Lignes directrices en matière de sécurité informatique

Exigences applicables aux partenaires

Sommaire

1 Introduction

Le présente document a pour but de lister les exigences de sécurité informatique applicables aux :

- Partenaires connectés à l'infrastructure mutualisée « Connected Mall » fournie par le client
- Partenaires « Real Estate » qui travaillent avec des actifs informatiques du client ou gérant des fonctions d'exploitation du centre (systèmes de gestion des bâtiments et/ou fonctions de sécurité et/ou fonctions de sécurité criminelle).

Ce document est l'instanciation des « Lignes directrices en matière de sécurité informatique des centres commerciaux et des centres d'exposition » qui décrit les mesures à mettre en œuvre par chaque partenaire.

Certaines exigences spécifiques (portant la mention [Sensible]) sont obligatoires pour les partenaires sensibles. Même si ces exigences ne sont pas obligatoires pour les partenaires « non sensibles », elles sont fortement recommandées.

Sont considérés comme des partenaires sensibles :

- Les fonctions de sécurité des biens et des personnes (vidéosurveillance)
- Les parkings partenaires
- Les partenaires gérant les cartes cadeaux

En cas de non-conformité avec un ou plusieurs des exigences suivants, le partenaire doit fournir une justification au client.

La sécurité informatique des actifs informatiques et des communications du partenaire est sous la responsabilité du partenaire. Le client ne sera pas tenu pour responsable si les actifs informatiques du partenaire sont compromis ou si ses communications sont sur écoute illicite.

Réaction attendue de la part du partenaire

Le partenaire doit réaliser une autoévaluation et envoyer au Client :

- La liste des exigences remplies, avec une courte description des mesures mises en place
- La liste des exigences qui ne sont pas remplies, avec une justification, à valider par le Client

Dans l'éventualité d'un contrôle, la non-conformité à un ou plusieurs exigences suivantes qui n'aurait pas été explicitement approuvée par le Client peut être sujette à pénalité.

Un élément non conforme est une exigence précédée par « ☐ ».

2 Exigences générales

2.1 Audit

☐ Le client se réserve le droit de réaliser chaque année un audit afin de vérifier si le partenaire respecte les présentes lignes directrices. L'audit peut être réalisé par le client lui-même ou par un tiers mandaté par le client.

☐ Le partenaire s'engage à collaborer pleinement durant les audits, et à fournir toute preuve demandée par les auditeurs.

2.2 Incidents de sécurité informatique

☐ Lorsqu'il est confronté à un incident de sécurité informatique (virus/logiciel malveillant, intrusion...) qui pourrait avoir un impact sur ses actifs informatiques connectés à l'infrastructure du client, le partenaire s'engage à en informer le client dans un délai de 48 heures.

☐ [Sensible] Le partenaire doit avoir mis en place une procédure de gestion des incidents de sécurité informatique, et cette procédure doit être applicable aux actifs informatiques connectés à l'infrastructure du client.

2.3 Autre

☐ Le partenaire s'engage à ne pas contourner les mesures de sécurité informatique mises en œuvre par le client sur l'infrastructure mutualisée.

☐ [Sensible] Le partenaire s'engage à sensibiliser ses employés aux problèmes et aux bonnes pratiques en matière de sécurité informatique.

☐ [Sensible] Le partenaire doit identifier un point de contact unique avec le client, lequel point de contact gérera toutes les questions de sécurité informatique du partenariat, veillera à ce que les exigences du client soient respectés et interagira avec l'équipe de sécurité informatique du client.

3 Exigences de sécurité informatique

☐ Le partenaire doit avoir obtenu la certification PCI-DSS lorsqu'il héberge et/ou traite des informations relatives à des cartes de crédit.

☐ Le partenaire doit respecter le règlement général européen sur la protection des données, lorsqu'il héberge et/ou traite des données à caractère personnel.

☐ Les informations sensibles (informations d'authentification, informations relatives aux cartes de crédit) doivent être cryptées, qu'elles soient en transit ou au repos.

4 Exigences de sécurité logique

4.1 Protection contre les logiciels malveillants

☐ Les stations de travail et les serveurs sous la responsabilité du partenaire doivent être dotés d'une solution antivirus. La base de signatures doit être tenue à jour.

