Décision Achats

PAYS : France
PAGE(S) :58-59
SURFACE :154 %
PERIODICITE : Mensuel

DIFFUSION :(44000)
JOURNALISTE : Mathieu Neu

► **1 décembre 2020 - N°221**

Les supply chain, porte d'entrée des cybermalveillances

Depuis le début de la crise sanitaire, les supply chain sont pointées du doigt en raison du risque élevé de rupture d'approvisionnements. Derrière cette faiblesse qui touche tous les secteurs économiques se cache un autre écueil majeur : elles draineraient l'essentiel des actes cybercriminels.

Les grandes organisations comptent en moyenne 1 013 fournisseurs dans leur écosystème, et 82 % d'entre elles ont été victimes d'une violation de données au cours des 12 derniers mois. C'est ce que souligne une étude menée par le spécialiste de la cybersécurité, BlueVoyant. En cause : des faiblesses et manquements imputables à la chaîne d'approvisionnement.
Dans un contexte où les grandes entreprises sont souvent mieux protégées que les plus petites structures, les auteurs de malveillance se tournent de plus en plus vers les fournisseurs pour s'immiscer dans le réseau des donneurs d'ordres, en passant inaperçus la plupart du temps. Un tiers des entreprises n'auraient que peu ou pas d'informations sur les intrusions de pirates informatiques au sein de leur chaîne d'approvisionnement. Celles-ci se confrontent dès lors à un schéma où elles ne sont pas en mesure de découvrir qu'elles ont été victimes d'un incident avant qu'il ne soit trop tard.
Le cloud est régulièrement pointé du doigt comme une porte d'entrée problématique. *« Il est vrai que le fait d'être plus ouvert sur le monde extérieur constitue en soi un facteur aggravant. On a souvent tendance à oublier que les difficultés sur les clouds publics sont les mêmes que celles concernant des infrastructures On Premise. Il est à noter que, désormais, les administrations de systèmes deviennent également joignables et accessibles par Internet, surtout avec les solutions de type SaaS »*, explique Philippe Rondel, senior security architect chez le spécialiste de la sécurité informatique CheckPoint.

Des intrusions protéiformes

Mais les sources des défaillances prennent des origines bien plus variées, comme en témoigne le programme malveillant NotPetya qui a infecté des milliers de systèmes en entreprise en Europe par l'intermédiaire de mises à jours de logiciels. Ce sont essentiellement des solutions de gestion comptable qui ont servi de biais lors de cette

Décision Achats

PAYS :France
PAGE(S) :58-59
SURFACE :154 %
PERIODICITE :Mensuel

DIFFUSION :(44000)
JOURNALISTE :Mathieu Neu

► 1 décembre 2020 - N°221

attaque, alors qu'il ne s'agissait nullement d'un fournisseur de premier plan. Les entreprises se reposent aujourd'hui sur un large éventail de sous-traitants, dans un contexte de relations de plus en plus numérisées. *« Il existe donc des flux de type d'EDI, pour la facturation, ou encore de type API, qui représentent des mécanismes par lesquels un ordinateur d'une entreprise interroge un ordinateur d'une autre entreprise du même écosystème. Ces flux relient les plateformes des différentes organisations par le biais de droits d'accès : un fournisseur peut par exemple être invité à récupérer des listes d'adresses en vue de livraisons à effectuer. On obtient ainsi des chemins d'attaque potentiels par l'intermédiaire desquels les cybercriminels peuvent passer d'une organisation à une autre en passant par un petit acteur disposant a priori de moins de ressources pour se prémunir des cyber-risques »*, explique Vincent Maret, associé, responsable du pôle Cybersécurité et Protection des données personnelles chez KPMG. La confiance accordée naturellement au fournisseur permet le reste du travail pour s'immiscer dans les systèmes d'information du donneur d'ordre.

« Les tentatives d'intrusion peuvent prendre une multitude formes », ajoute-t-il en citant l'exemple *« d'un casino de Las Vegas attaqué par le biais du prestataire chargé de la maintenance des aquariums »*.

