Support de Formation sur ALCASAR

Partie réglementaire

Alexandre Dey

Validation :

— Jean-François Bellanger

1 Introduction

Le présent document est un support complémentaire fournis dans le cadre de la formation réglementaire autour de l'outil libre ALCASAR. Cette formation a pour but de faire comprendre les enjeux et intérêt liés à l'intégration de cet outil aux Systèmes d'Information (SI).

Cette formation débutera par une présentation du projet ALCASAR, de son origine, sa philosophie, ses objectifs ainsi que des cas d'usage que l'on peut recenser au sein de l'association Antiskwat. Suite à cela, au travers des différents textes de loi et réglementations en vigueur en France, l'accent sera porté sur la nécessité de l'utilisation d'un outil tel qu'ALCASAR associé à la mise en place d'une charte d'utilisation des SI signée par les utilisateurs et les responsables. Enfin une découverte de l'interface de gestion d'ALCASAR sera proposée aux participants et mise en lien avec les problématiques soulevées en début de formation.

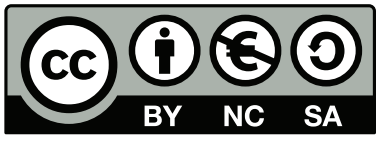

Table des matières

1 Introduction **2**

2 Présentation d'ALCASAR **4**
2.1 Création et évolution du projet 4
2.2 Philosophie et objectifs 4
2.3 Acteurs et utilisateurs 5
2.4 Cas d'usage pour Antiskwat 5
2.4.1 Stations blanches et antivirales 5
2.4.2 Les Kiosques 5
2.4.3 Matériel autonome 6
2.4.4 Les postes nomades 6

3 Les réglementations en vigueur **6**
3.1 À l'échelle européenne 6
3.2 Loi et décrets en France 7
3.3 Les textes institutionnels 7
3.4 Les décisions de justice 8
3.5 Évolution à venir 9

4 Etablir la charte d'utilisation du SI **11**
4.1 Les acteurs de la SSI 11
4.2 Le contenu de la charte 11

2 Présentation d'ALCASAR

2.1 Création et évolution du projet

Pendant la période de Richard Rey en tant que RSSI d'un grand Commandement, le besoin d'un outil à déployer à grande échelle et permettant d'être en accord avec la Loi pour la Confiance à l'Économie Numérique (LCEN) s'est imposé. Après un appel d'offre auprès des acteurs majeurs de l'époque, aucun n'était en mesure de répondre à la problématique, ou alors pour un coût trop important. C'est pourquoi le développement d'ALCASAR a commencé. Tout d'abord réservé à une utilisation au sein de l'armée, le projet a basculé dans le monde du libre suite à la découverte du potentiel de l'outil par le grand public. À partir de ce point, les utilisateurs ont commencé à suggérer des évolutions au projet qui ont été ajoutées par l'équipe de développement et qui font qu'ALCASAR répond maintenant à un large panel de besoins pour des entreprises comme pour des particuliers.

2.2 Philosophie et objectifs

Depuis son lancement, le projet ALCASAR évolue en suivant une éthique forte tout en répondant à des cas techniques assez complexes. En effet, il s'occupe de conserver les traces de connexions par tous les protocoles existant et ce pendant un an. De plus la consultation de ces traces n'est autorisée que par les autorités compétentes et est donc restreinte à celles-ci. Enfin une trace contient la durée et le volume de la connexion mais surtout elle doit être imputable à un humain (et non une machine). Sur ces contraintes de base, les améliorations proposées par les utilisateurs se doivent de respecter les mêmes contraintes éthiques et légales (notamment lorsqu'il s'agit du respect de la vie privée des usagers). Sur le plan technique, ALCASAR se veut être un outil « léger », ce qui fait qu'il n'est pas nécessaire d'avoir un équipement extrêmement performant pour le faire fonctionner. Il est aussi conçu dans une optique de sécurité et de fiabilité. Ceci se ressent par exemple dans le choix de la distribution linux sur laquelle il se base (Mageia), recevant des mises à jour de sécurité régulières et garantissant le bon fonctionnement après mise à jour.

