DÉCEMBRE 2022 | N° 1

Mag' Cyber

Edito

« La météo n'est pas très bonne objectivement » alertait samedi 15 octobre sur France Inter Guillaume Poupard, Directeur Général de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

Sur le plan de la cybersécurité, il est en effet difficile de se réjouir de la recrudescence des vagues d'attaques qui se manifestent depuis plusieurs mois dans tous les secteurs de l'économie. En témoigne celle par rançongiciel subie dans la nuit du 20 au 21 août par le Centre Hospitalier Sud Francilien (cf. notre analyse en page 3).

Si on en croit un rapport d'Hiscox en 2022, 52% des entreprises ont été ciblées par au moins une attaque au cours des 12 derniers mois, et cela ne va pas aller en s'améliorant.

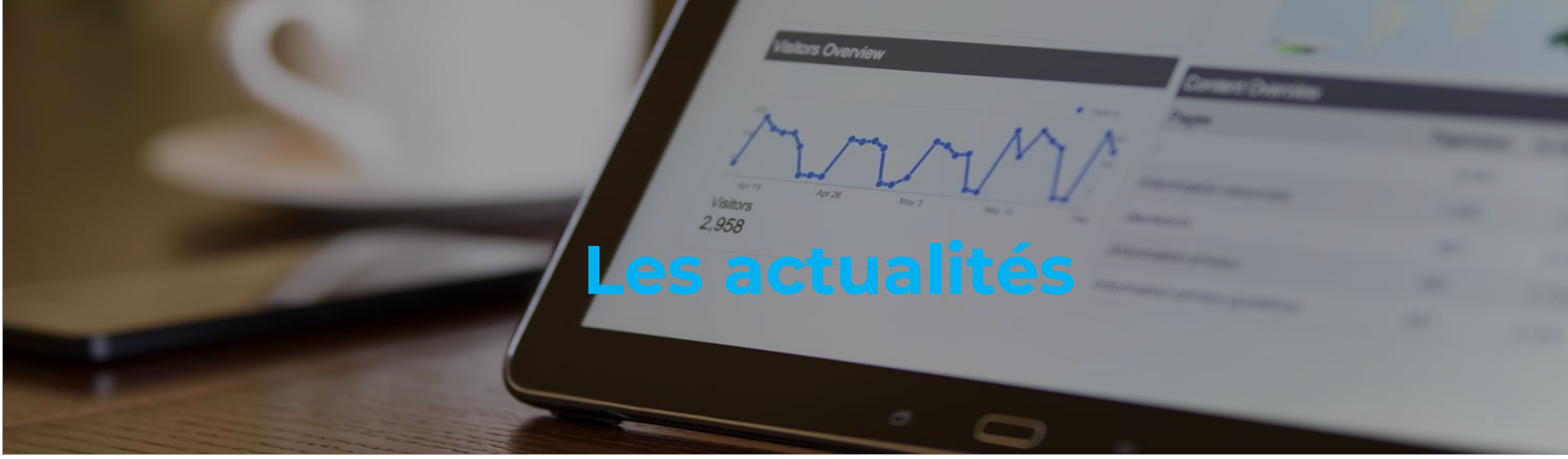
Pour toute entreprise, la question n'est pas de savoir si elle sera attaquée, mais quand.

Il est donc plus que jamais urgent de se tenir prêt car redémarrer ses activités après un tel événement ne s'improvise pas.

Bonne lecture ! »

Sommaire

Magellan Partners



Les actualités

PassKeys : Le fonctionnement du nouveau système d'authentification censé remplacer les mots de passe

Les principaux membres de l'alliance FIDO souhaitent mettre fin aux mots de passe en les remplaçants par des « passkeys », un système d'authentification en développement depuis des années.

L'arrivée des « passkeys » sur nos appareils pourrait être plus rapide que prévue. En effet, d'ici la fin de l'année, les géants du numérique (Apple, Google et Microsoft) confirment l'intégration des « passkeys » sur leurs appareils respectifs.

L'article du média « Le Monde » détaille le fonctionnement de ces « passkeys », le partage des clés entre les différentes marques d'appareils ainsi que les principaux obstacles auxquels doit faire face ce système.

