DAT

Introduction

Objet du document

Le présent document a pour objectif de décrire l'architecture technique du système d'information de l'entreprise Xspace pour son projet de défense en collaboration avec le ministère de la défense Tchèques, afin de fournir une base solide pour l'analyse des risques et la mise en œuvre des mesures de sécurité. Il constitue un support pour les activités de gestion des risques conformément à la méthode EBIOS RM et aux recommandations de l'ANSSI, et permet d'identifier les composants, flux et points sensibles du système.

Périmètre

Le périmètre de ce document couvre l'ensemble des systèmes, applications et services inclus dans le contexte du projet de défense confié par le ministère de la défense Tchèques, à savoir :

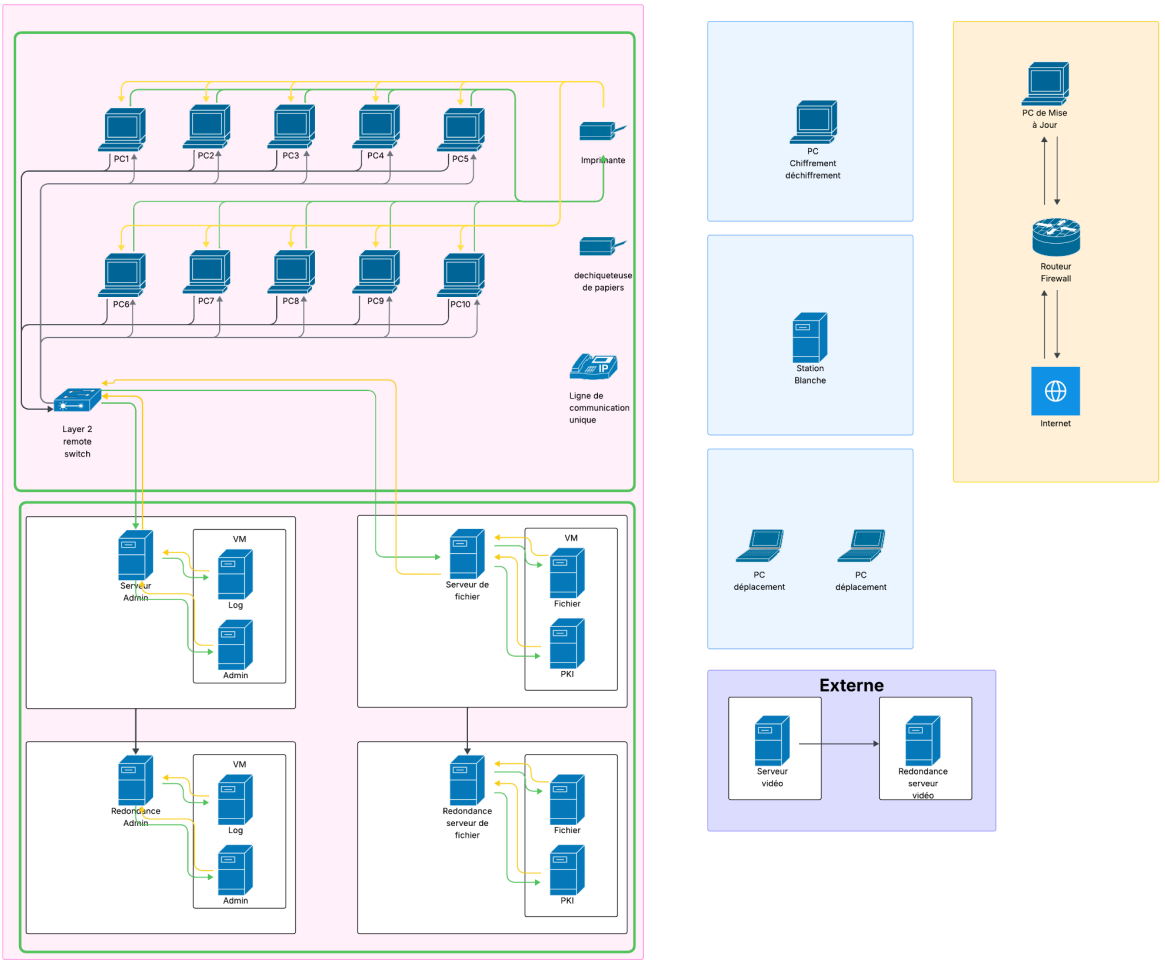
- Les serveurs et infrastructures réseau associés.
- Les services exposés aux utilisateurs internes et externes.
- Les dispositifs de sauvegarde.

