Activité à Distance du 19/03/2020

TP Noté

Etude de cas réel

UE SEC105

Ce TP a pour objet une étude de cas réel de sécurisation d'un système de GPAO installé sur des postes en réseau utilisant des sondes couplées en RS232 et un logiciel propriétaire développé en Visual Basic 6.0 ne fonctionnant que sous Windows 98 en envoyant les données de production sur une base Access sur un serveur.

Seul l'aspect GPAO est à étudier pour proposer une solution fiable au mieux disant sachant que l'achat des 5 nouveaux postes est acté, des DELL Precision 3630 Tower sous Windows 10 pro 64 bits, sauf que la DSI de la société ne sait pas comment faire pour les utiliser dans cet environnement. Il vous faut trouver un système sécurisé et sécurisant pour le reste de l'entreprise pour que ce changement puisse se faire. Si possible il vous faut rester dans l'enveloppe budgétaire matériel. Un petit écart peut-être envisagé en termes de matériel. La mise en place et le déploiement au niveau de la main d'œuvre de la solution n'ont pas été quantifiés mais sont acceptés sur le principe. A vous de quantifier le temps nécessaire à la mise en œuvre de votre solution.

Les PC existant sont obsolètes la société souhaite les changer, ils sont au nombre de 5 :

- Un poste « serveur » est en place en et supporte la base Access qui renvoie les données sur une Base MS SQL sur le service d'analyse de la gestion de production. Ce poste est aux normes du jour, Windows 10, et suite Kaspersky. Il bénéficie en outre d'une distribution de droits et de mises à jour via la mise en place d'un système Active Directory distribué par un serveur d'entreprise sous Windows Serveur 2012.
- 5 Postes supportant le logiciel de GPAO couplé aux machines de productions de l'atelier via un de leurs ports RS232 connecté à un boitier d'acquisition propriétaire.
- Le logiciel de GPAO est paramétrable sur l'IRQ et l'adresse de connexion du port RS232 via un fichier INI au format texte.
- Le Logiciel d'acquisition ne peut pas être modifié et ne bénéficie plus d'un support de la part de la société de développement qui n'existe plus. Pour fonctionner il a besoin d'une clef dongle cryptée qui se branche sur un des ports USB de l'ordinateur.

- Les postes ont besoin d'un accès à Internet pour recevoir des mails et faire des recherches de documentation et d'assistance sur les sites internet des constructeurs des machines de production. Ces sites sont au nombre de 5.

La société a décidé de changer son parc des 5 machines de GPAO par des ordinateurs plus fiables et surtout sécurisés au niveau du reste de l'Entreprise qui possède les équipements suivants :

- Serveur sous Windows 2012 DELL Smart Value PowerEdge T440 Server Optimal avec un lecteur de bande LTO
- Accès internet via la fibre Orange avec Firewall ZyXEL USG 40 en amont
- Les sauvegardes sont paramétrées en interne sur le serveur et en externe sur une solution Cloud cryptée, s'y rajoute des bandes LTO.
- Les 12 Workstation du reste de la société sont récentes, protégées et administrées via l'AD mis en place par le serveur Windows 2012.
- La société à une charte d'utilisation du SI hors GPAO

charte d'utilisation du SI hors GPAO

Périmètre: Système GPAO

Machines de productions
de l'atelier

Windows serveur 2012

Distribue les droits et MàJ

Acquisition des
données de prod

Local

Recevoir des mails
Recherches de documentation et d'assistance

Récupère
les données de prod

5 Sites internet
des contructeurs
des machines de production

5 postes
Windows 98
Logiciel GPAO
=> Ports RS232

Logiciel propiétaire d'envois de données
de production VB6
=> Clef dongle cryptée sur port USB