En lire plus

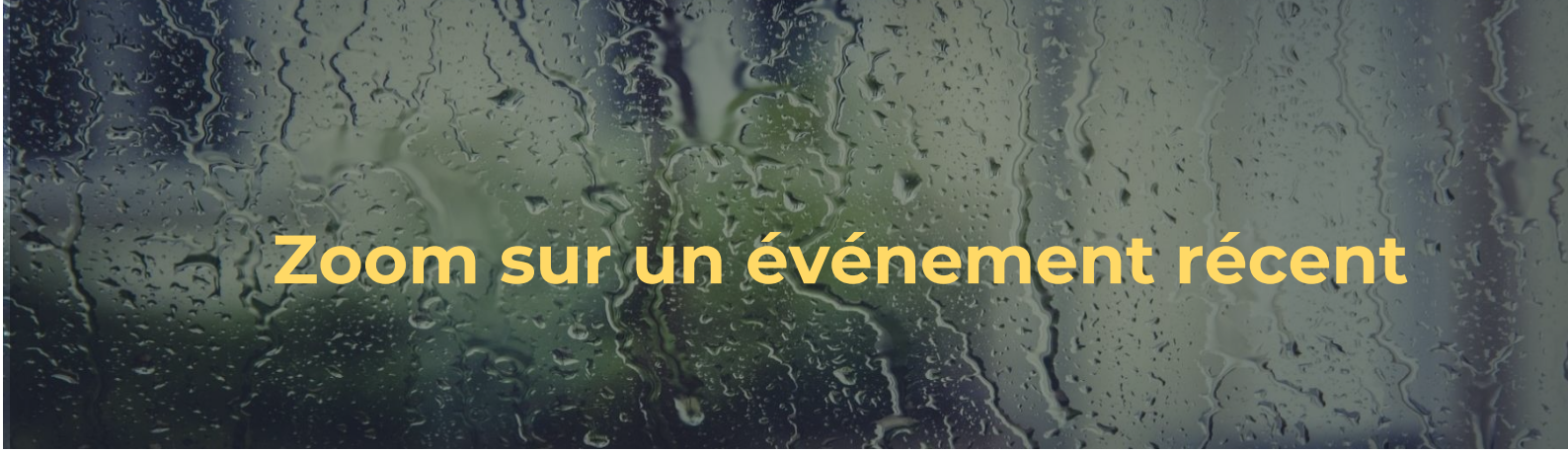
Le Cyber Resilience Act : La commission Européenne va imposer aux fabricants d'objets connectés un renforcement de la sécurité

La Commission européenne vient de proposer le jeudi 15 septembre 2022 un texte législatif ayant pour objectif d'encadrer la sécurité des appareils connectés et des produits numériques au sein de l'Union européenne.

Concrètement, ce nouveau texte vise à introduire des obligations en matière de cybersécurité auprès des fabricants. La réforme préconise également de mettre en place des obligations de suivi pour la gestion des vulnérabilités ainsi que l'imposition de mises à jour pendant au moins pendant cinq ans.

Pour faire respecter ces futures obligations, les sanctions administratives pourront aller jusqu'à 15 millions d'euros ou jusqu'à 2,5 % du chiffre d'affaires annuel mondial pour le régime de pénalités le plus élevé.

En lire plus



Zoom sur un événement récent

Retour sur la Cyberattaque du CHSF

Ecrit par Eloi GUILLAUD

Le Centre hospitalier sud francilien (CHSF) de Corbeil-Essonnes a été victime d'une attaque informatique de grande ampleur dans la nuit du samedi 20 au dimanche 21 août 2022. Une demande de rançon de 10 millions de dollars a été exigée par les initiateurs de l'attaque par ransomware.

L'attaque

Selon des sites spécialisés l'attaque aurait été conduite via le détournement du compte d'un prestataire externe au CHSF : la société Corilus et son programme Softalmo, client-serveur de gestion médicale et administrative des consultations d'ophtalmologie. La société Corilus n'a pas confirmé que l'attaque venait de son système mais a demandé à ses clients de déconnecter leur SI à son SI Softalmo.

Le groupe LockBit serait à l'origine de l'attaque. Cette attaque est en contradiction avec les « règles » édictées par le gang qui demande à ses affiliés de ne pas s'en prendre à des établissements de santé ou tout du moins de ne pas bloquer les services essentiels.

L'enquête a été confiée à la Gendarmerie Nationale. C'est aussi le ransomware LockBit 3 .0 qui avait paralysé le site de La Poste Mobile début juillet.