Cartographie des systèmes

Inventaire des composants

Equipement	Quantité	Commentaire
Ordinateur employé	12	10 employés + 2 en stock
Ordinateur mise à jour	1	
Ordinateur chiffrement / déchiffrement	1	
Câble antivol	14	
Câble HDMI blindé (braided and foil shielding)	14	
Câble RJ 45 blindé (S/FTP)	18	
Verrou rj45	14	
Ecran PC	14	
Câble d'alimentation écran	14	
SSD 256Go Samsung PM9B1 NVMe M.2 PCIe	14	SSD vierge afin de remplacer ceux des PC reconditionnés
PC de transport	2	PC portable pour déplacement pro
Serveurs (fichier, administration et redondance)	4	
Pare-feu+ licence (stormshield)	1	
1 switch (cisco)	1	
Ligne de téléphone unique (cuivre)	1	Sans wifi/bluetooth
Imprimante	1	Sans wifi/bluetooth
Destructeur de fichier (P-7)	1	Plus haute sécurisation, norme DIN 66399
Clé usb Kingstone	2	Avec clavier
Yubikey	13	Une par employé, une pour l'administrateur et 2 en stock
Station blanche	1	
Lecteur de bande LTO	1	
Bandes LTO	15	10 pour la rotation + 5 en stock
Verrou USB	200	

Schéma global



Accès et administration

Accès internes

Entité concerné	Droit et privilèges	Méthodes d'authentification
PDG	Accès aux locaux	Accès par badge
Employé projet	Accès aux locaux et documents	Accès par badge et yubikey pour les PCs
Administrateur	Accès aux locaux/salle des serveurs	Accès par badge et yubikey pour les serveurs
Employé hors projet	Aucun accès	

Accès externes

Entité concerné	Droit et privilèges	Méthodes d'authentification
Femme de ménage	Aucun accès	
Fournisseur télécom	Accès période de travaux, titre exceptionnel sous supervision de l'administrateur	
Organisme de certification/audit	Accès aux locaux sous supervision d'un employé projet ou du PDG. Accès sous supervision de l'administrateur pour la partie serveurs	Badge nominatif à la journée
Client (Tchèques)	Accès aux locaux sous supervisions d'un employé projet ou du PDG	Badge nominatif à la journée
Sous-traitants matériels (Station Blanche)	Accès aux locaux sous supervisions d'un employé projet ou du PDG	Badge nominatif à la journée
Transporteur bande LTO	Aucun accès locaux, remise en main propre des bandes LTO par l'administrateur	
Banque de stockage	Aucun accès aux locaux, remises des bandes LTO par le transporteur	

Sauvegardes

Infrastructure concernée :

- Deux serveurs principaux + un serveur de redondance pour chaque serveur.

Média de sauvegarde :

- Bandes magnétiques LTO (Linear Tape-Open) pour les sauvegardes complètes et incrémentales.

Fréquence et politique :

- Sauvegarde complète hebdomadaire, sauvegardes incrémentales quotidiennes.
- Rotation des bandes selon un calendrier défini.

Stockage et sécurité :

- Les bandes sont déposées dans un coffre-fort sécurisé hors site une fois par semaine.
- Transport sécurisé par un prestataire agréé ou procédure interne sécurisée.

Objectif :

- Garantir la disponibilité et l'intégrité des données en cas de sinistre, perte ou corruption des serveurs principaux.

