évolution de la protection des données contre les menaces

Compte Rendu

D’Annaëlle Champiau

— Avril 2025 —

Sommaire

Problématique :

Comment les entreprises peuvent-elles protéger leurs données et celle de leurs clients face aux menaces numérique en constante évolution ?

Contexte :

Toutes les entreprises utilisent des données comme les informations des clients (pour créer un compte client).
Le problème étant que les entreprises sont de plus en plus visées par des attaques comme :

- les ransomwares(un virus qui bloque l'accès à tes fichiers en demandant une somme d'argent).
- le phishing(c'est une attaque par mail ou sms en se fesant passer pour la banque).
- les fuites de données(lorsque les données sont rendus public).

Méthodologie :

Pour procéder à l'évolution de mon sujet de veille :

- J'ai utilisé deux outils de veille : Google Alert et Feedly.

Google Alerts

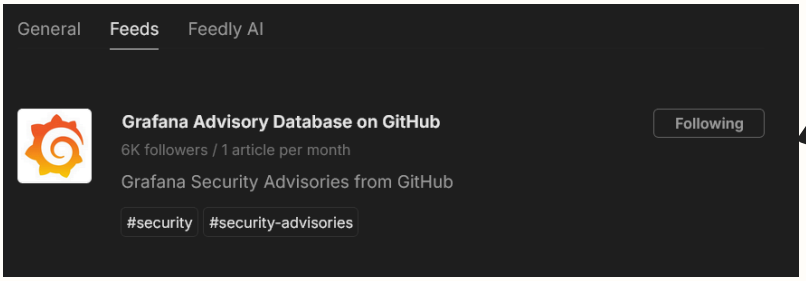
recevoir automatiquement des informations sur les mots-clés que j'ai choisis

feedly

regrouper plusieurs sites et blogs qui parlent du sujet que j'ai choisis

- Pour Feedly, j'ai crée un nouveau Feed, puis je me suis abonnées à différents Feeds qui correspondent à mon sujet de veille

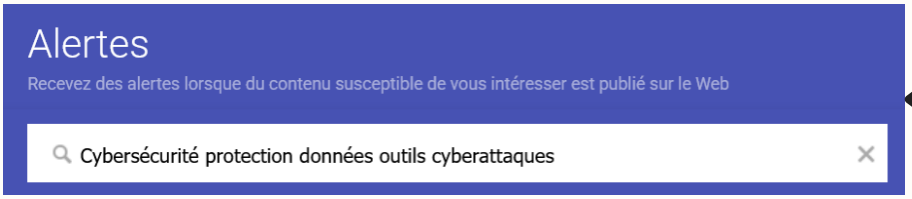
Feedly :



un exemple de feed

- J'ai saisie les mots clés suivant sur Gogle Alert : protection données, outils, cyberattaques

Google Alert :



Feeds aux quelle je me suis abonnée

- Ce que j'ai regardés lors de cette veilles : la sécurité numérique, attaques et les outils .

Résultat

Google Alert

Exemples de sources obtenu :

- Source : Comment l'IA devient une menace ?
  attaque : phishing date : 14/04.
- Source : La sécurité de notre PC ne dépend pas d'un antivirus.
  attaque : hameconnage (38%) date : 14/04.
- Source : Logiciel espions.
  attaque : rançonlogiciel, piratage date : 15/04.
- Source : Cyberattaque contre la CNSS.
  attaque : fuite de données date : 08/04.

Feedly

Exemples de sources obtenu avec les feeds aux quelles je me suis abonnée :

- Abonnée : CERT-FR. source : multiple vulnérabilité sur Moodle.
  attaque : fuite de données. date : 18/02.
- Abonnée : Zoom security bulletin source : Application sur Zoom Workplace Linux. attaque : faille de sécurité . date : 14/01.
- Abonnée : Red Hat CVE Database. source : Red Hat packages.
  attaque : FAULT+PROBE (récupérer la clé privé à partir des erreurs générées) date : 29/04.

Analyse

Google Alert

Durant l'analyse des résultats de la veille j'ai observé, les attaques les plus aperçu sont :

- phishing(c'est une attaque par mail ou sms en se fesant passer pour la banque).
- rançonlogiciel(c'est un virus qui bloque l'accès à tes fichiers en demandant une somme d'argent).
- hameçonnage(c'est une attaque qui consiste à manipuler la victime et lui demander ces informations personnelles).

Feedly

Durant l'analyse des résultats de la veille j'ai observé, les attaques les plus aperçu sont :

- la fuite de données(lorsque une personne malveillante possède des informations privés d'une entreprise ou d'un client).
- faille de sécurité(c'est une erreur dans une application ou un site web, qui va permettre à l'attaquant d'accéder à des données privés).
- FAULT+PROBE (Récupérer la clé privé à partir des erreurs générées)

Sources :

Google Alert

Les sources qui m'a été proposé lors cette veille :

- Orange Actu
- Global Security Mag
- Android MT
- Solution Numérique
- Siècle Digital
- Informatique News
- Boursorama
- et bien d'autres...

Feedly

Les feeds qui m'a été proposé pour cette veille :

- Adobe Security
- Apple Security Update
- Center for Internet Security
- CISCO Security Advisories
- Dell Security
- Github Advisory
- Google Security
- et bien d'autres...

Charte Graphique

TYPOGRAPHIES

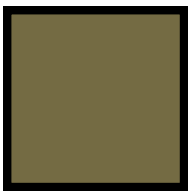
Nunito Sans

ABCDEFGHIJKLMNOPQRSTUVWXYZ

abcdefghijklmnopqrstuvwxyz

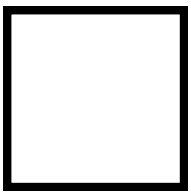
0123456789

PALETTE UTILISÉ



#746B43

#OOOOOO



#FFFFFF