Le ransomware Lockbit

LockBit s'apparente à un ransomware en tant que service. Les parties qui le souhaitent versent un dépôt en vue d'attaques personnalisées à louer, et en récupèrent les bénéfices via une structure affiliée. Les paiements des rançons sont répartis entre l'équipe de développeurs de LockBit et les filiales à l'origine des attaques, qui perçoivent jusqu'à ¾ du montant de la rançon. Le ransomware LockBit a des comportements similaires à ceux des ransomwares ciblés.

Les attaques par Lockbit :

- **se propagent automatiquement** au sein d'une entreprise et ne nécessitent aucune gestion manuelle ;
- **sont ciblées** et non dispersées à tout va comme les spams.

En outre, Lockbit utilise des outils dans des schémas natifs présents dans la quasi-totalité des systèmes informatiques Windows. Les systèmes de sécurité de terminaux ont du mal à détecter les activités malveillantes.

Le ransomware dissimule le fichier de chiffrement exécutable en le remplaçant par un format de fichier image .PNG ordinaire afin de tromper les défenses du système.

Le groupe exploitant activement le ransomware Lockbit 3.0, a déjà ciblé plus de 1200 entité à travers le monde

Les conséquences de l'attaque

Les jours suivants l'attaque , l'ANSSI a déclaré que « le retour à la normale prendra plusieurs semaines ». A ce jour, tous les services ne sont pas encore rétablis.

N'ayant pas reçu la rançon exigée, les hackers ont commencé (depuis le 26 Septembre) à divulguer les données de près de 700 000 patients. Les négociations avec le GIGN n'ont pas permis d'obtenir le déchiffrement des systèmes de l'hôpital.

La lutte contre Lockbit et ses effets

Les mesures de protection restent assez classiques :

- implémentation de mots de passe forts ;
- activation de l'authentification multi-facteurs ;
- limitation des comptes à privilèges ;
- suppression des comptes obsolètes et inutilisés ;
- maîtrise des interconnexions avec des SI tiers de partenaires ;
- mises à jour des SI et des correctifs de sécurité ;
- disponibilité des sauvegardes.

En outre, d'après le comportement du groupe d'attaquant, il apparait évident qu'aucune confiance ne peut leur être attribuée, pas plus que de crédit sur leur soi-disant « code éthique».

En conclusion

Bien que les services principaux soient rétablis au CHSF, il faudra attendre jusqu'en 2024 pour reconstruire le S.I sur des bases solides. La restauration d'un S.I prend du temps, notamment parce qu'il faut s'assurer que le SI n'est plus compromis avant d'y rétablir les données et services sauvegardés.

Il est important de définir et surtout de tester le fonctionnement des modes dégradés des services d'une organisation (ce qui va jusqu'à s'assurer qu'il y a assez de fournitures de bureau pour opérer en « mode papier »). Il est également primordial, bien que difficile, de disposer d'une cartographie des données dans le SI. Cela permettra de déterminer ce qui est compromis, et ce qui ne l'est peut-être pas. Pour continuer à opérer une rentrée des urgences en mode dégradé, il est impératif que le service local du SAMU ne soit pas sur le même réseau que le reste de l'hôpital.

Cependant en définitive, pour continuer à dispenser les soins essentiels, tout repose sur la résilience du personnel hospitalier.

Les écueils d'une Homologation de Sécurité DR

Ecrit par Florian GILET et Sophie KADJI-POLA

L'Homologation de sécurité est régie par l'Instruction Interministérielle 901 (II901) qui exige que, tout système d'information traitant de données sensibles, doit faire l'objet d'une homologation de sécurité avant sa mise en service ainsi que par le titre 6.2 de l'Instruction Ministérielle n° 900 (IM900) sur la protection du secret et des informations diffusion restreinte et sensibles.

Ce cadre est obligatoire pour un certain nombre d'organisations manipulant des données sensibles (certaines administrations de l'état, entreprises dans le domaine de la Défense nationale ou la protection du potentiel scientifique et technique de la nation (PPST), établissements sous tutelle du MINARM ou du CEA/DAM…) mais son application est également recommandée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) à toute organisation comme préalable à l'instauration de la confiance dans ses systèmes d'information et leur exploitation.
A ce titre, l'ANSSI a édicté un guide méthodologique en 9 étapes permettant à une entité de mettre en œuvre un système d'information conforme aux exigences de sécurité de l'II 901 ainsi qu'un corpus documentaire permettant de documenter l'ensemble des éléments constitutifs du dossier d'homologation.