Matrice de flux

Matrice de flux PC mise à jour								
N°	**source**	**destination**	**type de flux**	**description**	**Données échangées**	**Format / Protocole**	**Fréquence / Déclencheur**	**Sensibilité / Sécurité**
F01	Microsoft Update	PC de téléchargement	entrant	Téléchargement des mises à jour Windows	Paquets de mise à jour (KB, .msu/.cab)	HTTPS	Manuel	TLS, anti-malware sur PC
F02	PC de téléchargement	Clé USB	sortant	Copie des fichiers de mise à jour	Paquets de mise à jour téléchargés	Fichiers binaires (.msu/.cab)	Manuel, selon besoin	Vérification hash des fichiers

Station blanche								
N°	**source**	**destination**	**type de flux**	**description**	**Données échangées**	**Format / Protocole**	**Fréquence / Déclencheur**	**Sensibilité / Sécurité**
F01	Clé USB externe	Station blanche	entrant	tout type de fichier pour analyse	tout type de fichier pour analyse		Manuel	
F02	Station blanche	Clé USB externe	sortant	tout type de fichier pour analyse	tout type de fichier pour analyse		Manuel	

SI XSpace								
N°	**source**	**destination**	**type de flux**	**description**	**Données échangées**	**Format / Protocole**	**Fréquence / Déclencheur**	**Sensibilité / Sécurité**
F01	Postes utilisateurs	Active Directory	Réseau interne	Authentification et gestion des comptes	Identifiants, tickets Kerberos	LDAP(S), Kerberos	À la connexion / renouvellement	TLS interne, comptes AD
F02	Postes utilisateurs	Serveur de logs	Réseau interne	Envoi de journaux système et applicatifs	Logs Windows, événements sécurité	Syslog / agent (ex: NXLog)	En continu	TLS interne, anonymisation possible
F03	Postes utilisateurs	PKI	Réseau interne	Obtention et vérification de certificats	Requêtes de certificats, CRL	HTTP(S), RPC	Selon besoin	Certificats signés, authentification
F04	Active Directory	PKI	Réseau interne	Synchronisation / validation des identités	Informations utilisateurs / groupes	LDAP(S)	Régulier	Authentification mutuelle
F05	PKI	Tous composants	Réseau interne	Diffusion de la liste de révocation (CRL)	Fichiers CRL	HTTP(S)	Périodique	Intégrité assurée par signature
F06	Tous composants	Serveur de logs	Réseau interne	Centralisation de logs sécurité / système	Événements, alertes, erreurs	Syslog / agent	Continu	Accès restreint au SIEM
F07	Tous équipements réseau	Switch central	Réseau interne	Transmission des paquets / routage interne	Données diverses	Ethernet / TCP/IP	Continu	Contrôle des VLAN / ACL

F08	Administrateur	Tous serveurs	Interne (admin)	Supervision, maintenance, configuration	Commandes, scripts, logs	RDP / SSH / HTTPS	Selon besoin	Comptes à privilèges, MFA
F09	Postes utilisateurs	Serveur de fichiers	Réseau interne	Consultation, téléchargement et dépôt de documents confidentiels	Fichiers bureautiques (Word, Excel, PDF, etc.), métadonnées,	SMB v3 / CIFS	À la demande des utilisateurs (lecture/écriture)	Authentification Kerberos, chiffrement SMB, ACL par groupe AD
F10	Serveur de fichiers	Postes utilisateurs	Réseau interne	Transfert de fichiers depuis le serveur vers le poste (lecture)	Fichiers partagés, logs d'accès	SMB v3	À la demande	Chiffrement SMB, vérification des droits d'accès

Stockage bande LTO								
N°	**source**	**destination**	**type de flux**	**description**	**Données échangées**	**Format / Protocole**	**Fréquence / Déclencheur**	**Sensibilité / Sécurité**
F01	Serveurs	Transporteur	sortant	sauvegarde hors ligne	Toutes données		1/semaine	critique
F02	Transporteur	Banque de stockage	sortant	sauvegarde hors ligne	Toutes données		1/semaine	critique
F03	Transporteur	Serveurs	entrant	PRA	Toutes données		1/semaine	critique
F04	Banque de stockage	Transporteur	entrant	PRA	Toutes données		1/semaine	critique

Gestion des journaux d’évènement

Pour la gestion des journaux d'événements, nous allons utiliser la pile ELK (Elasticsearch, Logstash et Kibana) pour le SI Xspace.

Supervision

Pour la Supervision des serveurs, nous allons utiliser Centreon.