THE BRIGHTLETTER

BREAKING NEWS

BRIGHTWAY
Bring your business to the right way

LA BRIGHTLETTER

VOTRE DOSE MENSUELLE D'INFORMATIONS CYBER

La BrightLetter #2- Mai 2024

Une production signée Brightway

Bienvenue dans la deuxième édition de la BrightLetter, une newsletter mensuelle que, nous l'espérons, vous donnera les informations cyber à retenir.

Nous vous proposons d'explorer les actualités du cyberespace à travers des rubriques soigneusement choisies telles que :

- L'alerte Cyber : un résumé des dernières menaces et vulnérabilités ainsi que les recommandations essentielles pour s'en prémunir.
- Les actualités : les dernières tendances et actualités du monde de la sécurité informatique
- Le point tech' : explorez les tenants et aboutissants des concepts émergents et/ou des défis actuels.
- Conseils et astuces : des conseils pratiques sur l'hygiène numérique pour garantir une bonne posture de sécurité et éviter les risques.

BRIGHTWAY SAS.
16 Rue Troyon
92310 Sèvres

+33 1 45 34 35 38
contact@brightway.fr
www.brightway.fr

Au cœur de cette newsletter réside un objectif essentiel : élever le niveau de connaissance global en partageant l'information et renforcer votre résistance aux cyberattaques. Que vous soyez novice ou expert, nos articles sont conçus pour tous les niveaux de connaissance en cybersécurité.

Nous sommes déterminés à promouvoir une sensibilisation à la sécurité et une gestion des risques cyber axées sur l'humain. Ensemble, nous construisons une communauté numérique plus sûre et plus consciente.

-- L'équipe BrightwayCERT

SOMMAIRE

Dans cette édition, vous découvrirez :

- L'alerte cyber du mois
- Cyberattaques sur les infrastructures d'intelligence artificielle
- Le Point tech' : Les modèles Zéro Trust
- Participation de Brightway au Cyber Africa Forum 2024, 15 &16 Avril 2024

L'alerte Cyber du mois

Le Top des vulnérabilités

Une faille de sécurité critique a été identifiée dans CyberPower PowerPanel Enterprise

Cette faille a été découverte le 17 avril 2024 par Tenable Network Security, Inc, répertoriée sous le code **CVE-2024-32735,** est due à l'absence d'authentification pour certaines fonctionnalités, permettant à un attaquant d'accéder aux API REST PDNU. Un attaquant non authentifié pourrait ainsi compromettre l'application.

- **Impact :** Critique
- **Versions affectées :** Toutes les versions avant v2.8.3
- **Recommandations :** Il est recommandé de mettre à jour vers la version v2.8.3 ou ultérieure et de vérifier l'intégrité des systèmes qui auraient pu être exposés à cette vulnérabilité.

Découverte d'une vulnérabilité critique dans le module Visuels de Google Chrome

Affectant les versions avant 124.0.6367.201/.202 pour Mac et Windows, et 124.0.6367.201 pour Linux. Cette faille, identifiée sous le numéro **CVE-2024-4671**, a été signalée de manière anonyme le 7 mai 2024. Elle permet à un attaquant d'exécuter du code arbitraire sur le système de l'utilisateur à travers un exploit déjà présent dans la nature.

- **Impact :** Critique
- **Versions affectées :** Google Chrome versions antérieures à 124.0.6367.201/.202 pour Mac et Windows, et 124.0.6367.201 pour Linux.
- **Recommandations :** Il est urgent de mettre à jour Google Chrome vers la dernière version stable pour éviter toute exploitation de cette vulnérabilité. Les utilisateurs doivent également surveiller et appliquer les mises à jour de sécurité dès qu'elles sont disponibles pour se protéger contre les éventuelles exploitations futures.

