RFC 7632 : Endpoint Security Posture Assessment: Enterprise Use Cases

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 septembre 2017

Date de publication du RFC : Septembre 2015

https://www.bortzmeyer.org/7632.html

La sécurité est évidemment une préoccupation courante quand on gère un réseau (« "*enterprise network*" » dit ce document, mais cela s'applique à n'importe quel réseau, capitaliste ou pas). Parmi les problèmes, déterminer l'état de la sécurité de chaque machine du réseau (son logiciel est à jour ? Pas de RAT installé ?) est un des plus importants. Ce RFC décrit des scénarios où on cherche à analyser cet état de la sécurité.

Disons-le tout de suite, une grande partie du RFC est du jargon « "*process*" » (quand on remplace l'intelligence par la paperasserie). Si vous n'êtes pas "*manager*" chargé d'obtenir une certification ISO 27001, cela ne vous intéressera guère. La seule partie utile est, dans section 2.2 du RFC, quelques scénarios intéressants.

J'ai bien aimé le scénario de la section 2.2.5, où un groupe de chercheurs (ah, justement, ce n'est plus du « "*enterprise network*" ») travaille dans la station polaire Zebra (oui, c'est une référence au film) et doit maintenir à jour ses ordinateurs, malgré une liaison Internet intermittente, chère (et la recherche publique n'a jamais d'argent) à faible capacité <https://www.bortzmeyer.org/capacite.html> et énorme latence <https://www.bortzmeyer.org/latence.html>. Non seulement les conditions sont très dures, mais ils doivent en outre se plier à la « conformité » ("*compliance*"), le "*buzz word*" à la mode. Une partie du temps de recherche sera donc consommé à suivre les "*process*".