Les usurpations d'identité en général sont l'un des cas de figure les plus fréquents. Le problème vient aussi parfois d'informations sortantes de l'entreprise. Un donneur d'ordre peut charger un fournisseur d'envoyer certains e-mails ou lui communiquer des données dans le cadre d'une délégation d'activités. Ces informations sont alors récupérées par le biais du sous-traitant.

Mettre en place des ressources dédiées

Opter pour un audit global tenant compte des conditions dans lesquelles s'exerce la sécurité s'avère être une précaution intéressante. *« Dans ce cas, on regarde par exemple si tel fournisseur assurant la maintenance d'un équipement et disposant de fait d'un accès aux informations du donneur d'ordre, est en capacité d'avoir des consignes de sécurité suffisantes et conformes aux enjeux. La plupart des entreprises sont contaminées par des fournisseurs involontairement. C'est ce qu'on entend généralement par "une origine interne". Mais le collaborateur qui a quitté son entreprise en mauvais termes, dans un contexte de désaccord important, peut aussi être une source de problèmes et de craintes à ce niveau-là »*, indique Marc Lafeuriel, directeur exploitation et sécurité au sein de l'hébergeur de services et d'applications cloud Cyrès.

Si les vulnérabilités de la supply chain passent parfois inaperçues, c'est en raison de manquements quant à la gestion qui en dépend : il est souvent très délicat de savoir quel collaborateur est responsable des risques dans les relations avec les fournisseurs. Même les plus grandes organisations disposent d'une équipe limitée pour traiter les risques informatiques. Pouvoir surveiller l'ensemble de l'écosystème devient alors un véritable défi, surtout lorsque les fournisseurs se comptent par milliers. Mieux gérer cet aspect passe par la désignation d'un responsable de la gestion du cyber-risque des acteurs tiers, et l'adoption d'une stratégie adaptée. La mise en alerte et l'aide aux fournisseurs lorsque des risques sont identifiés dans la chaîne d'approvisionnement forment des hypothèses à envisager.

Des garanties fournisseurs dures à obtenir

Le RGPD stipule que les donneurs d'ordre doivent obtenir des garanties suffisantes de la part des fournisseurs sur ce plan. Mais les textes restent vagues pour ce qui est des détails qui doivent composer celles-ci. *« On constate dans les organisations la mise en place de processus d'auto-évaluation et d'évaluation auprès des fournisseurs. Mais ils sont souvent peu exigeants et donc insuffisants. Les certifications peuvent être une solution, comme ISO 270001, qui existe depuis longtemps. Certaines entreprises perdent parfois des marchés à cause de l'absence de garanties de ce type qui occupent toujours plus de place dans les critères de décision »*, indique Frédéric Thielen, Director, Customer and Operations au sein de KPMG.

Des agences de notation dédiées au cyber-risque apparaissent depuis quelques années. Mais elles se résument parfois à de simples analyses logicielles portant sur l'empreinte sur Internet d'une entreprise donnée. *« C'est une démarche intéressante mais trop légère, d'autant que ces éléments peuvent aussi être contournés ou manipulés »*, regrette Vincent Maret.

Les exigences vont galopantes dans ce domaine. *« Dans notre panel de clients, nous avons déjà des grandes entreprises ayant intégré des critères de cybersécurité pour leur démarche de référencement fournisseurs. Certains mettent sous contrôle des prestataires, et vont jusqu'à les blacklister pour des garanties insuffisantes. C'est encore quelque chose qui est à la marge, mais il est possible que ces sociétés soient en avance de phase par rapport à une tendance de fond dans ce domaine »*, témoigne Frédéric Thielen.

MATHIEU NEU

« Les tentatives d'intrusion chez les donneurs d'ordre peuvent prendre une multitude de formes »

***Vincent Maret**, associé, responsable du pôle cybersécurité et protection des données personnelles, KPMG*