Le Top des menaces

La justice américaine a divulgué l'identité de l'administrateur du groupe cybercriminel LockBit

Le mardi 7 mai 2024, les autorités des États-Unis, du Royaume-Uni et de l'Australie ont identifié Dmitry Khoroshev, un citoyen russe de 31 ans, comme étant le présumé administrateur de LockBit, un groupe de cybercriminels impliqué dans des attaques de rançongiciels. Selon l'inculpation américaine, Khoroshev, alias "LockBitSupp", dirige le groupe depuis 2019 et aurait accumulé environ 100 millions de dollars en rançons.
Les États-Unis ont mis en jeu une récompense substantielle de 10 millions de dollars pour toute information qui pourrait conduire à l'identification ou à la localisation de l'admin du groupe de ransomware Lockbit **[1]**.

Violation de données chez Dell : Des informations client limitées exposées, nombre d'impactés inconnu

Dell Technologies enquête sur une violation de données impliquant un portail de l'entreprise contenant des informations limitées sur les clients liées à des achats.
Bien qu'aucune donnée financière ou hautement sensible n'ait été accédée, Dell affirme que les noms, adresses physiques et détails de commande ont été exposés lors de cette violation.
Dell a déclaré que son enquête montre qu'une partie non autorisée a accédé à une base de données contenant des noms de clients, des adresses, des informations sur le matériel et les commandes, y compris les étiquettes de service, les descriptions d'articles, les dates de commande et les détails de garantie. Cependant, Dell a souligné que les informations de paiement, les adresses e-mail, les numéros de téléphone et d'autres données très sensibles ne faisaient pas partie de la base de données compromise.
Après avoir découvert l'incident, Dell a rapidement mis en œuvre des procédures de réponse à la sécurité, ouvert une enquête, pris des mesures pour contenir la violation et informé les autorités compétentes. L'entreprise a également engagé une société médico-légale tierce pour approfondir l'enquête **[2]**.

Les cyberattaques sur les infrastructures d'intelligence artificielle

L'intelligence artificielle (IA) joue un rôle central dans l'innovation et l'efficacité opérationnelle des infrastructures numériques modernes. Cependant, cette importance stratégique fait également de l'IA une cible privilégiée pour les cyberattaques. Les infrastructures IA sont particulièrement vulnérables en raison de la valeur de leurs données et de la complexité de leurs réseaux [3].

Les systèmes d'IA attirent les cybercriminels pour plusieurs raisons :

1. **Données de grande valeur :** Les systèmes d'IA gèrent de vastes quantités de données sensibles et de grande valeur, telles que des informations personnelles, des secrets commerciaux et de la propriété intellectuelle. Ces données sont extrêmement précieuses pour les cybercriminels.
2. **Importance opérationnelle :** L'IA est devenue un élément essentiel des processus opérationnels et décisionnels des entreprises. Une perturbation ou un compromis des systèmes d'IA peut donc avoir un impact économique et opérationnel majeur.
3. **Interconnectivité :** Les infrastructures d'IA s'appuient sur des réseaux complexes interconnectés, ce qui élargit la surface d'attaque potentielle. Une vulnérabilité dans une partie du système peut se propager rapidement à l'ensemble de l'infrastructure.
4. **Manque de maturité de la sécurité :** Étant une technologie relativement nouvelle, la sécurité des systèmes d'IA n'a pas encore atteint le même niveau de maturité que pour d'autres technologies plus établies. Cela en fait une cible de choix pour les cybercriminels.

Vecteurs d'attaque courants sur les infrastructures d'IA

Les cyberattaques contre les infrastructures d'IA varient largement, incluant :

- **Empoisonnement de données :** Les cybercriminels injectent des données malveillantes dans les ensembles de données d'entraînement des systèmes d'IA, dans le but de corrompre leurs processus d'apprentissage et de fausser leurs résultats.
- **Vol de modèle :** Des modèles d'IA propriétaires et hautement précieux sont dérobés, entraînant des pertes importantes en termes de propriété intellectuelle et d'avantage concurrentiel..
- **Attaques adverses :** Des altérations subtiles des entrées trompent les systèmes d'IA, sapant leur fiabilité.
- **Exploitations de la chaîne d'approvisionnement :** Récemment, des vulnérabilités ont été découvertes dans des outils et des serveurs utilisés pour le développement et le déploiement d'IA, comme MLFlow et Triton Inference. Ces failles ont permis des écritures arbitraires de fichiers, des injections de templates sur les serveurs et des exécutions de code à distance [4],[5].

