Argumentaire sécurité

Contexte

Objectif :

- PSSI
- Argumentaire clé en main sur les questions de sécurité liées à Publik et le SaaS Publik EO.

(Version initiale Argumentaire de sécurité)

Autres ressources

- Qualité logicielle : Modèle de réponse aux AO - chapitre "Gestion de projet" - section "Développements".
- Hébergement / SaaS Publik EO : Modèle de réponse aux AO - chapitre "Hébergement en mode Saas".
  - Détail sur les sauvegardes
- Maintenance / Support / Administration : Modèle de réponse aux AO - chapitre "Contrat de maintenance et administration".
- Synthèse dans le document modèle d'annexe aux AO "Plan d'assurance qualité"
- Architecture de Publik : composants, recommandations génériques de sécurité pour un déploiement, etc. dans le document modèle d'annexe aux AO "Architecture technique"

Mesures de sécurité

Entr'ouvert s'engage à mettre en œuvre les mesures de sécurité visant apporter une protection suffisante des données à caractère personnel. Ces mesures devront à la fois porter sur les données à caractère personnelles confiées (a) et sur les mesures générales de sécurité du système (b).

Les mesures de protection sur les données à caractère personnel

Les mesures mises en œuvre par Entr'ouvert doivent être adaptées à la sécurité des données confiées. Entr'ouvert détaillera les mesures de protection des données à caractère personnel mises en œuvre au sein de son organisation, le cas échéant parmi les mesures suivantes.

Le chiffrement des données

Moyens mis en œuvre pour assurer la confidentialité des données conservées (en base de données, dans des fichiers plats, dans les sauvegardes, etc.) ainsi que les modalités de gestion des clés de chiffrement (création, conservation, modification en cas de suspections de compromission, etc.).

Nous respectons le principe de base de la protection des données qu'est la proportionnalité des mesures préventives -- l'envergure de ces mesures étant directement liée à la criticité des données à caractère personnel collectées et traitées dans l'environnement Publik.
Notre moteur de base de données est le SGBDR (système de gestion de bases de données relationnelles) PostgreSQL, outil libre, reconnu pour sa robustesse et sa sécurité.
Nos bases de données, comme le reste de l'infrastructure Publik, sont situées sur des machines physiques hébergées par notre sous-traitant OVH, et accessible seulement à l'aide du protocole SSH par clé RSA (pas d'authentification par mot de passe, jugée d'une sécurité trop faible) par les techniciens de l'équipe d'Entr'ouvert.
L'ensemble de clés autorisées est maintenu de façon cohérente.
Par exemple, lorsqu'un technicien quitte l'équipe, sa clé est désactivée.

Nos bases de données sont aussi sauvegardées toutes les nuits et ces sauvegardes sont stockées sur un site tiers.
Des sauvegardes quotidiennes sont conservées une semaine, et des sauvegardes mensuelles quatre mois.
Les sauvegardes sont détruites au delà de ce délai.

Les mêmes critères de conservation sont appliqués à la sauvegarde des fichiers situés sur le système de fichier réseau NFS (Network File System).
Ces sauvegardes nous permettent entre autres de rétablir un état cohérent des bases de données en cas de compromission des données stockées.

Le chiffrement des flux

Description le cas échéant des moyens de chiffrement employés pour les flux de données (VPN, TLS, etc.) intégrés dans le traitement.

Les communication se font en HTTPS (HTTP sur TLS).
Le certificat HTTPS est soit délivré par la collectivité, soit obtenu via une autorité de certification reconnue (LetsEncrypt, par exemple).

D'un point de vue applicatif, l'interface entre logiciels métiers externes et la fabrique de formulaire contenant les données des utilisateurs se fait à l'aide de requêtes nécessairement signées, réduisant les risques d'usurpation d'identité numérique de l'un de ces logiciels.
Les signatures, de type HMAC (Hashed Message Authentication Code), se basent sur la fonction de hachage SHA-256 (Secure Hash Algorithm, produisant des hachés de 256 bits de longueur), considérée cryptographiquement robuste selon les critères en vigueur de nos jours.

Mesures de securité complémentaires

À défaut de procédure de chiffrement, description de l’existence de procédures garantissant que des tiers au contrat ne puissent pas avoir accès aux données confiées.

