

Etude de cas : Cyberattaque

Departement 77

Présenté par :

BAYERE Abdoul Fatahou

Sommaire

I. Introduction.....	1
II. Contexte de l'Attaque.....	1
III. Outils de Surveillance et Réponse à l'Attaque.....	1
IV. Politiques de Sécurité Renforcées.....	2
Authentification multifacteur (MFA).....	2
Limitation des horaires d'accès.....	2
V. Impact et Conséquences de l'Attaque.....	3
A. Communication avec les médias et le public.....	3
B. Coûts estimés de l'attaque.....	3
C. Impact sur l'image du département.....	3
D. Transmission de l'information et coordination interne.....	4
E. Rôle du Service Hotline et Mesures de Sécurité.....	4
F. Gestion de l'Exploitation des Serveurs et Sauvegardes.....	6
a. Les mission effectués.....	8
G. Infrastructure Réseau et Sécurisation.....	15
a. Infrastructure réseau - pare feux.....	16
H. Audits de Sécurité et Simulations d'Attaques.....	18
I. Stratégie de Formation en Cybersécurité et Préparation Future.....	18
VI. Bibliographie.....	19

I. Introduction

Le **6 novembre 2023**, le département 77 a été la cible d'une attaque par ransomware, paralysant l'ensemble de son système informatique. Face à cette menace, des mesures d'urgence ont été déployées pour contenir l'attaque, restaurer les services et renforcer la sécurité du réseau.

II. Contexte de l'Attaque

L'attaque a été déclenchée par une tentative de phishing, permettant aux attaquants d'obtenir des identifiants de connexion Citrix, un outil de bureau à distance. Une fois infiltrés dans le réseau, ils ont discrètement observé l'environnement jusqu'à identifier une faille zero-day, une vulnérabilité encore inconnue et non corrigée. Exploitant cette brèche, ils ont pu progresser au sein du système avant de déclencher une attaque par ransomware, chiffrant ainsi les données du département et paralysant ses services.

III. Outils de Surveillance et Réponse à l'Attaque

Suite à l'attaque, bien que les antivirus utilisés soient efficaces, ils restent néanmoins limités face à des menaces toujours plus sophistiquées, car ils reposent sur une base de menaces connues. Pour pallier cette lacune, un logiciel de surveillance des menaces, Sentinelle One qui s'appuie sur l'intelligence artificielle et l'analyse de données a été mis en place. Cet outil utilise la technologie Endpoint Detection and Response (EDR) pour détecter de manière proactive les menaces. Il collecte et analyse des données provenant des connexions réseau, de l'utilisation de la mémoire et du disque, ainsi que de l'accès à la base de données centrale. Ces informations sont ensuite acheminées vers un moteur d'analyse EDR, capable de repérer des comportements anormaux et d'anticiper, par exemple, des attaques de type zero-day. Dès la détection de

comportements suspects, l'EDR peut alors prendre des mesures immédiates telles que le blocage de processus, l'interruption d'exécution ou la mise en quarantaine de fichiers, permettant ainsi au département d'anticiper et de contrer efficacement de futures attaques.

IV. Politiques de Sécurité Renforcées

Dans le cadre du renforcement de la sécurité des systèmes, plusieurs mesures ont été mises en place :

Authentification multifacteur (MFA)

L'implémentation de l'authentification multifacteur représente une avancée majeure dans la sécurisation des accès aux systèmes critiques. Désormais, en plus de leur mot de passe, les utilisateurs doivent fournir un second facteur d'authentification, tel qu'un code envoyé sur un dispositif mobile ou une application dédiée. Cette double vérification réduit considérablement le risque d'accès non autorisé, même en cas de compromission des identifiants.

Limitation des horaires d'accès

Pour minimiser l'exposition du réseau aux tentatives d'intrusion, des plages horaires d'accès ont été instaurées. Les connexions aux ressources du département sont désormais restreintes aux heures d'activité préétablies, réduisant ainsi les risques d'attaques hors période de surveillance. Cette mesure permet d'optimiser le contrôle des accès et de renforcer la sécurité globale du système.

