d'un côté et des attaquants de l'autre, qui sont quasiment considérés comme des salariés », ajoute Yannick Fhima. Résultat : le nombre de victimes de ransomwares a augmenté de 143 % dans le monde au premier trimestre 2023, selon la dernière étude « cyber security trends » d'Allianz.

L'indispensable montée en compétences des partenaires

Face à une menace qui s'intensifie et vise de plus en plus la chaîne d'approvisionnement des grands groupes, ces derniers doivent être particulièrement vigilants quant au

Les risques liés aux tiers au cœur des enjeux réglementaires

DIRECTIVE NIS2

« La directive européenne Network and information systems security (NIS2), dont la transposition en droit français doit avoir lieu avant le 17 octobre 2024, imposera aux entreprises d'évaluer les risques liés aux tiers, leur dépendance vis-à-vis de leurs fournisseurs, mais également de prévoir des plans B ou C si jamais ces derniers étaient victimes d'une attaque qui les empêcherait de poursuivre leur activité », indique Pauline Mendiela, référente sécurité IT pour le cabinet de conseil Finegan.

RÈGLEMENT DORA

Le règlement européen Digital operational resilience act (DORA), dont l'entrée en vigueur est prévue pour le 1er janvier 2025, va imposer à certains partenaires des banques et établissements financiers qu'ils témoignent d'un niveau de sécurité suffisant pour pouvoir travailler avec eux. « Toute société qui rendra un service lié de près ou de loin à l'informatique ou à la communication d'un établissement financier devra forcément avoir le même niveau de sécurité que ce dernier, prévient Pauline Mendiela. Un prestataire IT devra donc se conformer, au même titre que l'établissement financier pour lequel il travaille, aux différentes exigences du règlement DORA. »

Option Finance
Le premier hebdomadaire des décideurs financiers

PAYS :France
PAGE(S) :14;15;16
SURFACE :185 %
PERIODICITE :Hebdomadaire

RUBRIQUE :Innovation et transformation
DIFFUSION :(20000)
JOURNALISTE :Joffrey Marcellin

► 11 décembre 2023 - N°1730

choix de leurs prestataires. « Le recours massif à l'externalisation est désormais considéré comme un grand risque, car il s'accompagne souvent d'ouvertures de flux et d'accès, confirme Pauline Mendiela. En effet, dans le cadre d'accords d'externalisation, des prestataires peuvent accéder à certaines parties du réseau du groupe avec lequel ils travaillent. Ces partages fragilisent forcément la sécurité des infrastructures, en l'occurrence celle des clients, et des données qui y transitent si les niveaux de sécurité ne sont pas équivalents. »

Pour limiter ce risque, les grandes entreprises ont tout intérêt à encourager, voire à aider leurs partenaires business, fournisseurs et prestataires de services à monter en compétences sur la partie cybersécurité. « Il s'agit d'ailleurs d'une requête très appuyée en ce moment de la part des grands groupes, qui réclament à leurs partenaires PME et ETI qu'ils s'alignent sur leurs standards de sécurité informatique », affirme Julien Lopizzo. Le législateur européen lui-même a bien compris l'importance de cette montée en compétences collective. Dans la directive NIS2 comme dans le règlement DORA, il oblige les acteurs les plus avancés à prendre leur part dans la montée en compétences des entreprises plus modestes (voir encadré).

Un effort important à fournir

Par conséquent, en plus du risque direct que fait peser sur elles la perspective d'une cyberattaque, les PME et ETI vont être de plus en plus poussées à agir par leurs partenaires business de plus grande taille, à qui elles doivent donner des gages d'une bonne gestion cyber. « Si elles ne veulent pas être ostracisées, elles sont désormais contraintes de définir un cadre de gouvernance, de cartographier les risques et d'identifier les actifs les plus importants de l'entreprise, afin de les protéger en conséquence, affirme Pauline Mendiela. Elles pourront dès lors déployer une feuille de route et lancer les chantiers les plus urgents. »

Les PME et ETI vont être de plus en plus poussées à agir par leurs clients ou fournisseurs de plus grande taille, à qui elles doivent donner des gages de bonne gestion cyber.

La plupart du temps, cependant, elles n'ont pas les ressources en interne pour effectuer ce travail préliminaire. Elles peuvent alors solliciter les services d'un cabinet de conseil. Pour une entreprise de 50 à 200 salariés, il faut tout de même prévoir une intervention de deux à trois mois, et une enveloppe de 20 000 à 30 000 euros. Un effort important qu'il faudra poursuivre dans la durée en formant les équipes en interne pour qu'elles puissent assurer la gestion opérationnelle des outils mis en place, les tester régulièrement et développer une véritable culture de la sécurité au sein de l'entreprise. L'enjeu est immense dans un contexte géopolitique tendu qui ne fait qu'aggraver la menace, comme le rappelle Julien Lopizzo : « La cybercriminalité a coûté 6 000 milliards de dollars en 2021 aux entreprises et institutions dans le monde. D'après les prédictions, ce chiffre devrait atteindre 8 000 milliards de dollars cette année puis 10 500 milliards dans les deux années à venir. » ■

Joffrey Marcellin
𝕏 @joffreymarcell3