Outre les procédures de chiffrement décrites plus haut, nous développons nos applications à l'aide du framework Django.
Ce dernier propose des mécanismes de prévention des attaques usuelles sur le Web (notamment la prévention contre injections SQL, les scripts inter-site (Cross site-scripting, XSS), le forgeage de requêtes inter-site (Cross-site request forgery, CSRF)).

Enfin, la partie publique des clés SSH autorisées à accéder aux différents serveurs est centralisée dans notre dépôt utilisé par l'outil de gestion de configuration de serveur Puppet.
Le retrait d'une clé, par exemple lorsque quelqu'un se voit retirer ses accès aux serveurs, se fait de façon directe, et est appliqué à l'ensemble de notre infrastructure.

L’anonymisation des données

Description des mécanismes d’anonymisation, des garanties qu'ils apportent contre une ré-identification éventuelle et à quelle fin ils sont mis en œuvre.

L'anonymisation des données des utilisateurs est paramétrable dans Publik.
Les mécanismes d'anonymisation sont les suivants :

- anonymisation des données métiers et des données personnelles, par simple effacement des données contenues dans les champs.
- les métadonnées relatives aux demandes des usagers sont aussi anonymisées.
  Parmi ces métadonnées figurent le contexte de soumission de la demande, l'identifiant de l'usager associé à cette demande, ainsi que les rôles destinataires et les données de workflow.
  Une fois anonymisées, les demandes servent encore à des fins statistiques, elles sont injectées dans l'outil de business-intelligence BiJoe.

D'une façon générale, le RGPD impose au minimum l'anonymisation (quand ce n'est pas la suppression) des données dès lors que leur conservation n'est plus utile au traitement auquel l'usager a consenti.
Avec l'accord de la CNIL, avec qui nous travaillons, nous nous imposons un délai maximal de trois mois pour l'anonymisation des demandes contenant des données personnelles des usagers.
Les formations données par nos chefs de projets aux agents, formations relatives à la construction des démarches Publik, tiennent compte de cette nécessité d'anonymiser les demandes contenant des données à caractère personnel.

Le cloisonnement des données

Description des méthodes utilisées pour cloisonner le traitement chez Entr'ouvert.

Le cloisonnement des données dans l'architecture Publik repose principalement sur les propriétés de multitenancy de notre moteur de base de donnée relationnelle PostgreSQL.

Le multitenancy (i.e. "multi-hôte") permet à PostgreSQL d'assurer la séparation des données de plusieurs sites d'une même application.
Dans le cadre d'une installation Publik multi-collectivités, le système de contrôle d'accès basé sur les rôles (Role-Based Access Control, RBAC) permet de s'assurer que les données d'une collectivité restent cloisonnées à cette collectivité et aux rôles qui y sont liés (et donc qu'elles ne puissent pas être lues par un membre d'un autre collectivité de l'instance Publik, ce membre ne possédant pas les rôles adéquats).

Le contrôle des accès logiques

Description de la manière dont les profils utilisateurs sont définis et attribués. Il conviendra de détailler les moyens d'authentification mis en œuvre en précisant, le cas échéant précisez les règles applicables aux mots de passe (longueur minimale, structure obligatoire, durée de validité, nombre de tentatives infructueuses avant blocage du compte, etc.).

Le fournisseur et gestionnaire d'identités de Publik, Authentic, reprend et étend les mécanismes de contrôle d'accès de Django.
Ce fournisseur définit un ensemble de rôles techniques, pour sa gestion en interne, et un ensemble de rôles métiers, voués à être approvisionnés dans les autres briques du logiciels Publik.

Authentic assure aussi l'authentification des comptes usagers de Publik.
Il fournit un mécanisme d'authentification modulaire.
Ainsi, l'usager s'identifie par login/mot de passe, ou bien, si Authentic est configuré pour, de recourir à une fournisseur d'identités tiers (lequel proposera alors indépendemment de Publik ses propres moyens d'authentification).

Le choix d'un mot passe pour l'authentification d'un usager doit respecter les contraintes suivantes :
8 caractères au minimum, dont au moins une lettre minuscule, un chiffre et une lettre majuscule.
La politique de complexité des mots de passe est paramétrable.
Il est aussi possible d'activer un temps d'attente exponentiel après chaque tentative d'authentification infructueuse.