V. Impact et Conséquences de l'Attaque

A. Communication avec les médias et le public

Face à l'attaque, le département 77 a adopté une stratégie de communication transparente et proactive. Des communiqués de presse officiels ont été diffusés pour informer la population et les médias de la situation, des mesures prises et de la continuité des services publics. Les mises à jour régulières sur le site internet et via les réseaux sociaux ont permis de rassurer le public et de démontrer le contrôle de la crise. (<https://www.interstis.fr/blog/la-cyberattaque-du-departement-seine-et-marne/>)

B. Coûts estimés de l'attaque

Les impacts financiers ont été évalués à plusieurs millions d'euros. Les dépenses englobent la migration des systèmes, la restauration des données, l'achat de nouveaux équipements, la mise en place d'une solution EDR ainsi que le changement ou l'achat de nouveaux firewalls. Ces investissements, bien que lourds, étaient indispensables pour sécuriser durablement les infrastructures du département. (<https://www.lemondeinformatique.fr/actualites/lire-le-departement-de-la-seine-et-marne-paralyse-par-une-cyberattaque-88540.html>)

C. Impact sur l'image du département

L'image du département 77 a été affectée par cette cyberattaque, notamment par la perturbation temporaire des services. Toutefois, grâce à une gestion rapide et efficace de la crise, illustrée par des mesures correctives et une communication transparente, le département a su démontrer sa résilience. En l'espace d'un an, la confiance des administrés a été progressivement restaurée.

D. Transmission de l'information et coordination interne

La gestion de la crise s'est appuyée sur l'organisation de réunions de crise régulières, permettant une coordination étroite entre les différents services et niveaux de gestion. Par ailleurs, des solutions de communication sécurisée (notamment par email) ont été mises en place pour assurer une diffusion rapide et fiable de l'information, malgré les contraintes imposées par l'attaque. Ces outils ont permis à l'ensemble des équipes de réagir efficacement et de repartir sur des bases renforcées.

La cyberattaque ayant immobilisé des services essentiels de la DSI, nous allons maintenant examiner les rôles et les mesures de sécurité appliqués au sein du service.

E. Rôle du Service Hotline et Mesures de Sécurité

Le service hotline du département est une assistance technique en direct destinée à aider les agents et à résoudre rapidement leurs problèmes informatiques. Concrètement, dès qu'un problème survient, l'agent contacte le service hotline, qui procède à :

1. **Réception de l'appel**
2. **Identification** (ex : demande de matricule pour confirmer l'identité, démarche également utilisée à des fins de sécurité)
3. **Diagnostic de l'incident**
4. **Résolution du problème** ou, si nécessaire,
5. **Transfert au niveau 2 ou 3 (prestataire, éditeur)**

Ce service s'appuie sur divers outils :

- **Zoom Workspace** : Gestion des communications et des réunions à distance.
- **Pytheas (GLPI)** : Système de gestion des tickets d'incident et de demandes.
- **TeamViewer tensor** : Connexion à distance sécurisée pour la résolution des problèmes

Exemples d'incidents observés :

- **Problème d'accès au disque dur** : En raison des mesures de sécurité, le département chiffre les données. Pour les décrypter, il est nécessaire de récupérer les clés BitLocker, soit via l'Active Directory (AD), soit par le Centre d'administration Microsoft Entra.
- **Problème d'enrôlement pour l'authentification (QR code)**
- **Problème de connexion lié à l'authentification par clé et mot de passe** : L'agent demande une modification de mot de passe, mais étant donné la présence de la clé d'authentification, le technicien préfère transférer l'incident au niveau 2 pour éviter tout risque.
- **Oubli du mot de passe d'un compte de domaine** : Accès à l'AD pour réinitialiser le mot de passe.
- **Oubli du mot de passe d'un compte professionnel** : Accompagnement de l'agent étape par étape pour résoudre le problème.
- **Problème de licence/certificat**
- **Écran noir, problème d'affichage sous Windows** : Les techniciens ont mis en place un contournement pour résoudre temporairement le problème, mais l'incident reste en suspens. Un ticket a été envoyé à Microsoft sans retour pour le moment.
- **Connexion à distance pour installation de logiciels**
- **Problème d'accès à Internet**

Mesures de sécurité :

En termes de sécurité au sein de ce service, la DSI a choisi d'utiliser teamviewer tensor qui est une solution de téléassistance conçue pour faciliter l'accès et le contrôle à distance des postes de travail tout en répondant aux exigences de sécurité.

Le choix de TeamViewer Tensor pour le service hotline repose sur ses fonctionnalités de sécurité et de gestion avancées. La plateforme assure un chiffrement de bout en bout avec un échange de clés RSA (4096 bits) et un encodage AES (256 bits), garantissant la confidentialité des communications. L'authentification à deux facteurs (MFA) renforce la protection en limitant l'accès aux seuls utilisateurs autorisés. De plus, les journaux d'audit détaillés offrent une traçabilité complète, assurant le suivi de toutes les actions réalisées.

F. Gestion de l'Exploitation des Serveurs et Sauvegardes

Service d'exploitation :



Salle de datacenter

Le datacenter est une salle dédiée à l'hébergement de serveurs. Au sein du département, cette salle abrite des serveurs de logs, des serveurs de sauvegarde ainsi que des serveurs qui hébergent leurs applications.

