|  |  |  |
| --- | --- | --- |
| logo | Registre des vulnérabilités | 1074 |

Responsable :

Mis à jour :

Une vulnérabilité est une faiblesse dans n'importe quel élément du système informatique qui peut être utilisée pour causer des dommages. Cela concerne tous les systèmes, réseaux, bases de données et applications.

La politique Vulnérabilités techniques permet d’identifier, évaluer et répondre aux vulnérabilités connues.

Les vulnérabilités techniques évoluent chaque jour. Le site [CERT-FR](https://www.cert.ssi.gouv.fr/) montre les dernières informations concernant :

* les alertes de sécurité (prévenir d’un danger immédiat)
* les menaces et incidents (l'état des connaissances et les investigations de l'ANSSI en analyse de la menace et traitements d'incidents)
* les avis de sécurité (faisant état de vulnérabilités et des moyens de s'en prémunir)
* les indicateurs de compromission (qualifiés ou non par l'ANSSI, partagés à des fins de préventions)

Quelques questions à se poser pour en tirer les conséquences :

* quelles compétences n’avions-nous pas ?
* quelles sont les mesures inappropriées que nous avons prises ?
* quelles mesures n’avons-nous pas prises à temps ?
* en quoi avons-nous perdu le plus de temps ?
* quelles informations nous n’avions pas ?
* quelles sont les documents qui n’étaient pas à jour ?
* quelles erreurs de communication avons-nous faites ?

Leçons apprises d’un incident :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| N° | Incident | Date | Action entreprise | Analyse des événements | Conclusions des décisions prises | Remarque |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Quelques exemples de vulnérabilités :

* altération du fichier support de données
* blocage des comptes utilisateurs
* classification inadéquate des informations
* connexion au réseau public non protégée
* contrôle insuffisant de l'accès physique
* destruction de média support de données
* destruction de média support de logiciel
* destruction d'un équipement
* disparition de média support de logiciel
* disparition d'un moyen nécessaire pour l'accès aux données (clés logiques ou physiques)
* divulgation de fichier support de données
* divulgation de média support de données
* effacement de configurations logicielles
* effacement du fichier support de données
* formation et sensibilisation insuffisantes du personnel à la sécurité
* gestion du changement inadéquate
* inaccessibilité à un local
* logiciels mal documentés
* manque de documentation
* manque de politique d'utilisation de la cryptographie
* manque de procédure pour la suppression des droits d'accès en cas de rupture de contrat
* manque de protection contre les désastres naturels
* manque de protection des équipements mobiles
* manque de restriction d’utilisation d’Internet
* matériels non protégés contre des variations :
  + de tension
  + d'humidité
  + de température
* mauvaise gestion des mots de passe
* mauvaise protection des clés cryptographiques
* mettre au rebut des supports de stockage sans effacer les données
* mots de passe par défaut ne sont pas modifiés
* non fonctionnement d’un logiciel (bug)
* non fonctionnement d'un équipement
* perte de données en transit ou messages
* perte des moyens nécessaires à la connexion au service
* programme d’audit interne non réalisé à temps
* sauvegarde irrégulière
* sécurité insuffisante du câblage
* séparation inadéquate des installations opérationnelles et d'essai
* système d'identification et d'authentification mal protégé
* tests insuffisants des logiciels
* trop d’accès privilégiés
* utilisation non raisonnable des systèmes d'information

Registre des vulnérabilités :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| N° | Vulnérabilité | Date | Apparition | Action entreprise | Analyse des événements | Remarque |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |