CybersÃ©curitÃ© : de lâ□□importance de sÃ©curiser la supply chain
Internet
PostÃ© par : JulieM
PubliÃ©e le : 3/4/2023 14:00:00

La plupart des organisations sont dÃ©sormais connectÃ©es numÃ©riquement Ã des centaines de fournisseurs et de vendeurs. Or, les faiblesses du dispositif de sÃ©curitÃ© d'un fournisseur peuvent permettre Ã un cybercriminel d'accÃ©der au rÃ©seau et de dÃ©ployer des logiciels malveillants. SolarWinds est l'une des attaques les plus connues de ce type. Mais qu'avons-nous appris depuis l'incident de 2020 ?

Selon Dirk Schrader, Resident CISO (EMEA) and VP of Security Research chez Netwrix, les exemples rÃ©cents d'attaques contre la supply chain ont Ã©tÃ© motivÃ©s par deux erreurs principales :

Â« La premiÃ¨re concerne la confiance et la mentalitÃ© "ne pas demander, ne pas dire". Les organisations se sentent encore mal Ã l'aise, non seulement lorsqu'il s'agit de partager les dÃ©tails des incidents survenus dans leurs propres systÃ¨mes, mais aussi quant Ã poser des questions sur les programmes de sÃ©curitÃ© de leurs partenaires.

Cependant, les maillons d'une supply chain Ã©tant Ã©troitement liÃ©s les uns aux autres, il est essentiel de procÃ©der Ã une Ã©valuation des risques en tenant compte des vulnÃ©rabilitÃ©s des acteurs de cette chaÃ®ne. Alors qu'une attaque n'est plus une question de "si" mais de "quand", les Ã©quipes informatiques ne peuvent pas se contenter d'ignorer les risques associÃ©s aux fournisseurs de son organisation.

La deuxiÃ¨me erreur repose sur le mantra "il y a toujours un plus gros poisson, nous ne sommes pas assez importants". Les petites organisations ont en effet tendance Ã penser qu'elles ne seront pas victimes d'une cyberattaque en raison de leur taille. En rÃ©alitÃ©, chaque organisation d'une supply chain a une responsabilitÃ© plus large, qui dÃ©coule de toutes les interconnexions qu'elle a Ã©tablies dans le passÃ© ; il peut s'agir notamment des API ou de l'accÃ¨s Ã distance des fournisseurs et des clients.

Les groupes APT considÃ¨rent de plus les supply chains comme un levier significatif pour une infiltration rÃ©ussie. C'est ainsi un moyen de propager des malwares et des portes dÃ©robÃ©es par le biais de connexions fiables et d'augmenter le nombre de victimes avec moins d'efforts.

Il est donc probable que ces acteurs malveillants continueront Ã faire Ã©voluer leurs tactiques pour couvrir davantage d'Ã©lÃ©ments de la supply chain et de vecteurs d'attaque ; en s'intÃ©ressant par exemple Ã des progiciels spÃ©cifiques Ã un secteur ou Ã des applications prÃ©fÃ©rÃ©es d'un groupe d'utilisateurs plus important.

Les organisations devraient par consÃ©quent structurer leur propre surface d'attaque Ã©largie en couches d'infrastructure, d'identitÃ©s et de donnÃ©s, afin de cartographier les chemins potentiels Ã travers ces diffÃ©rentes couches. L'important est de rÃ©duire l'exposition non seulement en termes de quantitÃ©, c'est-Ã -dire le nombre de vulnÃ©rabilitÃ©s ou de connexions, mais aussi de surveiller et de limiter les privilÃ¨ges utilisÃ©s, en leur appliquant une stratÃ©gie de "juste Ã temps" et "juste assez". Â»