VEILLE INFORMATIQUE

#CYBERSECURITE :

Δ Articles ANSSI :

Recommandations relatives à l'authentification multi-facteur et aux mots de passe[1]

- A cet article est relié une mise-à-jour du guide du même nom et est daté du 08/10/2021. Ce guide traite de l'authentification (de personnes vis-à-vis de machines) sur différente plateforme et a pour objectif de constituer un support technique pour accompagner une analyse de risque. Les principales recommandations mise en avant dans ce guide sont :
    - Mener une analyse de risque lors de la mise en place de moyens d'authentification,
    - Privilégier l'utilisation de l'authentification multi-facteur,
    - Privilégier l'utilisation de l'authentification reposant sur un facteur de possession (carte d'identité, jeton de sécurité, téléphone …),
    - Adapter la robustesse d'un mot de passe à son contexte d'utilisation,
    - Utiliser un coffre-fort de mots de passe (ex KeePass).

  Il présente un nombre de règle pour suivre ces recommandations :

    - R1 : Privilégier l'authentification multifacteur
    - R2 : Privilégier l'utilisation de moyens d'authentification forts
    - R3 : Conduire une analyse de risque
    - R4 : Créer les facteurs d'authentification dans un environnement maîtrisé
    - R5 : Générer les éléments aléatoires avec un générateur de nombres aléatoires robuste

[1] https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/

- R6 : 6 Remettre les facteurs d'authentification au travers de canaux sécurisés
- R7 : Mettre en place un processus de renouvellement des facteurs d'authentification
- R8 : Ne pas utiliser le SMS comme moyen de réception d'un facteur d'authentification
- R9 : Conserver les historiques d'utilisation des facteurs d'authentification
- R10 : Limiter dans le temps le nombre de tentatives d'authentification
- R11 : Réaliser l'authentification au travers d'un canal sécurisé
- R12 : Limiter la durée de validité d'une session authentifiée
- R13 : Protéger les données d'authentification stockées par le vérifieur
- R14 : Ne pas donner d'information sur l'échec de l'authentification
- R15 : Définir un délai d'expiration des facteurs d'authentification
- R16 : Définir une politique d'utilisation des facteurs d'authentification
- R17 : Sensibiliser les utilisateurs à la sécurité de l'authentification
- R18 : Mettre en place un processus de révocation des facteurs d'authentification
- R19 : Définir des délais adaptés de prise en compte des révocations
- R20 : Mettre en place une politique de sécurité des mots de passe
- R21 : Imposer une longueur minimale pour les mots de passe
- R22 : Ne pas imposer de longueur maximale pour les mots de passe
- R23 : Mettre en œuvre des règles sur la complexité des mots de passe
- R24 : Ne pas imposer par défaut de délai d'expiration sur les mots de passe des comptes non sensibles
- R25 : Imposer un délai d'expiration sur les mots de passe des comptes à privilèges
- R26 : Révoquer immédiatement les mots de passe en cas de compromission suspectée ou avérée

- R27 : Mettre en place un contrôle de la robustesse des mots de passe lors de leur création ou de leur renouvellement
- R28 : Utiliser un sel aléatoire long
- R29 : Utiliser une fonction de dérivation de mots de passe memory-hard pour conserver les mots de passe OU Utiliser une fonction de dérivation de mots de passe itérative pour conserver les mots de passe
- R30 : Proposer une méthode de recouvrement d'accès
- R31 : Mettre à disposition un coffre-fort de mots de passe
- R32 : [Utilisateur] Utiliser des mots de passe robustes
- R33 : [Utilisateur] Utiliser un mot de passe différent pour chaque service
- R34 : [Utilisateur] Utiliser un coffre-fort de mots de passe
- R35 : [Utilisateur] Protéger ses mots de passe
- R36 : [Utilisateur] Utiliser un mot de passe robuste pour l'accès à sa messagerie électronique
- R37 : [Utilisateur] Choisir un mot de passe sans information personnelle
- R38 : [Utilisateur] Modifier les mots de passe par défaut
- R39 : Utiliser un facteur de possession intégrant un composant de sécurité qualifié ou certifié / Utiliser un facteur de possession intégrant un composant de sécurité / Utiliser un facteur de possession même sans composant de sécurité
- R40 : Ne pas utiliser un facteur inhérent comme unique facteur d'authentification
- R41 : Utiliser un facteur inhérent uniquement associé à un facteur d'authentification fort
- R42 : Favoriser une rencontre en présence lors de l'enregistrement d'un facteur inhérent

#ACTUALITE

- 14/10/2021 - Alerte de Sécurité publié par Apple : Il faut mettre à jour son système d'exploitation iOS et iPad Os, car elle corrige une faille de sécurité critique et activement exploitée - Source : Cybermalveillance.gouv.fr

- 14/10/2021 - Google fait le bilan après avoir analysé 80 millions d'échantillons de ransomwares sur VirusTotal : Il en ressort un total de 130 familles de ransomwares, distribuant près de 30 000 virus, sur la période de janvier 2020 à septembre 2021 donc les 3 cibles principales ont été l'Israël, la Corée du Sud et le Vietnam. Ce rapport a pour objectif de fournir des données aux entreprises et aux organismes publicq dans le but d'adapter leur stratégie de sécurité informatique. Les familles de ransomwares les plus actives étant : GandCrab, Babuk, Cerber, Matsnu, Congur, Locky, Teslacrypt, Rkor et Reveon. - Source : L'UsineDigitale