THE BRIGHTLETTER

BREAKING NEWS

BRIGHTWAY
Bring your business to the right way

LA BRIGHTLETTER

VOTRE DOSE MENSUELLE D'INFORMATIONS CYBER

La BrightLetter #1 - Avril 2024

Une production signée Brightway

Bienvenue dans la première 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

A propos de Brightway

Brightway est un cabinet parisien d'audit, conseil et formation spécialisé en Cyber Sécurité et Gouvernance des données. Ce cabinet se veut un allié stratégique pour accompagner ses clients dans la réalisation de leurs projets et la sécurisation de leurs systèmes d'information dans un monde où les menaces informatiques prolifèrent.

Nos Services

- **Audit et évaluation :** Pour dresser un état des lieux clair d'un SI et ses vulnérabilités, un statut sur sa conformité et les risques encourus. **Brightway dispose du visa sécurité « PASSI » de l'ANSSI.**
- **Conseil et résilience :** Pour accompagner la sécurisation du SI et des données (GRC, pilotage de projets/programmes, architecture, résilience et gestion de crise). **Brightway est candidat pour l'obtention du visa sécurité « PACS » de l'ANSSI.**
- **Supervision et réaction :** Brightway met à disposition son Centre de Réponse aux urgences cybernétiques labellisé CERT® "BrightwayCERT" qui propose 3 services principaux: BrightSOC, BrightCTI et Brightwatch
- **Formation et sensibilisation :** La "Brightway Academy" est certifiée **« QUALIOPI »** pour ses actions de formation.

SOMMAIRE

Dans cette édition, vous découvrirez :

L'alerte Cyber du mois

Le Top des vulnérabilités

Découverte d'un code malveillant dans la bibliothèque XZ Utils pour les systèmes Linux

Un code malveillant inséré dans la bibliothèque open-source XZ Utils, un package largement utilisé dans les principales distributions Linux, a été découvert le 29 mars 2024 par l'ingénieur Microsoft Andres Freund. Ce code est présent dans le paquet téléchargeable et permet à un attaquant de contourner l'authentification de sshd sur des systèmes utilisant systemd. En présentant un certificat contenant des motifs spécifiques, un attaquant non authentifié peut ainsi exécuter du code arbitraire à distance. Ce problème de sécurité, identifié sous le numéro **CVE-2024-3094**, a **un score CVSS de 10**.

- **Impact :** Critique
- **Versions affectées :** 5.6.0 et 5.6.1
- **Distributions affectées :** Fedora Rawhide, Fedora 41, distributions Debian testing, unstable et experimental, openSUSE Tumbleweed, openSUSE MicroOS et Kali Linux.
- **Recommandations :** Nous recommandons de rétrograder XZ Utils à une version non compromise, telle que XZ Utils 5.4.6 stable, et de rechercher la présence de toute activité malveillante.

Découverte d'une vulnérabilité critique dans Microsoft SharePoint Server

Identifiée sous le numéro **CVE-2023-24955**, cette vulnérabilité permet l'exécution de code à distance. Classée comme grave avec **un score CVSS de 7.2**, elle soulève des préoccupations majeures pour la sécurité des informations.

- **Impact :** Grave
- **Recommandations :** Les organisations sont invitées à appliquer rapidement **les mises à jour** et les correctifs spécifiques pour SharePoint Server.

Découverte d'une vulnérabilité de corruption de mémoire dans iOS

Identifiée sous le numéro **CVE-2024-23225**, avec **un score CVSS de 7.8**, cette vulnérabilité permet à un attaquant, ayant la capacité de lire et écrire arbitrairement dans la mémoire du noyau, de contourner les protections de la mémoire du noyau. Apple a publié des mises à jour dans iOS 16.7.6, iPadOS 16.7.6, iOS 17.4, et iPadOS 17.4, adressant un problème de corruption de mémoire par une validation améliorée.

