

Le rapport de l'ANSSI sur le piratage de la DGFIP

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 octobre 2026

<https://www.bortzmeyer.org/anssi-dgfip.html>

Vous le savez, en ce moment, c'est la fête des fuites de données personnelles en France. Tout le monde (et son chat) a déjà été victime d'au moins une fuite. Au moins, grâce au RGPD, on est informé qu'il y a eu une fuite <<https://bonjourlafuite.eu.org/>>. Mais que s'est-il passé derrière ? En général, on ne le sait pas. Aucune enquête indépendante publiée et, souvent, rien du tout n'est publié, on doit se fier aux rumeurs propagées par des influenceurs en cybersécurité sur les réseaux sociaux, par des ministres menteurs et par des journalistes ignorants. Mais le piratage de la DGFIP, il est vrai particulièrement scandaleux, fait, lui, l'objet d'une publication assez détaillée <<https://cyber.gouv.fr/actualites/lanssi-publie-le-rapport-dincident-sur-les-cyberattaques-ayant-touche-la-dgfip/>>, par l'ANSSI.

Je vous recommande fortement la lecture de ce rapport <<https://cyber.gouv.fr/actualites/lanssi-publie-le-rapport-dincident-sur-les-cyberattaques-ayant-touche-la-dgfip/>>. Bien sûr, ce n'est pas une enquête indépendante (l'ANSSI, c'est l'État) mais c'est bien écrit (il y a beaucoup de sigles spécifiques à l'État mais un glossaire est présent), sérieux, modeste (l'ANSSI note bien ses propres faiblesses) et détaillé (attention, certaines parties ont été censurées par un gros pavé noir). Mais voici quelques points qui m'ont frappé (le principal étant le fait que ce rapport existe et ait été publié).

Le rapport contient un certain nombre de bons avis de sécurité. Mais beaucoup de gens l'ont interprété de manière binaire, s'indignant que le ministère n'ait pas mis en œuvre telle ou telle mesure. C'est oublier le principe de base de la sécurité (pas seulement informatique) : **il n'y a pas de solution idéale, seulement des compromis**. Par exemple, un EDR (mentionné par l'ANSSI) consomme des ressources informatiques importantes, a des faux positifs (j'en ai vu un protester contre du code binaire SuperH, considéré comme forcément suspect, alors que du code Sparc ou Alpha dans le même répertoire ne posait pas de problème), et peut avoir des bogues (c'était d'ailleurs le scénario du dernier exercice Remparts <<https://www.afnic.fr/observatoire-ressources/papier-expert/lexercice-de-cybersecurite/>>). Pire, ce sont souvent des logiciels privateurs. Bref, ne pas avoir d'EDR a des inconvénients, en avoir un a des inconvénients. On peut juste choisir son poison.

Le même raisonnement peut être appliqué aux autres conseils de l'ANSSI. Bien sûr, ils sont tous raisonnables mais tous ont un coût, pas seulement financier, mais aussi en gêne des employés pour leur

travail. Les organisations qui déploient les mesures citées ont souvent été victimes d'une « auto-attaque par déni de service », les mesures de sécurité empêchant de travailler.

J'ai quand même trouvé que le cas cité par le rapport d'une soi-disant « authentification à deux facteurs » qui consistait en l'envoi par courrier du second facteur... alors que le courrier était traité sur la machine qui servait à se connecter, était en effet assez incroyable. Si les deux facteurs sont sur la même machine, ce ne sont pas réellement deux facteurs (le rapport insiste, à juste titre, sur ce point).

Le rapport détaille les techniques mises en œuvre mais pas l'arrière-plan organisationnel. Par exemple, au moins une partie des accès pirates ont été faits depuis le ministère de l'Éducation nationale, apparemment moins protégé, mais le rapport ne dit pas pourquoi ce ministère avait accès aux données des impôts. Même chose pour des accès par des entités privées extérieures (comme le géomètre-expert mentionné dans le rapport).

La sécurité ne dépend pas uniquement du budget (on peut avoir un budget très élevé et le dépenser essentiellement dans du théâtre sécuritaire, par exemple l'achat de dispositifs techniques très chers, opaques mais bénéficiant d'un bon marketing). Mais il ne faut pas se faire d'illusion, la sécurité aura un coût : si on déploie toutes les mesures proposées par le rapport, il faudra embaucher beaucoup de fonctionnaires (par exemple pour les investigations suite à une alarme). Les mêmes politiciens qui s'indignent « comment se fait-il qu'il n'y ait pas davantage de sécurité dans les ministères » seront peut-être les premiers à râler si on leur demande d'augmenter le budget de l'État.

Je recommande de bien lire le rapport jusqu'au bout, les annexes contiennent des détails précis, notamment chronologiques. Ils montrent que de nombreuses alarmes avaient été levées et traitées, mais que l'ampleur et le sérieux de l'attaque n'avaient pas été clairement notés (le fameux problème de « relier les points »).