

GPLExpert et ses actualités SIS

"Spécial été / APSSIS"

Juillet 2023



#Le mot de la Direction

Comme chaque année depuis 7 ans, notre société était présente au Congrès National de la SSI Santé (APSSIS) en juin dernier.

Au-delà de l'opportunité de rencontrer nos clients, cette participation reste essentielle pour GPLExpert : elle nous permet de connaître les dernières statistiques et les nouvelles tendances en matière de réflexion appliquée à la sécurité de l'écosystème numérique de santé. Ces éléments d'informations donnent à leur tour lieu à des optimisations de processus internes.

Dans cette édition, mon ambition est de vous transmettre notre analyse qui sera à coup sûr utile (je l'espère vivement) pour une réelle sensibilisation au sein de votre structure et auprès de vos collaborateurs.

En ce mois de juillet, il m'a semblé pertinent de rappeler les bonnes pratiques en matière de sécurité du SI. Même à l'approche des départs en vacances, elles sont en effet à maintenir, les cyberattaques n'autorisant malheureusement aucune trêve.

Enfin, sachez que nous serons présents au 34ème congrès de la Société Française de Radiothérapie Oncologique du 20 au 22 septembre prochain au Corum de Montpellier, je serai très heureux de vous y rencontrer.

Je vous souhaite une agréable lecture, et un été rempli d'énergie positive.

Thomas BRETON

Dirigeant GPLExpert

Retour sur l'APSSIS 2023

Nos experts en sécurité, Damien RIBEIRO (RSSI) et Elhaouari CHANHHI (Responsable MCO/MCS) se sont immergés durant trois jours dans une "cyberbulle", se muant en véritables reporters GPLExpert sur place.

Les premiers constats divulgués par l'APSSIS sont encourageants :

 Une baisse des attaques informatiques est observée depuis mars 2023 par les Institutions.

→ *Ne perdons pas de vue que cette baisse est néanmoins associée à une complexité accrue en termes de méthodologie d'attaque.*

En effet, la détection et le solutionnement techniques s'avèrent de plus en plus difficiles.

 Lors de cyberattaques ciblées vers les établissements médico-sociaux, la déclaration obligatoire ainsi que l'accompagnement du CERT Santé* sont 2 notions désormais incontournables.

 La mise en place d'une « task force cyber » depuis l'attaque du Centre Hospitalier Sud Francilien est opérationnelle.

 Une augmentation des exercices de crise cybersécurité dans les établissements de santé est constatée depuis quelques mois, et ce n'est qu'un début.

Ces constats nous enseignent que la cybersécurité est au cœur des préoccupations gouvernementales. En ce sens, GPLExpert a mis en place une prestation "Exercice PCA" qui s'inscrit dans une démarche de sensibilisation et d'appropriation des automatismes de gestion de crise en matière de cybersécurité. **Cette prestation a été pensée et créée pour être totalement adaptée aux spécificités des établissements de santé.**

** Le CERT Santé apporte un appui aux établissements de santé, aux organismes et services exerçant des activités de prévention, de diagnostic ou de soins, ainsi que les établissements et services médico-sociaux dans la réponse à un incident de sécurité des systèmes d'information. Il assure une mission de prévention et d'alerte face aux menaces de cybersécurité.*

Contactez nos experts sécurité

Quelques chiffres marquants

Une importante partie des experts du secteur expliquent que la question n'est plus de savoir SI mais QUAND la prochaine cyberattaque surviendra.



12 heures : Temps nécessaire pour qualifier une nouvelle vulnérabilité.



45 minutes : Temps requis pour scanner la toile Internet.



5 minutes : Délai nécessaire à un attaquant pour commencer à scanner les logiciels présentant une vulnérabilité.

Face à cette industrialisation des attaques informatiques, votre système d'information doit être protégé en conséquence. Mais cela ne suffira pas totalement. En effet, 82 % des brèches de sécurité informatique proviennent du facteur humain. Pour une protection optimale, il est donc nécessaire de combiner technologie et montée en compétence cyber des salariés.

Étant reconnue prestataire terrain du parcours Cybersécurité, GPLExpert positionne ses experts sur une offre de prestation normée et financée par l'État, qui intègre des actions mêlant prévention et accompagnement.

Contactez nos experts sécurité

#Le conseil de l'expert

"L'été est propice aux cyberattaquants et la raison en est simple. Lorsqu'il s'agit de cybersécurité, le maillon faible ne vient pas uniquement de la technologie mais aussi de l'humain. Durant la période estivale, les effectifs sont réduits au sein des établissements, c'est une opportunité souvent saisie par les pirates pour pénétrer les failles des Systèmes d'Informations. Un rappel sur les bonnes pratiques à adopter par vos équipes permettra de réduire les risques."