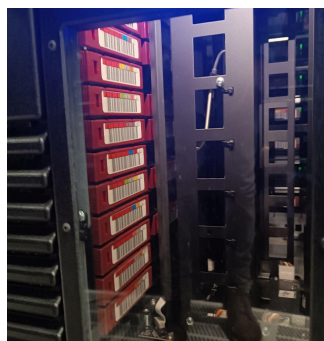
Au sein de la DSI, il existe un service d'exploitation chargé de garantir l'intégrité des données et de s'assurer qu'aucun problème n'est survenu lors des sauvegardes, réalisées à l'aide du logiciel Veeam Backup. Ce logiciel leur permet de suivre l'avancement et l'état des sauvegardes. Ils utilisent également un logiciel de supervision pour veiller à ce que les serveurs restent fonctionnels.

Les sauvegardes contiennent tout les modification enregistrés par les utilisateurs, et sont organisés de cette façon :

- les jours de la semaines ils effectuez des sauvegardes incrémentielles
- et le vendredi soir ils effectués une sauvegarde complètes
- sauvegarde mensuelles et hebdomadaire

Pour effectuer des sauvegarde on utilise ce qu'on appelle des bandes

En termes de sécurité, le département a veillé à ce que les sauvegardes soient stockées à la fois au sein du département et sur un autre site. Ainsi, en cas d'attaque, la restauration pourra se faire sans problème. Cette méthode existait déjà avant l'attaque, mais sa mise en œuvre est devenue plus stricte depuis cet incident.



a. Les mission effectués

Ce service s'occupe de certains tickets concernant la restauration de fichiers et l'attribution des droits soit des bouts mail soit à des lecteurs.

Résolution d'incident sur Pytheas :






Réception de ticket concernant l'ajout de droits à un dossier soit en modification soit en lecture.

INT - 130679

INT - 130680

INT - 130602

INT - 130627

 Outils ▾  Que voulez vous faire ▾

Intervention

N° Interne	INT - 130602	Parent	REQ - 94877	Etat*	Affectée
Créé	14/01/2025 09:58:24			Provenance	Demande
Désignation	Accès répertoire partagé réseau				
Utilisateur	[redacted]@departement77.fr/ [redacted]				
Site du bénéficiaire	TOURNAN-EN-BRIE				

Détail de l'intervention

Description/Actions

SLA

Divers

Documents

Autres objets liés

Equipements

Type

Accès répertoire partagé réseau

Description

Type d'accès : Lecture
Chemin réseau et nom de répertoire : G:\Tournan\Secrétariat ASE
Groupe d'utilisateurs :
Informations complémentaires :

Solution

Ressource*

DSIN-SDI-EXP /Grp-dsin-sdi-exp@departement77.fr/

Intervenant

Dans un premier temps, on cherche l'utilisateur en question dans l'AD.

Rechercher Utilisateurs, contacts et groupes

Fichier Edition Affichage

Rechercher : Utilisateurs, contacts et groupes Dans : cg77.infra Parcourir...

Utilisateurs, contacts et groupes Avancé

Nom : [Redacted]

Description : [Empty]