☐ Si une station de travail ou un serveur est accessible physiquement par du public, les ports USB doivent être désactivés. S'ils ne peuvent être désactivés, l'exécution d'un « autorun » (démarrage automatique) à partir des unités USB doit être désactivée.

4.2 Gestion des patchs

☐ Les actifs informatiques sous la responsabilité du partenaire doivent être tenus à jour. Ce qui signifie que des patchs de sécurité doivent être appliqués régulièrement.

☐ Les actifs informatiques sous la responsabilité du partenaire ne doivent pas être obsolètes (en d'autres termes, ils doivent bénéficier de l'assistance de leurs éditeurs).

4.3 Sécurité des stations de travail

☐ Les accès à distance aux stations de travail ne sont pas autorisés, sauf dérogation explicite du client.

☐ Le partenaire s'engage à ce que tous les logiciels installés sur ses stations de travail et ses serveurs soient strictement nécessaires à la réalisation de sa mission. Aucun autre logiciel ne doit être installé.

☐ Les utilisateurs ne doivent pas bénéficier de privilèges élevés (privilèges d'administrateur ou autres privilèges similaires) sur leurs stations de travail.

☐ Le partenaire s'engage à paramétrer un délai d'inactivité sur ses stations de travail.

☐ [Sensible] Les stations de travail doivent être dotées d'un pare-feu activé (par exemple le pare-feu intégré Windows), qui interdise toute connexion entrante vers la station de travail.

4.4 Autres mesures de sécurité informatique

☐ [Sensible] Les actifs informatiques sous la responsabilité du partenaire doivent être renforcés par le partenaire :

- Désactivation de tous les ports réseau inutilisés
- Désinstallation de tous les services inutiles

☐ [Sensible] Les actifs informatiques sous la responsabilité du partenaire doivent être surveillés par le partenaire afin de détecter tout incident de sécurité informatique (logiciel malveillant, intrusion...).

5 Exigences de gestion de l'identité et de l'accès

5.1 Gestion des comptes

☐ Une authentification doit être requise avant d'accéder à un actif du partenaire.

☐ Le partenaire s'engage à n'utiliser que des comptes individuels et nominatifs.

☐ Le mot de passe utilisé par le partenaire ne doit pas être partagé ni stocké. Le propriétaire du compte doit être le seul à connaître le mot de passe.

☐ Tous les comptes inutiles doivent être désactivés/supprimés, particulièrement les comptes invités et les comptes par défaut du fabricant.

☐ S'ils ne peuvent être techniquement désactivés, les mots de passe des comptes par défaut doivent être modifiés.

5.2 Politique en matière de mots de passe

☐ Le partenaire s'engage à mettre en œuvre la politique suivante en matière de mots de passe, pour ses actifs informatiques connectés à l'infrastructure du client :

- Longueur du mot de passe : 9 caractères
- Complexité du mot de passe : 3 des 4 familles suivantes de caractères (majuscules, minuscules, chiffres, caractères spéciaux)
- Le mot de passe doit être changé au moins tous les semestres
- Le partenaire s'engage à ne pas utiliser les 5 mots de passe précédents

☐ [Sensible] Une authentification multi-facteur doit être en place pour administrer à distance les actifs informatiques du partenaire.

6 Exigences de sécurité des réseaux

☐ Le partenaire s'engage à ne connecter, sur l'infrastructure du client, aucun équipement de réseau qui n'aurait pas été fourni par le client ni explicitement approuvé par le client.

☐ Le partenaire s'engage à n'utiliser qu'une seule interface réseau à la fois sur son serveur et sur ses stations de travail.

ⓘ *Exemple : Se connecter à l'infrastructure du client via une connexion câblée, et en même temps se connecter à tout autre réseau à l'aide d'une connexion sans fil est strictement interdit (et vice versa).*

6.1 Cryptage des réseaux

☐ Les communications qui pourraient acheminer des informations d'authentification (identifiant, mot de passe) doivent être cryptées (utiliser, par exemple, HTTPS, SSH, SFTP).

☐ Le partenaire s'engage à utiliser des technologies standard du marché qui ne sont pas considérées comme étant obsolètes, pour mettre en œuvre le cryptage (par exemple, TLS1.2 pour HTTPS).

6.2 Administration à distance

☐ Les partenaires doivent utiliser des protocoles sécurisés pour administrer les actifs informatiques sous leur responsabilité. Les protocoles non cryptés sont interdits.

