Les démarches, techniques et outils visant à sécuriser les résultats produits.

Les entreprises sont responsable de la protection des données de la Big Data. Par conséquent, elles doivent respecter l'ensemble des normes[1] sous peine de sanctions et de mauvaise image.

Les démarches et les techniques

- Les entreprises doivent limiter le nombre de personnes pouvant accéder aux référentiels de données massives. En effet, le regroupement des données augmente le risque d'une fuite des informations sensibles et des cybercriminels puissent les interceptées.
- Le contrôle d'accès pour assurer que seuls les utilisateurs accède à certaines données.
- Surveiller étroitement l'activité des bases de données Hadoop (outils permettant aux applications de travailler avec des milliers de nœuds et des pétaoctets de données) et NoSQL (désigne une famille de systèmes de gestion de base de données).
- Implémenter des contrôles automatisés et centralisés.
- Mettre en place un contrôle des changements pour contrôler le volume, la vélocité (=vitesse) et la variété du Big Data.
- Fonctions de blocage, de mise en quarantaine et d'alerte en cas d'attaque ou de mouvement suspect sur le Big Data.
- Faire des analyses approfondies car les cybercriminels ou attaquants internes laissent généralement des traces de leur passage ou des artefacts qui peuvent être détectés.
- Employer des techniques d'abstraction des données, telles que le chiffrement, le masquage ou l'occultation. Une fois fait, les cybercriminels ne peuvent généralement pas décoder ni récupérer les données.
- Faire des audits[2] et des rapport sur la sécurité.

- Évaluer et résoudre les faiblesses de l'environnement de manière à sécuriser l'ensemble du Big Data.

Les outils

Des entreprises se sont spécialisé dans la sécurité du Big Data pour aider les sociétés à protéger leur données :

- Voltage SecureData Enterprise
    1. Protection des données sensibles
    2. Sécurité pour Hadoop
    3. Sécuriser les analyses
    4. Confidentialité des données
    5. Cryptage et anonymisation
    6. Assistance multi-plateforme
- IBM Security Guardium
    1. Découverte et classification des données
    2. Analyses des vulnérabilités et évaluations des risques
    3. Surveillance et alertes relatives aux activités des données
    4. Chiffrement, blocage, masquage et mise en quarantaine
    5. Rapport et audit de conformité
    6. Analyse avancée de la sécurité des données
    7. Visibilité, automatisation et évolutivité de la protection
    8. Réduire la complexité
    9. Améliorer les résultats

Conclusion

Pour conclure, face à cette enjeu, les entreprises ont trouvé des solutions afin de protéger le Big Data. Elles ne cherchent pas seulement à protéger les données, mais elles essayent d’améliorer l’utilisations de celles-ci.

Annexe

Vocabulaire

Norme[1] : Règle à suivre. Ici les normes sont par exemple RGPD, ISO/IEC JTC 1/WG 9, …

Audit[2] : Procédure de contrôle.

Sources

- Démarche et technique :

http://www.infomania-services.fr/controle/file/180509044559000000_9561476186_1525884359.pdf

- Voltage SecureData Enterprise :

https://www.microfocus.com/fr-fr/products/voltage-data-encryption-security/hadoop-big-data-security/overview

- IBM Security Guardium

https://www.ibm.com/fr-fr/security/data-security/guardium

- Pixabay - image libre de droit sécurité

https://pixabay.com/fr/photos/s%C3%A9curit%C3%A9-protection-anti-virus-265130/