Rapport de cybersécurité de l'entreprise GameLuck

Date	Version	Description	Auteurs
05/04/2023	1	Création du document	Bialas Alexis Faussurier Marc

Sommaire

Introduction

Dans un monde de plus en plus connecté, où les technologies de l'information et de la communication sont devenues indispensables pour le bon fonctionnement des entreprises, la cybersécurité est devenue un enjeu majeur. Gameluck, une entreprise spécialisée dans le secteur du divertissement numérique, n'échappe pas à cette réalité. Les risques liés aux failles de sécurité sont nombreux, et peuvent engendrer des pertes financières, des atteintes à la réputation, voire des sanctions légales.Il est donc primordial pour Gameluck de mettre en place des mesures de protection efficaces.

Cette étude a pour objectif d'évaluer la posture de cybersécurité de Gameluck et de proposer des recommandations pour améliorer la sécurité de ses systèmes d'information. Pour cela, nous nous baserons sur un sommaire qui couvre les principales dimensions de la cybersécurité :

Sécurité de l'infrastructure : Nous analyserons l'architecture du réseau de Gameluck, les protocoles de communication utilisés, ainsi que les dispositifs de sécurité mis en place (pare-feu, antivirus, systèmes de détection d'intrusion, etc.). Nous identifierons les vulnérabilités potentielles et proposerons des solutions pour les corriger.

Sécurité des droits des utilisateurs : Nous étudierons la gestion des accès et des permissions accordées aux employés de Gameluck, ainsi que les politiques de gestion des mots de passe et de sensibilisation à la sécurité. Des recommandations seront formulées pour renforcer la sécurité des données et prévenir les risques liés à l'erreur humaine.

Sécurité du développement d'applications : Nous examinerons les processus de développement des applications de Gameluck, avec un focus particulier sur les pratiques de codage sécurisé, les tests de sécurité et la gestion des mises à jour. Des conseils seront donnés pour intégrer la sécurité dès la conception des produits et réduire les vulnérabilités.

Sécurité de l’infrastructure

L'infrastructure informatique est le socle sur lequel repose l'ensemble des systèmes d'information de l'entreprise Gameluck. Elle englobe les aspects physiques, tels que les locaux et les matériels, ainsi que les aspects logiques, tels que les réseaux et les systèmes d'exploitation. Assurer la sécurité de cette infrastructure est essentiel pour prévenir les intrusions, les attaques et les fuites de données.

Il est nécessaire de former l’équipe chargée des investissements IT sur les enjeux en matière de dépendance matérielle et de service afin de réduire les tiers de confiance au maximum. Il est aussi important de former l’équipe sur les risques de phishing et les enjeux autour de l'ingénierie sociale en matière de cybersécurité.

Sécurité Informatique

Sécurité des locaux

La sécurité des locaux dans le cadre de la cybersécurité fait référence à l'ensemble des mesures physiques et organisationnelles mises en place pour protéger les équipements informatiques et les données sensibles contre les intrusions physiques. Elle implique la mise en place de systèmes de surveillance vidéo, de serrures, d'alarmes et de contrôles d'accès, ainsi que la formation du personnel sur les politiques de sécurité physique. La sécurité des locaux doit être régulièrement révisée et mise à jour pour s'adapter aux nouvelles menaces et technologies. Elle constitue un élément clé de la cybersécurité pour garantir la protection des données et la continuité des opérations.

C’est pourquoi plusieurs points sont à revoir pour assurer une meilleure sécurité : La fermeture des locaux après les horaires de travail est obligatoire de plus des caméras de surveillance devraient être installées et les bureaux des personnes haut placé doivent être à l’étage. Puis un point important à souligner est l’accueil de clients ou autres personnes extérieures à la société gameluck, ces personnes devraient être accueillies dans des salles de réunions ou espace dédié à cela avec une wifi “invité” et non dans les bureaux des commerciaux.

Sécurité des salles en réseau déconnecté

Une société dans le divertissement numérique se doit de posséder une salle en réseau déconnecté pour assurer un niveau élevé de sécurité. Elle doit notamment s'assurer qu'elle soit bien protégée en respectant plusieurs principes : le contrôle d'accès à la salle en réseau déconnecté est strict, limitant l'entrée aux personnes autorisées. La salle est conçue pour protéger contre les menaces physiques et est bien isolée. La température, l'humidité et la qualité de l'air sont régulées pour préserver les équipements. L'alimentation électrique est stable et sécurisée grâce à des alimentations sans interruption et des générateurs de secours. La surveillance est doit être constante pour détecter les anomalies, avec des systèmes de détection d'incendie, d'inondation et d'intrusion.

