THE BRIGHTLETTER

BREAKING NEWS

BRIGHTWAY
Bring your business to the right way

LA BRIGHTLETTER

VOTRE DOSE MENSUELLE D'INFORMATIONS CYBER

La BrightLetter #3- Juin2024

Une production signée Brightway

Bienvenue dans cette nouvelle 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' : quleques concepts émergents et/ou 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

Le Top des vulnérabilités

Check Point met en garde contre des attaques zero-day sur ses produits VPN gateway

Cette faille a été découverte le 8 mai 2024 par Check Point Software Technologies, répertoriée sous le code **CVE-2024-24919**. Elle est due à une erreur de configuration dans la gestion des identifiants, permettant à un attaquant de contourner les mécanismes d'authentification sur les passerelles VPN. Un attaquant non authentifié pourrait ainsi accéder à des réseaux internes via la passerelle VPN et exécuter des commandes arbitraires.

- **Impact :** Critique
- **Versions affectées :** Toutes les versions de Check Point VPN Gateway avant R81.10.
- **Recommandations :** Il est recommandé de mettre à jour vers la version R81.10 ou ultérieure et de vérifier l'intégrité des systèmes qui auraient pu être exposés à cette vulnérabilité. En outre, il est conseillé de renforcer les configurations de sécurité et de surveiller les journaux pour détecter toute activité suspecte.

macOS root access exploit

La faille identifiée sous le code **CVE-2024-27822** a été publiée le 13 mai 2024. Cette vulnérabilité permettait potentiellement à une application d'obtenir des privilèges root sur le système affecté. L'exploitation de cette faille pouvait permettre à une application malveillante d'élever ses privilèges au niveau root, donnant ainsi un contrôle total sur le système affecté.

- **Impact :** Critique
- **Versions affectées :** La vulnérabilité affecte les versions de macOS avant Sonoma 14.5.
- **Recommandations :** Il est recommandé de mettre à jour vers macOS Sonoma 14.5 ou une version ultérieure. Il est également conseillé de surveiller et de limiter l'installation de logiciels provenant de sources non fiables, car les applications malveillantes pourraient exploiter cette faille.

Le Top des menaces

Cyberattaque Zadig & Voltaire : les données personnelles de 600 000 clients publiées sur le Dark Web

En juin 2024, **"Zadig & Voltaire"**, marque française de mode reconnue pour son style chic, a subi une cyberattaque majeure compromettant les données personnelles de plus de 600 000 clients, exposées sur le Dark Web. Les informations divulguées, incluant noms et adresses email, augmentent les risques de fraude et d'usurpation d'identité.
En réponse, "Zadig & Voltaire" a sécurisé ses systèmes, lancé une enquête détaillée, et informé les clients affectés en leur fournissant des ressources pour protéger leurs informations **[1]**.

Le ransomware Monti fait trois victimes en France

En mai 2024, la ville de Pau a été ciblée par une attaque de ransomware perpétrée par le groupe Monti, affectant des institutions clés comme l'aéroport de Pau-Pyrénées, l'école de commerce Eklore et le campus numérique. L'attaque, survenue en une seule nuit, a illustré la rapidité et la gravité des ransomwares qui menacent les entités publiques et privées.
Conséquences opérationnelles: l'attaque a perturbé les opérations sans paralyser totalement les institutions. Par exemple, bien que les vols à l'aéroport aient continué, d'autres services ont été affectés. À l'école de commerce, les cours ont persisté malgré l'accès limité aux outils numériques habituels.
Exposition et risques liés aux données compromises: Le groupe Monti a exposé des milliers de documents sensibles sur le Dark Web, augmentant le risque de phishing et d'usurpation d'identité pour les victimes potentielles **[2]**.

Risques cybersécurité de la 5G : Accélération des attaques DDoS et Brute Force

La 5G, avec ses vitesses et sa capacité à connecter de nombreux appareils, révolutionne la communication. Mais elle pose aussi de nouveaux défis en matière de sécurité **[3]**.