2.3 Acteurs et utilisateurs

Conçu initialement pour les besoins de l'armée, ALCASAR a conservé de ses origines militaires un mode de gestion très pyramidal. Bien que tous les utilisateurs peuvent proposer leurs idées d'améliorations, qui sont ensuite développées par la vingtaine de contributeurs au travers le monde., seuls trois ou quatre personnes parmi ces contributeurs sont autorisées à incorporer les modifications à l'outil qui seront publiées avec la prochaine version. Quant au nombre des utilisateurs, pour des raisons d'éthique, les responsables du projet se refusent de les recenser. En revanche, grâce aux forums et aux propositions d'améliorations, on peut voir qu'ALCASAR est employé dans différents types de structures, du contrôleur d'accès pour les réseaux internet hôteliers à son utilisation au sein de l'armée en passant par les entreprises. Ceci en fait un outil de plus en plus complet, adaptatif et répondant à des besoins très vastes.

2.4 Cas d'usage pour Antiskwat

2.4.1 Stations blanches et antivirales

Dans les locaux d'Antiskwat, on peut trouver des postes fixes connectés sur le réseau ALCASAR. Ils son utilisés pour effectuer des recherches sur Internet sans passer par la plateforme de l'association, parfois trop restrictive. Les communications étant filtrés par ALCASAR, un niveau de sécurité élevé est assuré et le risque d'infection par le biais d'Internet est très fortement réduit. Ceci permet d'utiliser ces stations blanches comme poste de détection des virus pouvant se cacher sur les périphériques des utilisateurs (ex : clefs USB). Ainsi, il est par exemple possible de s'assurer qu'un tel périphérique est sain avant de le connecter à un poste du réseau interne.

2.4.2 Les Kiosques

Les postes Kiosques sont des postes pour lesquels les possibilités d'utilisation sont limitées par un minimum de fonctionnalités. De ce fait, il est possible d'autoriser l'utilisation de ces postes au public, qui ne pourra effectuer d'autres manipulations que celles prévues. Leurs autorisations d'accès au réseau se basent sur une liste blanche : seules les URLs de cette liste sont accessibles aux utilisateurs. On peut utiliser ces Kiosques pour permettre à ceux qui en ont le

besoin d'utiliser les ressources en lignes de l'association, sans pour autant compromettre la sécurité du réseau et/ou de la machine de consultation.

2.4.3 Matériel autonome

Ceci regroupe tous les équipements branchés en réseau mais n'ayant pas les capacités de sécuriser leurs communications. On peut notamment citer parmi ces équipements les imprimantes et les affranchisseuses. Les placer derrière ALCASAR permet de leur éviter les attaques provenant d'Internet tout en permettant aux autres postes connectés au réseau d'y accéder.

2.4.4 Les postes nomades

Ces postes sont des postes pouvant être utilisés à divers endroits et par plusieurs personnes. De ce fait, la sécurité est primordiale. ALCASAR limite les risques de transmissions d'agent infectieux récupérés lors des déplacements et permet en plus la traçabilité des connexions.

3 Les réglementations en vigueur

3.1 À l'échelle européenne

Depuis le 15 mars 2006, la directive européenne 2006/24/CE impose aux fournisseurs d'accès aux systèmes de communication un certain nombre d'obligations relatives aux données de ces communications. Il est tout d'abord imposé de conserver ces données (Article 3). Les autorités nationales compétentes doivent être en mesure d'accéder à ces données dans les plus brefs délais après validation de leur requête (Article 4). La directive s'attarde surtout sur le contenu des données à conserver (Article 5). Ainsi, il doit être possible d'identifier la source de la communication (ex : le nom et l'adresse de l'utilisateur à qui une adresse IP est attribuée), le destinataire de la communication, quand et sur combien de temps la communication a eu lieu, quel type de communication (ex : utilisation d'un service de messagerie, navigation web, ...), le matériel de communication concerné et la localisation de cet appareil. Mais le contenu de la communication ne doit pas être conservé. La directive précise aussi un cadre pour le stockage des données. Tout d'abord, la durée de conservation doit être comprise entre 6 mois et 2 ans (Article