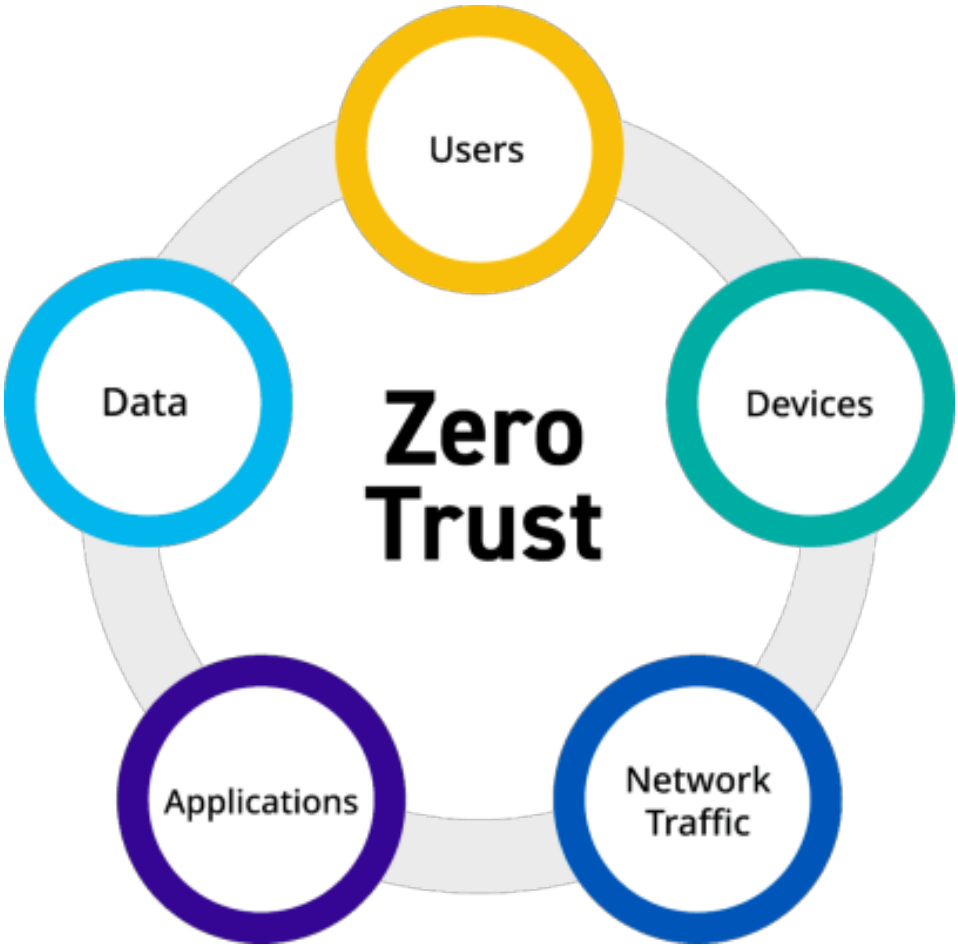
Mesures de défense stratégiques

Ces différentes formes d'attaques démontrent la nécessité de mettre en place des mesures de sécurité robustes tout au long du cycle de vie des systèmes d'IA, depuis la collecte des données jusqu'au déploiement en production, en passant par le développement des modèles.
Les défenses efficaces incluent :

- Sécurité multicouche
- Audits réguliers et tests de pénétration
- Formation et sensibilisation des employés
- Conformité légale et réglementaire
- Planification de la réponse aux incidents Un plan robuste de gestion des incidents est essentiel pour une récupération rapide et minimiser les dommages.

Le point tech' : Les modèles Zéro Trust

Le cadre Zero Trust ne fait confiance à personne et vérifie toutes les identités, même celle des utilisateurs internes de l'organisation.



