Sites intéressants :

* [https://numerama.com](https://numerama.com.html)
* <https://www.sans.org/fr_fr/> (parle de la cybersécurité)
* <https://www.nist.gov/>
* <https://www.eccouncil.org/>

Sources :

* <https://www.numerama.com/cyberguerre/1246704-riot-games-editeur-de-league-of-legends-admet-avoir-ete-pirate.html>

Riot Games subit une attaque informatique par usurpation d’identité et voit ses données compromises.

<https://www.lebigdata.fr/base-de-donnees>

Une base de données (que nous nommerons BDD par commodité) est une **collection d’informations organisées afin d’être facilement consultables, gérables et mises à jour**. Au sein d’une database, les données sont organisées en lignes, colonnes et tableaux. Elles sont indexées afin de pouvoir facilement trouver les informations recherchées à l’aide d’un logiciel informatique. Chaque fois que de nouvelles informations sont ajoutées, les données sont mises à jour, et éventuellement supprimées.

Elles se chargent elles-mêmes de créer, de mettre à jour ou de supprimer des données. Elles **effectuent également des recherches parmi les données qu’elles contiennent sur demande de l’utilisateur**, et de lancer des applications à partir des données.

Les bases de données sont utilisées par de nombreuses entreprises dans toutes les industries. Elles sont notamment utilisées par les **compagnies aériennes pour gérer les réservations**. Elles sont utilisées pour la gestion de production. Pour **les enregistrements médicaux dans les hôpitaux**, ou encore pour les **enregistrements légaux dans les compagnies d’assurances**. Les bases de données les plus larges sont généralement utilisées **par les agences gouvernementales**, les grandes entreprises ou les universités.

Les bases de données sont stockées sous forme de fichiers ou d’ensemble de fichiers sur un disque magnétique, une cassette, un disque optique ou tout autre type d’appareil de stockage (date centers pour les gros stockage : entreprises). Les bases de données traditionnelles (hiérarchiques) sont organisées par **champs (fields), enregistrements et fichiers**. Un champ est une seule pièce d’information. Un enregistrement est un ensemble de champs. Un fichier est une collection d’enregistrements.

Par exemple, un **répertoire téléphonique est l’équivalent d’un fichier**. Il contient un ensemble d’enregistrements, et chaque enregistrement regroupe trois champs : nom, adresse et numéro de téléphone. En guise d’exemple, on peut aussi citer les catalogues de produits ou les inventaires.

La faculté de consulter ou de modifier une database (lire ou écrire) est conférée aux divers utilisateurs par un **database manager (gestionnaire de base) et par un database administrator pour l’administrer**. Les bases de données sont principalement présentes au sein des systèmes mainframe (des ordinateurs hautes performances dotés de grandes quantités de mémoire et de processeurs qui traitent des milliards de calculs et de transactions simples en temps réel. Le mainframe est essentiel pour les bases de données commerciales, les serveurs de transaction et les applications qui nécessitent une [résilience](https://www.ibm.com/fr-fr/it-infrastructure/z/capabilities/resiliency), une [sécurité](https://www.ibm.com/fr-fr/it-infrastructure/z/capabilities/enterprise-security) et une [agilité](https://www.ibm.com/fr-fr/it-infrastructure/z/capabilities/cloud-native-development) élevées [https://www.ibm.com/fr-fr/topics/mainframe#:~:text=Le%20mainframe%20est%20essentiel%20pour,sécurité%20et%20une%20agilité%20élevées](https://www.ibm.com/fr-fr/topics/mainframe#:~:text=Le%20mainframe%20est%20essentiel%20pour,s%C3%A9curit%C3%A9%20et%20une%20agilit%C3%A9%20%C3%A9lev%C3%A9es) ) les plus larges, mais on les retrouve aussi au sein de workstations distribuées de moindre envergure et autres systèmes midrange comme les IBM AS/400 ([https://blog.present.ca/fr/pme-serveurs-power-i-as400-ibm#:~:text=Le%20système%20d%27opération%20i5,de%20bases%20de%20données%20concurrents](https://blog.present.ca/fr/pme-serveurs-power-i-as400-ibm#:~:text=Le%20syst%C3%A8me%20d%27op%C3%A9ration%20i5,de%20bases%20de%20donn%C3%A9es%20concurrents). ) connu sous le nom de System I () ou même les ordinateurs personnels

<https://www.lemondeinformatique.fr/actualites/lire-microsoft-lance-officiellement-sql-server-2022-88663.html>

<https://www.lemondeinformatique.fr/actualites/lire-une-faille-par-injection-sql-frappe-zoho-manageengine-89111.html>

L’entité ManageEngine a subi une vulnérabilité dans sa sécurité de type injection SQL qui fut exploitée par plusieurs attaques par exécution de code à distance, Access Manager et Password manager Pro aussi détenus par Zoho ont été aussi détenus. En 2021,les serveurs de Manage Engine furent aussi attaquées par des hackeurs épaulés par un état sur une faille critique qui a été rapidement patchés

<https://www.lemondeinformatique.fr/actualites/lire-le-fleau-persistant-des-attaques-par-injection-sql-et-xss-87320.html>

Selon un rapport donnée par l’agence Breachlock situé au Pays-bas, spécialisée dans des services de sécurité informatique, l’injection SQL reste une menace très élevée pour les entreprises en 2021. Un tiers des risques critiques trouvés dans les applications web (35 %) peuvent être attribués à l'injection ou à l'exposition des données. Ce qui est assez préoccupant sachant que énormément d’applications sont hébergés sur internet.« Même si, depuis des années, l'injection SQL est une vulnérabilité très répandue, je suis surpris de voir qu'elle est toujours aussi fréquente qu'en 2014, 2015. Plus de 27 % des vulnérabilités que nous avons identifiées résultent d'injection SQL », a déclaré Prateek Bhajanka, vice-président des produits de BreachLock.