- **Impact :** Grave
- **Versions affectées :** iOS 16.7.6, iPadOS 16.7.6, iOS 17.4, et iPadOS 17.4.
- **Recommandations :** Apple a publié des **mises à jour** pour remédier à ce problème. Il est recommandé aux utilisateurs de mettre à jour leurs appareils vers ces versions pour se protéger contre l'exploitation de cette vulnérabilité.

Le Top des menaces

Une version Linux du malware multiplateforme DinodasRAT détectée dans des cyberattaques à travers plusieurs pays

Une version Linux du malware multiplateforme appelé ***DinodasRAT*** a été détectée dans la nature, ciblant la Chine, Taïwan, la Turquie et l'Ouzbékistan, selon de nouvelles découvertes de Kaspersky. ***DinodasRAT***, également connu sous le nom de ***XDealer***, est un malware en C++ qui permet de récupérer une grande variété de données sensibles sur les hôtes compromis.
En octobre 2023, ESET a révélé qu'une entité gouvernementale en Guyane avait été ciblée dans le cadre d'une campagne d'espionnage cyber baptisée Opération Jacana, déployant la version Windows de l'implant.
La semaine dernière, Trend Micro a pointé du doigt un groupe d'activités menaçantes - opérant sous le nom d'Earth Krahang - qui utilise ***DinodasRAT*** depuis 2023 dans ses attaques visant plusieurs entités gouvernementales dans le monde.
L'utilisation de ***DinodasRAT*** a été attribuée à divers acteurs de la menace liés à la Chine, notamment LuoYu, reflétant - à nouveau - le partage d'outils répandu parmi les groupes de pirates identifiés comme agissant au nom du pays. ***DinodasRAT*** est capable d'effectuer des opérations de fichiers, de changer les adresses de contrôle et de commande, d'énumérer et de terminer les processus en cours d'exécution, d'exécuter des commandes shell, de télécharger une nouvelle version du backdoor et même de se désinstaller.

Les pirates nord-coréens du groupe Lazarus exploitent une faille Zero-Day de Windows

Les acteurs notoires du groupe Lazarus ont exploité une faille de privilège d'escalade récemment corrigée dans le noyau Windows pour obtenir un accès de niveau noyau et désactiver les logiciels de sécurité sur les hôtes compromis.

La vulnérabilité en question est **CVE-2024-21338**, **de score CVSS 7,8**, qui peut permettre à un attaquant d'obtenir des **privilèges système**. Elle a été résolue par Microsoft plus tôt ce mois-ci dans le cadre des mises à jour du Tuesday Patch.
Pour exploiter cette vulnérabilité, un attaquant devait d'abord se connecter au système. Il pourrait alors exécuter une application spécialement conçue pour exploiter la vulnérabilité et prendre le contrôle du système affecté.
Les pirates ont utilisé cette faille Zero-Day pour exécuter leur rootkit ***FudModule***, un outil particulièrement sophistiqué dans l'arsenal du groupe ***Lazarus***. Le rootkit leur a permis de désactiver la surveillance de toutes les solutions de sécurité sur les hôtes infectés.
Bien que Microsoft ait corrigé la vulnérabilité, la découverte de son exploitation active souligne l'importance des mesures de sécurité robustes et de la correction rapide des vulnérabilités pour se protéger contre les groupes de pirates sophistiqués comme Lazarus.

La France cible de cyberattaques - Observations et recommandations

La France fait face, actuellement, à **une vague sans précédent d'attaques cybernétiques** ciblant les services numériques de l'État. Ces cyberattaques s'inscrivent dans un contexte géopolitique et économique tendu, avec notamment l'approche des **Jeux olympiques de Paris 2024**.

Ces incidents ont gravement perturbé le fonctionnement des services publics et soulevé de sérieuses inquiétudes quant à la sécurité des infrastructures critiques du pays.
Les hackers cherchent à perturber les activités gouvernementales, voler des données sensibles et affaiblir la confiance des citoyens envers les institutions publiques et privés.
Citons, à titre d'exemple, les attaques suivantes depuis janvier 2024 :

- Le centre hospitalier universitaire de Nantes a été victime d'une attaque par déni de service distribué bloquant notamment le réseau Internet de l'établissement **[1]**.
- Un ordinateur, contenant les plans d'accès aux JO de Paris, a été volé à Drancy **[2]**.