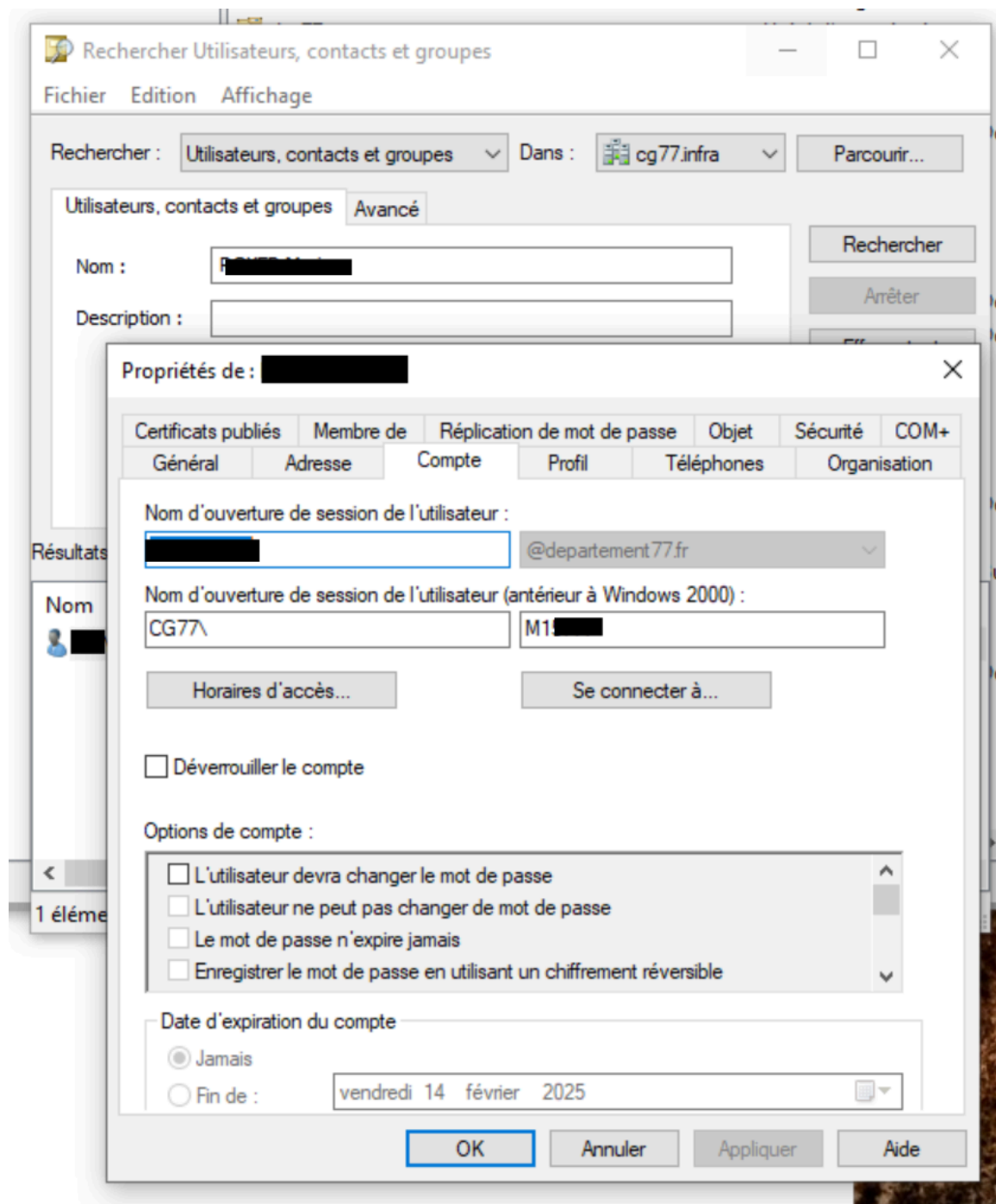
Rechercher Arrêter Effacer tout

Résultats de la recherche :

Nom	Type
[Redacted]	Utilisateur

1 élément(s) trouvé(s)

Ici, nous récupérons son numéro de matricule, qui sera utilisé dans un script pour afficher les lecteurs auxquels il a accès.

