Cahier des charges

-

ACME Corp

Contexte

L'augmentation de l'activité d'ACME, répondant à une demande du marché croissante, impose une refonte du fonctionnement logistique de l'entreprise. Il a été constaté des failles de sécurité sur le système informatique de l'entreprise, ainsi que des pertes réseaux et des pannes matérielles répétées. Ces manquements ont un impact direct sur la santé commerciale de l'entreprise.

Interlocuteurs

CEOs d'ACME Corp:
Maud Becam
Phi Tran
Mickaëlle Aubrée
Corentin Villiermet

Consultant Sécurité, Réseau, Développement :
Mickael Gaillard

Cheffe du Service Informatique :
Magali Pannetier

SOMMAIRE

Objectifs

Les objectifs clés de la refonte du fonctionnement logistique d'ACME tendent à assurer une durabilité de l'infrastructure de l'entreprise.

Productivité

La résolution des manques constatés de performance sur le réseau permettra d'assurer une productivité optimale.

L'acquisition d'une application CRM facilitera l'enregistrement des ventes et la gestion des clients. Les statistiques de vente enregistrées via l'application offriront une vision des performances commerciales, et guideront la stratégie marketing de l'entreprise.

Sécurité :

La mise à jour des machines et outils utilisés, tels que les systèmes d'exploitation des serveurs, permettra de bénéficier du maintien technique des logiciels, incluant la surveillance et les patchs de sécurité.

La sauvegarde des données automatisée, et effectuée à intervalle régulier, sur un serveur externe, permettra de protéger l'entreprise face au risque d'une perte ou de compromission de données.

L'aménagement de l'infrastructure réseau permettra d'assurer des communications fiables entre les machines.

Des tests de sécurité seront mis en place pour confirmer ou infirmer la robustesse des mesures préventives et correctives installées sur l’application.

Périmètre d’activité

L’entreprise ACME Corp opère dans le secteur de l'espionnage et de l'élimination ciblée. Ce secteur d'activité est un marché porteur, reposant sur des besoins intemporels et universels d'un public d'acheteurs dynamique. Opérant au service des mafias à l'international, ACME a pour ambition de devenir leader de la vente de meurtres ciblés et de matériel d'espionnage.

Stratégie Développement et sécurisation

I. Sécurisation du réseau local de l'entreprise

1 : Monitoring réseau

La supervision du fonctionnement du réseau de l'entreprise sera mise en place et maintenue avec attention, au moyen d'un monitoring à l'aide de l'outil Centreon. La configuration des templates Hosts dans Centreon sera définie selon les services réseaux à superviser. Des vues personnalisées seront mises en place pour superviser des métiers et services (bases de données, serveurs web). Les regroupement de machines permettra de superviser des sites locaux. L'agrégation de données, et les graphiques évoluant en temps réel sur Centreon offriront une vue d'ensemble du fonctionnement du parc de machines et des services supervisés.

2 : Architecture réseau flexible par Spanning Tree

Dans l'optique de prévenir les risques de perte totale de communication sur le réseau, il a été convenu que l'infrastructure inclura une architecture en modèle Spanning Tree. Le protocol Spanning Tree a pour essence l'élection d'un switch racine, par lequel transite la communication entre les machines. La création d'une boucle de connexion, par la mise en place d'un switch supplémentaire. Si pour n'importe quelle raison, le switch racine venait à cesser de fonctionner, le switch supplémentaire prendrait le relai pour maintenir la connexion sur le réseau.

3 : Renforcement du réseau par double routage

Afin de renforcer et d'assurer le maintien des communications au sein de l'entreprise, une architecture à double routage sera mise en place entre les serveurs et les sous réseaux de l'entreprise. Cette stratégie s'inscrit dans un plan de prévention contre les risques encourus par un point de défaillance unique (single point of failure ou *SPOF* en anglais).
L'attribution d'une adresse ip virtuelle sera configurée pour indiquer une gateway aux serveurs et aux postes clients . Ainsi, si le routeur principal, configuré avec les instructions "standby priority" et "standby preempt", sera le routeur par défaut. En cas de panne de ce routeur principal, le second routeur prendra le relais pour assurer la continuité des communications.

