Sécuriser Microsoft Office 365 face à la nouvelle normalité

Autrefois conside?re? comme un avantage strate?gique, le cloud est rapidement devenu indispensable au sein des entreprises. Son adoption, ainsi que l'efficacite? et l'agilite? qu'il procure, figurent en bonne place de l'ordre du jour des conseils d'administration depuis plusieurs anne?es maintenant.

Toutefois, il a fallu attendre 2020 pour que la plupart des entreprises voient leurs strate?gies cloud re?ellement mises a? l'e?preuve.

Face a? l'adoption rapide du te?le?travail, il n'est pas e?tonnant que l'utilisation de Microsoft Office 365 ait gagne? du terrain au sein de nombreuses entreprises a? des fins de collaboration. En mars 2020, 258 millions d'utilisateurs actifs étaient recensés, soit une hausse de plus de 70 millions par rapport a? l'anne?e pre?ce?dente.

Cette transition contrainte et force?e a bouleverse? irre?me?diablement le paysage informatique.

Cette adoption acce?le?re?e, qui tient plus du bapte?me du feu compte tenu des circonstances, semble avoir apporté? des avantages tangibles pendant la pande?mie, tels que l'amélioration de la productivité ou la satisfaction au travail. Ne?anmoins, les ale?as des confinements aux quatre coins du monde ont aussi mis a? rude e?preuve tous les secteurs e?conomiques. Outre les re?percussions sur les effectifs, l'e?volution rapide du paysage informatique et l'acce?le?ration force?e de la migration vers le cloud ont aussi exacerbe? la vulne?rabilite? des entreprises aux cybermenaces.

E?volution rapide du paysage des menaces

En acce?le?rant le de?ploiement de Microsoft Office 365 et d'Azure AD, de nombreuses entreprises ont e?tendu leur surface d'attaque et isole? des effectifs qu'elles ne sont peut-e?tre pas en mesure de surveiller et de prote?ger efficacement. Dans cette nouvelle normalite?, les responsables de la se?curite? ont du retard a? rattraper. Ils doivent en effet comprendre et se?curiser leurs environnements cloud, avec des outils et des strate?gies de se?curite? souvent lacunaires. Les cybercriminels n'ont pas tarde? a? flairer le bon filon et a? multiplier les attaques. De?s avril 2020, Google indiquait bloquer quotidiennement plus de 18 millions d'e-mails de phishing et contenant des malwares sur le the?me de la COVID.-19.

Si la pre?valence des attaques de phishing en lien avec la COVID-19 semble aujourd'hui en recul, les failles de se?curite? lie?es a? l'essor des de?ploiements dans le cloud n'ont quant a? elles pas disparu.

De leur co?te?, les attaquants peaufinent leurs techniques et mettent leur expe?rience a? profit pour s'aventurer sur ce nouveau terrain et en exploiter les failles. C'est ainsi que les attaques de malware traditionnelles sont aujourd'hui de?laisse?es au profit d'attaques ciblant les comptes, les identifiants, les autorisations et les ro?les, que les outils de se?curite? traditionnels sont totalement incapables de de?tecter.

En re?alite?, compte tenu des progre?s majeurs enregistre?s par des outils tels que les solutions de de?tection et d'aide a? la re?solution des incidents (NDR) re?seau ou les analyses optimise?es par l'intelligence artificielle (IA), ce devrait e?tre l'inverse. Une fois que les attaquants parviennent a? infiltrer un environnement, ils comptent habituellement sur leur aptitude a? se faire oublier dans le tourbillon des activite?s normales de l'entreprise. Les pirates prudents n'he?sitent pas a? exploiter les applications me?tiers le?gitimes (tactique du « live off the land »), notamment celles inte?gre?es a? la suite Microsoft O365, telles que Power Automate et eDiscovery, pour se de?placer late?ralement, se cacher dans le trafic HTTP, HTTPS et DNS, et exfiltrer des donne?es. Les solutions NDR optimise?es par l'IA qui s'inte?grent aux applications et services cloud sont capables d'exposer cette couverture et d'identifier rapidement le moindre indice qu'un intrus est a? l'oeuvre.

