Hervé Schauer (HS2)

« La protection périmétrique est caduque »

Aujourd'hui à la tête du cabinet de conseil HS2, Hervé Schauer a été l'un des pionniers de ces technologies dans les années 80. Nous lui avons demandé de dresser un bref panorama de ces évolutions technologiques, et sa vision du futur !

CyberRisques : M. Schauer, vous êtes un expert reconnu en sécurité des systèmes d'information. Pourriez-vous nous décrire l'historique du firewall, et dans un contexte de virtualisation, quels sont les gains opérationnels et les mesures de sécurité à déployer ?

Hervé Schauer : *« Tout d'abord je ne suis pas spécialiste et justement je ne trouve pas de spécialistes Cybersécurité Azure ou AWS pour dispenser des formations. En effet J'ai coinventé le proxy firewall en 1991 avec Christophe Wolfhugel. Cela a été présenté à Usenix à Baltimore en 1992.*

Lors de l'avènement des réseaux dans les années 80, la sécurité passait par le mot de passe pour authentifier l'utilisateur. En 1986 Bull a couplé un lecteur de carte à puce au PC et en 1988 je prédisais que tous les claviers auraient un lecteur de carte à puce et que nous nous authentifierions avec. Raté. Il a fallu attendre les ports USB, des bus série comme le lecteur de carte à puce, mais pour une authentification par un facteur autre que le mot de passe, ce sont les ordiphones qui le permettent enfin, c'est récent, il aura fallu 30 ans.

Dans l'intervalle TCP/IP a pris le pas sur Novell Netware et la sécurité d'accès aux applications totalement défaillante, que ce soit sur des PC de l'époque ou des stations de travail Unix (rlogin, NFS et les Yellow Pages de Sun, etc). Puis en 1988 TCP/IP a quitté le réseau local pour passer en inter-sites et le vers Morris a montré les conséquences. Il fallait pouvoir échanger avec Telnet et FTP, voir avec X11 ou SQL, entre entreprises distinctes, et aucun moyen d'authentifier les flux n'existait. Donc en 1989 Network Systems (devenu StorageTek puis EMC) a inventé le filtrage IP sur un contrat Darpa, et il a été programmé dans Wellfleet (devenu Bay Networks puis Nortel) en 1991, puis dans CISCO IOS aussi en 1991. J'ai co-inventé le proxy firewall sur un contrat CNES en 1991, afin d'aller au-delà du filtrage IP en identifiant et authentifiant l'utilisateur en coupure dans la communication. Pas de brevet, de là tous les éditeurs ont repris le principe, les firewalls ont permis la protection périmétrique et l'expansion d'Internet de 1994 à nos jours.

En 1999 j'ai fais des présentations aux USA et même dispensé un "Short Course" à la conférence SANS à Orlando sur "The doom of the firewall" pour démontrer que la protection périmétrique était insuffisante et qu'il fallait impérativement cloisonner les réseaux. C'était le paroxysme de la sécurité dans le réseau, qui n'a cessé de se développer des années 2000 à nos jours. En 2003 des réflexions chez Cisco ont mené à la création du Jéricho Forum qui a fait une campagne en 2004 pour la dépérimétrisation. J'ai répondu en 2005 avec une présentation ci-jointe à la JSSI de l'OSSIR que ce n'était pas pour tout de suite. Cédric Blancher m'a emboité le pas avec une présentation plus complète à SSTIC en 2008.

Mais quand j'ai clamé haut et fort aux Assises de la Sécurité toujours en 2008, appellé à l'improviste à la conférence plénière à la tribune, que "le RSSI allait survivre au DSI", j'ai fait scandale, il y a beaucoup de DSI invités aux Assises, pas que des RSSI, j'ai froissé du monde. Pourtant, le directeur cybersécurité des années 2020 va prendre l'importance et le grade qu'ont eu les DSI dans les années 2000 et 2010.

Maintenant les applications sont dans le cloud, elles seront gérées majoritairement par les métiers directement, localement, plus par une DSI centralisée, les DSI sont un service d'accès à Internet et de gestion d'annuaires (eux-mêmes dans le cloud), comme les gestionnaires de téléphonie l'étaient avant eux. Les applications utilisent des webservices dans tous les sens, seuls les auditeurs en cybersécurité retracent quel composant appelle quel composant, les DSI ne savent plus. Et les utilisateurs sont hors du réseau protégé, chez eux avec la crise sanitaire, avec des appareils divers et personnels... La protection périmétrique est donc caduque, la sécurité doit être mise au plus proche des données auxquelles l'utilisateur réclame l'accès. Google a très bien expliqué comment il le faisait en 2017 et maintenant c'est sous le terme "ZeroTrust" que ce mouvement est popularisé. »