Mise en place d'une politique de sécurité dans les systèmes d'information

Le 13 octobre 2020

Nicolas TOURRETTE

Ingénieur Sécurité et Qualité des Réseaux • Développeur • Auteur
www.nicolas-t.ovh • contact@nicolas-t.ovh

Résumé

Le système d'information d'une organisation représente un point de vulnérabilité important compte tenu de son importance stratégique. Il convient donc de veiller à la protection de ce système afin de garantir la sécurité numérique de l'organisme. Pour ce faire, les responsables de tels systèmes d'information mettent en place une politique bien définie afin de protéger les données et de garantir leur disponibilité auprès de leurs collaborateurs. Cette politique de sécurité du système d'information (PSSI) doit être établie en lien avec la direction de l'organisme.

Cet article a été rédigé à partir d'un projet universitaire (ESIREM) commun avec Anindo MOUSSARD. Nous étions encadrés par le professeur Albert DIPANDA (Professeur classe exceptionnelle à l'Université de Bourgogne, directeur de l'ESIREM).

Mots-clés : *PSSI, sécurité, système d'information, stratégie.*

Plan

1 Introduction **1**

2 Sécurité d'un système d'information **2**
2.1 Définition . . . 2
2.2 Grands principes de la sécurité d'un système d'information . . . 2

3 Politique de sécurité d'un système d'information **2**
3.1 Définitions . . . 2
3.2 Rôle de la PSSI . . . 3
3.3 Mise en place d'une PSSI : méthodologie . . . 3
3.3.1 Phase 0 : phase préparatoire . . . 3
3.3.2 Phase 1 : élaboration des éléments stratégiques . . . 3
3.3.3 Phase 2 : sélection des principes et rédaction des règles . . . 4
3.3.4 Phase 3 : finalisation . . . 4

4 Conclusion **4**

1 Introduction

De nos jours, les réseaux ont un impact de plus en plus important sur la vie des entreprises. En effet, le réseau (ou plus généralement le système d'information ou SI) d'une organisation est un élément critique de son fonctionnement. Sans lui, pas de gestion des données de l'organisme, pas de comptabilité, pas d'échanges à l'international, etc. De très nombreuses fonctions sont traitées par le ou les systèmes d'information de l'organisme.

Ce SI étant un élément très sensible, il peut être la cible d'attaques malveillantes dans le but de récupérer des informations sur l'organisme ou encore ralentir son fonctionnement par exemple. Il convient donc alors de mettre en place des procédures et des méthodologies de sécurité communes à l'ensemble du système d'information afin d'en assurer la sécurité.

Nous allons nous voir comment mettre en place une politique de sécurité dans un système d'information.

Dans un premier temps, nous présenterons quelques aspects de la sécurité d'un système d'information pour ensuite détailler une méthodologie de conception d'une politique de sécurité adéquate.

2 Sécurité d'un système d'information

2.1 Définition

Sécurité d'un système d'information — La sécurité d'un système d'information est un ensemble de règles qui permettent de rendre ce système disponible, confidentiel, intègre et accessible uniquement au travers de processus d'identification et d'authentification.

2.2 Grands principes de la sécurité d'un système d'information

La sécurité des systèmes d'information s'appuie donc sur six grands principes que sont la disponibilité, la confidentialité, l'intégrité, l'identification, l'authentification et la non-répudiation.

La disponibilité du système d'information doit être garantie afin que le système reste accessible avec le meilleur temps de réponse. Pour cela, on utilise généralement la règle dite *des 9*, c'est-à-dire garantir que le système reste accessible par les utilisateurs avec une disponibilité de 99,999 % du temps pour cinq "9". Cela revient à limiter le temps d'interruption à environ cinq minutes par année, soit six secondes par semaine.

La confidentialité permet d'assurer la protection des données contre des attaques ou une divulgation indésirable à des personnes non concernées. Il s'agit alors de contrôler l'accès aux données avec une politique de sécurité, notamment en mettant en place des procédures d'identification et/ou d'authentification.

