Cybersécurité et gestion des risques

1. Gestion des risques :

Les politiques suivantes traitent de l'évaluation des risques en vue de la mise en œuvre de mesures de sécurité, de la hiérarchisation des menaces les plus importantes et de la garantie d'une réactivité appropriée :

8 – Réponse aux incidents 2022.docx
14 – Évaluation de la sécurité et autorisation.docx
16 – Politique d'évaluation des risques de sécurité informatique 2022.docx
Plan de réponse aux incidents.docx

2. Configuration sécurisée :

Pour garantir une configuration adéquate, éviter les violations de données, la suppression ou la désactivation de fonctions inutiles du système et traiter rapidement les vulnérabilités connues, nous utilisons MS ATP, Manage Engine Patch Management et RBAC sur tous nos systèmes.

3. Travail à domicile et travail mobile :

Bitlocker est installé sur tous nos terminaux et le MFA est obligatoire pour tous les accès à distance.

4. Gestion des incidents :

Afin de répondre rapidement à un incident de sécurité, d'atténuer les dommages et d'effectuer des sauvegardes le plus rapidement possible, le Plan de réponse aux incidents est mis en œuvre, de même que la sauvegarde VEEAM sur un NAS Linux secondaire et les répliques sur des installations de secours hors site inactives.

5. Prévention des logiciels malveillants :

Nous employons la formation et les rapports de Knowbe4 et utilisons MS ATP pour la prévention des incidents et la détection des logiciels malveillants.

6. Gestion de l'accès des utilisateurs :

Pour garantir que notre personnel ne peut accéder qu'aux informations pertinentes pour son travail, nous utilisons les groupes de sécurité AD et les groupes d'application (RBAC). Les utilisateurs finaux ne peuvent pas installer d'applications et ont besoin d'une autorisation pour installer des applications sensibles.

7. Surveillance :

Pour surveiller nos systèmes afin d'identifier rapidement les incidents et d'initier des efforts de réponse, MS Advanced Threat Protection (ATP) est utilisé sur tous nos points de terminaison et serveurs.

8. Sécurité du réseau :

Pour réduire la probabilité que la connexion de nos réseaux à l'Internet soit exploitée, nous utilisons la protection contre les menaces Meraki sur les NAT de notre pare-feu et MS ATP sur les serveurs.

9. Contrôle des supports amovibles :

Pour souligner la nécessité de protéger numériquement et physiquement les dispositifs amovibles afin d'éviter et de réduire les problèmes de sécurité, nous avons des serveurs situés dans un centre de données restreint qui nécessite une authentification biométrique et qui sont en outre physiquement verrouillés dans une armoire nécessitant une combinaison. Les règles de groupe AD autorisent l'accès à certaines informations avec l'AMF pour tous les accès à distance. MS ATP analyse tous les supports amovibles lors de leur insertion. Les terminaux sont verrouillés par une politique de groupe après 5 minutes d'inactivité pour protéger les données.

10. Responsabilité, éducation et sensibilisation des utilisateurs :

Afin de sensibiliser et d'éduquer notre personnel sur la manière de créer un environnement de cybersécurité efficace, nous utilisons des vidéos de formation Knowbe4, des tests mensuels d'hameçonnage (« phishing ») et des quiz/formations sont donnés aux utilisateurs finaux.

Notre administrateur de système informatique est responsable de tous les éléments liés à la gestion de la cybersécurité.

Notre entreprise contrôle et révise ses procédures au moins une fois par an afin de garantir une gestion efficace de la cybersécurité en réduisant le risque de cybercriminalité. Coalition Inc. procède à des examens annuels de notre cybersécurité. En 2022, nous avons demandé à Vulnerability Scout d'effectuer une analyse des écarts par une tierce partie afin d'examiner nos politiques et de recommander des mises à jour, ce qui a été fait.

Pour démontrer que notre procédure de gestion de la cybersécurité a été communiquée au personnel interne, nous disposons de rapports montrant que des tests mensuels d'hameçonnage sont effectués et d'un registre de formation montrant que le personnel a été informé et formé de manière adéquate à la cybersécurité grâce à l'utilisation de vidéos de formation.