4 : Sécurisation du réseau par Firewall

La mise en place d'un firewall permettra de définir les communications autorisées ou prohibées entre le réseau local et le net. Le firewall contrôlera les flux de données en entrée et en sortie par un filtrage suite à une analyse des communications selon les règles de sécurité établies par l'entreprise.
Les firewalls de nouvelles générations (NGFW) sont recommandés par exemple Fortinet. Ils permettent d'avoir les fonctionnalités des firewalls classiques : filtrage de paquet par en-tête, inspections du trafic, mais aussi des fonctionnalités d'antivirus, l'analyse approfondie des paquets et une mise à jour constante.

5 : Mise en place d'un serveur Proxy

Le serveur intermédiaire sera mis en place pour transmettre les requêtes via un filtrage des accès du réseau interne de l'entreprise en direction du net. La définition des listes blanches et listes noires incarnera la fondation de la stratégie de filtrage du serveur proxy. Le filtrage de contenu lourds envoyés vers l'application s'ajoutera aux mesures de prévention d'injection. L'enregistrement des requêtes effectuées permettra le suivi des connexions au moyen de logs de navigation.

II. Sécurisation de la base de données et du serveur hébergeant les données de l'application

1 : Droits d'accès à la BDD

Dans l'optique de limiter l'exposition et la compromission de données sensibles de l'entreprise, une gestion rigoureuse des accès à la base de données devra impérativement être mise en place. La gestion de ces accès reposera sur la discrimination des droits des utilisateurs sur la base de données, les informations qu'elle regroupe, et le paramétrage du serveur de base de données.

Il a été convenu que les accès seront gérés comme suit :

- un compte "root" créé par défaut, il dispose d'absolument tous les droits
- des utilisateurs "admin" disposent de droits de configuration, administration et maintenance de la base de données
- des utilisateurs lambda (commerciaux en charge de la vente des produits du catalogue ACME) disposent de droits de lecture et d'écriture des données contenues dans la base

2. Sécurisation des données sensibles

Les données à caractère sensible contenues dans la base de données de l'entreprise devront être rigoureusement sécurisées. Dans cette optique, les mots de passe et des utilisateurs seront entrés en base de données après une phase de chiffrage au moyen d'un hash et salt puissants. Pour ce faire, la fonction intégrée du framework Spring Boot *BCrypt PasswordEncoder*, sera mise en place sur l'interface de connexion. BCrypt est une puissante fonction de hashage, et permet d'encoder les mots de passe de façon à les stocker de façon sécurisée.

3. Suivi des requêtes SQL

La mise en place d'une réplication de la base de données sur un serveur esclave permettra un backup des données, en prévention à des problèmes sur le serveur maître. Le serveur maître effectuera des logs de chaque modification apportée à la base de données. L'observation attentive des logs de requêtes SQL effectuées sur la base de données permettra d'identifier d'éventuelles requêtes intruses.

III. Sécurité de l’application

L’application CRM de l’entreprise ACME sera développée en respectant les bonnes pratiques de programmation sécurisée. Ainsi, les champs de type input seront protégés face aux injections de code XSS, par une conversion des entrées en caractères HTML.

Ces champs seront également soumis à une validation par expression régulière, permettant notamment l’exclusion de caractères d’échappement pouvant mener à des injections SQL. Ces validations seront réalisées au niveau du serveur, dans le but de contrecarrer l’interception et la modification des données saisies dans le navigateur par un serveur proxy. Une validation côté client pourra être mise en place pour informer l’utilisateur du format de donnée attendu et permettre une utilisation simplifiée de l’application.
L’ensemble des champs de type input seront transmis au serveur en utilisant la méthode POST du langage HTML. Celle-ci ne fera pas apparaître les données du formulaire dans la barre d’adresse du navigateur ni dans les fichiers de log du serveur web, contrairement à la méthode GET. Le recours à la méthode POST sera essentiel à la sécurité des données sensibles renseignées dans l’application.