L’étude annonce aussi que 50 % de ces failles ont pour cause une erreur de scripting. Le rapport précise que les dévellopeurs préfèrent une approche dite « liste de refus » plutôt qu’une approche « liste d’autorisation », ayant pour conséquence l’exploitation de faille par des nouvelles données. Les sites webs seraient cependant mieux sécurisées avec l’utilsiation du programme « DevSpecOps » avec une chance de 5 % de risque critique. Il a été trouvé que la plupart des risques dans les entreprises surgissait de l’infrastructure interne plutôt qu’externe. Les applications mobiles seraient aussi moins touchés. 87 % de tous les risques critiques et élevées proviennent d’entreprise de moins de 200 employées

<https://www.journaldugeek.com/2021/12/07/les-data-centers-sont-de-plus-en-plus-problematiques-pour-la-planete/>

<https://www.cnil.fr/fr/garantir-la-securite-des-donnees>

Ici, la CNIL (Commission nationale de l'informatique et des libertés) présente la façon afin de garantir la sécurité des données, qui commence surtout par se poser les bonnes questions sur les conséquences que pourraient engendrés les données sur les utilisateurs, quels scénarios pourraient mettre en danger les données de ces utilisateurs et comment et quelles mesure doivent être pris afin d’éviter ces scénarios

<https://www.reseaux-telecoms.net/actualites/lire-les-pannes-dans-les-datacenters-de-plus-en-plus-issues-de-problemes-reseaux-27727.html>

L’article de reseaux-telecoms.net présente ici le problème des pannes des data centers qui se font de plus en plus présent ce qui a pour conséquence l’arrêt de plus en plus de service. Les causes de ces pannes sont souvent un défaillance dans les systèmes IT et les erreurs réseaux. L’institut Uptime s’est penché sur ce problème en décortiquant 162 interruptions de service signalées dans les médias traditionnels ou sociaux au cours des trois dernières années

<https://www.usine-digitale.fr/article/canicule-les-datacenters-echappent-au-coup-de-chaud.N339664>

Dans cet article, on peut voir que les épisodes de canicules qu’à fait face la france à mis les data centers à risque. Du fait que les data centers doit être toujours sous sytème de refroidissement, ces périodes ont été beaucoup plus gourmands en énergie que le reste du temps.

L’article signal que le systèmes du « free-cooling » est utilisé pour refroidir les salle des serveurs qui doivent se maintenir à une température de 20 à 22°C selon la norme, pour cela ce système utilise la température de l’air extérieur pour refroidir les salles. Cependant, quand l’extérieur dépasse les 30°C, le système est changé pour utiliser la climatisation pour refroidir. Cependant, les services non toujours pas enregistrer de panne à cause des contraintes « draconiennes » qui sont soumis à la conception et l’exploitation des serveurs où lorsqu’une pièce est en panne, un autre prend le relais. La chaleur peut aussi révéler des défauts dans la maintenance.

<https://www.lemondeinformatique.fr/actualites/lire-un-bug-informatique-bloque-les-vols-aux-etats-unis-89177.html>

Le 11 Janvier 2022, aucun vol n’a pu partir des aéroports aux Etats-Unis jusqu’à 9h. Ce bloquage a été choisi par la FAA (Federal Aviation Administration) après une panne qui a surgit dans le système Notam, pendant la nuit. Le système Notam est une base de donnée centralisée qui est gérée par l’aviation civil Américaine, elle fournit des informations de sécurité essentielles pour tout les voyage aériens sur le territoire national. La cause de la panne est en cours entrain d’être recherché mais l’hypothèse d’une cyberattaque n’est pas écartée.

<https://www.lemondeinformatique.fr/actualites/lire-10-conseils-pour-ameliorer-la-securite-des-bases-de-donnees-71925.html>

<https://www.isaca.org/resources/isaca-journal/issues/2020/volume-3/practical-data-security-and-privacy-for-gdpr-and-ccpa>

<https://owasp.org/www-project-proactive-controls/v3/en/c3-secure-database>

<https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/base-de-donnees/>

<https://pixees.fr/lhistoire-des-base-de-donnees-ou-presque/>

<https://www.lemondeinformatique.fr/actualites/lire-des-e-mails-de-militaires-de-la-defense-us-exposes-89609.html>

Aux Etats-unis, Un serveur cloud Azure, hébergée par Microsoft, contenant des e-mails sensibles mais non archivées,envoyées par l’armée Américaine. Le serveur été mal configuré est ne contenait pas de mot de passe, TechCrunch explique qu’une personne ayant l’ip et un navigateur pouvait accéder aux données. Après une enquête, il a été révélé que personne n’a eu accès aux données.