Ce corpus documentaire comporte l'ensemble des documents suivants :

- Stratégie d'Homologation (indispensable)
- Procédures d'Exploitation de Sécurité (indispensable)
- FEROS
- Analyse de Risques et Risques Résiduels (indispensable)
- Audit de sécurité et plan de remédiation
- Plan de Sécurité (indispensable)
- Plan d'amélioration continue de sécurité
- Matrice de conformité II901 :
- Décision d'homologation

L'homologation permet d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité acceptable pour le système d'information considéré.

L'homologation est délivrée par une **autorité d'homologation** interne à l'organisme (on parle d'auto-homologation) pour un système d'information donné avant sa mise en service opérationnelle.

L'autorité d'homologation est la personne physique chargée de prendre la décision d'homologuer le système en acceptant les éventuels risques résiduels. Son niveau hiérarchique dans l'organisation doit être suffisamment élevé pour lui permettre d'assumer les responsabilités rattachées à la décision (par exemple, Directeur Général (adjoint) ou Secrétaire Général)

Pour prendre cette décision, il est accompagné des **membres de la commission d'homologation,** choisis en fonction des métiers impactés par l'homologation (experts techniques ou fonctionnels).

Le rôle de la **commission d'homologation** est donc d'assister l'autorité d'homologation dans sa décision. Elle est notamment chargée de préparer la **décision d'homologation** en analysant l'ensemble des documents versés au dossier d'homologation et en se prononçant sur leur complétude et leur pertinence.

Difficultés rencontrées

Prononcer une décision d'homologation est une tâche d'autant plus compliquée que le **périmètre à homologuer** est important. L'erreur consiste à vouloir homologuer tout le système d'information existant sans se poser au préalable les questions suivantes :

- Où sont les informations sensibles cœur de l'entreprise ?
- Pourquoi ces informations doivent être protégées ?
- Qui est (sont) le(s) malveillant(s) ?
- Quelles sont les portes que l'on va fermer ?
- Qu'est-ce qui est homologable actuellement ?
- Qu'est-ce qui est homologable en cible

Par ailleurs, l'homologation de sécurité est un **projet à part entière** qui nécessite du temps, des ressources (internes ou externes), un budget dédié et un chef de projet. Or, trop souvent le temps nécessaire à la production de la documentation est sous-estimé : l'homologation est gérée en interne en plus des activités courantes des différents acteurs ce qui entraîne des retards de production de la documentation et donc de l'homologation.

Enfin, la **qualité du dossier d'homologation** est clé dans la prise de décision. Or, le processus de constitution du dossier met souvent en évidence le manque de formalisation de documentation des différents processus de sécurité dans l'entreprise : par exemple, des audits de sécurité sont régulièrement réalisés mais la mise en œuvre du plan de remédiation des vulnérabilités identifiées est incomplète et non suivie. Autre exemple, la cartographie des applications et les processus de sécurité (gestion des habilitations, plan de continuité des activités…) ne sont **pas documentés** et c'est au projet d'homologation qu'incombe leur formalisation alors que la charge n'avait pas été anticipée.

Bonnes pratiques

Pour mener à bien une homologation de sécurité, il convient de procéder comme suit :

- Au préalable, se poser les bonnes questions et cadrer le besoin.
- Rédiger une note de cadrage précisant le périmètre à homologuer, les besoins de sécurité du système, les acteurs-clé, la gouvernance à mettre en place et la feuille de route.
- Nommer les acteurs en interne et leur dégager du temps, nommer un chef de projet, allouer un budget dédié.

- Découper le projet en chantiers structurés les piloter de manière renforcée.
- Mener les ateliers d'analyse de risque avec les métiers (5 ateliers si Ebios RM)
- Aider à choisir les membres de la CH et de la désignation de l'AH.
- Rédiger et aider à la rédaction des procédures et documents
- Participer à la commission d'homologation.
- Une fois l'homologation prononcée, mettre en place un processus de maintien en condition de sécurité approprié et le piloter.
- Le Plan d'amélioration continue de la sécurité est un document clé, c'est souvent lui qui permettra une homologation malgré des risques résiduels (acceptation du risque) => ce plan doit être suivi d'actions et de comités de vérification.