6). Enfin, une sécurisation de ces données est imposée afin de s'assurer que les données ne seront pas perdues et que seules les autorités compétentes puissent y avoir accès (Article 7). Pour finir, est laissée à la charge de l'État l'établissement d'une loi répondant à la directive ainsi que son application, avec notamment la désignation de l'autorité compétente.

3.2 Loi et décrets en France

La Loi pour la Confiance dans l'Economie Numérique (LCEN) du 21 juin 2004 et les différent décrets la consolidant (n°2011-219 du 25 février 2011 et art 1 de la loi n°2016-444 du 13 avril 2016) définissent les données à conserver, de manière similaire à la directive européenne. En plus obligations énoncées précédemment, elle ajoute quelques clauses complétant cette directive. Premièrement elle définit que toute personne fournissant un accès à un réseau de communication au public, se doit de conserver les données et ce pendant 1 an. Sont ainsi concernés tous les chefs d'entreprise, directeurs, gérant d'hôtel camping cybercafé etc, élus responsables d'un réseau public, responsables d'évènements, ... Tout manquement à cette directive est passible d'une amende de 75000€ et de 1 an d'emprisonnement. La LCEN décrit également la procédure d'extraction de ces données dans le cadre d'une enquête judiciaire. Celle-ci est effectuée par des agents désignés par la police nationale ou la gendarmerie nationale. En revanche, la loi n°70-643 du 17 juillet 1970, relative au respect de la vie privée, interdit la consultation de ces données hors du cadre d'une enquête (ou sans l'autorisation expresse et sans réserve de la personne concernée).

3.3 Les textes institutionnels

Différentes institutions françaises s'occupent de réguler l'application de ces lois. La Commission Nationale de l'Informatique et des Libertés (CNIL) impose aux responsables des réseaux un certain nombre de points. Premièrement, les usagers du réseau doivent être informés des données qui sont conservées et ce qui en est fait. Deuxièmement, le responsable doit s'assurer de la sécurité de ces données en mettant en œuvre tous les moyens utiles pour les protéger. Il doit aussi s'assurer que le droit des usagers est respecté (données sensibles, vie privée, ...) et que tout traitement de données soit déclaré à la CNIL. Enfin, sauf dérogation, les données

se doivent d'être stockées dans l'Union Européenne. Tout manquement à ces règles peuvent donner suite à de fortes sanctions pénales (typiquement une amende de 300000€ et 5 ans d'emprisonnement). Relativement à la sécurité, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est chargé de s'assurer de la conformité des réseaux à un niveau minimum de sécurité requis (dépendant des données traitées). Elle fournit également son guide d'hygiène informatique, listant des recommandations à suivre pour améliorer la sécurité d'un SI. Ceci passe premièrement par une étape de sensibilisation et formation des usagers aux bonnes pratiques informatiques. Vient ensuite pour le responsable/administrateur un besoin de connaître son SI (où est doit être quelle machine, quelles sont les postes à risque, ...). Il est aussi important de contrôler et d'authentifier les accès au SI et de s'assurer de la sécurité à la fois des postes, du réseau et du système d'administration du SI. Si certaines machines sont amenées à bouger, il faut être en mesure de gérer ces mouvements (pouvoir retrouver la machine, s'assurer de sa sécurité si elle est connectée à un autre réseau, ...). Il est également fortement recommandé de s'assurer que les composantes du SI soit maintenues à jour. Enfin, il faut continuellement contrôler la sécurité du SI (supervision du système, audit, ...) et préparer un plan d'action en cas de défaillance de celui-ci (attaque, panne, ...).