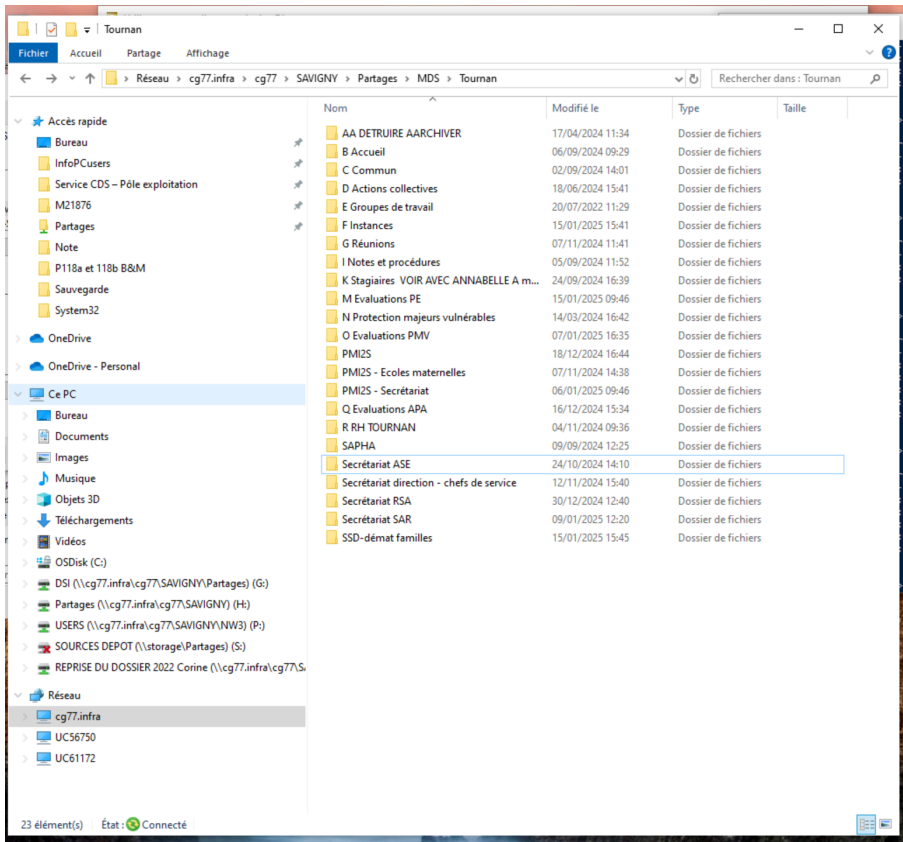


```
PS C:\Users\██████_SU\Desktop> .\Get-ADUserLectrezo.ps1 ██████

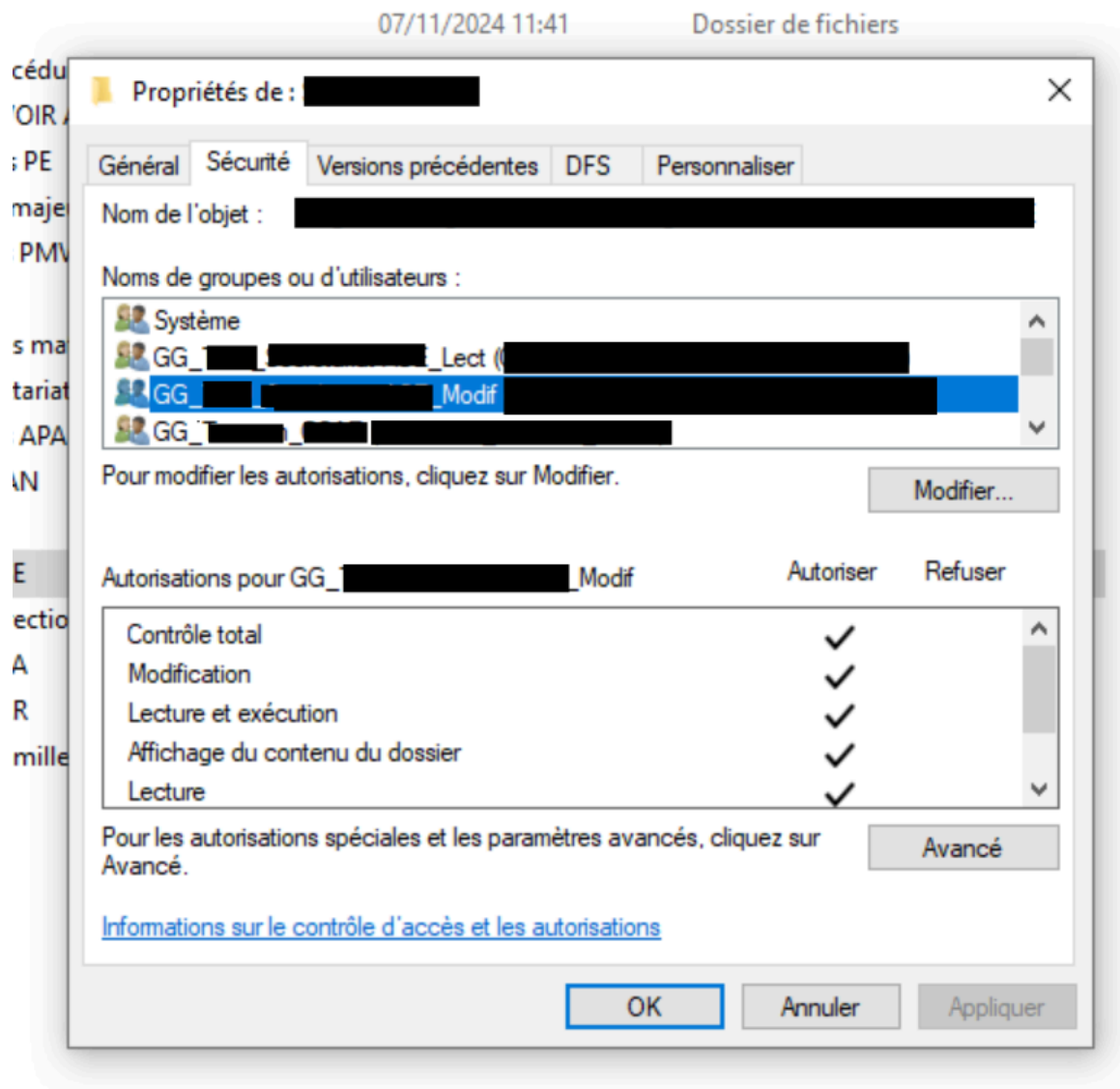
FilterGroupName      DriveLetter DrivePath                                     GPOName
-----
CG77\GLS-LECTREZO-F-Central F:          \\v-dsisav-fl-02\Agents\%username%    USR-MappagesLecteurs
CG77\GLS-LECTREZO-W-Savigny W:          \\cg77.infra\cg77\SAVIGNY\Applications USR-MappagesLecteurs
CG77\GLS-LECTREZO-H-Savigny H:          \\cg77.infra\cg77\SAVIGNY\Partages    USR-MappagesLecteurs
CG77\GLS-LECTREZO-G-DR      G:          \\cg77.infra\cg77\SAVIGNY\Partages\DR  USR-MappagesLecteurs
CG77\GLS-LECTREZO-W-Savigny W:          \\cg77.infra\cg77\SAVIGNY\Applications SU-MappagesLecteurs

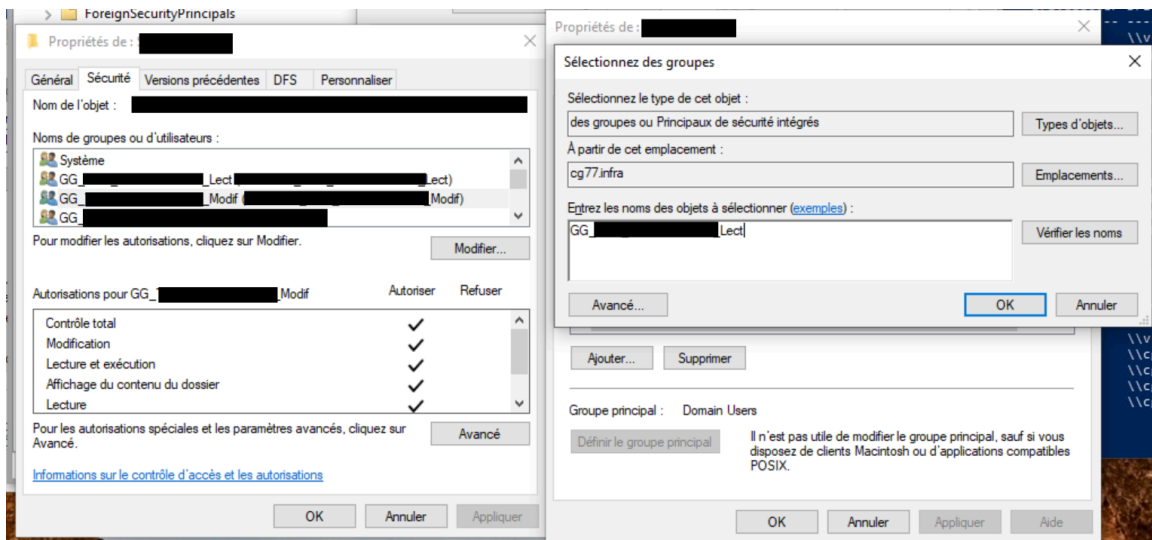
PS C:\Users\M21876_SU\Desktop>
```