IV. Automatisation de sauvegardes sécurisées des données

Afin de préserver l'intégrité des données de l'entreprise, une sauvegarde automatique vers un serveur tiers sera mise en place. Grâce à l’utilisation d’un logiciel de sauvegarde, tel que Veeam Backup, les données de l’entreprise seront régulièrement enregistrées sur un serveur externe. Les options d’automatisation de Veeam Backup vont apporter un gain de temps conséquent, en comparaison avec des méthodes de sauvegarde manuelles. Lors de cette sauvegarde, les données seront chiffrées.

Dans une optique de prévention de l’intégrité des données enregistrées par l’entreprise, il a été convenu qu’un plan de backup régulier sera mis en place, grâce à un recours aux fonctions d’exportation de MySQL. La fonction *mysqldump* sera invoquée pour formater dans un fichier “dump”, les requêtes SQL nécessaires pour recréer la base de données existante dans son intégralité, telle qu’elle était au moment de la sauvegarde.

V. Gestion automatisée du parc de machines

L'automatisation des installations logicielles et configurations sera appliquée grâce à l'outil d'automatisation Ansible. Dans l’optique de réduire les tâches et configurations manuelles, le logiciel d’automatisation Ansible sera installé sur le poste administrateur de l’entreprise. Ansible permet l’automatisation des configurations système, des déploiements logiciels, l’orchestration des déploiements continus, et la livraison des mises à jour.

Les tâches à automatiser seront détaillées dans les playbooks exécutés par Ansible. L’écriture Yaml des playbook a pour avantage majeur d’être accessible, et permet d’indiquer avec facilité les hôtes ciblés et les processus à exécuter. Une phase de tests de chaque playbook sera menée à l’aide des commandes “--check” et “--syntax - check” afin de vérifier et valider chaque étape d’automatisation.

VI. Optimisation de l’infrastructure pour supporter la croissance de l’entreprise

1. Optimisation Infrastructure

Devant le constat indéniable d’une activité fortement croissante, la stratégie de refonte d’ACME doit inclure les spécificités techniques nécessaires pour son développement futur. Dans cette optique, l’infrastructure et la configuration réseau doit permettre l’ajout de postes

DHCP : centraliser la gestion de la configuration réseau
La configuration du serveur DHCP sera accès sur la mise en place d’une plage d’adresses IP adaptée à la taille existante de l’entreprise, tout en permettant l’adressage de nombreux futurs postes. Des mesures de protection seront mises en place pour protéger le serveur contre les DOS.

2. Accessibilité de l’accès à l’application

Dans l'optique de permettre aux commerciaux de l'entreprise, l'application CRM utilisée par ACME Corp devra être rendue accessible sur tous les postes de travail, au moyen d'un raccourci launcher.

3. Accessibilité à distance

Les commerciaux sont souvent en mission de prospection. Ils ont aussi besoin d’accéder aux ressources de l’entreprise. La mise en place d’un VPN permettra d’assurer l’accessibilité à distance de ses ressources de manière sécurisée. Notre préconisation est d’utiliser la solution de VPN incluse dans le pack de Fortinet.

VII Amélioration du serveur existant

Afin de répondre aux pertes de performances dues à la vétusté des serveurs linux, ACME a décidé d'opter pour un système d'exploitation récent. Une Fresh Install d'un serveur Ubuntu permettra de bénéficier des dernières améliorations et patchs de sécurité. Ainsi, les données contenues dans le serveur existant seront sauvegardées sur un disque externe, le serveur Linux Ubuntu 12.04 sera supprimé, et un nouveau serveur Ubuntu 20.04 sera installé. Les données de l'entreprise seront importées sur ce nouveau serveur.

VIII RGPD

Soucieux de développer son marché au sein de l'Union Européenne, l'entreprise souhaite que la protection des données de ses utilisateurs et de ses clients soit conforme à la RGPD. Acme Corp prévoit donc de suivre le plan en 6 étapes afin d'assurer sa conformité :

1. désigner un pilote
2. cartographier les traitements de données personnelles
3. prioriser les actions à mettre en place
4. gérer les risques
5. organiser les processus internes
6. documenter la conformité

Ces étapes et leur contenu sont détaillés de façon plus approfondie dans de la documentation dédiée, en particulier celle de la CNIL (Commission nationale de l'informatique et des libertés) qui les publie en français.