Boite de service
"Analyse de risques" et recommandations SSI
Mars 2018
Rédacteur : Eric CASSETTE
Version : 20180313

Définition :

Boite aux lettres partagées entre plusieurs personnes (même service ou même projet)

Besoins (exemples) :

Afin de faciliter le suivi des requêtes, permettre les échanges de courriers entre un usager et un Service de l'Université en utilisant une adresse générique (service-abcdef@univ-lille.fr) plutôt que des adresses individuelles. L'adresse générique devra pouvoir être utilisée aussi bien en réception (To : service-abcdef@univ-lille.fr) qu'en émission (From :service-abcdef@univ-lille.fr).

Assurer une continuité de service (en cas d'absence ou de départ de personnel).

Réduire les risques de fuites de données sensibles (pas de copie des données dans plusieurs boites aux lettres, y compris dans des boites de personnels n'ayant plus le "besoin d'en connaître").

Minimiser le stockage (pas de duplication des mails et des pièces-jointes).

Vulnérabilités spécifiques au mécanisme des boites partagées :

Si le mécanisme technique choisi implique de partager un mot de passe entre les membres du groupe, un sentiment d'anonymat peut apparaître

Si une adresse générique est utilisée aussi bien en réception qu'en émission, un sentiment d'anonymat peut apparaître.

Si le mécanisme technique implique la définition et la gestion de droits d'accès, le système est vulnérable à des erreurs de configuration.

Si le mécanisme technique implique la définition et la gestion de droits d'accès, le système est vulnérable à une mauvaise gestion du "cycle de vie" des membres du groupe.

Si le mécanisme technique implique de déléguer la gestion des droits d'accès à un utilisateur "Propriétaire", la compromission du compte de cet utilisateur pourrait être utilisée pour commettre des actes malveillants.

Une mauvaise configuration du client de messagerie des membres du groupe pourrait faire apparaître leurs adresses individuelles dans l'adresse d'émission ou l'adresse de réponse.

Les courriels sont stockés uniquement dans la boite partagée, ce qui les rend plus vulnérables à une erreur de manipulation ou à un acte de malveillance

Exemples de scénarios de menaces sur les boites partagées :

Encouragé par le sentiment d'anonymat, un personnel envoie à un usager un courriel "non conforme", contraire à la déontologie ou à la loi

Le Propriétaire se trompe dans la gestion des droits d'accès et accorde des droits en lecture à un ensemble bien trop large

Une personne malveillante profite d'une session non verrouillée de l'utilisateur Propriétaire pour ajouter des accès à la boite partagée

Une personne change de fonction ou de Service, mais conserve des droits de lecture à la boite partagée de son ancien Service, ce qui lui permet de consulter des informations confidentielles (remarque : même principe pour les listes de diffusion si la gestion des abonnés est défaillante)

Un membre du groupe "shunte" l'adresse de service en répondant en son nom propre, ce qui interrompt le circuit normal de la chaîne de courriels (certains courriels concernant un événement n'arrivent plus dans la boite de service partagée)

Un des membres du groupe supprime des courriels dans la boite partagée tout en pensant faire du ménage dans sa boite personnelle

Recommandations de sécurisation (et liste des chargés de leur mise en œuvre) :

Choisir une solution technique permettant de ne pas avoir besoin de partager un mot de passe (Service Messagerie)

Désigner formellement l'utilisateur Propriétaire de la boite partagée (Service Fonctionnel demandeur)

Configurer des droits d'accès à la boite partagée pour accorder des autorisations nécessaires et suffisants à chaque membre du groupe (Propriétaire)

Dans la définition des droits d'accès, différencier éventuellement ces droits en fonction de chaque membre du Groupe ; en particulier, il peut être utile de réserver au Propriétaire les droits de suppression de courriels, ou de répartition dans des sous-dossiers des courriels entrants (Propriétaire)

Gérer les modifications ("cycle de vie") dans la composition du groupe (Service Fonctionnel demandeur, Propriétaire)

Mettre en œuvre un mécanisme de sauvegarde et de restauration de la boite partagée (Service Messagerie pour la sauvegarde, Propriétaire pour la restauration ?)

Recommander la plus grande prudence dans la manipulation de la boite partagée, en particulier dans la suppression des messages ou leur classement (Service Messagerie, Service Fonctionnel, Propriétaire).