Enfin, le support de l'authentification à plusieurs facteurs est en voie de développement dans notre fournisseur d'identités Authentic.

La politique de journalisation

Description de la politique de journalisation des événements et de conservation des traces qui en résultent.

Une fonction de journalisation des actions impliquant les logiciels métiers externes est mise en place directement dans la base de connecteurs Passerelle.
Par ailleurs, une application de journalisation pour le fournisseur d'identité est en cours de développement.

La politique d'archivage

Description de la politique de conservation et gestion d'archives électroniques contenant des données à caractère personnel destinées à garantir leur valeur, notamment juridique, pendant toute la durée nécessaire (versement, stockage, migration, accessibilité, élimination, politique d'archivage, protection de la confidentialité, etc.).

La conservation des données des systèmes de fichiers réseau inclut l'ensemble des logs Web et applicatifs.
Ces données, bien évidemment à caractère personnel, et à valeur juridique potentielle, bénéficient de la même politique de conservation stricte des sauvegardes des données des serveurs de l'architecture Publik.

La politique de sécurisation des documents papiers

Description de la sécurisation de la gestion des documents papiers (de l'impression au stockage jusqu'à la destruction et aux échanges de documents).

Nous ne proposons pas de service impliquant une gestion de documents au format papier.

La politique de minimalisation des données collectées

La sensibilité des données peut être réduite à l'aide des méthodes suivantes : filtrage et retrait, réduction de la sensibilité par transformation, réduction du caractère identifiant des données, réduction de l'accumulation de données, restriction de l'accès aux données.

La réduction de la collecte des données à ce qui est strictement nécessaire pour mener à bien le traitement fait partie de notre activité d'accompagnement à la conception des démarches dans Publik.
Les formation à la conception de ces démarches ont pour objectif majeur la sensibilisation à la nécessite de minimaliser la collecte de données.

Les mesures générales de sécurité du système

Les mesures mises en œuvre par Entr'ouvert doivent être adaptées à la sécurité des données confiées. Entr'ouvert détaillera les mesures générales de sécurité du système mise en œuvre au sein de son organisation, le cas échéant parmi les mesures suivantes.

La sécurisation de l'exploitation

Description de la politique permettant de limiter la vraisemblance et la gravité des risques visant les biens supports utilisés en exploitation (documenter les procédures d'exploitation, inventaire et mise à jour des logiciels et matériels, correction des vulnérabilités, duplication des données, limiter l'accès physique au matériel, etc.).

L'architecture redondée propose une conteneurisation des applications formant l'environnement Publik. Ces applications sont présentes sur chacun des deux serveurs.
La base de données est elle aussi redondée, sur deux serveurs.
La charge des requêtes Web est répartie entre les deux nœuds du système redondé, et l'attribution à l'un ou l'autre des deux nœuds se fait en fonction de l'adresse IP du terminal de l'usager.

Cette répartition de charge est à la fois disponibles sur les plateformes de devéloppement, de recettes et de production, et les spécifications matérielles de celles-ci sont adaptées à cette charge :

- Plateforme de développement :
  - Processeur : Intel Xeon E5-1660v3 - 8c/16t - 3GHz /3,5GHz
  - Mémoire vive : 128Go DDR4 ECC 2400 MHz
  - Disque : 1,2TB SSD NVMe
- Plateformes de recette et de production :
  - Processeur : Intel 2 x Xeon E5-2640v3 - 16c/32t - 2,6GHz /3,4GHz
  - Mémoire vive : 128Go DDR4 ECC 1866 MHz
  - Disque : 1,2TB SSD NVMe

Les principaux logiciels utilisés et maintenus à jour sont :

- le système d'exploitation Debian.
- la gestion de la configuration des serveurs par Puppet.
- la réplication des données sur périphériques de bloc, par DRBD.
- la répartition de charge par HAProxy.
- le serveur Web nginx.
- l'interface uWSGI entre service Web et applications.
- le framework Web Django.
- nos propres applications formant l'environnement Publik.
  Les mises à jour se font à l'aide du gestionnaire de paquets Debian, apt.

Un système de monitorage (Nagios) des serveurs permet de prévenir et détecter les différents pannes envisageables (serveur down ou saturation de l'espace mémoire RAM ou de l'un des disques notamment).

