Supply chain : stopper lâ□□Ã©lan des cybercriminels
Internet
PostÃ© par : JPilo
PubliÃ©e le : 18/3/2022 15:00:00

Selon le dernier baromÃ¨tre du CESIN sur la cybersÃ©curitÃ© des entreprises en France, les attaques indirectes par rebond via un prestataire ont augmentÃ© de 5 % pour atteindre 21 % en 2021. Pour les organisations, la principale difficultÃ© rÃ©side dans le fait que la dÃ©fense de la supply chain est une mission difficile Ã accomplir compte tenu des centaines, voire des milliers de points dâ□□entrÃ©e qui doivent Ãªtre surveillÃ©s tout au long de la chaÃ®ne.

Selon Laurent Nezot, Sales Director France chez Yubico, bien que le dÃ©fi soit grand, il existe bel et bien des mesures, ainsi que des bonnes pratiques, qui permettent de rÃ©duire considÃ©rablement le risque dâ□□attaques rÃ©ussies, une fois le pÃ©rimÃ¨tre de la supply chain dÃ©fini :

Â« Une chaÃ®ne dâ□□approvisionnement englobe un large Ã©ventail de relations. Chaque entreprise possÃ¨de une supply chain, mÃªme si elle ne porte pas cette Ã©tiquette, puisque celle-ci comprend tous les partenariats et toutes les relations commerciales quâ□□une entitÃ© est susceptible dâ□□entretenir.

Il peut sâ□□agir dâ□□une Ã©quipe de dÃ©veloppement de logiciels travaillant avec des tiers qui soumettent du code Ã son systÃ¨me, ou bien de lâ□□achat de produits IT ou de code auprÃ¨s de ressources tierces qui doivent Ãªtre intÃ©grÃ©s dans la base de code interne. En rÃ©alitÃ©, une supply chain tournÃ©e vers lâ□□extÃ©rieur peut dÃ©signer tout produit, code ou matÃ©riel, et service utilisÃ© â□□tel quelâ□□ pour dÃ©velopper le propre produit ou service dâ□□une entreprise.

Une fois que lâ□□organisation dispose dâ□□une vue dâ□□ensemble de sa chaÃ®ne dâ□□approvisionnement, elle peut se fixer un objectif trÃ¨s prÃ©cis en matiÃ¨re de sÃ©curitÃ© : veiller Ã ce que chaque produit entrant â□□ quâ□□il sâ□□agisse dâ□□un logiciel achetÃ© et utilisÃ©, dâ□□un code dÃ©veloppÃ© par un tiers, ou service utilisÃ© â□□ soit sÃ©curisÃ© et respecte les bonnes pratiques. Plus important encore, il faut Ãªtre capable dâ□□identifier et de contrÃ´ler toute personne ayant accÃ¨s Ã un systÃ¨me dâ□□entreprise, par quelque moyen que ce soit.

Une entreprise peut exploiter du code dÃ©veloppÃ© par des Ã©quipes internes ou par des sources externes. Dans tous les cas, il est primordial de veiller Ã ce que le processus de gestion du code soit validÃ©. DÃ¨s lors quâ□□il y a une collaboration avec des sources extÃ©rieures, il est particuliÃ¨rement important de conserver des clÃ©s de signature et des certificats sÃ©curisÃ©s pour garantir lâ□□authenticitÃ©.

De plus, la mise en place dâ□□un systÃ¨me de gestion du code source est primordiale. Cela permet de s'assurer que les versions du code sont correctement gÃ©rÃ©es et que chaque personne qui se connecte au systÃ¨me est authentifiÃ©e avec les autorisations appropriÃ©es. Le systÃ¨me horodate le code et enregistre ses mouvements afin qu'il ne puisse pas Ãªtre manipulÃ© de faÃ§on malveillante Ã tout moment sans Ãªtre dÃ©tectÃ©.

La signature doit par ailleurs Ãªtre utilisÃ©e et intÃ©grÃ©e au systÃ¨me de gestion de code pour protÃ©ger tous les types de modules logiciels et d'exÃ©cutables, y compris les pilotes de logiciels, les applications, les fichiers d'installation, les scripts et les modules de micrologiciels dans les systÃ¨mes industriels.

De plus, Ã lâ□□heure oÃ¹ les dÃ©veloppeurs sont trÃ¨s sollicitÃ©s, et oÃ¹ la quantitÃ© de code open-source disponible est considÃ©rable, il est nÃ©cessaire de savoir dâ□□oÃ¹ vient le code. Tous les codes open-source ne sont pas Ã©gaux et les attaquants ont tirÃ© parti de vulnÃ©rabilitÃ©s connues.

Si un code source ouvert est utilisÃ©, il doit Ãªtre divulguÃ©. L'identification des composants open source permet de remÃ©dier plus rapidement aux vulnÃ©rabilitÃ©s qui pourraient apparaÃ®tre Ã l'avenir, qu'il s'agisse de code que lâ□□organisation a gÃ©rÃ© ou de logiciels achetÃ©s.

Au regard de lâ□□omniprÃ©sence des cybermenaces, les entreprises doivent Ãªtre en mesure de protÃ©ger toutes les formes de code contre tout accÃ¨s non autorisÃ© et toute manipulation au cÅ□ur de leur supply chain. De maniÃ¨re gÃ©nÃ©rale, elles doivent sâ□□assurer que ce quâ□□elles reÃ§oivent de lâ□□extÃ©rieur ne crÃ©era pas de vulnÃ©rabilitÃ©s Ã lâ□□intÃ©rieur une fois ingÃ©rÃ©.

Lâ□□authentification multifacteur rÃ©sistante au phishing, ainsi que la signature de code constituent des contrÃ´les et des mesures de sÃ©curitÃ© efficaces pour amÃ©liorer leur protection tout en rÃ©pondant aux besoins de conformitÃ© ; un enjeu crucial alors quâ□□il faut sâ□□attendre Ã de nouvelles attaques ciblant la supply chain dans les mois Ã venir. Â»