Sécurité des serveurs

La sécurité physique des serveurs de la société gameluck est un élément clé dans la prospérité de l'entreprise. Cette sécurité englobe la mise en place de diverses mesures pour prévenir l'accès non autorisé, les dommages accidentels et les catastrophes naturelles.

Pour prévenir l'accès non autorisé, il est nécessaire de déployer des contrôles d'accès stricts tels que des cartes d'accès, des codes PIN et des scanners biométriques, pour limiter l'entrée aux salles de serveurs. De plus, des caméras de vidéosurveillance et des systèmes d'alarme doivent assurer la surveillance continue des zones sensibles. Enfin les serveurs ainsi que tous les objets d'interconnexion sont actuellement soumis aux mécanismes d'authentification de type « tacacs ». Pour augmenter la sécurité des serveurs, les serveurs ainsi que les objets d'interconnexion devraient être soumis aux mécanismes d'authentification de type "tacacs+" qui permet une meilleure protection et prévention aux intrusions.

Sécurité des réseaux

Architecture par service :

L'architecture réseau par service est une approche qui consiste à regrouper les différents services de l'entreprise en fonction de leurs besoins spécifiques en matière de sécurité. Cette architecture comprend plusieurs éléments clés :

- 1 NAS (Serveur de stockage en réseau) : pour stocker les données de manière centralisée et sécurisée.
- 1 AD (Active Directory) : pour gérer l'authentification et les autorisations des utilisateurs et des ordinateurs sur le réseau.
- 1 pfSense : pour contrôler le trafic réseau et garantir la sécurité des communications entre les différents services.
- 1 VLAN : pour segmenter le réseau en fonction des différents services et éviter les attaques de type « espionnage ».

Architecture des salles en réseau déconnecté :

Une salle en réseau déconnecté est un environnement informatique isolé physiquement et logiquement du reste du réseau, généralement utilisé pour la conception et le développement d'applications critiques ou sensibles. L'architecture de la salle en réseau déconnecté doit garantir un accès strictement contrôlé et des mesures de sécurité renforcées pour protéger les informations sensibles.

- 1 LAN déconnecté d'Internet : pour éviter tout accès non autorisé à la salle en réseau déconnecté et garantir la sécurité des données qui y sont manipulées et stockées.

Architecture par site :

L'architecture réseau par site est une approche qui consiste à répliquer l'infrastructure réseau dans chaque site géographique de l'entreprise, en veillant à garantir la disponibilité des services et la sécurité des communications entre les différents sites.

- Accès redondant à Internet : pour garantir la disponibilité des services même en cas de panne d'un fournisseur d'accès Internet.
- pfSense entre WAN et réseau privé : pour contrôler le trafic réseau et garantir la sécurité des communications entre les différents sites.
- Filtrage d'IP et paquets : pour éviter les attaques de type déni de service et garantir la sécurité des données en transit.

Architecture des serveurs:

L'architecture des serveurs doit garantir la sécurité physique et logique de l'infrastructure, ainsi que la disponibilité des services en cas de panne, de catastrophe naturelle ou d’attaque.

- Redondance des composants critiques (alimentation électrique, climatisation, accès internet; etc.) : pour garantir la disponibilité des services même en cas de panne d'un composant.
- Contrôle d'accès physique : pour éviter tout accès non autorisé au datacenter.
- Surveillance des environnements : pour détecter les problèmes avant qu'ils ne deviennent critiques.
- DMZ : pour réduire les risques sur les systèmes internes

Architecture mondiale de l'intranet :

L'architecture réseau mondiale de l'intranet de GameLuck garantit la confidentialité, l'intégrité et la disponibilité des données en transit entre les différents sites.

- Tunnels IPsec entre les différents sites de la boîte : pour garantir la sécurité des communications entre les différents sites géographiques.
- Authentification forte : pour garantir que seuls les utilisateurs autorisés ont accès

Sécurité des points d’accès Wi-Fi

Tout d'abord, il est recommandé de couper le wifi dans les zones où il est inutile, car cela permet de réduire les risques de piratage et d'attaque de type "man in the middle". Par exemple, le wifi n'a pas besoin d'être activé dans les zones de stockage où les employés n'ont pas besoin d'accéder à Internet. Cette mesure permet également de réduire les interférences avec les autres réseaux wifi dans l'entreprise.

Ensuite, il est recommandé de mettre en place l'identification serveur EAP-RADIUS dans les salles de réunion pour renforcer la sécurité de ces espaces. Cette mesure permet d'authentifier les utilisateurs avant de leur accorder l'accès au réseau wifi de la salle de réunion. Ainsi, seuls les employés autorisés peuvent accéder au réseau wifi de la salle de réunion et éviter tout risque d'intrusion ou de piratage.