3.4 Les décisions de justice

Sur certains points, la loi n'est pas suffisamment explicite vis-à-vis des systèmes d'information et de leur sécurité. Dans ces cas, des décisions de justices prise par la Cour de cassation font office de référence.

N°08-17.191 : La société Dassault Systèmes, suite à une loi américaine, a décidé de mettre en place un code de conduite. Ce code contient notamment des règles relatives à la diffusion des informations confidentielles et à usage interne à l'entreprise. Il définit aussi un système d'alerte permettant aux employés de référer des manquements aux codes constatés aux personnes compétentes. La CGT a saisi le Tribunal de Grande Instance en demandant l'annulation de ce code, car il porterait atteinte aux libertés fondamentales des salariés. Le 8 Décembre 2009, la Cour de cassation casse l'arrêt de La Cour d'appel qui avait déclaré le code licite. Premièrement, le code ne définissant pas précisément les informations à usage interne, il n'est pas possible de déterminer si la restriction de la

liberté d'expression est proportionnée et justifiable. Deuxièmement, concernant le système d'alerte professionnel, le code de Dassault contient des clauses non prévues par la CNIL, et de ce fait, n'a pas émit de demande d'autorisation de ces clauses à la Commission. Le Cour de cassation casse l'appel qui déclarait licite le code, car la réglementation française n'autorise le système d'alerte que dans le cadre définit par la CNIL, et uniquement sous autorisation de celle-ci. Enfin, l'appel est cassé car même après déclaration de toutes les données recueillies à la CNIL il est obligatoire d'informer les employés de manière exhaustive sur ces données.

N°00-22.626 : le 19 juin 2003, la Cour de cassation casse et annule un arrêt de la Cour d'appel relatif à une employée qui a utilisé le système d'information de la compagnie d'assurance pour laquelle elle travaille, afin de déclarer de faux sinistres dans le but de payer ses dettes et s'enrichir. La Cour d'appel statuait qu'étant données les carences du système d'information fournit par une compagnie il n'était pas possible de surveiller et restreindre l'utilisation de celui-ci, ce qui a permis à l'employée de l'utiliser hors de ses fonctions, et donc la rend responsable des conséquences de ses actes. La Cour de cassation quant à elle statut qu'étant donné que l'employée a agis sur son lieu de travail pendant son temps de travail et en utilisant le logiciel mis à disposition par son employeur pour effectuer sa mission, elle reste dans le cadre de ses fonctions et par conséquent, l'employeur est tenu pour responsable.

3.5 Évolution à venir

Dans le but d'unifier les lois relatives à la SSI et d'harmoniser la règlementation entre les états membres, l'Union Européenne a promulgué le 24 mai 2016 le Règlement Général sur la Protection des Données (**RGPD**). En plus de cela, elle complète et renforce certains points de la règlementation française détaillée précédemment. Premièrement, la loi s'appliquera à toutes les entreprises et organismes (même hors de l'Europe) qui traitent des données de citoyens de l'UE. Le droit à l'oubli est renforcé en précisant six motifs pour lesquels un usager peut demander la suppression dans les plus brefs délais de données personnelles (*Article 17*). Elle instaure également les principes de "sécurité par défaut" et de "protection des données dès la conception" impliquant que tous les SI doivent être sécurisés dès la conception (*Article 25*). Dans le cas d'une fuite de données repérée,

l'autorité nationale ainsi que les usagers doivent être prévenus immédiatement afin que des mesures puissent être prises rapidement (*Article 33*). La RGPD désigne aussi un nouveau rôle en matière de protection des données personnelles, le *Data Protection Officer* (**DPO**), chargé de s'assurer que la règlementation est bien appliquée et d'être le point de contact avec les autorités. Enfin, les peines encourues pour manquement à ce règlement sont très fortement augmentées, et les amendes s'élèvent à 4% du chiffre d'affaire annuel de l'organisme ou 20 Millions d'euros, en fonction de ce qui est le plus chère. Afin de laisser le temps aux états membres de s'adapter à la nouvelle règlementation, la RGPD ne sera applicable qu'à partir du **25 mai 2018**.