Poste serveur
Windows 10 + Patché
Kaspersky Small Ofice Security

Base Access

Service d'analyse
de la gestion de production

Base MS SQL

Cloud cryptée

Backup externe

Backup internes + bandes LTO

Fibre Orange

Administre

Internet

Firewall ZyXEL USG 40

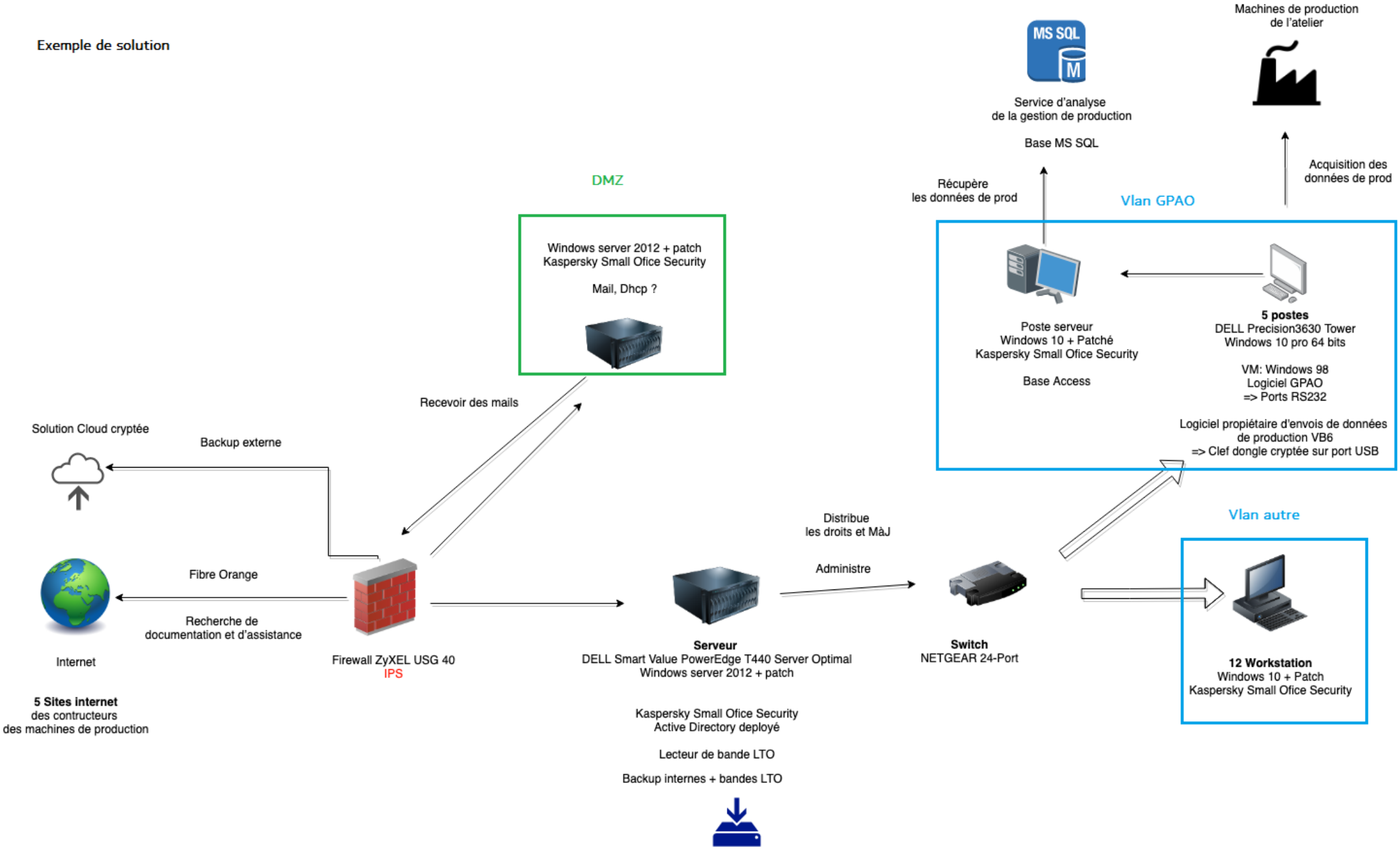
Serveur
DELL Smart Value PowerEdge T440 Server Optimal
Windows server 2012

Active Directory deployé

Lecteurde bande LTO

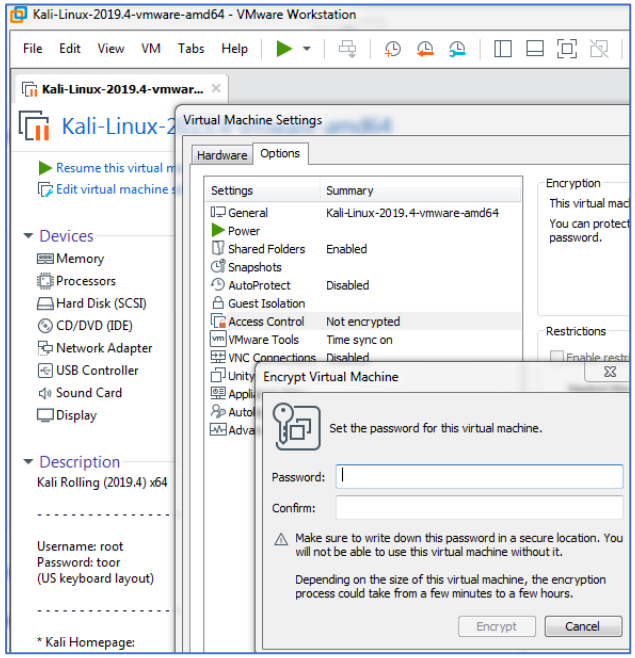
12 Workstation
Windows 10 + Patché
Kaspersky Small Ofice Security

Exemple de solution



Précisions par rapport à la solution proposée :

Périmètre d'action autorisé par le client : principalement le système GPAO
On part d'un principe qu'une appréciation des risques + traitement des risques ainsi qu'une analyse d'impact PIA + protection des locaux ne relèvent pas de notre mission, car non précisé dans l'énoncé par le client.
Achat de nouveau matériel très limité. La formation, les coûts de maintenance et d'installation sont acceptés par le Codir.
A propos du « Service d'analyse de la gestion de production » où est situé la base de données MS SQL, on ignore s'il est composé de plusieurs ordinateurs, switchs, routeurs, lot, onduleurs…



Pour la problèmatique des GPAO : Si des solutions citrix ou vmware sont disponibles, réaliser des VM pour windows 98 et y installer le logiciel GPAO ; Emuler les ports et pilotes pour les ports RS232. La clef dongle cryptée permet de faire une double authentification combinée au mot de passe pour lancer une VM (voir l'exemple avec VMware workstation). Mettre le fichier INI qui contient les adresses MAX fixes en read-only.

