L'INFORMATICIEN

PAYS :France
PAGE(S) :18
SURFACE :80 %
PERIODICITE :Mensuel

DIFFUSION :(15000)

► 1 décembre 2021 - N°202

SÉCURITÉ

En 2022, l'IT n'a plus d'excuse

Quel début de décennie, mes aïeux ! La menace a décollé tandis que cette bonne vieille sécurité périmétrique explosait en vol, Cloud et travail à distance aidant. Si jusqu'en 2021 les DSI et RSSI pouvaient prétexter l'impréparation à la crise sanitaire, ils n'ont désormais plus d'excuse.

Alors qu'on nous rabâche que la question n'est plus *« si je suis attaqué »* mais *« quand je serai attaqué »*, on peut difficilement prétexter l'impréparation. *« Lors de la première vague, personne n'était prêt à ce que tout s'arrête en même temps, ça excuse l'IT de ne pas avoir, en amont, adapté son système. Quatre vagues plus tard, on sait que ça va durer : si ce n'est pas le Covid, ce sera autre chose. En 2022, rien ne va venir réduire les risques : work from everywhere, utilisation du cloud et des API, télétravail... »* assène Victor Desteucq, Regional Sales Manager chez Netskope. *« On ne peut plus dire qu'on ne savait pas, il faut maintenant prendre le problème à bras-le-corps ».*

Car les attaquants ne vont pas faiblir. Certes, les autorités étatiques mettent la pression sur les groupes cybercriminels. Mais désormais même les acteurs « low profile » (entendre par là des cybercriminels de faible envergure) ont à portée de main des ransomwares, grâce au modèle du Ransomware as a Service. Ce n'est pas neuf, mais Semperis craint que le phénomène ne s'accélère l'année prochaine. Louis-Frédéric Laszlo, Director of Product Management chez Atempo, partage cette inquiétude. D'autant que, selon lui, *« une connectivité accrue et l'accélération massive du SaaS complexifient la menace, tandis que l'atomisation des données élargit la surface d'exposition. Le BYOD, avec le retour dans les bureaux, est lui aussi un risque majeur ».*

S'ajoutent à ces problématiques deux menaces. Elles ne sont pas nouvelles, mais 2022 leur donnera un nouveau souffle. La première, *« la menace interne reste la principale cause des cyberattaques, qu'elle soit intentionnelle ou accidentelle »* souligne Victor Desteucq. Or, la pandémie a augmenté le recours à des contrats courts dont on ne ferme pas les accès après le départ. De même, de nombreux salariés ont, surtout aux Etats-Unis, démissionné lors de cette crise. Là encore, les comptes ont-ils bien été supprimés ? Les mécontents sont-ils partis avec plusieurs Go de données, augmentant le risque de fuite ? La deuxième menace arrive, quant à elle, plus tôt que prévu. On sait que l'IA et le machine learning seront des instruments utiles dans le secteur de la cybersécurité. Mais ils serviront aussi les acteurs malveillants. Juniper s'émeut de l'augmentation des risques de fuite de données sensibles ou privées utilisées par les algorithmes. Victor Desteucq va lui plus loin : les attaquants vont intoxiquer les données utilisées pendant l'apprentissage (empoisonnement), ou les récupérer pour comprendre les paramètres du modèle et être en mesure de l'attaquer (inférence), voire corrompre progressivement des modèles pour fausser des décisions (évasion). Ainsi, une attaque pourra, au choix, rendre un portique de sécurité insensible aux armes ou encourager un algorithme à conseiller d'investir dans un marché ou bien d'accepter toutes les demandes de crédit...

Louis-Frédéric Laszlo, Director of Product Management chez Atempo.

« L'atomisation des données élargit la surface d'exposition. »

Consolider pour consister

Bref, on n'a pas fini de trembler. Face à ces menaces toujours plus présentes, on pourrait imaginer que les entreprises vont continuer à empiler des outils de cybersécurité, espérant que l'accumulation suffira à combler les brèches. Faux, nous répond Victor Desteucq. *« On observe chez nos clients depuis trois ans une volonté de consolidation de leurs systèmes informatiques, et non d'empilement. Cette consolidation est nécessaire en 2022 »* nous confie-t-il. Une consolidation qui permettra la mise en place de règles consistantes dans des environnements mouvants. Louis Laszlo observe, quant à lui, une démocratisation, une vulgarisation de la part des éditeurs, dont les solutions descendront en 2022 des grands comptes vers les ETI et les « SMB », que ce soient des outils de IAM, de PAM, des SIEM ou encore du MDM.

Une dernière tendance en cybersécurité nous semble notable et c'est Renaud Ghia, le CEO de Tixeo, qui met le doigt dessus. Selon lui, le chiffrement de bout en bout commencera à se généraliser, notamment en Europe. *« On se rend compte qu'il y a une vraie demande, notamment pour éviter les fuites de données »* observe-t-il. *« Je pense que le chiffrement de bout en bout va devenir un standard de facto pour les solutions qui stockent de la donnée, j'en suis convaincu. Sans doute pas partout, mais l'Europe est un très bon prétendant, le chiffrement étant un outil de souveraineté autant que de sécurité ».* □