De plus, une connexion WIFI pour visiteur devrait être établie dans le cas de l'accueil de personnes extérieures comme les clients avec un système de connexion par parrainage, ce système ne doit pas être utilisé par les équipes en interne.

Sécurité des matériels informatiques

En ce qui concerne la sécurité des matériels informatiques Gameluck n'est pas le meilleur des élèves et devrait se concentrer sur la migration de ces OS vers windows 10 ou 11 ce qui réduirait grandement les risque d'attaque et augmenterait donc la sécurité, de plus un système de journalisation devrait être installer sur les AD afin d'avoir une meilleur traçabilité des événements.

Une sauvegarde des fichiers importants devrait être réalisée en s'assurant bien que la sauvegarde à été réalisée et que l'intégrité des données ait été respectée. Les sauvegardes automatisées peuvent être vulnérables à des attaques de type ransomware si les copies de sauvegarde ne sont pas correctement sécurisées. Il est important de mettre en place des mécanismes de sécurité pour protéger les données de sauvegarde, y compris la sauvegarde hors site et la mise en place de politiques de gestion de la sécurité des données.

De plus les données en mobilité jouent un rôle majeur dans la sécurité des données et aussi des matériels car ils sont en première ligne d'une potentielle attaque, c'est pour cela que Gameluck doit impérativement avoir une politique stricte sur l'utilisation d'ordiphones ou de tout autre appareils en déplacement. Ainsi qu'une politique stricte interne avec l'interdiction d'utiliser des téléphones portables dans les locaux de gameluck (Des téléphones IP doivent être disponibles avec un VLAN VoiP installé sur les switchs).

Puis Gameluck laisse la possibilité à l'utilisateur de chiffrer ces données, ce qui devrait être obligatoire pour assurer l'intégrité des données communiquées et devrait utiliser une DLP pour ce protéger d'intrusion.

Enfin un des principal critère pour la sécurité des matériels informatique est la disponibilité et par conséquent la maintenance du parc informatique qui doit être renforcé via une nouvelle stratégie de maintenance du parc qui consiste à louer les ordinateur avec des contrats de maintenance avec remplacement sous 24 heures,ce qui est à un coût mais cela réduits considérablement les problèmes de pertes de disponibilité en ce qui concerne les attaques informatiques ou bien même des érreur du quotidien ce qui pourrais ce faire de manière progressive au même titre que le changement du parc informatique et la migration vers windows 10 qui peut ne pas être brutal.

Réponse à incident

Une bonne protection informatique réside dans l'efficacité de la réponse à incident, pour que l‘on puisse se rétablir le plus efficacement en suivant des procédures précises à créer pour une perte de disponibilité moins importante.

De plus la facilité à retrouver la source du problème et sont émetteur est aussi une forme de réponse à incident, pour ce faire l’utilisation de log améliorera grandement cette partie de la cybersécurité.

Sécurité des droits des utilisateurs

Une gestion rigoureuse des droits des utilisateurs permet de prévenir les fuites de données, les erreurs humaines et les tentatives de fraude, en garantissant que chaque employé dispose uniquement des permissions nécessaires pour accomplir ses tâches.

Il est important de former l'équipe sur les enjeux autours des droits afin de limiter au maximum les droits de chacuns et d'éviter la prolifération de l'utilisation des comptes super admins.De plus les comptes administrateurs étant actuellement cacher devrait être effacé pour garantire une meilleur protection contre les malware qui pourrait potentiellement s'introduire via un téléchargement non autorisé.

Une application portails d'entreprise avec les applications nécessaires au travail pourrait être installée avec des comptes active directory pour pouvoir gérer les configurations et les mises à jours des téléphones.

Groupes

- G_Admin: groupe pour les utilisateurs du département de l'administration (compta, marketing, etc.)
- G_Compta
- G_Marketing
- G_Commercial
- G_IT: groupe pour les utilisateurs du département informatique (techniciens, administrateurs système, etc.)
- G_Compta
- G_Dev: groupe pour les développeurs de logiciels
- G_Tec: groupe pour les techniciens informatiques
- G_CyberSec: groupe pour les responsables de la cybersécurité

Domaines Locaux

- DL_Access_NAS_PROJET_R: domaine local pour l'accès par projet aux différents fichiers sur les serveurs de stockage en réseau (NAS); ce domaine local pourrait aussi être utilisé par le CRM maison de GameLuck afin d'éviter une redondance des permissions.
- DL_Access_NAS_PROJET_RW: idem mais avec en plus les droits d'écriture

- DL_Access_Git_PROJECT_R: domaine local pour l'accès aux dépôts Git d'un projet via id rsa en lecture
- DL_Access_Git_PROJECT_RW: domaine local pour l'accès aux dépôts Git d'un projet via id rsa en lecture / écriture
- DL_Access_AD_DOMAINE: domaine local pour l'accès au serveur Active Directory d'un domaine en admin.
- DL_Access_SQL_PROJET : domaine local pour l'accès au SQL Server de production d'un projet en SA.