4 Etablir la charte d'utilisation du SI

4.1 Les acteurs de la SSI

Dans sa recherche d'exhaustivité, la loi impose que chaque utilisateur soit informé de toutes les personnes responsables de la Sécurité des Systèmes d'Information. Un moyen simple d'informer les usagers est de mettre à disposition un récapitulatif de l'organisation de la SSI. Pour ceci, la mise en place d'un organigramme est fortement conseillée.

4.2 Le contenu de la charte

La charte d'utilisation du système d'information est avant tout un document à valeur légale. C'est pourquoi l'idéal est de la découper comme un texte de loi, sous formes d'articles. Ceci impose aussi d'être le plus exhaustif possible dans l'établissement de la charte.

Concernant le contenu, en préambule, il faut définir qui sont les différentes parties concernées par la charte. Il s'agit donc préciser qui est l'institution proposant l'accès au système d'information. Le terme de "système d'information" doit aussi être clarifié. Il s'agit aussi de définir qui sont les "utilisateurs" du SI. Enfin, on rappelle les engagements pris par l'institution et les utilisateurs à la signature de la charte.

Viennent ensuite les conditions d'utilisation du système d'information. Tout d'abord, le SI est mis à disposition dans un cadre professionnel, en tant qu'outil de travail. La suite de la charte régit cette utilisation profesionnelle. Il est toutefois possible d'autoriser l'accès au SI dans un contexte privé. Dans ce cas, il faut préciser que l'utilisateur est totalement responsable de son utilisation et qu'il doit explicitement déclarer cette utilisation. On peut aussi rappeler à l'utilisateur les contraintes légales qui s'applique à ce type d'utilisation.

Pour clôturer les conditions d'utilisation, on rappelle l'ensemble des moyens et services mis à disposition des utilisateurs.

Relatif aux règles de sécurité, et pour des raisons légales, en plus des règles d'hygiène du SI, il est important de préciser explicitement les habilitations des usa-

gers et de s'assurer que les informations ne sont accessibles que par les personnes habilitées à y accéder. Il est nécessaire d'interdire spécifiquement à l'utilisateur l'accès et la tentative d'accès aux informations pour lesquelles il n'est pas habilité. Ainsi, si il trouve un moyen d'accèder à ces informations, il ne respecte plus la charte et donc n'accède plus au SI dans le cadre de ses fonctions et par conséquent il est totalement responsable de son utilisation (cf : section 3.4 - **N°00-22.626**). Les mesures mises en place par l'institution pour contrôler la sécurité du SI sont aussi portées à l'attention de l'utilisateur. Celles-ci regroupe notament la maintenance du système d'information, ainsi que les mesures de surveillance de celui-ci.

La charte est chargée de faire prendre connaissance à l'utilisateur de tous les moyens de communication mis à sa disposition et des conditions d'utilisation de ces moyens. En accord avec la LCEN (3.2) et la CNIL (3.3), pour chacun des moyens, des traces sont conservées et certaines limitations peuvent être imposées. Il d'agit ici de spécifier exhaustivement toutes les traces concervées, quelles sont les limitations et pourquoi ces limitations sont imposées. Il est rappelé que toutes les communications peuvent avoir une valeur juridique et que par conséquent, l'utilisateur est responsable de ses communications. Enfin, pour chaque sous-système du SI requiérant une utilisation particulière (ex : logiciels), la charte réfère aux conditions d'utilisation de ce sous-système.

Enfin, la charte rappelle les lois relatives à la propriété intellectuelle et à l'informatique. L'institution s'engage à respecter ces lois et incite l'utilisateur à en faire de même, dans le cas contraire, il en est le seul responsable.

Pour que cette charte soit valable légalement, elle est à signer par la personne juridiquement responsable du système d'information, ainsi que par l'usager. Avant son application elle doit être validée par les délégués du personnel, puis elle doit être déposée au greffe du conseil de prud'hommes et enfin, l'inspection du travail doit en recevoir une copie.