Les risques cybersécurité

1. **Attaques DDoS plus puissantes:** Grâce à la 5G, les cybercriminels peuvent lancer des attaques par déni de service distribué (DDoS) plus rapides et plus massives, utilisant des objets connectés pour submerger les réseaux et les rendre inutilisables.
2. **Brutes Forces à grande vitesse:** Avec la 5G, les attaques par force brute, qui consistent à deviner des mots de passe, deviennent plus rapides. Les hackers peuvent tester plus de combinaisons en moins de temps, augmentant les risques de compromission.
3. **Plus de Points d'entrée pour les Hackers:** La 5G augmente aussi le nombre de points faibles dans les réseaux, rendant plus facile l'accès des hackers. Avec plus de connexions et d'appareils, il y a plus de portes pour les attaques.

Protéger les réseaux 5G

Pour protéger efficacement les réseaux 5G, il est crucial de:

- Mettre en place des systèmes capables de surveiller en temps réel l'ensemble du réseau et de détecter les anomalies.
- Maîtriser le périmètre en suivant attentivement tous les éléments constitutifs du réseau de l'entreprise, assurant ainsi une visibilité complète sur les équipements, les connexions et les dispositifs connectés.

La directive NIS 2 bientôt en vigueur !

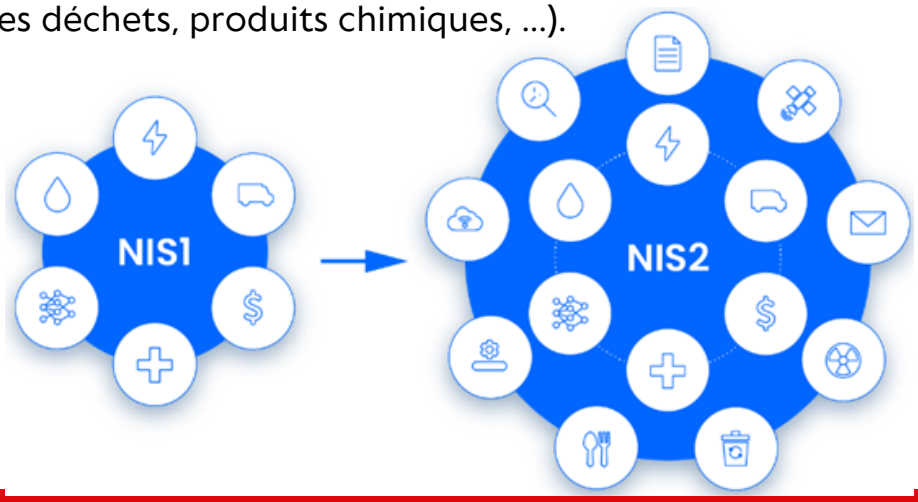
En réponse à la montée des cybermenaces globales, surtout en Europe, l'UE a établi une première directive en 2016 pour renforcer la cybersécurité (NIS). Cette directive a été actualisée par NIS 2 en décembre 2022, devant être adoptée d'ici le 17 octobre 2024.

En quoi consiste la directive NIS 2 ?

NIS2 a pour objectif de définir les mesures à mettre en œuvre pour toutes les organisations fournissant des services essentiels ou importants afin de se protéger des cybermenaces. Elle vise également à améliorer la collaboration entre les états de l'UE en matière de cybersécurité [4].

Quels secteurs d'activités sont concernés par la nouvelle version ?

La directive NIS 2 élargit le champ d'application de la directive NIS pour inclure 18 secteurs, répartis en secteurs hautement critiques (energie, ransports, santé, bancaire, ...) et critiques (postaux, gestion des déchets, produits chimiques, ...).



BRIGHTWAY SAS.
16 Rue Troyon
92310 Sèvres

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

Des sanctions financières lourdes prévues

À l'instar du RGPD, la législation européenne inclut dans NIS 2 des sanctions financières considérables en cas de non-conformité. Ces sanctions peuvent aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires pour les organisations opérant dans des secteurs essentiels, et jusqu'à 7 millions d'euros ou 1,4% du chiffre d'affaires pour celles des secteurs importants.

