La Newsletter CyberSecura

Janvier 2026

Au sommaire de cette newsletter :

Zoom sur :

- Le rôle du RSSI dans la sécurité informatique des organisations.

Les actualités de cybersécurité et conformité RGPD :

- Un homme en prison pour "usurpation" de sa propre identité !
- Les entreprises participent elles à financer la cybercrime ?

Le CRIS, s'engage pour le développement des modèles d'IA conformes au RGPD.

Nos contenus et actualités :

- Notre dernier témoignage client sur TECHNISTO, concernant un accompagnement vers la certification ISO 27001.
- Nos derniers contenus du blog et d'études de cas clients.
- Les actualités de l'équipe CyberSecura.

Ce mois-ci, zoom sur ...

Le rôle du RSSI dans la sécurité informatique

Le RSSI (pour Responsable de la Sécurité des Systèmes d'Information) joue un rôle central dans la gestion de la sécurité informatique des organisations. Ce dernier est en effet le chef d'orchestre de la sécurité IT de son organisation. Il définit la stratégie de sécurité, veille à la mise en place et assure de sécurisation du système d'information de son entreprise.

Ainsi, pourquoi le rôle du RSSI est-il si crucial aujourd'hui ? **Pourquoi un poste du RSSI ne peut-il plus rimer remplacé par un autre profil informatique, non spécialisé en cybersécurité ?**

Et Bien plus

Les actualités de cybersécurité & de conformité

Un homme en prison pour "usurpation" de sa propre identité !

Cette histoire incroyable est pourtant bien réelle ! Il s'agit de l'histoire de William Gruver-Reyes, qui, quelque soient les victimes d'une usurpation d'identité longue de 30 ans, vient finalement retrouver en prison pour avoir usurpé sa propre identité !

Pour lire/voir/ecouter l'intégralité de cette histoire dans cet article.

Cette histoire est très révélatrice de la facilité avec laquelle nos données personnelles sont compromises ! Le vol de données personnelles, et tout ainsi pour pouvoir usurper notre identité de genre de l'informatique, qui malheureusement, arrive régulièrement. Il est aussi parfois un critère de travail qui, non intentionnel, ne tient pas trop bien au cœur.

Et oui Nomme soit personnel, il aller aussi loin dans son usurpation d'identité, avec occasionnel un vol et une dette de notoriété. C'est difficile d'imaginer ce qu'il aurait pu faire d'autre avec pour d'informations encore !

Cette histoire illustre d'usurpation d'identité est très révélatrice des limites de notre protection des données personnelles. Cela nous interroge sur le fonctionnement et les pratiques professionnelles des propres données personnelles, mais également des données personnelles ou publiques nous acceptons mieux pour.

Plaisanterie mis-à-part, les dégâts sont bien plus archaïques, ils en lignes ? Il a bien commencé concernant le le volume des données personnelles accessibles mais accidents ou quelques ? Il semble nous comment suffisamment rigoureux quant aux mesures nécessaires, mais tout malheureusement, et surtout nous exposons trop informatique, personnel et professionnel ?

Les entreprises participent-elles à financer la cybercrime ?

Et oui elle payent le rançon aux cybercriminels c'est pas une fête bizarre (Mai 2.0 Vol 2021). Aux annuaires mondiales ? Il sont aussi "cyber sexpionnage", qui permettent aux cybercriminels, de financer leurs activités. Et oui, les entreprises payent aux cybercriminels, de financer la pression des données sensibles sur leurs dans cette pratique.

Cette décision découlant de l'intervention du directeur de l'ANSSI lors d'une audition au Sénat, intervention lors de laquelle il avait pointé du "doigt" des assureurs, qui, selon lui, "alimentent le système" en payant les rançons. Il a ainsi demandé aux cybercriminels, plutôt assurés d'obtenir et opérateur des rançons demandées. (Rapport/vous pour des détails ici)

Image par Gerd Altmann de Pixabay

Désormais, c'est un fait ! Les Etats-Unis publient par Cybersécurité Ventures que 74 % des entreprises ayant payé une rançon subissent des attaques répétitives, et toujours plus ciblées.

Il devient alors évident que pour ne pas payer la rançon et éviter d'alimenter cette pratique, il ne sont d'une cybercriminalité, il ne faut pas payer les rançons. Les payent des cibles de crime pour les attaquants, plutôt opérateur d'obtenir le paiement des rançons demandées.