Ensuite, nous copions le chemin du lecteur obtenu grâce au script, que nous collerons dans l'explorateur de fichiers. Nous localisons le dossier concerné, auquel nous souhaitons appliquer les droits, puis nous vérifions le groupe associé. Dans notre cas, il s'agira, par exemple, d'appliquer des droits en modification.



Nous identifions le bon nom de groupe (GLS, par exemple). Enfin, nous retournons dans l'Active Directory (AD) pour ajouter l'utilisateur dans le groupe que nous avons précédemment identifié.





Une fois les droits appliqués, on retourne sur le ticket afin de changer l'état de celui-ci en « terminé ».

Restauration de fichier via Veeam :

- **Contexte** : Un utilisateur a effectué des modifications sur un fichier le mercredi 15/01, entre 15h00 et 17h00, sans les sauvegarder.
- **Problème** : La sauvegarde incrémentielle sur le serveur de sauvegarde n'a eu lieu qu'à 20h00, rendant la récupération des modifications impossibles.
- **Solution** : Afin de permettre à l'utilisateur de récupérer le fichier sans les modifications non sauvegardées, une restauration de la version sauvegardée du 14/01 a été effectuée.

Modification du nom dans l'adresse mail :

- **Contexte** : L'utilisateur souhaitait raccourcir son nom de famille dans son adresse e-mail.
- **Problème** : Modifier directement le nom dans l'adresse e-mail était complexe.
- **Solution** : Un alias a été créé pour raccourcir le nom de famille dans l'e-mail, permettant ainsi de contourner le problème sans modifier la boîte mail de l'utilisateur.