En conclusion, l'homologation de sécurité est un processus complexe qui nécessite de bien identifier le besoin et le périmètre au préalable. Après une revue de l'existant, il convient ensuite de découper les travaux en chantiers bien structurés dans le cadre d'un projet auquel seront affectés un budget et des ressources dédiés et un planning réaliste.

SOC & SIEM… Kézako ?

Ecrit par Rick HAYOUN

Commençons par définir ce qu'est un **SOC** (Security Operations Center). C'est une plateforme d'administration et de supervision en temps réel permettant de suivre, détecter et remédier aux comportements anormaux et aux failles de sécurité.

Pour y parvenir, elle s'appuie sur son principal allié, le **SIEM** (Security Information and Event Management) qui permet de collecter, normaliser, corréler et fournir des rapports de sécurité sur tous les évènements qui ont lieu au sein d'un SI. Cependant, le nombre d'évènements au sein d'un SI est gigantesque et ne peut pas être géré à taille humaine. L'objectif est donc d'anticiper les comportements jugés à risque et de définir des alertes afin que les analystes du SOC se focalisent uniquement sur de réels comportements suspicieux.

La collecte des logs se fait à partir de sources hétérogènes telles que des pares-feux, des annuaires d'authentification ou encore des formats divers comme Syslog, SNMP, etc. Ils sont ensuite enregistrés dans un format brut et, dans la plupart des cas, il faut passer par une étape de **normalisation** afin que ces logs soient reconnus et traités par le SIEM. Vient ensuite l'étape de **la corrélation** qui consiste à relier plusieurs évènements pouvant aboutir à la détection d'un comportement anormal ou malicieux puis à lever des alertes de sécurité si ces évènements se produisent. Enfin, il est également possible **d'établir des rapports** si l'on souhaite avoir une vue synthétisée sur l'interface du SIEM.

Pour faire simple, imaginons que le format d'un log attendu par notre SIEM ressemble à cela : *MMM JJ HH:MM:SS @IP Hostname Product Version EventID Description ;* et que l'on reçoive des logs d'une source quelconque qui ne respecte pas ce format ; il faudra passer par l'étape de normalisation afin de réécrire le log sous le bon format pour qu'il puisse être compris et catégorisé comme il se doit par le SIEM. Une fois normalisés, les logs peuvent être corrélés afin de lever des alertes concrètes pour l'équipe SOC. Elles consistent en une succession de OU et de ET afin de parvenir à un scénario complet.

Créons une règle de sécurité contre les attaques par force brute sur un compte administrateur (tentative de crack de mot de passe) :

1. Si l'utilisateur appartient au groupe « Admins »

ET

2. Si l'utilisateur rate 5 authentifications en 10 secondes

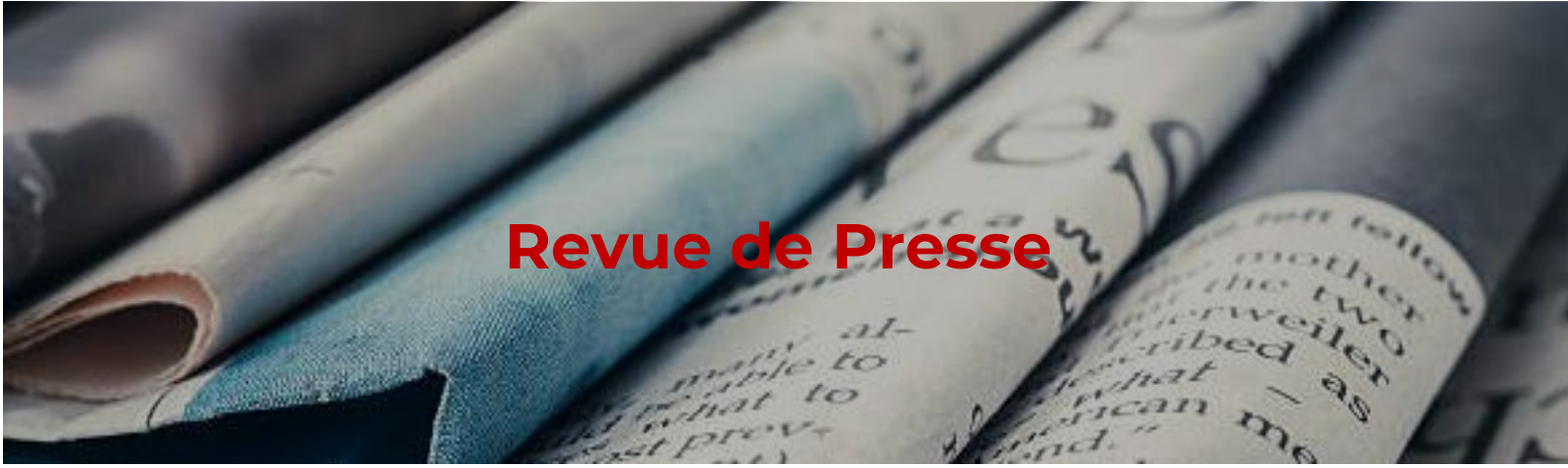
alors lever l'alerte « Brut Force Admin ».

