CYBERSECURA
Cybersécurité & Conformité

La Newsletter CyberSecura

Avril 2024

Profils dirigeants & partenaires | Profils techniques

PRESTATAIRE RÉFÉRENCÉ | OFFENSIVE OSCP | PECB ISO/IEC 27001 LEAD IMPLEMENTER

Au sommaire de cette newsletter :

1️⃣ L'alerte du mois

✔️ **Cisco comble une vulnérabilité critique** dans son logiciel de gestion de serveurs IMC.

2️⃣ Les actualités en cybersécurité et conformité RGPD

✔️ Comment pouvez-vous empêcher les nouveaux modèles d'IA de **se former avec vos données** ?

✔️ La CNIL s'engage pour le développement de modèles d'IA conformes au RGPD.

✔️ Une **PSSI sans implication de la direction** n'a aucune utilité.

3️⃣ Nos contenus et actualités

✔️ Notre dernier **témoignage client** par TECHNIDATA, concernant un accompagnement vers la **certification ISO 27001.**

✔️ **Nos derniers contenus** de blog et d'études de cas clients.

✔️ Les **actualités de l'équipe** CyberSecura.

Alerte du mois

Cisco comble une vulnérabilité dans son logiciel de gestion de serveurs IMC

Photo de NASA sur Unsplash

Une faille de sécurité menace les appareils Cisco sur lesquels fonctionne le logiciel «Integrated Management Controller» (IMC). La faille dans le logiciel de gestion des systèmes de serveurs Cisco permet aux pirates d'obtenir des droits d'administrateur (accès root) sur un système et de procéder ainsi à des modifications à volonté. Un accès en lecture au système IMC attaqué suffit pour déclencher l'attaque.

Cisco a corrigé la faille avec une mise à jour de sécurité.

L'entreprise fait remarquer qu'elle n'a pas encore observé d'attaques effectives exploitant cette faille. Toutefois, l'Exploit Code - c'est-à-dire un exemple de code montrant comment la faille de sécurité pourrait être exploitée - a été publié sur le web. **Ce ne devrait donc être qu'une question de temps avant que des cybercriminels ne commencent à lancer des attaques**.

Si vous utilisez des appareils fonctionnant sur le logiciel "Integrated Management Controller", vous êtes invités à appliquer les correctifs le plus tôt possible !

En lire plus

Les actualités de cybersécurité & de conformité

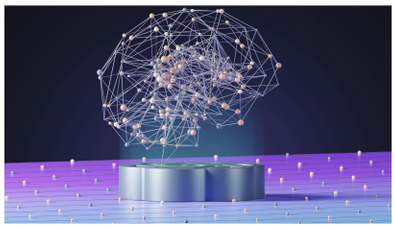
Comment pouvez-vous empêcher les nouveaux modèles d'IA de se former avec vos données ?

L'émergence, mais par dessus tout, l'utilisation croissante de l'utilisation de l'IA dans un contexte professionnel a contribué à complexifier la tâche des responsables de la sécurité des organisations.

On le sait : les nouveaux modèles d'IA ont besoin de traiter un grand nombre de données afin d'entraîner et de former leurs algorithmes, cela fait partie intégrante de leur développement.

ChatGPT, de Open IA, est certainement le logiciel d'IA qui a le plus fait parler ces derniers temps. Sorti en novembre 2022, ChatGPT est désormais utilisé par de très nombreux professionnels, dans le cadre de la réalisation de leurs missions au quotidien. Les équipes commerciales utilisent le logiciel pour rédiger rapidement et sans effort des emails de prospection ou de relance client. Les équipes de développement s'appuient sur les propositions de cet outil pour faciliter la création de leurs logiciels. Les équipes marketing s'en servent pour produire des contenus rapidement, facilement et à moindre coût.

Seulement, savez-vous vraiment lesquelles de vos données sont utilisées pour entraîner ces nouveaux logiciels d'IA, et savez-vous comment elles sont utilisées ? Comment le responsable de sécurité peut-il s'assurer que les salariés d'une entreprise ne partagent rien de confidentiel avec ces nouveaux outils d'intelligence artificielle ?



