PSSI

Politique de sécurité des Systèmes d'Information

Mars 2021

[0. Sommaire]

[1. Introduction]

[1.1 Contexte de la PSSI]

Argumentons.fr est un site répertoriant des arguments sur divers sujets de débat créé en 2021 par 2 étudiants en informatique basés sur Bordeaux. Il héberge en son sein les courriels utilisés pour la connexion au site ainsi que l'activité de chaque utilisateur sur l'application. Dû à cette collecte d'informations, une sécurité élaborée de la plateforme est nécessaire.

[1.2 Périmètre de la PSSI]

La sécurité des systèmes d'information (SSI) de *Argumentons.fr* couvre l'ensemble des systèmes d'information du site avec toute la diversité que cela implique dans les usages, les lieux d'utilisations, les méthodes d'accès, les personnes concernées…
En termes d'actifs, le périmètre de la PSSI inclut notamment :

- Les actifs matériels :
  - Les systèmes d'information des services et des entités à usage individuel (ordinateur fixe ou portable, logiciels bureautiques, de développement…)
  - Les systèmes de support de l'information (disques, clé USB…) et d'impression
- Les actifs immatériels :
  - Les données liées aux utilisateurs du site
  - Les données associées aux développeurs du site
- Les ressources humaines et morales :
  - Les personnes impliquées dans le développement du site
  - Les utilisateurs du site

- Les tiers définis comme étant toute personne morale ou physique (entreprises, associations…) qui n'est pas placée sous l'autorité du responsable de *Argumentons.fr*.

L'usage des systèmes d'informations est soumis à de nombreux textes législatifs et réglementaires : la loi relative à l'informatique et aux libertés (loi « Informatique et Libertés »), la loi relative à la fraude informatique (loi Gaudfrain), la loi pour la confiance dans l'économie numérique (LCEN), les instructions et recommandations interministérielles provenant du Secrétariat général de la défense nationale (SGDN). S'y ajoutent des dispositions relevant du Code de la propriété intellectuelle et des dispositions pénales. La délinquance informatique a connu une progression fulgurante au cours de ces dernières années. Tout cela conduit à la mise en place de mesures permettant de restreindre les risques encourus.

Le présent document a pour ambition d'établir une référence pour la mise en œuvre de la politique de la sécurité des systèmes d'information (PSSI) au sein du site en prenant en compte ses différentes spécificités.

Cette PSSI fera l'objet de mises à jour en fonction de l'évolution interne ou externe des systèmes d'information et de l'usage qui en est fait.

Ce document s'appuie sur la norme ISO 27001 et suivantes, portant sur la sécurité des systèmes d'information.

[1.3 Le besoin de sécurité]

Tout système d'information comporte de nombreuses vulnérabilités d'origines diverses : structures organisationnelles insuffisamment robustes, routines de gestion ou procédures défaillantes, pannes d'équipements, environnement physique mal contrôlé, multiplicité des intervenants, dépendance à des tiers défaillants, assemblage de composants dont la compatibilité n'est pas garantie, défaillance humaine, etc. Ces vulnérabilités, si elles sont « exploitées », peuvent avoir des conséquences dommageables pour *Argumentons.fr* en termes de temps de travail, de perte d'information, de coût financier, d'image de marque, de réputation…

Le « système d'information » doit donc impérativement être placé à l'abri de menaces internes ou externes. Les données doivent être protégées afin de garantir qu'elles ne soient ni accessibles à des tiers, ni altérées. Les services et applications fournis doivent être disponibles, fiables et garantir des résultats corrects. De plus, la mise en œuvre des systèmes d'information s'inscrit dans un cadre législatif et réglementaire destiné en particulier à protéger les droits de propriété intellectuelle (droits d'auteurs, brevets…) et ceux de la vie privée (fichiers nominatifs, cybersurveillance…). Dans ce cadre peuvent être recherchées les responsabilités administratives ou pénales des différents acteurs : l'utilisateur, les administrateurs systèmes et réseaux et leurs hiérarchies.

La protection du système d'information suppose au préalable d'identifier les actifs en réalisant un inventaire qui intègre notamment les biens matériels (équipements, infrastructure…) et les biens immatériels (données, services…). A chacun de ceux-ci doivent être associés un « propriétaire » et une estimation de sa valeur. Outre l'aspect financier, cette valeur inclut l'intérêt stratégique de l'actif pour *Argumentons.fr*. Celui-ci se définit en termes de besoin en disponibilité, en intégrité, en confidentialité auquel s'ajoutent éventuellement les contraintes juridiques. Il convient ensuite de déterminer les menaces potentielles associées à chacun de ces biens et leur probabilité d'occurrence dans le contexte particulier de leur exploitation. On doit distinguer ce qui relève d'une volonté délibérée ou d'une situation accidentelle. Ces éléments sont la base de l'analyse de risque qui conduit au choix stratégique des mesures à appliquer. Celles-ci peuvent consister à réduire le risque, à le transférer à des tiers ou à l'accepter avec ses conséquences.