G. Infrastructure Réseau et Sécurisation

Au sein du département plusieurs mesures de sécurité ont été mises en place conformément aux recommandations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Ces mesures incluent la mise en œuvre d'un modèle de **tiering** pour la gestion des accès, l'établissement d'une **matrice RACI** pour clarifier les responsabilités, et l'adoption de **l'authentification multifacteur** (MFA) pour renforcer la sécurité des accès.

Tiering : Le tiering de l'ANSSI consiste à segmenter et hiérarchiser les systèmes d'information ainsi que les droits d'accès administratifs. Cette approche permet de réduire l'exposition aux cybermenaces en limitant les accès administratifs et en compartimentant les privilèges, ce qui facilite également la gestion des accès en distinguant les rôles et les niveaux de responsabilité.

Une fois mis en place ca donne cela :

- T0 : Correspond à un niveau très sensible, où se trouvent les éléments les plus importants du SI, tels que le réseau et l'Active Directory (AD).
- T1 : Correspond au niveau sensible, incluant les bases de données (BDD), les applications et les switches administratifs.
- T2 : Représente le niveau normal, non critique, correspondant aux utilisateurs de l'infrastructure et aux utilisateurs externes.

Le tiering permet ainsi d'établir le niveau de sécurité en fonction du degré de sensibilité (critique ou non). Après avoir suivi les recommandations de l'ANSSI, la segmentation du réseau a été effectuée en classant les niveaux du plus critique au moins sensible.

Exemple d'application :

Lorsqu'un PC de niveau T2 souhaite établir une communication avec des ressources de niveau T0, plusieurs conditions doivent être remplies pour garantir la sécurité de cette interaction :

1. Présence dans l'Active Directory (AD) : L'utilisateur doit être authentifié dans l'AD pour que sa connexion soit validée.
2. Appartenance à un groupe spécifique : L'utilisateur doit appartenir à un groupe ayant des droits d'accès supplémentaires. Cela peut inclure l'accès à des ressources sensibles comme des serveurs ou des switchs administratifs.

En résumé, un utilisateur d'un PC de niveau T2 peut établir une connexion avec des ressources de niveau T0, à condition qu'il soit enregistré dans l'AD et qu'il appartienne à un groupe disposant des autorisations appropriées pour accéder à ces ressources critiques.

Matrice RACI : Une matrice RACI (Responsable, Autorité, Consulté, Informé) a été élaborée pour définir clairement les rôles et responsabilités au sein de l'équipe de sécurité.

Authentification multifacteur (MFA) : Conformément aux recommandations de l'ANSSI, le département a renforcé la sécurité des accès en mettant en place l'authentification multifacteur.

Ces initiatives ont été entreprises pour corriger les vulnérabilités identifiées et renforcer la sécurité globale de notre infrastructure, en alignement avec les directives de l'ANSSI.

a. Infrastructure réseau - pare feux

L'infrastructure réseau du département 77 a subi des améliorations importantes après une cyberattaque, visant à renforcer la sécurité et à assurer une protection plus robuste des données et des connexions. Avant l'attaque, l'entreprise utilisait un seul pare-feu Fortinet avec un clustering actif de deux pare-feux pour gérer les connexions sortantes via un routeur unique. Ce pare-feu intégrait plusieurs solutions de sécurité telles qu'un proxy, des antivirus, un reverse proxy, et un système de prévention des intrusions (IPS).

Avant la cyberattaque, l'organisation ne possédait qu'un seul pare-feu Fortinet en cluster actif pour filtrer le trafic sortant. Bien que les pare-feux étaient redondants, la politique de filtrage était centralisée et se passait par un seul point logique de contrôle. Le pare-feu Fortigate offrait des fonctionnalités avancées comme l'analyse approfondie des paquets (DPI), la gestion des connexions via un proxy et un reverse proxy, ainsi que la protection contre les intrusions avec un IPS. Cependant, l'architecture réseau n'était pas suffisamment segmentée pour garantir une protection optimale des flux internes et externes.