Les entreprises qui travaillent au développement de ce genre de logiciels gardent généralement le secret quant aux données qu'elles ont vraiment récupéré, acheté ou utilisé pour former leurs systèmes.

Ces dernières ajouteraient également des "frictions", car bien conscientes que les gens "ne chercheront pas".

La plupart de ces entreprises utilisent les données de leurs utilisateurs pour former leurs logiciels d'IA de manière quasi-automatique : la personne concernée n'a pas vraiment d'autre choix. C'est le cas par exemple des réseaux sociaux, qui utilisent les données de leurs utilisateurs pour entraîner leurs algorithmes, sans laisser la possibilité aux personnes concernées de s'opposer à l'utilisation de leurs données et contenus. L'utilisateur n'a pas d'autre choix que d'accepter ce traitement de données s'il souhaite accéder à la plateforme.

D'autres entreprises, même si cela est plus rare, laissent la possibilité à leurs utilisateurs d'accepter ou de refuser que leurs données et contenus soient automatiquement utilisés dans le cadre de la formation des logiciels d'IA.

Et pour finir, il existe une troisième catégorie d'entreprises qui elles, utilisent automatiquement les données de leurs utilisateurs pour entraîner leurs logiciels d'IA, mais qui permettent cependant aux personnes concernées de s'opposer à ces traitements de données, tout en continuant d'accéder à leurs outils.

Découvrez quelles sont ces entreprises qui vous permettent de refuser que vos données soient utilisées pour former l'IA, ainsi que la marche à suivre pour vous opposer à ce traitement de données.

La CNIL s'engage pour le développement de modèles d'IA conformes au RGPD !

L'intelligence artificielle ainsi que les enjeux de cybersécurité et de protection des données liés à l'utilisation de l'IA au quotidien sont des sujets dont on entend de plus en plus parler.

On le sait, les modèles d'IA ont besoin de données (parfois personnelles) pour entraîner leurs algorithmes. Seulement, les entreprises développant ces mêmes modèles d'IA sont bien souvent incapables de garantir la sécurité des données personnelles utilisées dans ce cadre-là.

L'enjeu est double : permettre aux entreprises développant des modèles d'IA de poursuivre leurs activités, et de développer leurs solutions, tout en garantissant le respect de la vie privée des personnes concernées, et la sécurité des données personnelles traitées par ces logiciels.

Dans ce cadre-là, et afin d'accompagner au mieux les entreprises travaillant sur le développement de modèles d'IA, la CNIL a publié 7 fiches pratiques, destinées à "clarifier le cadre juridique" et à "sécuriser les acteurs" du secteur.

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 pour entraîner ces nouveaux modèles d'IA.
3. Déterminer une qualification juridique des fournisseurs des systèmes d'IA.
4. Définir une base légale pour le traitement des données, afin de s'assurer que le traitement des données est licite, et qu'il le reste en cas de réutilisation des données utilisées.
5. Réaliser une analyse d'impact (AIPD) pour évaluer les impacts potentiels d'une violation de données sur la vie privée des personnes concernées.
6. Tenir compte de la protection des données dans la conception des systèmes d'IA.
7. Tenir compte de la protection des données également dans la collecte et la gestion des données.

Certaines de ces recommandations sont formulées à titre de bonnes pratiques, et permettent d'aller plus loin que le respect de la réglementation RGDP. Ainsi, la CNIL précise que ces recommandations n'ont rien de contraignant ou d'obligatoire : les responsables de traitements peuvent décider de s'en écarter, à condition d'être en mesure de justifier leur choix, et sous leur propre responsabilité.

Retrouvez ces 7 fiches pratiques proposées par la CNIL en cliquant ici.

Une PSSI (i.e.Politique de Sécurité des Systèmes d'Information) sans implication de la Direction n'a aucune utilité

Une PSSI, pour Politique de Sécurité des Systèmes d'Information, est un document qui reflète les politiques internes d'une organisation en termes de sécurité des systèmes d'information et de gestion des risques.

Malheureusement, malgré son caractère à la fois stratégique et incontournable, ce document de sécurité est encore bien trop souvent perçu comme une obligation contraignante.

