



Veille Technologique

Les failles informatiques

Par POTTIER Nicolas

18/02/2023

Table des matières

Introduction	1
Qu'est ce que la veille technologique ?	1
Sujet Choisi : Les failles informatiques.....	1
Outils utilisés pour la veille	1
Les informations obtenues	2
Conclusion	3

Introduction

Qu'est ce que la veille technologique ?

La veille technologique consiste à rester informés des dernières actualités sur un sujet précis. Elle permet de prévenir et alerter d'un quelconque changement, d'une nouveauté ou d'une innovation. Cela va de l'acquisition des informations, à la transmission et au stockage interne jusqu'à la synthèse des informations collectées.

Afin que la veille technologique soit efficace, il faut que le service soit flexible et soit prêt à être modifié afin d'être à jour avec les derniers changements.

Elle permet aussi de surveiller ces concurrents sur leur dernières nouveautés, leurs avantages, leur brevets...

En soit, la veille technologique est un composant de la veille stratégique permettant de suivre les évolutions et les innovations de services ou technique, mais aussi d'établir une carte de marché et de surveiller ces concurrents et de rester au-dessus du marché.

Sujet Choisi : Les failles informatiques

Les failles informatiques sont très surveillées par tous les services informatiques étant donné que ce sont des entrées pour les personnes malveillantes afin de pouvoir modifier l'intégrité, la disponibilité et/ou la confidentialités des applications et/ou des données.

Cela peut être possible en injectant des commandes, en rendant indisponible la donnée, en publiant des fichiers confidentiels, en diffusant un ransomware sur tout le réseau local...

Le service Informatique doit-donc surveiller les failles informatiques de ses périphériques réseau ainsi que son contenu et pouvoir intervenir dès que la faille est connue afin de limiter au mieux les risques.

Outils utilisés pour la veille

Pour cette veille, j'ai utilisé feedly ainsi que Google alerts pour avoir des alertes sur les dernières failles informatique. Je n'ai pas choisi de logiciel précis, mais nous pouvons imaginer que pour une entreprise, en plus de créer une alerte sur les failles informatique en général, nous pouvons préciser le logiciel, par exemple : « faille informatique firefox ESR ».

J'ai aussi recherché sur internet divers failles informatique, notamment sur le site.

<https://www.cert.ssi.gouv.fr/alerte/> .

Les informations obtenues

J'ai pu obtenir plusieurs sujets concernant les failles informatique grâce à cette veille technologique :

Une faille permettant d'exécuter du code arbitraire à distance sur VMWare ESXI :

<https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/>

Plusieurs failles sur plusieurs systèmes d'exploitation Windows permettant d'exécuter du code arbitraire à distance :

<https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-007/>

Suite à la faille de VMWare ESXI (première alerte), énormément de serveurs en France et en Italie notamment ont reçu un ransomware et ont leur serveur bloqué :

<https://www.numerama.com/cyberguerre/1259082-internet-coupe-en-italie-la-france-en-alerte-tout-comprendre-a-la-vague-de-cyberattaque.html>

Près de 80 failles ont été repéré sur Windows 11, le patch de Février 2023 corrige ces erreurs :

<https://www.tomsguide.fr/windows-11-pres-de-80-enormes-failles-de-securite-reperes-installez-vite-la-mise-a-jour/>

Firefox corrige 10 failles de sécurité :

<https://www.cnetfrance.fr/news/mozilla-corrige-encore-10-failles-de-securite-dans-firefox-2-39378335.htm>

Conclusion

Grâce à cette veille technologique, j'ai pu constater l'utilité de mettre en place une veille technologique grâce à la faille de VMWare ESXI qui, a été utilisé par de nombreuses personnes malveillantes afin de déployer des ransomwares sur les serveurs d'entreprises. Cela aurait pu-être évité si une veille technologique aurait été mis en place, cela aurait pu permettre de corriger la faille le plus vite possible et éviter d'être infecté.