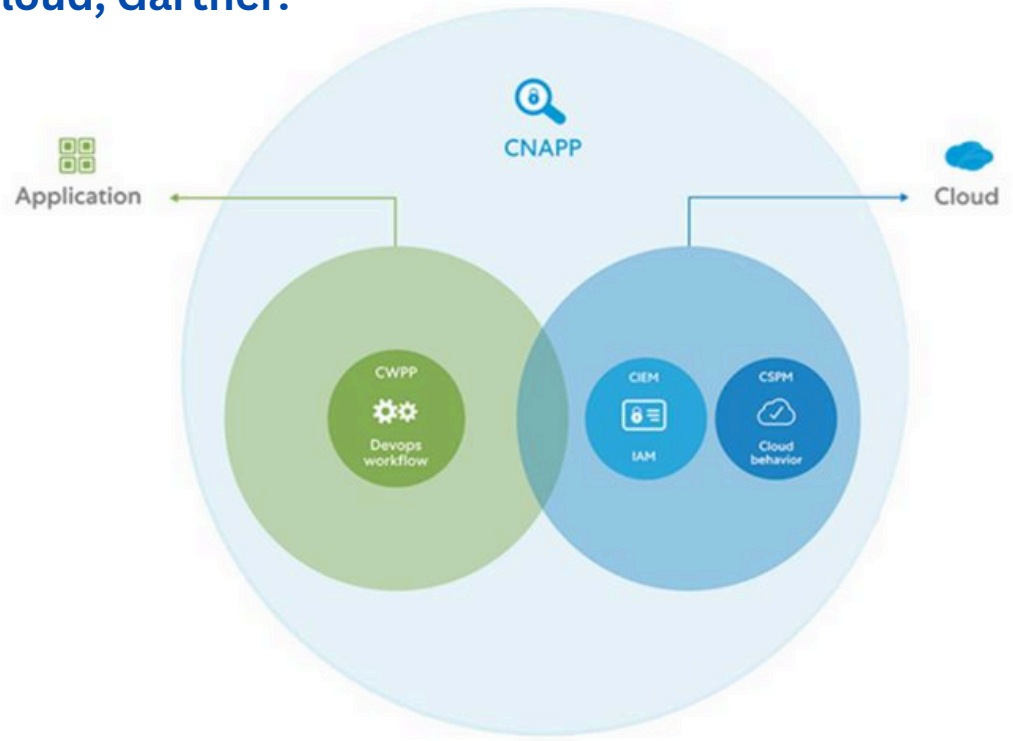
- Une attaque par déni de service distribué (DDoS) a visé la banque Crédit Agricole, paralysant l'accès à ses services en ligne pendant plusieurs heures **[3]**.
- France Travail (ex-Pôle Emploi) a annoncé avoir été la cible d'une cyberattaque, avec un risque de divulgation des données personnelles de 43 millions de personnes **[4]**.

Face à cette menace, il est essentiel que les organisations publiques et privées renforcent leurs mesures de cybersécurité. Cela passe par :

- La mise en place de solutions de détection et de protection avancées.
- Le renforcement des procédures de sauvegarde et de reprise après incident.
- La réalisation d'audits de sécurité réguliers.
- La sensibilisation et la formation du personnel (informatique ou pas) aux bonnes pratiques de cyber hygiène.

Le point tech' : les plateformes de protection des charges de travail dans le Cloud

> *" La combinaison des capacités de CWPP et de CSPM crée une synergie, et de nombreux fournisseurs adoptent cette stratégie. Cette combinaison créera une nouvelle catégorie de protection des applications cloud natives (CNAPP) qui analyse les charges de travail et les configurations en cours de développement tout en protégeant les charges de travail et les configurations en cours d'exécution ".*
> **Guide du marché des plateformes de protection des charges de travail dans le cloud, Gartner.**



Composants intégrés dans la CNAPP (Image adaptée de « Comment protéger vos Cloud avec CSPM, CWPP, CNAPP et CASB », Gartner, 6 mai 2021)

Qu'est-ce qu'une CNAPP ?