Firexall ZyXEL USG 40 : On considère que la partie DNS est géré par le FAI. Activer la détection anti-malware et IDP du boitier. A paramétrer pour générer des logs hebdomadaires et des notifications d'alertes quotidiennes.
Pour les flux entrants : Deny by Default en fermant les tout les ports sauf 80 et 443 pour le web.
Afin de recevoir des mails et selon le type de client web lourd ou léger : port 25 – 465 (SSL/TLS) si usage du SMTP, 143 - 993 pour IMAP, 110 – 995 pour POP3.
Pour les flux sortants/entrants : whiteliste pour accéder aux sites externes des constructeurs et les quelques sites à visées professionnelles uniquement.

Sur tout les postes workstations (sont sur windows 10):

- Activer Windows defender et Windows Information Protection (qui inclut le DLP)
- Windows Defender SmartScreen pour la navigation web en complément d'un navigateur protégé.
- Compte utilisateur avec droits appropriés
- Unités centrales et moniteurs cadenassés, MàJ/ Patchs des Bios, drivers, firmwares de tous les postes y compris serveurs.
- GPO pour les mises à jour Windows update lorsque les employés quittent l'entreprise et fermeture de tous les ordinateurs.

Pour le serveur en DMZ :

- Vu qu'on ne peut pas acheter un autre boitier firewall, j'ai isolé ce dernier qui servait initialement de gestionnaire AD pour les postes gpao. Etant exposé à l'externe, j'ai retiré AD en laissant son utilité de base pour stocker les mails reçus.

Pour le serveur DELL Smart Value PowerEdge T440 Server Optimal :

MàJ + Réalisation des backups incrémentales le soir et bloquer toutes les connections la nuit du côté firewall. Stockage sécurisé des sauvegardes LTO. La solution Kasperky Small Office Security est déployée sur tous les postes, serveurs compris.

Concernant le cloud crypté qui héberge les backups cryptées : l'entreprise en question est responsable du traitement des données de son Si et de ses clients qui se rapportent à toutes personnes identifiables (RGPD). Il s'agit de s'assurer que le fournisseur a contractuellement mis en place les mesures de sécurité nécessaires (principe de security by default). Les données doivent être anonymisées (privacy by default) adéquates, pertinentes et limitées à ce qui est nécessaire en lien avec la finalité pour laquelle les données sont traitées (principe de minimisation des données). De préférence choisir un hébergeur certifié ISO27001 et ISO 27018 ainsi qu'un data center qui hébergera les backups en Europe.

Dans une logique de défense en profondeur (Vu qu'aucun routeur, ni switch ont été mentionnées) achat d'un Switch NETGEAR 24-Port Gigabit (70 euros) pour créer les 2 Vlans séparés et isolés. Je suppose que des switchs étaient déjà en place (ne serait-ce que pour le NAT) mais vu que l'énoncé/topologie ne le précise pas, j'en rajoute un.

A propos d'AD : déployé sur postes, le -les contrôleur (s) de domaines qui sont des infrastructures critiques, n'apparaissent sur le schéma qui ne montre qu'une partie du parc informatique.

Séparation des tâches : limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation. Veiller à ce que personne ne puisse accéder à, modifier ou utiliser des actifs sans en avoir reçu l'autorisation ou sans avoir été détecté

Activer SNMP pour collecter les logs et surveiller les équipements afin de lutter contre le BYOD non autorisés et le Shadow It (outils non autorisés et inconnus du SI) En l'absence d'une PSSI, l'usage de la charte d'utilisation des ressources informatiques et internet doit couvrir l'ensemble du SI. Pas d'achat de DPI, d'Endpoint ni de SIEM pour ne pas alourdir le budget ni ralentir les ressources systèmes et bande passante (disponibilité).

PCA/PRA : création d'image pour les workstations avec mots de passe à changer pour chaque poste après l'installation. Réaliser un scan anti-malware et surtout rootkit. On ignore s'il existe un générateur de secours et des onduleurs. On ne sait pas s'il existe des ordinateurs portables avec serveur VPN pour continuer de travailler à distance suite à un incendie dans le bâtiment par exemple.

Planning (pour 2 Admins, 1 technicien et 1 formateur) : 3 journées pour la mise en place du switch et paramétrer les autres équipements + 1 après-midi pour sensibiliser le personnel + 1 journée pour revoir et renforcer la charte d'utilisation à l'ensemble du SI.