BRIGHTWAY SAS.
16 Rue Troyon
92310 Sèvres

+33 1 45 34 35 38
contact@brightway.fr
www.brightway.fr

Qu’est-ce que le modèle Zero Trust ?

Le modèle Zero Trust part du principe que le réseau est potentiellement compromis et que le périmètre de sécurité est défaillant. Ainsi, chaque utilisateur et appareil, qu'il soit interne ou externe au réseau, doit prouver son identité et sa légitimité avant d'accéder aux ressources. Cette approche repose sur une vérification stricte des identités et restreint les accès latéraux en cas d'intrusion, renforçant la sécurité globale.

Fonctionnement de la sécurité Zero Trust

L'approche de sécurité Zero Trust est une méthode exhaustive qui mobilise diverses technologies et processus pour garantir la protection des organisations face aux menaces sophistiquées et aux violations de données.

Voici les éléments clés du cadre Zero Trust :

1. **Données** : Limitation de l'accès aux informations sensibles.
2. **Utilisateurs** :Limitation, surveillance et contrôle d'accès des utilisateurs aux ressources, en adoptant une approche de confiance vigilante pour protéger contre les erreurs humaines et les actions malveillantes.
3. **Appareils** : Capacité pour les équipes de sécurité d'isoler, sécuriser, et gérer chaque appareil connecté au réseau.
4. **Réseau** : Utilisation des techniques de segmentation, d'isolation et de restriction, renforcées par des technologies telles que les pare-feu de nouvelle génération.
5. **Application** : Identification et correction des vulnérabilités des outils et des applications permettant les interactions des clients avec l'entreprise.

Les trois principes du modèle de sécurité Zero Trust

Le respect des trois principes fondamentaux du modèle de sécurité Zero Trust constitue la base de la création de votre propre environnement de cybersécurité Zero Trust.

- **Exigez** un accès sécurisé et authentifié à toutes les ressources
- **Adoptez** le principe du moindre privilège pour contrôler les accès
- **Inspectez** et enregistrez chaque événement sur le réseau et chaque fichier

Participation au Cyber Africa Forum (CAF) 2024, 15 & 16 avril 2024

Brightway a récemment eu le privilège de prendre part à la quatrième édition du salon **Cyber Africa Forum**, qui s'est déroulée les 15 et 16 avril 2024 à Abidjan. Sous le thème captivant **"Risques cybernétiques et intelligence artificielle : quelles stratégies de défense face aux nouvelles menaces numériques ?"**, cette rencontre a réuni les esprits les plus brillants du continent pour discuter des défis et des opportunités dans le domaine de la cybersécurité.

Notre participation à cet événement d'envergure a été une opportunité unique d'échanger avec des experts du secteur, de partager nos connaissances et d'explorer de nouvelles perspectives. Nous avons pu constater une prise de conscience croissante des risques cybernétiques et de l'importance cruciale de l'intelligence artificielle dans la lutte contre ces menaces.

Une tendance remarquable qui émerge est la nécessité d'une approche collaborative entre les acteurs publics et privés pour renforcer la résilience cybernétique sur le continent. Les gouvernements, les entreprises et les organisations de la société civile reconnaissent l'importance de partager des informations, des ressources et des bonnes pratiques pour mieux se protéger contre les attaques numériques, surtout avec l’émergence des technologies connectées qui crée de nouveaux défis en matière de sécurité.

Notre CEO, Sami Chamam, a saisi cet évènement pour sceller de nouveaux partenariats visant à renforcer notre présence sur le continent.

Cette nouvelle présence, pour la 3ème année consécutive, au Cyber Africa Forum nous a permis de constater une prise de conscience croissante des défis cybernétiques et de renforcer notre engagement à contribuer à la sécurisation des données et systèmes d’information sur le continent.

BRIGHTWAY SAS.
16 Rue Troyon
92310 Sèvres

+33 1 45 34 35 38
contact@brightway.fr
www.brightway.fr