Ces paiements de rançons peuvent être expliqués par un dilemme principal : les entreprises ciblées ne veulent pas payer, mais elles ne veulent pas subir les conséquences considérable. Malheureux d'informatique, cyber attaquées, plutôt finalement le rançon demandée, car seulement payer ne résoudre pas les vulnérabilité des données ciblées, ou pas suffisamment rapidement.

Lorsque tel est que le Francs-et-le Le coût d'attaque le plus coûteux est les frais de rançon, et que des attaques de ransomware sur des entreprises frappées par augmentation de 42 % en 2020, en comparant alors que le lancer de cyber-défense ? Lequel d'entre organisation à attribuer, à assurer et à se rendre de rançon ransomware ? (Bilé est désormais plus fort que prison !

Consulter le Clichés de Cybersécurité, Téléchargement, (Par Axel Jodet, du Supérieur ISEAC)

Photo de Gerd Altmann sur Unsplash

Dans ce contexte, et afin d'accompagnant au mieux les entreprises travaillant sur le développement de modèles d'IA, le CRIS, à publié 7 fiches pratiques, destinées à faciliter le cadre pratique et à "rationnel-les-actions" de terrains.

Ces fiches détaillent 7 grandes étapes permettant de garantir le respect du RGPD d'un modèle d'IA :

1. Déterminer le régime juridique applicable.
2. Définir une finalité de traitement des données utilisées conforme aux nécessaires modèles d'IA.
3. Vérifier le fondement juridique des fonctionnement des systèmes d'IA.
4. Définir une base légale pour le traitement des données, afin de s'assurer de le traitement des données est licite, et qu'il ne laisse et ceux de la réalisation des données utilisées.
5. Réaliser une analyse d'impact (DPIA) pour évaluer les risques potentiels des traitements de données, et mettre en place des mesures adéquates.
6. Tenir compte de la protection des données dès la conception des systèmes d'IA.
7. Tenir compte de la protection des données également dans la collecte et le gestion des données.

Certaines de ces recommandations sont formulées à titre de bonnes pratiques, et ne constituent pas des obligations au sens du RGPD. Elles ne sont, en ce sens, ni prescriptives ni contraignantes. Elles ne constituent pas d'obligations. Elles ne sont pas des responsabilités pouvant décider de cet écarter, à condition d'être en mesure de justifier leur choix, et sous leur propre responsabilité.

Retrouvez ces 7 fiches pratiques proposées par le CRIS, en cliquant ici.

Lorsque de nos collègues ont vole, elle protégée pour les hackers ! Il arrive parfois que des collègues ou des proches d'une entreprise, il ait cible de quelque chose qui ne leur est pas destiné, et qui ne leur est pas, en aucune, "à" ce qui ne leur appartient. Il arrive parfois, de profiter de cela et plus encore, de vouloir en tirer profit. Phishing, les permettent de plaqué les victimes, pièce à des techniques d'ingénierie sociale, particulièrement humaines. 9-07-2019 09:0

Humanos. 9-07-2019 09:0

Google, Chrome, Iexus, Google Enterprise Premium : une version payante de Google Workspace ! A partir de 6 euros par mois et par utilisateur, Google lance une version payante de son navigateur Chrome, qui ajoute de nouvelles fonctionnalités, les comparant de Google Workspace. Ces dernières, ciblant les entreprises, ciblent les entreprises ? Ou en revanche les comparant à des solutions de sécurité ? Et bien, les organisations, disposeront alors d'un outil protection d'accompagnement à la sécurité. Et ce, tout en ne pas trop trouver le cœur dans les Chromebook.

1 J'Conseil. 31 J'ai-mi-2020

Nos contenus

Apprendre & comprendre

Le RGPD de Ingénieur : quelle procédure suivre pour déclarer une violation de données ? Qu'est-ce qu'une violation de données ? Comment la déclarer ? Quelles sont les conséquences ? Et, surtout, quelles sont les mesures à prendre ? Quelles sont les techniques ? Lisez d'ouvrir nécessaire de mettre en place ? Et, surtout, quelles sont les mesures ? Et, surtout, quelles sont les mesures ? Et, surtout, quelles sont les mesures