Entre le Cloud et le système d'information local, l'angle mort de la cybersécurité

En cybersécurité, les angles morts sont probablement tout aussi dangereux qu'au volant. Dans le numérique, il s'agit de zones sur lesquelles les mesures de contrôle et de supervision ne sont pas aussi effectives que sur le reste du système d'information. Elles permettent alors à un attaquant d'opérer plus librement avec des outils « bruyants » sans risquer la détection, ou de se déplacer latéralement plus facilement d'un environnement à l'autre. Car souvent, ces zones naissent à la frontière entre deux environnements.

De la théorie ? Pas vraiment. Même si tous les détails ne sont pas encore connus — l'investigation est toujours en cours — il semble acquis que les attaquants responsables de la compromission de l'éditeur SolarWinds ont pu évoluer librement entre le système d'information local et son extension dans le Cloud, en particulier dans l'environnement Microsoft 365.

Pour bien comprendre toute l'efficacité d'une telle approche, il faut se souvenir que chez bien des entreprises les environnements locaux et Cloud sont souvent distincts dans leur administration et leur supervision, mais parfaitement imbriqués dans leur utilisation quotidienne.

Ainsi l'email d'Outlook 365 ou les données stockées dans OneDrive ou SharePoint online sont certes manipulés sur le poste client, au sein du SI local (où ils peuvent aussi être backupés), mais ils vivent dans le Cloud, où ils bénéficient peut-être d'une politique d'accès différente, voire d'administrateurs différents.

Et pourtant, l'annuaire Active Directory local de l'entreprise — le sésame complet — est toujours synchronisé dans le Cloud via ADconnect ou ADFS. Ce qui fait que le vol d'un identifiant d'un côté peut ouvrir des portes de l'autre, et inversement.

C'est d'ailleurs ce qui semble s'être passé dans l'affaire SolarWinds : une fois les attaquants ayant élevés leurs privilèges au sein du système d'information local, ils ont pu exploiter ces acquis pour se fabriquer des sésames leur permettant d'accéder à l'infrastructure Cloud.

L'exploitation ultérieure des contrôles d'authentification locaux a en effet permis aux attaquants de pivoter vers le Cloud et d'opérer dans Microsoft 365 sans être détectés pendant une longue période.

En dehors de la quantité d'information qui y réside, c'est bien tout l'intérêt du Cloud du point de vue de l'attaquant : il s'agit d'un environnement dans lequel il peut opérer longuement avec un risque de détection bien moindre.

Il profite pour cela de deux facteurs contribuant à créer l'angle mort parfait : des relations de confiances avec l'infrastructure locale qui lui permettent d'abaisser le niveau de sécurité vis-à-vis de l'extérieur, et un manque de visibilité sur les actions menées dans le Cloud en corrélation avec celles initiées localement, qui lui permettent de masquer ces modifications (en particulier s'il n'exploite que des outils et des fonctionnalités légitimes de Microsoft 365 tels l'authentification OAuth, le MFA, les outils de recherche eDiscovery, etc.).

Nous avons d'ailleurs identifié cette tendance depuis plusieurs mois. Dans une étude récente* portant sur 4 millions de comptes Microsoft 365, nous avons identifié des comportements de déplacements latéraux chez 96 % des entreprises, notamment le contournement de l'authentification multifacteurs (MFA) et des contrôles de sécurité intégrés.

Dès lors, un attaquant peut en quelques clics, reconfigurer les règles du courrier électronique, compromettre les magasins de fichiers SharePoint et OneDrive, et mettre en place des capacités de reconnaissance et d'exfiltration persistantes en utilisant les outils intégrés du M365 tels que eDiscovery et Power Automate. Les possibilités de ce type d'attaques sont vastes et croissantes. Deux mois avant que n'éclate l'affaire SolarWinds, cette mise en garde était prémonitoire !

La cause principale, ici, est le manque de visibilité d'un environnement à l'autre : être en mesure d'associer les actions locales d'un poste de travail et du compte utilisateur associé avec, par exemple, les droits sur les *tenants* Cloud utilisés habituellement, et donner l'alerte lorsque des incohérences sont détectées.

Plus largement, l'enjeu devient clairement d'obtenir une vue réellement consolidée des droits d'administration sur tous les environnements, et d'être en mesure d'appliquer à l'environnement Cloud la même vigilance sur les accès privilégiés que ce qui devrait être désormais la norme *on-premise*.

Ce dernier point est crucial, car si l'on observe les actions de l'attaquant dans l'affaire SolarWinds, l'on constate qu'il a pu ajouter des identifiants (certificats X.509 ou mots de passe) probablement volés ou générés en local à des applications Cloud, afin de profiter par exemple des droits implicites de lecture des emails de ces dernières, voire — lorsqu'elles n'en disposaient pas — de leur ajouter les permissions Mail.Read or Mail.ReadWrite.

Du point de vue du défenseur, il est ainsi possible d'observer localement la création ou la modification d'un compte qui semble n'être ensuite jamais utilisé (et qui passera donc peut être sous le radar), alors qu'en réalité celui-ci a servi à étendre les droits d'une application Cloud capable désormais de piller les emails ou les documents stockés dans SharePoint Online.

En local, le compte n'a rien fait de malveillant, et dans le Cloud, la modification des droits a été réalisée par un compte de confiance, donc tout va bien.

Ce manque de coordination entre une action initiée localement et ses implications dans le Cloud est l'un des angles morts les plus courants, et peut-être le plus complexe à identifier, car cela exige de pouvoir tracer l'ensemble du comportement et des déplacements d'une machine ou d'un compte utilisateur à travers des environnements distincts.

Mais d'autres approches plus directes sont également mises en œuvre par les attaquants, donc l'exploitation du cadre de fédération des identités de Microsoft afin de contourner l'authentification à double facteur (MFA). Ainsi, grâce à un accès local compromis l'attaquant est en mesure se connecter à l'avenir librement à la ressource détournée depuis n'importe quelle machine et n'importe quelle connexion.

Si aujourd'hui ces attaques peuvent sembler privilégiées par des groupes avancés, comme en témoigne l'opération contre l'éditeur SolarWinds, il est très probable que, demain, les mêmes

angles morts seront exploités de manière massive par tous les petits rançonneurs.