CEO-VISION
Technology made simple

TRIBUNE

• SÉCURITÉ DES DONNÉES • DIGITAL WORKPLACE
• COLLABORATION • SERVEUR DE FICHIERS

La Digital Workplace Open Source au service de la sécurité de votre SI

CEO-Vision est l'entreprise éditrice de la solution GoFAST Digital Workplace : une alternative innovante et Open Source à Office 365, SharePoint, Teams.

Depuis 10 ans CEO-Vision accompagne les utilisateurs de GoFAST pour concilier les bonnes pratiques de sécurité avec les nouveaux usages : accès simple et à tout moment à ses outils, documents et processus métiers, sans dépendre d'un VPN, ni d'un PC pro, au bureau ou en télétravail pour collaborer avec ses collègues et ses partenaires externes.

La cible principale des ransomwares : le serveur de fichiers classique

Parmi les systèmes les plus vulnérables, le serveur de fichiers classique Windows est la cible de la plupart des attaques de ransomware, avec des **conséquences catastrophiques** : plusieurs jours à plusieurs semaines d'interruption de service. On peut citer les ransomware Ryuk, Egregor, Ragnar Locker, Clop, Maze, Wanna Cry, Petya[1]...

Amélioration significative de la gestion documentaire

Diminution des échanges de documents par emails

Sécurisation optimale des données

De nombreuses villes ont été touchées ces derniers mois, ainsi que des hôpitaux, Dassault Aviation US, Sopra-Steria, Wagons-Lits, CMA-CGM... En général, ce type d'attaques se déclenchent à la suite de **l'ouverture d'un email ou pièce-jointe** sur un poste n'ayant pas d'antivirus à jour. L'ensemble du serveur de fichiers est alors verrouillé et une rançon importante est exigée (parfois plusieurs millions) pour pouvoir récupérer ses données. Selon l'ANSSI en octobre 2020, Ryuk serait responsable de **75 % des attaques sur le secteur de la santé**, secteur qu'il attaquerait depuis début 2019.

Dans certains cas, les données sont en plus subtilisées et les pirates menacent de diffuser les contenus sensibles. Les opérateurs du ransomware Ragnar Locker avaient divulgué des données volées à l'avionneur Dassault Falcon Jet (une archive présentée comme pesant 3,5 Go et nommée Falcon 6x project Archive.7z).

GoFAST Digital Workplace pour protéger les données contre les ransomwares

La sécurité des données dépend à la fois des technologies et du type et lieu d'hébergement, mais aussi des bonnes pratiques des utilisateurs. Le concept GoFAST Digital Workplace tient compte de ces facteurs clefs pour un niveau de sécurité optimal face aux ransomwares.

Avant tout, l'accès à la plateforme et donc aux documents, se fait directement via le navigateur web, totalement cloisonné du poste de travail. **Cela réduit significativement le risque de contaminer la base documentaire à partir d'un fichier qui serait présent sur le poste de travail**.

GoFAST permet toutefois le montage d'un lecteur réseau Windows (WebDAV). Certains utilisateurs peuvent donc créer un lien entre leur poste de travail et la plateforme. Très pratique dans les cas des reprises de données, cet usage reste vivement déconseillé en temps normal.

Dans tous les cas, **la gestion fine des accès aux espaces collaboratifs limite le risque**. En effet, la gestion documentaire par les responsables métiers est séparée de l'administration système. Aucun compte-utilisateur n'a donc accès à tout l'entrepôt ! Dans le cas où un ransomware vient à toucher la plateforme, celui-ci n'affecterait qu'une partie restreinte des documents (selon les accès du compte-utilisateur victime).

[1] https://attack.mitre.org/techniques/T1486/

Les bénéfices de l'utilisation de GoFAST Digital Workplace

- La plateforme GoFAST dédiée "**Cloud Act free**" : soit On Premise, soit en SaaS souverain : hébergement SecNum Cloud possible avec notre partenaire Outscale
- Un accès sécurisé aux documents, gestion métier séparée de l'administration système RGPD
- ***Versionning*** automatique des modifications des fichiers et dans le cas d'un cryptage, il est possible de récupérer les versions précédentes,
- **Zéro pièce-jointe** : fichiers partagés via des liens sécurisés (audités, limités dans le temps),
- Gestion de l'**authentification** déléguée à l'annuaire interne (AD/LDAP) pour respecter votre politique de gestion des mots de passe ou SSO.
- **Technologie Open Source** : auditez votre plateforme jusqu'aux sources ("boîte blanche")
- Offre qui comprend la **veille sécurité, les audits automatisés et les correctifs de type Hotfix** nécessaires sur tous les composants Open Source. Cela décharge les DSI d'un travail très important et évite d'avoir des composants obsolètes vulnérables

À propos de CEO-Vision

CEO-Vision est l'éditeur de GoFAST : le Digital Workplace au service des organisations et de leurs utilisateurs pour gagner en productivité. Il est une alternative unique et open source à Office365, Sharepoint, Google Workplace... Sa devise : "technology made simple". Son savoir-faire est concentré sur des technologies Open-Source :

- **Drupal** pour les Portails (CMS),
- **Alfresco** pour la Gestion Électronique de Documents (GED),
- **Element et Jitsi.meet** (messagerie instantanée et webconférence)
- **Bonitasoft** (Workflows),
- **OnlyOffice** (Suite Collaborative Office)
- **Solr Apache** (Moteur de recherche)

Les ransomwares cryptent les documents pour en bloquer l'accès, mais comme GoFAST sauvegarde automatiquement chaque version, il est toujours possible de récupérer les versions précédentes non cryptées. Contrairement à une attaque sur serveur de fichiers, non seulement les documents sont récupérés, mais le travail de la journée est préservé.

Selon notre politique de sécurité sur la protection du serveur GoFAST, celui-ci embarque de nombreuses protections comme un antivirus, un IDS (Intrusion Detecting System), un Mandatory Access Control permission system (MAC) basé sur "selinux", et bien d'autres protections, pare-feu et reverse proxy intégré.

Des audits de la solution pour toujours plus de sécurité

GoFAST Enterprise vient avec une politique de mise à jour très stricte, notamment au niveau des correctifs de potentielles failles exploitables, avec des audits réguliers (Web Application Vulnerability Scanner de la société leader Tenable) pour détecter rapidement toute faille connue. De même, la communauté Open Source très présente, contribue à la forte réactivité dans leur identification et les mises-à-jour des technologies intégrées à GoFAST, ce qui est rarement le cas sur des serveurs de fichiers internes. Pour les solutions GAFAM, il n'est pas possible de faire des audits en boîte blanche, les sources n'étant pas disponibles.

À noter que la "charge utile" (partie offensive du malware) est souvent véhiculée par des macros VBA dans des fichiers bureautiques MS-Office (partie "transport", c'est-à-dire le Cheval de Troie). Dans ces cas, tant que les utilisateurs ne font que consulter l'aperçu du document sur l'interface Web, sans l'éditer avec leur MS-Office, il n'y a aucun risque.

Reste donc uniquement le cas, d'un utilisateur sans antivirus à jour et qui dépose un fichier infecté sur GoFAST, puis que celui-ci soit ouvert en édition par un autre utilisateur, ayant lui aussi un anti-virus non à jour. Si aucun montage réseau, il n'y a aucun dommage sur les autres fichiers stockés sur GoFAST.

GoFAST apporte donc de nombreuses protections supplémentaires par rapport à un serveur de fichiers Windows, même lorsque la sécurité de base du poste de travail est compromise.