La limitation des accès physiques au matériel est assurée par notre hébergeur sous-traitant OVH, conformément à ses mesures prises pour le respect de la réglementation européenne en vigueur (https://www.ovh.com/fr/protection-donnees-personnelles/securite.xml).

La lutte contre les logiciels malveillants

Description des mesures destinées à protéger les accès vers des réseaux publics (Internet) ou non maîtrisés (partenaires), ainsi que les postes de travail et les serveurs contre les codes malveillants qui pourraient affecter la sécurité les données à caractère personnel.

Nos services sont déployés sur des machines constamment maintenues à jour (via les dépôts officiels Debian) et accessibles pour administration seulement en SSH (avec clé seulement, pas d'authentification par mot de passe acceptée), réduisant ainsi les risques d'attaque par force brute (attaquer par force brute un mot de passe d'une dizaine de caractère de longueur est très largement faisable, mais en faire de même pour la partie privée d'une clé RSA de 2048 ou 4096 octets de longueur est en pratique fantaisiste).
Nous utilisons strictement des logiciels libres reconnus pour leur rigueur dans la prise en compte des principes de sécurité, et notamment pour la rapidité de fourniture de correctifs logiciels en cas de faille nouvellement identifiée (Common Vulnerability Exposures ou CVE)

Par ailleurs, notre hébergeur OVH s'engage aussi à nous envoyer une alerte courriel dès lors qu'un de leurs outils de monitorage, installés sur nos serveurs, requiert une mise à jour de sécurité.

La gestion des postes de travail

Description des mesures prises afin de diminuer la possibilité que les caractéristiques des logiciels (systèmes d’exploitation, applications métiers, logiciels bureautiques, paramétrages…) ne soient exploitées pour porter atteinte aux données à caractère personnel (mises à jour, protection physique et des accès, travail sur un espace réseau sauvegardé, contrôleurs d’intégrité, journalisation, etc.).

Les mêmes critères de sécurité sont appliqués sur les postes de travail : machines à jour, exécutant des logiciels libres reconnus pour leur rigueur dans la prise en compte des principes de sécurité.

La protection des sites web

Description des méthodes et moyens mis en place pour diminuer la possibilité que les sites web soient exploitées pour porter atteinte aux données à caractère personnel (référentiel général de sécurité, chiffrement TLS des flux, politique de dépôt de cookies, audits de sécurité, etc.).

Nous utilisons une version de support à long-terme (LTS) de Django.
Les mesures de sécurité prescrites ici sont gérées par ce framework, qui fonctionne dans une version maintenue à jour sur notre SaaS.
Comme décrit plus haut dans ce document, ce framework inclut les mécanismes de sécurité adéquats pour faire face aux tentatives d'attaque usuelles sur le Web (injections SQL, session-hijacking, XSS, CSRF, etc.)

La sauvegarde des données

Description de l'existence d'une politique de sauvegarde permettant d'assurer la disponibilité et/ou l'intégrité des données à caractère personnel, tout en protégeant leur confidentialité (régularité des sauvegardes, chiffrement du canal de transmission des données, test d'intégrité, etc.).

La haute-disponibilité des services Publik est assurée par la redondance de l'architecture publique sur notre plateforme SaaS, laquelle bénéficie d'un système de répartition de charge (HAProxy).
L'ensemble des services composant l'environnement Publik sont donc redondés, permettant la continuité en cas de panne (logicielle ou matérielle) d'un des services.
Outre les sauvegardes quotidiennes décrites plus haut, la conservation des transactions récentes sur la base de données permet le rejeu de ces transactions sur le serveur Postgres, assurant ainsi, en cas d'attaque ou d'incohérence des données, un rétablissement de la base à l'instant voulu.

Notre hébergeur OVH assure aussi l'intégrité et la disponibilité des services par diverses mesures telles que la redondance des liaisons réseau, leur propre système de backup et la mise en place de groupes électrogènes de secours assurant plusieurs dizaines d'heures d'autonomie pour leurs sites hébergeant leurs salles serveurs.

La maintenance

Description de l'existence d'une politique de maintenance physique des équipements, précisant le recours éventuel à la sous- traitance. Elle devra encadrer la maintenance à distance si elle est autorisée, et préciser les méthodes de gestion des matériels défectueux.

Tout ce qui est de l'ordre de la maintenance physique est assuré par notre hébergeur sous-traitant OVH.
OVH assure une maintenance physique "au mieux", pour assurer une disponibilité des services 24/7.