Damien RIBEIRO

RSSI GPLExpert

#Le Question / Réponse

Quelles précautions avant votre départ en vacances ?

Il va s'en dire que malheureusement, les pirates ne prennent pas de vacances. Pour prévenir des risques liés à un manque de vigilance certain durant les périodes de congés, nous vous avons préparé quelques conseils à glisser dans votre valise !



Le partage de vos vacances sur les réseaux sociaux

Il est très tentant de partager ses vacances sur les réseaux sociaux.

Pour autant, cette pratique est fortement déconseillée.

En exposant votre vie privée, vous risquez d'être victime [de phishing](#). Dans la mesure du possible, n'indiquez pas trop de détails dans votre réponse automatique par mail (lieu, date...).



Sécurisez votre connexion à distance

Si votre fonction nécessite de garder votre matériel informatique, nous préconisons de sécuriser vos connexions en amont avec la mise en place d'un VPN (Réseau Virtuel Privé) qui permettra de chiffrer vos informations et donc de limiter l'accès à vos données.



Sauvegardez vos données

Pour cela, il faut sauvegarder vos données et les stocker dans un réseau sécurisé. Il s'agit notamment de stocker vos données sur un serveur ou cloud sécurisé.

En complément, effectuez une sauvegarde de vos données sur un support physique (clef USB, disque dur...), afin de ne pas perdre totalement vos données, en cas de perte ou de vol de votre ordinateur pendant vos vacances.



Protégez votre boîte mail

Les boîtes mail représentent la principale source des cyberattaques. Même en vacances, il est essentiel de les protéger !

Utilisez un [mot de passe complexe](#), au besoin, utilisez un générateur de mot de passe, tel que KeePass, qui est certifié par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

Une sensibilisation auprès de vos collaborateurs pourra être profitable à votre société. Précisez leur l'importance de se méfier des mails : objet, lien, pièce jointe... et le risque qu'un simple mail peut entraîner.



Sécurisez votre ordinateur

(et tout autre matériel informatique)

Là aussi, l'utilisation d'un mot de passe robuste pour verrouiller l'accès à votre ordinateur est essentielle.

Antivirus, antimalware ou encore antiransomware sont des outils efficaces pour la sécurité de votre poste de travail.

En bonus, le filtre de protection écran vous permettra d'utiliser votre ordinateur tout en évitant les regards malveillants, dans les lieux publics ou dans les transports.

Besoin d'un accompagnement en sécurité ?

#Les événements à venir

 Du 20 au 22 septembre 2023

■ SFRO

GPLExpert innove et sera présente pour la première fois au Corum de Montpellier à l'occasion du 34ème congrès de la SFRO - Société Française de Radiothérapie Oncologique. **Stand 37**

 Les 21 et 22 septembre 2023

■ Rencontres FHP

GPLExpert vous attendra aux Rencontres de la FHP les 21 et 22 septembre 2023 à Bordeaux, Hangar 14. **Stand 31**

Prendre rdv avec nous sur un salon

#GPLExpert recrute !

Le recrutement du moment !

Assistant(e) de gestion administrative	Polyvalent(e) ★★★	→ La mission principale de l'assistant(e) de gestion administrative consiste à gérer l'organisation générale de la structure (groupe projet, service, entreprise, ...) ainsi que de la gestion et du suivi administratif de dossiers techniques.
	Discret(ète) ★★★	
	Diplomate ★★★	
	Synthétique ★★★	Poste à pourvoir en île-de-France , dans une ambiance sympa avec un travail vraiment intéressant et porteur d'évolution 🚀
	Communicant(e) ★★★	Nous recherchons surtout un savoir-être .



Organisé(e)
★★★

Pour le savoir-faire, les bases administratives sont nécessaires mais nos équipes veilleront à bien vous intégrer.

Administrateurs systèmes et réseaux

→ Être administrateur systèmes et réseaux nécessite des connaissances en **gestion de réseau** et en **développement informatique**. Son rôle est d'**installer**, de **configurer**, et de savoir **dépanner un parc informatique**. Il doit donc maîtriser les techniques nécessaires pour interconnecter les réseaux et les systèmes informatiques.

3 postes sont à pourvoir en **Ile-de-France et à Caen**.

Vous souhaitez intégrer une équipe compétente et apporter votre pierre au grand édifice de la Santé, GPLExpert attend votre candidature.

Techniciens systèmes et réseaux

→ Les techniciens systèmes et réseaux **administrent** au quotidien les **parcs bureautiques** et en assurent le bon fonctionnement. Ils savent alors déployer et supporter les postes de travail. Les qualités requises pour ce poste résident en **l'autonomie**, le **dynamisme** et le **sens du relationnel**.

3 postes sont à pourvoir en **Mayenne (Laval), Seine et Marne et Ile-de-France**.

Je postule