Les conditions doivent être **précises et exhaustives** afin de ne pas générer trop de faux positifs (alerte levée sans qu'il n'y ait de réelle menace) ni de faux négatifs (l'alerte ne se lève pas alors qu'il y a une menace).

Or, ces configurations sont manuelles, compliquées et fastidieuses, sans compter le fait qu'il est impossible pour un SIEM de détecter des failles encore non dévoilées (zero-day).

Dans le cadre de nos activités de conseil et d'intégration nous avons trouvé intéressant *de renforcer le dispositif avec des solutions faisant appel à de l'Intelligence Artificielle (IA*).

Nous vous en dirons davantage dans un prochain article dédié à ce sujet.



Revue de Presse

1

Les hôpitaux, cibles de choix des cybercriminels

Les systèmes d'information des hôpitaux vulnérables aux cyberattaques.

Le 20 août, le centre hospitalier de Corbeil-Essonnes a subi une cyberattaque d'envergure (ransomware) qui a paralysé une partie importante de son système d'information. Cet événement montre une nouvelle fois que les hôpitaux sont devenus des cibles privilégiées par les cybercriminels depuis plusieurs années. Plusieurs raisons peuvent expliquer cela...

En lire plus

2

La sécurisation de données dans le cadre du travail hybride

Le développement du travail hybride depuis la crise sanitaire augmente les failles de sécurité et les comportements à risque.

La récente crise sanitaire ayant touché le monde entier a obligé les entreprises à mettre en place urgemment une organisation de travail hybride pour leurs collaborateurs. Cette pratique a renforcé les failles de sécurité et a engendré l'apparition de nouveaux comportements à risque. La protection des données doit être considérée comme un enjeu majeur de sécurité pour les entreprises et ses collaborateurs. Cela implique l'adoption de bonnes pratiques pour protéger les données sensibles.

En lire plus

3

L'urgence de former les équipes à la sécurité informatique

65 % des organisations ont signalé une hausse du nombre d'attaques pendant la pandémie.

Pour faire face à la pandémie, les entreprise ont dû mettre en place dans l'urgence des environnements de travail à distance. Malheureusement, la plupart de ces environnements ne sont pas suffisamment sécurisés et les cybercriminels en ont profités pour intensifier leurs activités malveillantes. L'erreur humaine étant à l'origine de la majorité des cyberattaques réussies et dans un contexte de montée de la cybercriminalité, il devient urgent d'agir auprès des collaborateurs pour les sensibiliser et les (in)former sur l'adoption de nouveaux réflexes en matière de sécurité.

En lire plus

4

Villes, hôpitaux, services publics... Peuvent-ils résister aux cyberattaques ?

La menace d'une nouvelle cyberattaque plane sur les différentes administrations.

Récemment des cyberattaques d'envergure ont ciblé des administrations comme l'hôpital de Corbeil-Essonnes cet été et la ville de Caen au mois de septembre. Les conséquences d'une cyberattaque sur une administration peuvent être désastreuses, par exemple selon l'ANSSI, il faut environ deux ans à une ville attaquée pour se remettre sur pied. On constate que ces dernières années, des mesures ont été mises en place pour tenter de protéger les plus importantes administrations comme la loi de Programmation militaire qui vise à améliorer la sécurité des opérateurs dits « d'importance vitale ». Néanmoins, les moyens (Temps, Personnel, Finances, etc.) semblent manquer pour les plus petites administrations comme les petites villes ou les hôpitaux.

En lire plus