Les mesures générale de sécurité du système

Description des mesures en fonction du type de réseau sur lequel le traitement est mis en œuvre (isolé, privé, ou Internet), Entr'ouvert doit mettre en place des systèmes de protection adéquats (par exemple pare-feu, sondes de détection d'intrusion ou autres dispositifs actifs ou passifs sont chargés d'assurer la sécurité du réseau).

Notre hébergeur OVH dispose d'un mécanisme de détection et prévention des attaques par déni de service distribuées (DDoS).
Sur l'ensemble de notre serveur, toute opération jugée suspecte provoque l'envoi d'un mail d'alerte à l'administrateur du serveur
Une restriction des adresses IP à une ensemble d'adresses connues ou préalablement déclarées est en place pour l'accès en SSH aux machines.

Les mesures de sécurité physique

Description de l'existence d'un contrôle des accès physique aux locaux hébergeant le traitement (zonage, accompagnement des visiteurs, port de badge, portes verrouillées, etc.) et description le cas échéant des moyens d'alerte en cas d'effraction.

Les mesures de sécurité physiques sont prises par notre hébergeur OVH et sont détaillées sur leur documentation en ligne (https://www.ovh.com/fr/protection-donnees-personnelles/securite.xml).

La mise en place d'une traçabilité

Description de l'existence de mesures mises en place pour être capable de détecter les incidents concernant des données à caractère personnel de façon précoce et de disposer d'éléments exploitable

s pour les étudier ou pour fournir des preuves dans le cadre d'enquêtes (architecture et politique de journalisation, respect des obligations en matière de protection des données à caractère personnel, etc.).

Les erreurs applicatives ("traces") Django provoquent l'envoi d'un rapport d'erreur à l'adresse électronique de l'administrateur technique de l'application.
En interne, un recueil de fiches post-accident ("postmortem") contenant les mesures correctrices prises est maintenu à jour en continu.

Les mesures de sécurisation des matériels

Description de l'existence de mesures prises pour diminuer la possibilité que les caractéristiques des matériels (serveurs, postes fixes, ordinateurs portables, périphériques, relais de communication, supports amovibles, etc.) soient exploitées pour porter atteinte aux données à caractère personnel (inventaire, cloisonnement, redondance matérielle, limiter l'accès, etc.).

La sécurisation du matériel utilisé par les employés fait écho aux mesures prises en termes de cloisonnement et de traçabilité décrites plus haut.
Une clé SSH par poste et par employé est utilisée pour l'accès aux serveurs, permettant une gestion aisée des accès (octroi ou révocation des droits d'accès aux serveurs, notamment).
Par ailleurs, aucune donnée des usagers n'est stockée sur support amovible.

Notre hébergeur OVH s'engage aussi à maintenir une politique de sécurisation des accès physiques, telle que disponible dans leur documentation (cf https://www.ovh.com/fr/protection-donnees-personnelles/securite.xml → 16. Gestion des accès physiques des tiers → Engagements pris par OVH en sa qualité d'hébergeur).

Les mesures proposées visant à éloigner les risques

Description de l'existence de mesures pour éviter que des sources de risques, humaines ou non humaines, auxquelles il est possible de ne pas être confronté, portent atteinte aux données à caractère personnel (produits dangereux, zones géographiques dangereuses, transfert des données en dehors de l'UE, etc.) Les mesures visant à protéger les données confiées visant à les protéger des sources de risque non humaine (Existence de mesures pour réduire ou éviter les risques liés à des sources non humaines (phénomènes climatiques, incendie, dégât des eaux, accidents internes ou externes, animaux, etc.) qui pourraient affecter la sécurité des données à caractère personnel (mesures de prévention, détection, protection, etc.)

Les mesures de sécurité face à des risques physiques sont prises par notre hébergeur sous-traitant OVH.
Des mesures matérielles telles que la redondance des alimentations électriques, des supports mémoires, des systèmes de refroidissement notamment, sont prises par OVH.

Par ailleurs, notre architecture est redondée sur deux machines physiques différentes, permettant de répondre aux risques d'altération de données ou d'indisponibilité des services sur l'une de ces deux machines.
Les sauvegardes se situent quant à elles sur un autre site géographique encore.