[1.5 Inventaire des biens à protéger]

Locaux

Ensemble de moyens	Responsable
Accès à la salle serveur	OVH / Développeur
Accès aux espaces de travail	Développeur

Matériels

Ensemble de moyens	Responsable
Serveur de bases de données	OVH / Développeur
Ordinateurs de travail	Développeur

Logiciels

Ensemble de moyens	Responsable
Base de données	Développeur
Dépôt GitHub	Développeur
OS Linux et Windows	Développeur
Logiciels bureautiques	Développeur

[2. Principaux risques et stratégie de traitement]

[2.1 Origine des risques]

Le périmètre de la PSSI de *Argumentons.fr* considère des origines de menace et risques différents :

- Des risques résultants d'actions ou d'actes malveillants d'origine humaine :
  - Le personnel interne
  - Des criminels auteurs de vandalismes ou de vols
  - Des hackers
- Des menaces d'origine non humaines
  - Des catastrophes naturelles ou des incidents sur le réseau électrique
  - L'espionnage industriel

En revanche, le périmètre de la PSSI du site ne prend pas en compte l'origine de certains risques particuliers, comme les menaces d'origine étatique.

[2.2 Principaux risques identifiés]

Cette section synthétise les différents risques qui pèsent sur le SI du site, les impacts éventuels et l'évaluation de leur gravité, de leur vraisemblance et in fine du niveau de risque associé.

Événement redouté	Source	Impact	Gravité	Probabilité	Niveau de risque
Accès physique au serveur	Intrusion	Destruction du bien ou récupération des données	Fort	TI	Limité
Accès à la BDD	SSH, Web	Vol des données utilisateurs	Fort	P	Modéré
Accès au code source	Dépôt github, ordinateur portable	Code de la BDD	Moyen	P	Modéré
Accès aux mots de passe	Gestionnaire de mot de passe	Tous les codes	Fort	TI	Limité
Accès au dossier	SSH, Web	Code de la BDD, CRUD du site	Fort	P	Modéré

[2.3 Stratégie de traitement]

Les actions de SSI mises en place ont pour objectif de réduire de manière globale l'exposition aux risques. Le tableau précédent précise la stratégie adoptée spécifiquement à chaque risque de manière à ce que le risque résiduel global soit amené au niveau « Limité ».

Cette stratégie de mitigation des risques s'appuie sur un ensemble de règle organisationnelles et techniques valables sur l'intégralité du SI.

[3. Mise en œuvre de la PSSI]

[3.1 Applicabilité de la PSSI]

Après validation des documents, la politique de sécurité des systèmes d'information est applicable.

[3.2 Manquement à la politique de la sécurité des systèmes d'information]

[3.2.1 Mesures applicables par les responsables du site]

Les responsables du site peuvent si nécessaire user de mesures conservatoires :

- Déconnecter un utilisateur, avec ou sans prévis selon la gravité de la situation
- Restreindre ou interdire à un utilisateur l'accès à son compte sur le site
- Imposer un changement de mot de passe à un utilisateur
- Suspendre l'activité d'un processus qui nuirait au bon fonctionnement du site
- Isoler un système d'information du réseau si celui-ci présente un comportement qui mettrait en péril la sécurité du site
- Isoler ou neutraliser provisoirement toute donnée ou fichier qui mettrait en péril la sécurité du site
- Imposer l'installation de logiciels ou de mises à jour de sécurité sur le ou les systèmes d'information concernés

[3.3 Organisation - Responsabilités]

[3.3.1 Responsabilité des différents acteurs]

Les acteurs intervenant en matière de sécurité des systèmes d'information doivent être informés de leurs responsabilités en matière de SSI. Dans l'exercice de leur activité, ils sont liés à leur devoir de réserve voire à des obligations de secret professionnel.

[3.3.2 Responsable de la Sécurité des Systèmes d'Information]

Le responsable de la Sécurité de la Sécurité des Systèmes d'Information (RSSI) exerce sous l'autorité directe du Président de *Argumentons.fr*, les activités suivantes :

- Contribuer activement à l'élaboration d'une politique de sécurité cohérente admise par tous et la mettre en œuvre.
- Coordonner, animer le réseau des correspondants sécurité du site.
- Exploiter et relayer les informations relatives à la sécurité en provenance du CERT-FR.
- Proposer et mettre en œuvre des actions de sensibilisation et d'information de tous les utilisateurs aux aspects sécurité de systèmes d'information.
- Être l'intermédiaire direct en cas de problème en cas de problème entre le Président de *Argumentons.fr* et les autorités compétentes.

[3.4 Protection des données]

[3.4.1 Disponibilité, confidentialité et intégrité des données]

Le traitement et le stockage des données numériques, l'accès au site et services et les échanges de données entre systèmes d'information doivent être réalisés selon des méthodes visant à prévenir la perte, la modification et la mauvaise utilisation des données ou la divulgation des données ayant un caractère sensible.

Une sauvegarde régulière des données avec des processus de restauration régulièrement validés doit être mise en place. On distinguera les sauvegardes de production des sauvegardes de recours. Une étude fine des données permettra de définir la périodicité et le type de sauvegarde ainsi que la durée de rétention dans le respect des législations en vigueur.

[3.4.2 Données à caractère personnel]

Les traitements de données susceptibles de contenir des informations à caractère personnel (au sens de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés) doivent faire l'objet des formalités requises de déclaration ou de demande d'autorisation auprès de la CNIL, via la correspondant CIL du site.

Les données à caractère personnel constituent des données sensibles et comme telles doivent faire l'objet de protection.

[3.4.3 Chiffrement]

Le chiffrement, en tant que moyen de protection, est obligatoire pour le stockage et l'échange de données sensibles. Les produits matériels et logiciels utilisés doivent faire l'objet d'un agrément par la DCSSI. Une copie des clés permettant de restituer les données en clair doit être stockée dans un lieu externe et sécurisé.

ROUZIERE JORIS MICKHAIL JEAN