Communiqué de presse du 06 octobre 2022

Le Groupe Asten, partenaire premium du Breizh Cyber Show

Le Groupe Asten est partenaire premium de la 1e édition du Breizh Cyber Show se déroulant pendant le mois de la cybersécurité et réunissant les entreprises du Finistère autour de la thématique de la cybersécurité.

Notre pôle cyber proposera notamment tout au long de la soirée deux ateliers pratiques aux participants : l'un pour s'initier à quelques techniques de hacking grâce à un « capture the flag » (exercice ludique consistant à exploiter des vulnérabilités et récupérer un drapeau en preuve de réussite) et l'autre pour tester leur dextérité au crochetage de serrure.

GACYB : groupement d'acteurs en cybersécurité

Le Groupe Asten est membre fondateur de GACYB. Crée en 2017, cette association est issue d'un groupe de travail réunissant plusieurs dirigeants d'entreprises informatiques et digitales autour d'une thématique commune « comment sensibiliser tous les acteurs économiques d'un territoire, le Finistère, à un enjeu qui les concerne tous, à savoir la cybersécurité ? » et nous en avons porté la première présidence.

C'est tout naturellement que nous avons répondu présent pour soutenir cette première édition du Breizh Cyber Show et que nous sommes heureux d'apposer notre nom au côté de cet événement amené à se dérouler tous les ans à la pointe bretonne.

Groupe Asten et la cybersécurité

Depuis plus de 25 ans, le Groupe Asten s'engage et investit pour le développement économique, social et numérique de la Bretagne. Nous accompagnons nos clients dans le développement, l'évolution et la sécurisation de leur système d'information et de leurs services numériques, les aidons à améliorer leurs performances en étudiant leurs besoins et métiers, en auditant et optimisant leurs infrastructures et applications, en leur conseillant les technologies les plus adaptées.

Nous intervenons notamment sur les sujets d'**infogérance, sauvegarde et sécurisation des systèmes d'information** et sommes propriétaire de **2 datacenters** à Brest métropole.

Aussi, **la cybersécurité est au cœur de nos préoccupations et de nos offres de services.** Nous avons à protéger notre informatique, celles de nos clients mais avons également une responsabilité vis-à-vis de notre territoire et nous faisons fort de répondre présent lorsqu'une entreprise se trouve en difficulté.

Les entreprises ont encore du mal à intégrer la cybersécurité dans leur stratégie et donc au niveau nécessaire de dépense dans leur budget. Il est de notre devoir de les sensibiliser et de leur proposer des solutions, de les aider à trouver et comprendre leurs failles… et aussi de constituer des équipes d'alerte pour les accompagner lorsqu'elles sont victimes d'une attaque.

Nous disposons pour ce faire d'un **pôle Cybersécurité**, au sein d'Asten Cloud, qui intervient pour le Groupe Asten, et pour nos clients sur toute la France (et même en Europe dans le cas de clients en multi-sites). Nous soutenons les entreprises de façon proactive, en les accompagnant dans la sécurisation de leur architecture informatique dans le cadre d'audit de cybersécurité et de tests d'intrusion physique et virtuelle.

Nous intervenons également en **réponse à un incident** : à la suite d'une indisponibilité voire d'une situation critique à résoudre urgemment, nos spécialistes de la cybersécurité, épaulés de nombreux autres profils (ingénieurs réseaux, architectes, communicants…) et partenaires, vont tout mettre en œuvre pour permettre à l'entreprise de poursuivre son activité, en mode dégradé.

Ils vont remonter la chaîne de traçabilité pour identifier la source du problème, la corriger, s'assurer que toutes les failles ont été comblées, avant de reconstruire le système et remettre le service en route durablement. Ils vont bien entendu établir le plan d'action et guider l'entreprise pour que cela ne se reproduise plus.

La cybersécurité, l'affaire de tous ?

Mais la cybersécurité, ce sont aussi et surtout les moyens organisationnels, technologiques et financiers que l'on met en place pour se protéger contre toutes ces menaces, sans oublier ceux que l'on devra mobiliser pendant et après une attaque.

La cybersécurité couvre les sujets de sensibilisation, formation, d'identification et appréhension des menaces liées à l'utilisation de l'informatique et des réseaux (internet, privés d'entreprises ou publics). Elle couvre évidemment la mise en œuvre des démarches de sécurité, la gestion de crise, la remédiation, les enseignements que l'on en retire, les retours d'expérience que l'on en fait…

Un euro investit en cybersécurité ne rapportera pas un seul euro de chiffre d'affaires. En revanche, ne pas investir dans la sécurité peut faire perdre beaucoup à l'entreprise ; voire la faire disparaitre. Comme un dégât des eaux, un incendie… cela n'arrive pas qu'aux autres. Trop souvent, les entreprises considèrent la sécurité informatique comme une charge, se disent qu'elles sont trop petites pour « intéresser des hackers », alors même que le sujet de la cybersécurité occupe l'espace médiatique.

Les chiffres clés des attaques sont dramatiquement en hausse et sans appel.
Par exemple, l'organisation mafieuse Conti dispose d'un budget de 200 mille dollars et aurait généré en 2020 un chiffre d'affaires de plus de 500 millions de dollars. Attaquer est rentable !

De plus, **attaquer est à la portée de tous ou presque** : se fournir un kit sur internet est rapide et peu cher ! Une fois le kit en main, en quelques paramètres, il est possible à un individu d'attaquer une cible et demander des rançons.

Être moins vulnérable que le voisin…

Les attaques ne sont plus sporadiques, elles sont massives et constantes ; l'heure n'est plus à la mesure du risque mais bien à la protection des entreprises.

Certaines failles sont faciles à combler et permettent de garantir un premier rempart autour de votre entreprise et votre savoir-faire. Plus de 70% des attaques passent par des failles de sécurité connues au niveau des serveurs et des postes de travail, ainsi que par la messagerie.

L'application systématique **des mises à jour** ainsi que le **renforcement de l'active directory** (annuaire des utilisateurs et gestion de droits d'accès au système d'information) élèveront immédiatement le niveau de sécurité de l'entreprise. Ces actions sont par ailleurs peu couteuses au regard des impacts et conséquences d'une attaque.

Concrètement chez Groupe Asten…

Parmi nos différentes offres et solutions et pour couvrir les risques de cyberattaques de nos clients, nous proposons depuis 2008 de nombreux services.

- **L'hébergement et l'infogérance des systèmes d'information des entreprises dans nos datacenters :** les serveurs sont infogérés et protégés (failles de sécurité comblées par mises à jour systématiques).
  Nous garantissons la sécurité face aux attaques, par un très haut-niveau de protection qui freine les attaquants et les détournent vers une autre cible.

- Pour les structures qui ont des serveurs au sein de leur entreprise, nous proposons **une infogérance du système d'information**, comprenant les mises à jour de sécurité.

- Pour toutes les entreprises, qu'elles hébergent leur SI chez Groupe Asten ou non, nous menons des missions **d'audit** et de **renforcement des configurations** des annuaires (AD).

- Nous proposons une offre de **sécurisation de la messagerie** : l'objectif étant de contrôler tous les mails entrants et de ne délivrer que ceux qui ne présentent aucun risque.

- Pour renforcer la sécurité des sauvegardes, nous proposons leur hébergement dans nos datacenters, ainsi que l'étude d'un plan de secours (PRA) et le test régulier de celui-ci.