Résultat : de nombreuses organisations ont bien compris l'intérêt de faire rédiger une PSSI, mais nombre d'entre elles ne comprennent pas encore l'importance de l'état d'esprit positif des acteurs de l'organisation, et tout particulièrement des dirigeants, dans le cadre de la mise en oeuvre d'une PSSI.

Les équipes dirigeantes doivent ainsi être impliquées dans la création d'une PSSI ainsi que dans sa mise en oeuvre quotidienne.

La norme ISO 27001:2013 mentionne que « La direction doit établir une politique de sécurité de l'information », tandis que l'ISO 27002:2013 précise que la PSSI doit être définie et approuvée par le plus haut niveau de direction de l'organisme. **La validation de la PSSI par la direction traduit donc la reconnaissance officielle accordée à la sécurité de son système d'information.**

La PSSI est donc un acte de direction : ce document doit être approuvé par le Directeur d'une manière officielle, et ce dernier doit s'engager à veiller à son respect. Pour être une ressource utile, il est nécessaire de "faire vivre" cette PSSI.

Alors concrètement, quelles sont les clés de la réussite dans l'implémentation d'une PSSI ?

- **Une PSSI doit être réaliste et pragmatique**. Il est nécessaire de trouver le "bon équilibre" entre les moyens mis en oeuvre et les gains de sécurité attendus. Pour renforcer les chances de voir la PSSI s'ancrer concrètement dans les pratiques quotidiennes d'une organisation, il est tout à fait proscrit de proposer des consignes de sécurité démesurées.

- **La conception d'une PSSI doit être partagée**, et non pas accaparée par la DSI (i.e. Direction des Systèmes d'Information), et tout le monde doit "s'y plier". De nombreuses PSSI ont été "disqualifiées" du fait du manque d'exemplarité des dirigeants ou de l'encadrement. "*Quand une équipe médicale se prépare à entrer en bloc opératoire, tous ses membres se lavent soigneusement les mains, y compris le chirurgien en chef*".

- **La PSSI doit être un document pédagogique**, qui vise à l'évolution des mentalités et à l'implantation de nouveaux réflexes, plutôt qu'à la contrainte. Ainsi, une PSSI doit être un document plutôt court, d'une quinzaine de pages maximum, et chaque mot doit être soigneusement pesé, notamment pour distinguer "ce qu'il faut obtenir" du "comment l'obtenir".

- Enfin, **une PSSI doit être contrôlable et auditable**. Sa mise en oeuvre doit être maîtrisable, et des indicateurs doivent permettre de juger de son respect et de sa pertinence.

Source de ces informations : "PSSI : contrainte ou opportunité ?", par Bruno Rasle, Expert RGPD et Formateur de DPO, le 15 mai 2021.

À quel point votre Active Directory est-il sécurisé ?

L'Active Directory (AD) de Microsoft sert de système nerveux central pour le réseau de votre organisation : il protège les ressources de l'entreprise tout en garantissant que seuls les utilisateurs autorisés ont accès à des sections données du réseau et de la base de données. Découvrez-en plus sur ces 5 vulnérabilités courantes dans l'Active Directory.

Cybersecurity News - le 17 avril 2024

5 outils sandbox pour l'analyse du phishing en 2024

Il existe une grande variété de solutions permettant d'enquêter sur les attaques de phishing. Pourtant, dans la plupart des cas, les analystes peuvent se contenter d'un seul outil : un bac à sable d'analyse des logiciels malveillants. Grâce à sa combinaison de fonctionnalités statiques et dynamiques, un bac à sable est bien équipé pour lutter contre les menaces de phishing les plus complexes.

Cybersecurity News - le 17 avril 2024

Nos contenus

Apprendre & comprendre

LE BLOG

Éditeurs de logiciels : quelle procédure suivre pour déclarer une vulnérabilité (CVE) ?

En-dehors du développement sécurisé des solutions logicielles, de la surveillance des vulnérabilités et de leur résolution technique, il peut s'avérer nécessaire de déclarer publiquement une vulnérabilité. Déclarer une CVE permet notamment de prévenir l'exploitation de la vulnérabilité, en proposant et diffusant des correctifs adéquats ou des alternatives de sécurité pertinentes.