Calendrier

- **17 octobre 2024 :** Date limite pour que les États membres adoptent la directive NIS 2.
- **17 avril 2025 :** Date limite pour l'identification des entités concernées.
- **1er octobre 2025** : Date limite pour que les entités concernées se conforment aux exigences de la directive.

Notre accompagnement sur NIS 2

En tant qu'organisme qualifié PASSI, Brightway vous propose une offre d'accompagnement complète et transversale pour la mise en œuvre de la directive NIS 2. De l'analyse d'écart jusqu'à la mise en conformité, nous adoptons une approche structurée et personnalisée selon vos besoins spécifiques, assurant ainsi une transition fluide vers une conformité totale.

Le point tech' : SSDLC

Le SSDLC (Secure Software Development Life Cycle) vise à intégrer la sécurité à chaque étape du cycle de développement logiciel

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 SSDLC ?

Contrairement aux approches traditionnelles où la sécurité est souvent ajoutée à la fin du cycle de développement, le SSDLC intègre des pratiques de sécurité dès la conception jusqu'au déploiement de l'application. Cette approche proactive permet de détecter et de corriger les failles de sécurité le plus tôt possible.

Les 5 phases du cycle de vie du développement logiciel sécurisé

Examinons un exemple de cycle de vie de développement d'un système de gestion de conférences:

1- Exigences:

Les exigences relatives aux nouvelles fonctionnalités sont recueillies.

- **Exemple d'exigence fonctionnelle :** L'utilisateur doit pouvoir soumettre une proposition de conférence et voir ses propositions existantes.
- **Exemple de considération de sécurité :** L'utilisateur ne doit avoir accès qu'à ses propres propositions et ne doit pas pouvoir voir ni modifier celles des autres utilisateurs.

2- Conception:

Cette phase traduit les exigences en éléments concrets de l'application.

- **Exemple de conception fonctionnelle :** La page doit récupérer et afficher les propositions de conférence de l'utilisateur depuis la table "PROPOSALS" de la base de données.
- **Exemple de problème de sécurité :** Nous devons vérifier que l'utilisateur est authentifié avec un jeton de session valide avant de récupérer les informations de la base de données.

3- Développement:

Lors de la mise en œuvre de la conception, il est essentiel de s'assurer que le code respecte toutes les garanties de sécurité. Cela inclut des directives de codage sécurisé et des révisions de code manuelles ou automatisées via des technologies telles que les tests de sécurité des applications statiques (SAST).

4- Vérification:

La phase de vérification implique des tests complets de l'application pour s'assurer qu'elle répond aux exigences de conception et de sécurité. C'est un moment idéal pour introduire des tests de sécurité des applications dynamiques (DAST).

5- Déploiement:

La sécurité ne s'arrête pas à la publication de l'application. Des vulnérabilités peuvent être découvertes après le déploiement, souvent dans les composants open source sous-jacents. Ces vulnérabilités doivent être corrigées rapidement par l'équipe de développement

Conseils et astuces

BRIGHTWATCH
One step closer to the right way

La mise en place d'un outil centralisé pour surveiller, suivre et gérer les vulnérabilités des technologies utilisées par votre entreprise est essentielle pour garantir la sécurité de votre infrastructure informatique. Cela permet une vue d'ensemble, une identification rapide des failles et une réaction prompte aux menaces grâce à une surveillance en temps réel. De plus, la gestion centralisée optimise les ressources, priorise les actions correctives et assure la conformité réglementaire.

Dans ce contexte, nous vous présentons notre outil innovant **Brightwatch**, conçu pour s'adapter à votre environnement spécifique et offrir une visibilité instantanée sur les vulnérabilités de votre périmètre. Notre solution centralise les informations, facilite la gestion des vulnérabilités et permet une réaction rapide grâce à des alertes proactives. Vous êtes ainsi toujours informé des menaces émergentes, renforçant la sécurité de votre infrastructure et protégeant vos actifs les plus précieux.

BRIGHTWAY SAS.
16 Rue Troyon
92310 Sèvres

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