Comment un cybercriminel peut infiltrer votre réseau ?

Comment un cybercriminel peut infiltrer votre réseau ?

La sécurité est plus que jamais une priorité pour les entreprises, contribuant activement à sa réussite. Les RSSI doivent désormais s'assurer que leurs projets en matière de sécurité IT sont en phase avec les objectifs de l'entreprise.

Nous sommes tous connectés à Internet, ce qui est très positif. Mais ce lien permanent implique que nous sommes tous au cœur d'un écosystème de grande envergure. Il est essentiel de comprendre que tout ce qui touche une organisation impactera également de nombreuses autres entreprises, et notamment ses partenaires.
Ainsi, en cas de piratage d'une entreprise, ce sont des données personnelles identifiables qui sont détournées. Ces données peuvent être revendues à des spécialistes de l'usurpation d'identité ou constituer un terreau favorable aux attaques de phishing. Plus l'assaillant disposera d'informations sur vous, plus l'email qu'il vous enverra apparaîtra comme légitime et vous incitera à cliquer sur un lien malveillant.
Notons que les tactiques d'attaques actuelles sont similaires à celles d'il y a quelques années : récupération de mots de passe faibles, attaques de type phishing et téléchargement de logiciels malveillants à partir de sites web infectés ou de publicités malveillantes. Sauf qu'aujourd'hui, l'assaillant a gagné en furtivité et en efficacité lorsqu'il mène son attaque.

Penchons-nous, par exemple, sur les réseaux sociaux et les services en ligne. Nous sommes très nombreux à les utiliser, qu'il s'agisse de Facebook, de LinkedIn, ou encore des sites de rencontres en ligne. Les assaillants l'ont parfaitement compris et capitalisent sur la fibre émotionnelle de chacun. Ils établissent ainsi leur passerelle d'entrée vers les dispositifs des utilisateurs en s'aidant de ces sites et de techniques d'ingénierie sociale. Ainsi, si les méthodes d'ingénierie sociale restent les mêmes, les vecteurs et la surface d'attaque ont, en revanche, progressé. Parallèlement, ce sont les techniques de furtivité qui ont gagné en précision, avec des assaillants toujours plus aptes à se dissimuler. Se contenter d'utiliser les antivirus traditionnels n'est donc tout simplement plus suffisant.
Parmi les techniques utilisées, l'attaque de type phishing est la méthode principale pour s'immiscer au sein des réseaux d'entreprise.
Un email de phishing, conçu pour paraître le plus légitime possible, est envoyé avec un fichier joint ou une URL malveillante, et incitant l'utilisateur à ouvrir le fichier ou à cliquer sur l'URL. L'attaque par téléchargement furtif (ou drive–by attack) est une autre technique utilisée par les assaillants. Ces derniers piratent un site Web et y installent un script java malveillant qui redirigera l'utilisateur vers un autre site hébergeant un logiciel malveillant téléchargé en arrière-plan vers l'équipement de l'utilisateur. Dans le cas d'une attaque ciblée, les assaillants peuvent passer des mois à identifier les sites Web les plus consultées par les organisations ciblées, pour ensuite les infecter.
Le malvertising (publicité malveillante) compte également parmi les techniques utilisées. Cette attaque emprunte les codes des attaques drive-by, mais l'assaillant se focalisera sur l'infection des sites de publicités. Il devient possible d'infecter un seul de ces sites qui, à son tour, pourra infecter jusqu'à 1 000 autres sites Web. Ou l'art d'industrialiser son attaque.
Enfin, n'oublions pas l'attaque mobile. Nombre de ces attaques sont similaires à celles mentionnées plus haut, mais elles ciblent les dispositifs mobiles. Notons qu'il est possible d'infecter un dispositif mobile via un message SMS, ou à l'aide d'un logiciel malveillant qui se présente en tant qu'application ludique ou de contenu pour adultes.
Lorsque l'assaillant est rentré dans un réseau et qu'il réside sur le dispositif d'un utilisateur (ordinateur de bureau ou portable, équipement mobile), il doit désormais injecter de nouveaux logiciels malveillants et outils pour mener à bien sa mission. Généralement, les informations de valeur ne sont pas stockées sur les postes de travail, mais plutôt sur les serveurs et des bases de données.

Voici donc un aperçu des étapes supplémentaires pouvant être mises en œuvre par un cybercriminel déjà présent dans le réseau:
• Téléchargement d'autres outils et logiciels malveillants pour compromettre davantage le réseau.
• Exploration du réseau pour identifier les serveurs hébergeant les données ciblées.
• Recherche du serveur Active Directory contenant tous les identifiants d'authentification, dans l'objectif de pirater ces données, véritable sésame pour le cybercriminel.
• Une fois les données ciblées identifiées, recherche d'un serveur provisoire pour y copier ces données. Le serveur idéal est un serveur stable, à savoir toujours disponible, et disposant d'un accès sortant vers Internet.
• Exfiltration furtive et lente de ces données vers les serveurs des assaillants, généralement déployés dans le cloud, ce qui rend la neutralisation des communications plus complexe.

Les cybercriminels présents au sein du réseau sur une longue durée pourront obtenir tous types d'informations disponibles puisque les données d'entreprise, dans leur grande majorité, sont archivées sous format électronique. Plus le cybercriminel est présent sur le réseau, plus il en apprend sur les processus et les flux de données de votre entreprise. L'attaque Carbanak qui a ciblé de nombreuses banques dans le monde en est la parfaite illustration. Lors de cette exaction, les cybercriminels sont remontés jusqu'aux ordinateurs des administrateurs ayant accès aux caméras de vidéosurveillance. Ils ont ainsi pu surveiller de près le fonctionnement du personnel bancaire et enregistrer tous les processus dans le détail. Ces processus ont été reproduits par les cybercriminels pour transférer des fonds vers leurs propres systèmes.
Comme déjà souligné, une brèche dans le réseau s'initie généralement par un simple clic d'un utilisateur sur un lien malveillant. Après avoir investi le poste de l'utilisateur piraté, l'assaillant commence à explorer le réseau et à identifier les données qu'il souhaite détourner. C'est dans ce contexte que la notion de segmentation de réseau devient essentielle. Cette segmentation permet de maîtriser l'impact d'un piratage puisque l'entreprise victime peut isoler la faille et éviter tout impact sur le reste du réseau. D'autre part, elle permet de cloisonner les données sensibles au sein d'une zone hyper-sécurisée qui rendra la tâche bien plus complexe pour ceux qui souhaitent les exfiltrer. Pour conclure, gardons à l'esprit qu'il est impossible de protéger et de surveiller le réseau dans sa totalité, compte tenu de son périmètre étendu et de sa complexité. Il s'agit donc d'identifier les données les plus sensibles, de les isoler et de porter son attention sur les chemins d'accès vers ces données.

Réagissez à cet article

Source : *Comment un cybercriminel peut infiltrer votre réseau | Data Security Breach*