Le 17 avril 2024 - 6 minutes de lecture

En lire plus

LES CONTENUS VIDÉO

Chit-Chat with CyberSecura - "La France est-elle en retard dans le domaine de la cybersécurité ?" Découvrez l'avis de notre experte.

Accédez à nos contenus pour en apprendre toujours plus !

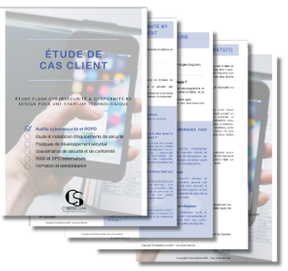
Les contenus de blog

La chaine YouTube

Nos témoignages clients

En lire plus

Les études de cas clients à découvrir



Étude flash de cybersécurité pour CountAct

Vous n'avez pas encore de produit, vous êtes encore en phase de réflexion, de développement, mais souhaiteriez vous assurer que vous partez bien dans la bonne direction, et que vos enjeux de cybersécurité et/ou de conformité réglementaire au RGPD sont bien pris en compte ? Découvrez-en plus sur notre prestation d'étude flash à travers l'étude du cas client de CountAct.

Accompagnement à la certification SOC 2 Type II pour Checkstep

Les certifications de sécurité deviennent désormais incontournables pour de nombreuses entreprises, dont les clients, partenaires et potentiels investisseurs demandent des preuves de sécurité et de gouvernance de la sécurité dans les organisations. Découvrez-en plus sur notre prestation d'accompagnement à la certification SOC 2 Type II à travers l'étude du cas client de Checkstep.

L'actualité de CyberSecura

CyberSecura accueille Magali Perez pour un stage DPO

Étudiante en deuxième année de Master Droit International - Carrières juridiques et numériques, Magali a récemment rejoint les équipes de CyberSecura pour un stage RGPD et DPO. Dans un contexte de fort besoin en conformité réglementaire, nos experts RGPD sont ravis de pouvoir partager leur expertise et leurs connaissances avec les futurs professionnels de la protection des données.

CyberSecura devient partenaire de Pépite oZer !

Pépite oZer a pour mission la sensibilisation et l'accompagnement des étudiants et jeunes diplômés dans le développement de leurs projets entrepreneuriaux. Dans le cadre de ce

partenariat, CyberSecura aura le plaisir d'accompagner les étudiants entrepreneurs de Pépite oZer dans la prise en compte des enjeux de cybersécurité et de conformité réglementaire au RGPD dans la création de leur activité.

Consulter l'article de presse

Ne manquez aucune de nos offres !

Abonnez-vous à nos offres promotionnelles en cybersécurité et en conformité réglementaire au RGPD !

Si vous vous abonnez à ces communications, vous recevrez chaque mois un nouvel email promotionnel. Vous aurez la possibilité de vous désabonner de ces envois à tout moment via un lien de désabonnement disponible en fin de chaque email.

Je m'abonne

Choisissez quel contenu de newsletter vous souhaitez recevoir !

Vous avez la possibilité de choisir à quelle(s) liste(s) de diffusion vous souhaitez être abonnée en cliquant sur le boutons ci-dessous.

Choisir ma liste de diffusion

Cet email vous a été envoyé par CyberSecura car vous êtes inscrit à notre newsletter ou bien faites partie de notre écosystème en échangeant avec nos collaborateurs. Vous avez la possibilité de vous désabonner à tout moment via le lien en vas de page ou via le bouton "Choisir ma liste de diffusion" ci-dessus.

Retrouvez-nous sur les réseaux sociaux !

Contactez-nous

CyberSecura, 3 Avenue du 8 Mai 1945, Échirolles, FRANCE

Consulter cet email dans un navigateur

Copyright © 2024 CyberSecura, All rights reserved.

Nous contacter :
contact@cybersecura.com

Cliquez ici pour vous désabonner de tous nos envois.

This email was sent to <<Email Address>>
why did I get this? unsubscribe from this list update subscription preferences
CyberSecura · 3 Avenue Du 8 Mai 1945 · Echirolles 38130 · France

INTUIT mailchimp