Suite à la cyberattaque, l'organisation a renforcé la sécurité de son infrastructure en ajoutant plusieurs dispositifs de sécurité. Un deuxième pare-feu Fortigate a été mis en place sous forme de cluster actif/passif, avec deux boîtiers Fortigate. Les connexions sortantes passent désormais d'abord par le pare-feu Sud, qui effectue toutes les vérifications nécessaires telles que le proxy, l'antivirus et l'IPS. Si le trafic est jugé conforme, il est ensuite transmis au pare-feu supérieur, qui autorise la sortie vers l'extérieur. De plus, un troisième pare-feu Palo Alto, d'un autre éditeur, a été ajouté pour offrir une couche de sécurité supplémentaire. Ce pare-feu utilise une technologie différente, permettant de protéger l'infrastructure en cas de faille sur les pare-feux Fortinet. Il facilite également la gestion des connexions entre les périphériques du niveau T0 et le reste du réseau. Grâce à l'utilisation de ces dispositifs, la segmentation interne et externe est optimisée : le pare-feu interne (Fortigate) filtre les communications entre les VLANs et empêche tout passage non autorisé, tandis que le pare-feu externe (Palo Alto) gère les flux entrants et sortants vers Internet, bloquant ainsi les menaces avant qu'elles ne pénètrent le réseau. En outre, les pare-feux intègrent des fonctionnalités avancées telles que le proxy, le reverse proxy, l'antivirus, l'IPS, le DPI et le filtrage applicatif, permettant de bloquer des applications non autorisées et d'offrir une protection renforcée contre les intrusions et les attaques. Cette architecture, composée de deux Fortigate en cluster et d'un troisième pare-feu Palo Alto, assure une sécurité périmétrique complète, avec des proxys et reverse proxies contrôlant et anonymisant les connexions sortantes tout en protégeant les serveurs exposés sur Internet. Un système IPS bloque les attaques en temps réel, et des

solutions de gestion centralisée comme FortiManager et Panorama facilitent la surveillance et la gestion cohérente des règles de sécurité à travers l'ensemble du réseau. J'ai également eu l'opportunité d'assister l'administrateur dans la gestion des pare-feux, en apprenant à gérer les règles de flux, les appliquer, et effectuer des tâches de nettoyage lorsqu'un serveur est retiré de l'infrastructure.

H. Audits de Sécurité et Simulations d'Attaques

Pour garantir une évaluation continue de la sécurité, des tests d'intrusion (pentests) sont réalisés tous les six mois. Ces simulations permettent d'identifier les vulnérabilités et d'améliorer les défenses du système d'information. La fréquence de ces tests est ajustée en fonction de l'évolution des menaces et des besoins spécifiques du département.

Ces initiatives témoignent de l'engagement du Département de Seine-et-Marne à renforcer sa résilience face aux cybermenaces et à assurer la protection des données ainsi que des services publics.

I. Stratégie de Formation en Cybersécurité et Préparation Future

La formation du personnel est essentielle pour renforcer la sécurité. Le Département a mis en place des "Cyberateliers" mensuels, offrant des sessions pratiques sur les menaces actuelles et les meilleures pratiques de sécurité. En août, un atelier spécifique a été organisé pour sensibiliser aux risques cyber, en partenariat avec la CCI Seine-et-Marne et la Gendarmerie. De plus, une collaboration avec KAMAE a été établie pour fournir des formations spécialisées, renforçant les compétences internes en cybersécurité.

VI. Bibliographie

- **Le Monde Informatique** (2023). *Le département de Seine-et-Marne paralysé par une cyberattaque*. [En ligne]. Disponible sur : <https://www.lemondeinformatique.fr/actualites/lire-le-departement-de-la-seine-et-marne-paralyse-par-une-cyberattaque-88540.html>
- **Interstis** (2023). *La cyberattaque du département Seine-et-Marne : une stratégie de communication transparente*. [En ligne]. Disponible sur : <https://www.interstis.fr/blog/la-cyberattaque-du-departement-seine-et-marne/>
(Cet article détaille la stratégie de communication adoptée par le département 77 pour gérer la crise et informer le public après la cyberattaque.)
- **ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)** (2023). *Recommandations pour la sécurisation des systèmes d'information*. [En ligne]. Disponible sur : <https://www.ssi.gouv.fr>
(Source officielle pour les recommandations de sécurité, notamment le tiering et l'authentification multifacteur)
- **CCI Seine-et-Marne** (2023). *Formations en cybersécurité pour les entreprises et administrations*. [En ligne]. Disponible sur : <https://www.seine-et-marne.cci.fr>
(Informations sur les formations et ateliers en cybersécurité organisés en partenariat avec le département)
- **Gendarmerie Nationale** (2023). *Sensibilisation aux risques cyber pour les collectivités locales*. [En ligne]. Disponible sur : <https://www.gendarmerie.interieur.gouv.fr>
(Ressources et programmes de sensibilisation aux cybermenaces)
- **KAMAE Consulting** (2023). *Formations spécialisées en cybersécurité*. [En ligne]. Disponible sur : <https://www.kamae-consulting.com>
(Informations sur les formations proposées par KAMAE pour renforcer les compétences en cybersécurité)