Une CNAPP est une solution de sécurité et de conformité qui aide les équipes à développer, déployer et exécuter des applications cloud natives sécurisées dans les environnements de cloud public dynamiques et hautement automatisés d'aujourd'hui. Les CNAPP permettent également aux équipes de sécurité de mieux collaborer avec les développeurs et les équipes DevOps. Les CNAPP constituent une nouvelle catégorie de plateforme de sécurité cloud qui regroupe des capacités telles que :

- Gestion de la posture de sécurité cloud (CSPM)
- Gestion des autorisations d'accès aux ressources cloud (CIEM)
- Gestion des identités et des accès (IAM)
- Protection des charges de travail cloud (CWPP)
- Protection des données

Pourquoi les entreprises ont-elles besoin d'une CNAPP ?

Les outils et approches de sécurité traditionnels, conçus pour protéger les centres de données et les terminaux sur site, ne sont pas adaptés aux applications et services cloud natifs. Les environnements cloud dynamiques et éphémères, avec une forte automatisation, des cycles de déploiement plus rapides et des pratiques de développement modernes, nécessitent une nouvelle approche de sécurité. Les CNAPP permettent d'identifier - assez tôt dans le développement - les problèmes de sécurité et les vulnérabilités, d'accélérer la correction et d'assurer une sécurité et une conformité continues, le tout, en minimisant les frictions avec les équipes DevOps.

Principaux avantages des CNAPP :

- Visibilité et contrôle unifiés sur l'infrastructure et les applications cloud,
- Détection et correction plus rapides des problèmes de sécurité et de conformité,
- Meilleure collaboration entre les équipes de sécurité, de développement et d'exploitation,
- Réduction de la complexité et des coûts grâce à l'intégration de plusieurs outils de sécurité.

Pour conclure, les plateformes CNAPP représentent une solution de sécurité cloud holistique et cohérente, qui habilite les entreprises à maximiser les avantages du cloud, tout en minimisant les risques associés.

Aujourd'hui, des acteurs majeurs comme **Microsoft** et **Zscaler** se distinguent en tant que fournisseurs principaux de solutions CNAPP, offrant des outils avancés pour la protection et la gestion des applications cloud natives.

Ces solutions permettent une visibilité accrue et une meilleure gestion des menaces, assurant ainsi une sécurité robuste et adaptative dans un paysage technologique en constante évolution.

Participation au Forum InCyber (FIC) Europe 2024, 26-28 mars 2024

Brightway a récemment participé au salon **InCyber 2024** qui s'est tenu à Lille Grand Palais du 26 au 28 mars. Cette édition était consacrée aux bouleversements engendrés par l'intelligence artificielle et la croissance exponentielle des données sur la cybersécurité.

Notre présence à cet événement majeur et plateforme incontournable pour les entreprises innovantes dans la cybersécurité a été une occasion précieuse pour échanger avec nos paires experts du secteur, découvrir les dernières tendances et présenter nos services et solutions, comme **Brightwatch**.

Au cours de cet événement, nous avons observé plusieurs tendances marquantes qui façonnent l'avenir de la cybersécurité. La croissance de l'intelligence artificielle et de l'apprentissage automatique dans la détection et la prévention des cyberattaques permettent une analyse plus rapide et plus précise des menaces, renforçant ainsi la sécurité des systèmes informatiques.

Par ailleurs, l'entrée en vigueur de nouvelles réglementations comme **DORA** ou **NIS 2** a été un thème récurrent lors des discussions obligeant les entreprises à redoubler d'efforts pour garantir la confidentialité et l'intégrité de leurs données.

Notre participation au salon InCyber 2024 a été une expérience enrichissante qui nous a permis de rester en contact avec nos clients et partenaires, à la pointe des tendances en matière de cybersécurité et de renforcer notre position dans le domaine.

BRIGHTWAY SAS.
16 Rue Troyon
92310 Sèvres

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