Supply chain : pourquoi c'est devenu une priorité de sécurité

Cette découverte a impacté des millions d'utilisateurs et d'entreprises à travers le monde, qui se sont frénétiquement employés à installer des patches et des mises à jour dans leurs systèmes, sans parler des fournisseurs de logiciels et de matériels qui ont dû corriger des millions de lignes de code pour remplacer des composants vulnérables.

Mais cette faille critique révélait d'autres problèmes sans doute encore plus importants. L'un d'entre eux était une large et presque aveugle dépendance envers un code développé par une équipe à la fois restreinte et sans grandes ressources. Un autre était cette croyance fallacieuse que si autant de monde utilisait ce code, il devait bien avoir été testé, entièrement validé et dépourvu de bugs et d'autres erreurs éventuelles.

Même si le code OpenSSL était entièrement visible et librement accessible comme toute initiative open source, ce n'est que plusieurs années après que la faille ait été malencontreusement introduite en 2012 qu'elle a été découverte par des analystes de sécurité.

Cet exemple ne représentait alors que les premices d'une vague de risque bien plus large qui est l'utilisation ou la faiblesse de la supply chain dans les attaques cyber.

De l'attaque sur la supply chain logicielle, en passant par le mythe du risque hardware, ou encore via des implants dans des logiciels, le risque est aujourd'hui multi facette. L'actualité avec des groupes comme APT 41ou APT10 ou encore la crise Not Petya auront mis en lumière les impacts que peuvent avoir les attaques sur la supply chain.

Quelles soient ciblées comme dans les cas d'usages d'APT41, quelles soient d'une ampleur large comme pour APT10 qui vise les Services Providers à travers le monde ou qu'elles soient pandémiques comme pour Not Petya, ces attaques deviennent un point d'attention majeur de toutes les entreprises, de tous les gouvernements et même dans certains cas des citoyens.

Aujourd'hui, alors que les organisations s'épuisent à suivre le rythme des demandes sans cesse croissantes de la part de leurs utilisateurs pour de nouveaux services, de nouvelles fonctionnalités et une meilleure satisfaction client, les équipes informatiques sont contraintes d'exploiter et d'intégrer de plus en plus, aussi bien en intégrant des composants tierce partie à leur développement ou en se connectant à des partenaires à différents endroits de leur infrastructure.

Une fois ces nouvelles venues intégrées dans des systèmes internes, il devient plus difficile d'identifier les risques de chacun d'entre eux, et de déceler clairement les interdépendances.

Enfin, les organisations ont certes beaucoup de partenariats formalisés avec des partnaires tiers (logiciels, entreprises…), mais il peut y en avoir beaucoup d'autres qui n'ont pas été référencés et n'ont pas fait l'objet d'une procédure d'achat centralisée. Ceux-ci passent donc sous le radar de tout audit de sécurité ou même de toute identification basique.

Et même des fournisseurs et des partenaires référencés peuvent être exposés à une 'supply chain'

non documentée, car ils exploitent aussi des solutions et du code logiciels issus de tierces parties avec les mêmes objectifs de respect des délais.

Que pouvons-nous faire ?

Force est d'admettre cette vérité simple : il est impossible en pratique de tester et de contrôler de manière exhaustive chaque ligne de code intégrée dans toute application, tout service mis en production ou tout prestataire externe rattaché au réseau de l'entreprise. Ceci peut être comparé au problème lié à la surcharge d'alertes auquel la plupart des équipes de sécurité sont confrontées quotidiennement.

Toutefois, tout comme des équipes de sécurité qui voient les choses d'un point de vue différent et sont capables de traiter une montagne d'événements en utilisant une approche basée sur le renseignement pour accélérer le processus d'identification des menaces majeures, il est possible d'agir en avance de phase pour minimiser les risques associés à la 'supply chain'.

Le référencement, l'évaluation et le suivi des éléments de Supply Chain devient donc un élément fondamental de la gestion du risque des entreprises.

Une des approches, ces partenaires une fois référencés, ils peuvent être régulièrement surveillés pour tout problème touchant leur réputation, leur marque ou autre en détectant tout article de presse, publication ou mention dans des forums au sujet de l'organisation elle-même, des tierces parties qui composent leur 'supply chain', de leurs dirigeants, leur personnel, etc.

Cette tâche peut être fastidieuse si elle est effectuée manuellement, mais des fournisseurs de services peuvent aussi offrir ce type d'informations. Typiquement, elles sont proposées dans le cadre d'un service de surveillance des menaces digitales. La plupart des entreprises sont intéressées par ces services pour leur propre organisation, leurs propres marques et leurs dirigeants, mais leur rayon d'action peut être étendu pour couvrir des partenaires et des tierces parties.

En combinant la visibilité obtenue de ces services avec des informations de renseignement sur les menaces offrant une étroite surveillance des problèmes potentiels associés aux divers composants déployés dans un environnement, les organisations peuvent bénéficier d'une vision à 360 degrés des menaces et des risques associés à leur 'supply chain'.

Cette combinaison peut également servir de base à une évaluation régulièrement mise à jour des réputations et des risques, capable d'identifier rapidement de nouvelles sources de menaces avant qu'elles n'atteignent un seuil critique.

Conclusion

Alors que les organisations deviennent plus dépendantes de composants, de plates-formes, de services, de prestataires, de partenaires, de sous-traitants et d'autres éléments issus de partenaires tierces qui leur fournissent des fonctionnalités critiques pour leurs propres déploiements, elles

doivent mettre en place en parallèle un processus de contrôle des risques que leur ‘supply chain’ représente pour leur propre infrastructure de sécurité.