Sécurité du développement d’applications

Dans cette sous-partie, nous nous intéresserons à la sécurité du développement d'applications, un aspect essentiel pour assurer la protection et la confidentialité des données des utilisateurs.

Le développement d'applications sécurisées est un enjeu majeur pour les entreprises, en particulier dans le secteur du jeu vidéo, où la propriété intellectuelle et les informations sensibles sont au cœur de la réussite commerciale.

Il est important de former l’équipe sur le bon sens en matière du choix des dépendances, en effet il faut éviter d’utiliser des CDN pour des ressources statiques qui peuvent être hébergée par l’entreprise, et il faut former les développeurs aux risques liés aux pyramide de confiance en matière de software afin de réduire au maximum les dépendances.

Sécurité du développement d’application clientes

Il est nécessaire d’établir et de respecter strictement des procédures afin d’éviter des failles de sécurité pendant la compilation et le déploiement d’une application cliente.

Ainsi nous préconisons de compiler (sans les symboles de débogage); d’obfuscer et de signer les applications clientes en salle en réseau déconnecté.

La compilation sans symboles de débogage et l'obfuscation rend l'ingénierie inversée plus difficile pour les tiers malveillants, tandis que la signature garantit l'authenticité et l'intégrité du code.

Nous préconisons d’échanger des données entre la salle en réseau déconnecté et l'extérieur par supports amovibles de confiance. La réalisation de ces opérations en salle en réseau déconnecté permet de se prémunir des attaques par porte dérobée, en effet la salle en réseau déconnecté n’est pas connectée à aucun autre réseau et les technologies wifi et bluetooth ne sont pas présentes.

Sécurité du développement d’application serveurs

En ce qui concerne la sécurité du développement d'applications serveurs, plusieurs mesures de sécurité sont à mettre en place.

Tout d'abord, il est important de sécuriser les bases de données en utilisant des outils tels que le chiffrement des disques durs, la séparation des données sensibles et non sensibles, le hachage des mots de passe stockés et l'utilisation de mots de passe et de protocols sécurisés pour les connexions entre les instances SQL Server et l’extérieur.

Aussi, les failles SQL et XSS doivent être évitées en utilisant des bibliothèques spécifiques, en limitant les entrées utilisateur et en validant toutes les entrées de données.

Il est également important de sécuriser les accès aux fichiers HTTP en limitant les autorisations et en configurant correctement les serveurs Web, afin d’empêcher un tiers de déterminer par bruteforce les fichiers disponibles ou bien d’accéder à un fichier sensible depuis un simple historique de navigation d’un navigateur compromis.

La durée des sessions web des utilisateurs doit aussi être limitée dans le temps pour éviter les usurpations de cookies. Les utilisateurs doivent avoir accès à tous leurs devices autorisées pour pouvoir gérer au cas par cas les autorisations d’accès à leurs données.

Enfin, tout comme pour le frontend la compilation et la signature devrait être effectuée dans une salle en réseau déconnecté. Le déploiement de l'application serveur vers son serveur dédiée ou sa machine virtuelle doit être effectué depuis un réseau de confiance indépendant du réseau de l’entreprise, il en va de même pour la maintenance du système d'exploitation de l’application serveur.

Lors du déploiement de l’application serveur et lors des connexions par SSH ou RDP au serveurs hôtes , il est nécessaire de vérifier l’authenticité des certificats lors de l’établissement des connexions afin de se prémunir des attaques par l’homme du milieu.

Conclusion

En conclusion, ce rapport de cybersécurité souligne l'importance de la protection des actifs numériques et des données sensibles au sein de l'entreprise. La mise en œuvre de mesures de sécurité efficaces, telles que la sécurisation des infrastructures, la gestion des accès, la sensibilisation et la formation du personnel, est essentielle pour prévenir les cyberattaques et les fuites de données.

Il est également primordial d'adopter une approche proactive et évolutive face aux menaces en constante évolution dans le paysage de la cybersécurité. Cela implique de maintenir les systèmes à jour, de surveiller régulièrement les activités suspectes et de mettre en place des processus de réponse aux incidents pour réagir rapidement en cas de problème.

L'engagement de la direction et la collaboration entre les différents départements de l'entreprise sont également indispensables pour instaurer une culture de cybersécurité solide et durable.