Les 5 tendances cybersécurité en 2021

Explosion de la fraude en ligne : les défenses existantes sont mises à rude épreuve

Les outils des fraudeurs ont fortement évolué depuis les cinq dernières années, tandis que la génération actuelle de défenses commence à montrer son âge. En particulier, les attaquants savent désormais beaucoup mieux imiter le comportement de leurs victimes (jusque dans leur environnement domestique), ce qui leur permet de contourner plus facilement l'authentification multifactorielle et les différentes mesures basées sur l'évaluation du risque (dont le rate limiting).

Les outils qui permettent ce type d'approche n'en sont qu'à leurs débuts, mais lorsqu'ils seront parvenus à maturité ils obligeront les entreprises à réévaluer leurs défenses face à la fraude.

Les imprimantes 3D vont bousculer la sécurité biométrique

Initialement vendues au grand public comme de coûteux jouets pour passionnés d'innovation, les imprimantes 3D coûtent désormais moins cher qu'une console Nintendo. Et avec elles, les empreintes digitales et les visages imprimés en 3D capables de tromper l'authentification biométrique n'appartiennent plus à la science-fiction. Et pour y parvenir, il ne sera pas non plus nécessaire de scanner la victime en haute définition.

Car en réalité, l'authentification biométrique repose avant tout sur une approche probabilistique, et un « passe-partout » imprimable pourrait alors ressembler davantage à un assortiment de modules assemblés qu'à une vrai réplique du visage ou des empreintes digitales d'une personne.

Les contrôles de sécurité migrent vers la périphérie

Acheminer des données à travers tout Internet pour finalement les rejeter parce qu'elles ne sont pas valides est un gaspillage de ressources. La bande passante d'Internet et les budgets télécom sont limités.

Faire migrer des fonctions de sécurité telle la protection contre les bots ou la validation des données à la périphérie permettra de réduire à la fois le temps de traitement et le coût de la bande passante.

Rust & Wasm vont changer la sécurité des

applications

WebAssembly (Wasm) a commencé comme un runtime alternatif pour les navigateurs web, une sorte de complément de JavaScript. Mais il est en train de devenir un moyen ultraléger et ultraportable d'exécuter des binaires n'importe où : sur le serveur, le navigateur, à la périphérie des réseaux, etc.

En parallèle, le langage Rust est devenu populaire en mettant l'accent sur la sécurité de la mémoire – la cause des principaux problèmes de sécurité. Il dispose en outre du meilleur support pour Wasm. La combinaison de ces deux technologies peut laisser présager des changements fondamentaux dans le domaine du développement des applications… web, mais pas que !

Une vague de fuites de données fin 2021

Le cadre de travail a radicalement changé en 2020. En quelques semaines, des millions de travailleurs ont quitté le bureau traditionnel pour leur domicile, et les systèmes IT ont dû suivre. Le problème, bien sûr, n'est pas le travail à distance en lui-même. C'est surtout que les critères et les indicateurs qui permettent d'identifier une fuite de données ont changé.

Il faudra un certain temps pour que les entreprises retrouvent leurs marques. Et lorsqu'elles auront reconnu à quoi ressemblent les nouvelles fuites de données, nous verrons probablement une cascade d'annonces…