L'intégrité permet de garantir que la donnée est retransmise sans altération au cours d'une communication. On doit alors limiter les interférences ou les modifications de cette donnée lors d'une communication, que celles-ci soient volontaires ou non.

La non-répudiation consiste à s'assurer qu'une action a bien été réalisée par une personne autorisée vers une autre personne, elle aussi autorisée. Il faut donc mettre en place des processus de traçabilité et d'auditabilité.

3 Politique de sécurité d'un système d'information

3.1 Définitions

Commençons par définir les grands principes de la politique de sécurité d'un système d'information. Ces définitions proviennent du *Guide d'élaboration de Politiques de Sécurité des Systèmes d'Information* édité par le Secrétariat général de la défense nationale et l'Agence nationale de la sécurité des Systèmes d'information [1].

1. *Guide pour l'élaboration d'une politique de sécurité de système d'information*, 3 mars 2004, DCSSI/ANSSI.

Politique de sécurité d'un système d'information – PSSI — La politique de sécurité d'un système d'information est l'ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du système d'information de l'organisme.

Principe de sécurité — Les principes de sécurité sont l'expression des orientations de sécurité nécessaires et des caractéristiques importantes de la SSI en vue de l'élaboration d'une PSSI.

Règle de sécurité — Les règles de sécurité définissent les moyens et les comportements définis dans le cadre de la PSSI. Elles sont construites par déclinaison des principes de sécurité dans un environnement et un contexte donnés.

Ainsi, on peut le voir dans ces définitions, la politique de sécurité d'un système d'information est un ensemble composé de principes et de règles de sécurité. Cette politique est appliquée à l'ensemble du système d'information et chacun doit se conformer à cette politique afin d'être acteur de la protection de ce système. Un non-respect de la PSSI peut entraîner un risque majeur dans la sécurité du SI.

3.2 Rôle de la PSSI

Avec l'évolution de la numérisation des procédés dans les entreprises et les administrations (on parlera par la suite d'organismes), on peut voir que le système d'information occupe une place fondamentale dans la vie de celui-ci. Il convient donc d'établir des règles, regroupées dans la PSSI, afin de garantir le bon fonctionnement du SI (et donc de l'organisme) ainsi que la confidentialité nécessaire aux données, même s'il existe deux types de systèmes d'information : les SI usuels et les SI sensibles [2].

On peut donc dire qu'une faille dans la sécurité d'un système d'information peut entraîner l'impossibilité (parfois irréversible) de réalisation des objectifs stratégique de l'organisme. Comme le rappelle le guide, « *la PSSI traduit la reconnaissance formelle de l'importance accordée par la direction générale de l'organisme à la sécurité de son ou ses systèmes d'information.* ». Ainsi, il est important qu'elle soit correctement définie et validée par la direction de l'organisme.

3.3 Mise en place d'une PSSI : méthodologie

La PSSI repose principalement sur quatre dimensions : juridique, organisationnelle et économique, technique et humaine. Finalement, on s'aperçoit qu'on ne peut pas construire ou mener à bien une politique de sécurité sans l'intégration de ces quatre dimensions à celle-ci. La démarche de conception d'une PSSI est découpée en quatre phases.

3.3.1 Phase 0 : phase préparatoire

La première phase du projet d'élaboration a pour objectif principal de définir les objectifs et moyens à mettre en œuvre pour l'élaboration de la PSSI. Elle est menée par le responsable de la sécurité du système d'information (SSI) ou par l'initiateur du projet de PSSI. Il s'agit de définir le cadre documentaire de la PSSI et d'en définir les grandes lignes. Cela conduit à l'élaboration d'une note de cadrage qui devra faire l'objet d'une validation par la direction de l'organisme.