Exercer la plus grande prudence dans la manipulation de la boite partagée, en particulier dans la suppression des messages ou leur classement (Membres du Groupe)

Préférer l'archivage des courriels à leur suppression (Propriétaire, membres du Groupe)

Activer un mécanisme de conservation de l'historique des actions (Service Système ou Exploitation)

Prévenir les membres du Groupe que l'utilisation d'une adresse de messagerie de service n'accorde aucun anonymat (Propriétaire)

Prévenir qu'un historique des actions est conservé (Service Messagerie, Service Fonctionnel, Propriétaire)

Configurer les clients de messagerie des membres du groupe pour que les correspondances émises au nom du groupe aient l'adresse générique en adresse d'expéditeur et en adresse de réponse (Informatique de Proximité ou co-administrateurs des postes de travail)

Lors de l'émission d'un courriel au nom du groupe, vérifier que l'adresse générique soit bien sélectionnée en adresse d'expéditeur et en adresse de réponse (Membres du groupe)

Configurer les clients de messagerie pour conserver systématiquement dans la boite partagée une copie de tous les courriels envoyés, ou pour toujours mettre en copie l'adresse de service (Informatique de Proximité ou co-administrateurs des postes de travail)

Configurer les clients de messagerie pour ne pas conserver dans les boites aux lettres individuelles des membres du groupe des copies des courriels envoyés au nom de l'adresse de service (Informatique de Proximité ou co-administrateurs des postes de travail)

Recommandations classées selon le chargé de mise en œuvre :

DSI

Service Messagerie

Choisir une solution technique permettant de ne pas avoir besoin de partager un mot de passe

Mettre en œuvre un mécanisme de sauvegarde et de restauration de la boite partagée

Recommander au Service Fonctionnel la plus grande prudence dans la manipulation de la boite partagée, en particulier dans la suppression des messages ou leur classement

Prévenir le Service Fonctionnel qu'un historique des actions est conservé

Service Système ou Exploitation

Activer un mécanisme de conservation de l'historique des actions

Informatique de Proximité ou co-administrateurs des postes de travail

Configurer les clients de messagerie des membres du groupe pour que les correspondances émises au nom du groupe aient l'adresse générique en adresse d'expéditeur et en adresse de réponse

Configurer les clients de messagerie pour conserver systématiquement dans la boite partagée une copie de tous les courriels envoyés, ou pour toujours mettre en copie l'adresse de service

Configurer les clients de messagerie pour ne pas conserver dans les boites aux lettres individuelles des membres du groupe des copies des courriels envoyés au nom de l'adresse de service

SERVICE DEMANDEUR

Service Fonctionnel demandeur

Désigner formellement l'utilisateur Propriétaire de la boite partagée

Gérer les modifications ("cycle de vie") dans la composition du groupe

Recommander au Propriétaire la plus grande prudence dans la manipulation de la boite partagée, en particulier dans la suppression des messages ou leur classement

Prévenir le Propriétaire qu'un historique des actions est conservé

Utilisateur Propriétaire (administrateur) de la boite partagé

Configurer des droits d'accès à la boite partagée pour accorder des autorisations nécessaires et suffisants à chaque membre du groupe

Dans la définition des droits d'accès, différencier éventuellement ces droits en fonction de chaque membre du Groupe ; en particulier, il peut être utile de réserver au Propriétaire les droits de suppression de courriels, ou de répartition dans des sous-dossiers des courriels entrants

Gérer les modifications ("cycle de vie") dans la composition du groupe

Vérifier la possibilité de restauration de la boite partagée

Recommander aux membres du groupe la plus grande prudence dans la manipulation de la boite partagée, en particulier dans la suppression des messages ou leur classement

Préférer l'archivage des courriels à leur suppression

Prévenir les membres du Groupe que l'utilisation d'une adresse de messagerie de service n'accorde aucun anonymat

Prévenir les membres du Groupe qu'un historique des actions est conservé

Membres du groupe accédant à la boite partagée

Exercer la plus grande prudence dans la manipulation de la boite partagée, en particulier dans la suppression des messages ou leur classement

Préférer l'archivage des courriels à leur suppression

Lors de l'émission d'un courriel au nom du groupe, vérifier que l'adresse générique soit bien sélectionnée en adresse d'expéditeur et en adresse de réponse