Cependant, si l'e?cart entre attaquants et de?fenseurs se réduit sur papier, cela ne concerne que les entreprises qui ont investi dans de telles fonctionnalite?s. Pour celles qui ne disposent pas des capacite?s ne?cessaires pour de?tecter les signes subtils d'activite? malveillante, l'e?cart va continuer a? se creuser, et les attaquants pourront profiter pleinement de leur infrastructure cloud.

Se?curiser Microsoft Office 365 est une priorite? absolue

Microsoft Office 365 continue de jouer un ro?le essentiel dans la continuite? des activite?s me?tiers. Les entreprises doivent de?s lors veiller a? disposer des capacite?s ne?cessaires pour se?curiser leurs environnements cloud. Le proble?me est particulie?rement pressant pour les entreprises qui ont du? revoir rapidement leur fonctionnement au cours de l'anne?e e?coule?e et qui pourraient avoir du mal a? adapter les de?fenses du pe?rime?tre aux frontie?res plus floues du cloud. La priorite? absolue doit e?tre de se pre?munir contre la prise de contro?le des comptes d'utilisateur.

Le manque de visibilite? induit un exce?s de confiance

Les responsables de la se?curite? sont confiants en leur capacite? a? pre?venir les prises de contro?le de comptes d'utilisateur, une confiance en totale contradiction avec le nombre croissant d'attaques et les longues dure?es d'implantation. La dure?e moyenne d'une attaque est estime?e a? 43 jours* - et les outils de se?curite? pre?ventifs sont incapables de de?tecter les prises de contro?le de comptes d'utilisateur.

De manie?re ge?ne?rale, les responsables de la sécurité sont e?galement assez confiants en leurs capacite?s a? identifier et a? endiguer d'autres formes d'attaques. La plupart estiment avoir une bonne visibilite? sur les attaques qui contournent leur pe?rime?tre et e?tre en mesure de de?tecter et de neutraliser tout de?placement late?ral. De nouveau, on note une discordance avec le fait que 96 % des environnements Microsoft Office 365 analyse?s pre?sentent des signes de de?placement late?ral.

Un centre d'ope?rations de se?curite? (SOC) peut e?tre confronte? a? des centaines de menaces au quotidien. Si l'on conside?re le nombre d'incidents de?joue?s comme principal indicateur de succe?s, tout va pour le mieux dans le meilleur des mondes. Cependant, cette approche e?lude les vraies questions a? se poser : combien de temps a-t-il fallu avant de de?tecter les menaces et de les neutraliser ? Combien d'entre elles constituaient des tentatives re?pe?te?es ? La capacite? a? neutraliser les nombreuses attaques en masse de bas niveau est a? distinguer de la de?tection des menaces sophistique?es, en particulier celles qui visent les utilisateurs.

Une confiance adapte?e a? la re?alite?

Pour se faire une ide?e pre?cise des capacite?s de se?curite?, il est indispensable de disposer des bons indicateurs. Les trois plus importants sont les suivants :

De?lai moyen de de?tection d'une menace
De?lai moyen de re?ponse
Fre?quence de re?pe?tition des me?mes proble?mes

L'analyse de ces trois indicateurs permettra de recueillir des informations contextuelles pre?cieuses sur l'efficacite? des dispositifs de se?curite? de l'entreprise. Les attaques a? longue dure?e d'implantation constituent la principale menace pour les entreprises. L'acce?s a? une se?rie de donne?es et d'applications en quelques secondes seulement suffit pour causer de nombreux proble?mes dans les entreprises. Il est e?galement essentiel de repe?rer a? quel endroit le me?me proble?me survient continuellement. C'est le signe qu'il est temps d'envisager un changement fondamental de strate?gie ou d'infrastructure.

Toute mesure doit reposer sur un flux suffisant de donne?es reproductibles. La re?alisation de tests d'intrusion et d'exercices de simulation d'attaques peut contribuer a? obtenir davantage de donne?es fiables sur les menaces. C'est un moyen d'identifier rapidement les failles de la strate?gie de se?curite? et l'efficacite? re?elle des de?fenses en place.

Outre l'aspect « mesure », ce type de test est une compe?tence essentielle des analystes en se?curite? : les serruriers ne doivent pas seulement re?parer les serrures, ils doivent aussi pouvoir les forcer.

*Etude Vectra - mars 2021