La cadre documentaire doit recenser les aspects légaux et réglementaires, les grands principes d'éthique, les obligations contractuelles auxquelles l'organisme s'est engagé, les obligations contractuelles des prestataires ou partenaires et le référentiel de sécurité interne (document visant à renforcer la confiance des usagers dans les services électroniques proposés par l'organisme : il peut aussi être considéré comme un recueil de bonnes pratiques [3]). Ce document comporte entre autres le schéma directeur informatique et SSI, les analyses de risques ainsi que les résultats d'audits de sécurité du SI.

2. Lire *Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte*, ANSSI, 28 août 2020.

3. Voir *Référentiel général de sécurité*, ANSSI, 13 juin 2014, page 5.

3.3.2 Phase 1 : élaboration des éléments stratégiques

Dans cette phase, il convient de déterminer les axes principaux de la politique de sécurité que nous souhaitons mettre en place. Il va pour cela falloir identifier un certain nombre d'éléments que nous allons détailler.

Il faut tout d'abord délimiter correctement notre SI afin de déterminer sur quel ensemble nous souhaitons mettre en place de la sécurité. Cela permet de ne pas se focaliser sur les éléments qui ne sont pas forcément sensibles : on gagne ainsi du temps et de l'argent.

Il faut ensuite isoler les éléments à plus haut risque afin de déterminer sur quels équipements nous allons concentrer nos efforts. Afin de connaître ces derniers, il est important de réfléchir aux enjeux et contexte de notre politique et cela passe par l'étude des menaces potentielles.

Avec ces éléments, nous pourrons donc réfléchir à l'orientation que va prendre notre stratégie SSI (tout en prenant en compte les aspects légaux) et commencer à réfléchir à nos besoins concernant les grands principes de la SSI.

À noter que les résultats de cette réflexion doivent être présentés à la Direction Générale sous la forme d'une note de stratégie de sécurité.

3.3.3 Phase 2 : sélection des principes et rédaction des règles

Cette phase consiste à rédiger le document contenant la PSSI. Ce document expliquera les choix stratégiques en terme de sécurité et dictera l'ensemble des règles directement applicables afin de garantir cette dernière. Cela aboutira à la rédaction d'une note de synthèse justificative des choix de règles et d'une seconde portant sur les impacts organisationnel et financier.

Il va donc falloir dans un premier temps choisir quels principes de sécurité nous allons mettre en place. Le choix des principes de sécurité s'effectue sur la base des éléments suivants : le référentiel du système d'information (qu'on retrouve dans la note de cadrage rédigée à l'étape 0), la définition du périmètre de la PSSI, la liste de besoins de sécurité identifiés et la liste des origines de menaces retenues (qu'on retrouve dans la note de stratégie de sécurité rédigée à l'étape 1).

Par la suite seront rédigées des consignes à respecter afin de mettre en œuvre les principes de sécurités précédemment déterminés.

3.3.4 Phase 3 : finalisation

Cette dernière phase consiste tout simplement à terminer et faire valider la politique de sécurité du SI. Pour cela, la direction générale de l'organisme devra valider et signer le document. Cela permet de vérifier la cohérence et l'exhaustivité des différentes règles énoncées ce qui va mener à la mise en place d'un plan d'action.

Le plan d'action est la mise en œuvre pratique de le politique de sécurité. Pour cela, il est nécessaire que le personnel compétant soit formé et sensibilisé afin que ce dernier puisse correctement mettre en place ce plan d'action.

4 Conclusion

Cette étude nous aura permis de mettre en exergue la problématique de la sécurité dans les systèmes d'information. Elle en effet primordiale afin de protéger la part numérique de l'organisme et doit répondre à certains critères qui sont la disponibilité, la confidentialité, l'intégrité et la non-répudiation.

Afin de mettre en place une politique de sécurité pour le système d'information, il convient de suivre une stratégie découpée en quatre phases afin de rédiger un ensemble de principes et de règles de sécurité à appliquer dans l'organisme. Ces quatre phases sont la préparation, l'élaboration d'éléments stratégiques suivis de la sélection des principes et de la rédaction des règles et enfin la finalisation de la PSSI.