6.3 Interconnexions

☐ Si possible, un VPN site à site doit être installé entre l'infrastructure du partenaire et son sous-réseau à l'intérieur de l'infrastructure du client.

☐ Le partenaire doit fournir une matrice précise des flux de réseau, qui indique toutes les communications réseau dont il a besoin. Le client se réserve le droit de réviser la matrice et de la valider/rejeter.

6.4 Connexions entrantes

ⓘ *Les connexions entrantes sont toutes les connexions provenant d'Internet (directement d'Internet ou à travers un VPN) et ayant accès aux actifs informatiques du partenaire.*

☐ Les connexions entrantes ne sont pas autorisées sauf si le partenaire peut justifier ce besoin.

Si des connexions entrantes sont nécessaires :

☐ Le partenaire s'engage à remplir tous les exigences obligatoires concernant la totalité des actifs informatiques déclenchant des connexions entrantes vers l'infrastructure du client.

6.5 Connexions sortantes

ⓘ *Les connexions sortantes sont toutes les connexions provenant des actifs informatiques du partenaire au sein de l'infrastructure du client et ayant accès à Internet.*

☐ Le partenaire s'engage à utiliser de façon appropriée l'infrastructure du client, au regard de la loi en vigueur. Le client se réserve le droit de mettre en place des mécanismes de filtrage du Web et/ou un suivi de l'utilisation d'Internet par les partenaires qui utilisent Internet par le biais de l'infrastructure du client.

Spécificité : systèmes de sécurité des biens et des personnes

Toutes les exigences ci-dessus sont applicables aux systèmes de sécurité des biens et des personnes (vidéosurveillance, contrôle d'accès).

☐ Les systèmes et dispositifs de sécurité doivent être hébergés sur un réseau câblé (aucun WI-FI autorisé).

☐ Les dispositifs doivent être hébergés sur un réseau qui est isolé des autres réseaux (au moins d'un point de vue logique).

☐ Les dispositifs ne doivent pas être en mesure de communiquer les uns avec les autres. A titre d'exemple, les caméras ne sont autorisées à communiquer qu'avec les serveurs de vidéosurveillance.

ⓘ Ceci pourrait être réalisé en hébergeant tous les dispositifs dans un « PVLAN isolated » et en filtrant les communications à partir de l'équipement de routage (via des ACL ou des règles de pare-feu).

☐ La mise en œuvre et la maintenance d'un système de sécurité doivent être en conformité avec la loi locale en vigueur.

☐ Les interfaces d'administration du dispositif ne doit être accessibles qu'à partir du réseau de sécurité.

7 Annexes

7.1 Description de « Connected Mall »

Le client fournit quatre types de services pour les partenaires :

- **Infrastructure réseau :** le partenaire connecte son équipement à l'infrastructure LAN Connected Mall
- **Infrastructure physique :** le partenaire installe son équipement dans une baie spécifique du client
- **Infrastructure de câble :** le partenaire se connecte à l'infrastructure de fibre optique
- **Accès Internet :** le partenaire ne s'abonne qu'à un accès Internet

Ces quatre services peuvent être catégorisés en deux types de risques de sécurité informatique :

- L'interconnexion avec l'infrastructure LAN Connected Mall du client, et par conséquent au système d'information du client
  - Service d'infrastructure réseau
  - Service d'infrastructure physique
- L'utilisation des installations réseau pour se connecter à un réseau qui n'est pas sous le contrôle du client (Internet, réseau du partenaire). Dans ce cas, même si le client est responsable de la fourniture d'un service de connectivité, l'utilisation de ce service est sous la responsabilité du partenaire.
  - Service d'infrastructure de câble
  - Service d'accès Internet

7.2 Glossaire

Incident de sécurité de l'information	Un ou plusieurs événements non désirés et inattendus liés à la sécurité de l'information, qui sont significativement susceptibles de compromettre des opérations commerciales et menacent la sécurité de l'information.
Système d'information	Applications, services, actifs informatiques ou autres éléments gérant des informations.
Risque	La possibilité qu'une menace exploite les vulnérabilités d'un actif informatique ou d'un groupe d'actifs informatiques et, par conséquent, nuise à l'organisation. Le risque s'exprime souvent par une combinaison des conséquences d'un événement et de la probabilité de survenance associée.
Exigence de sécurité	Besoin ou attente formulé(e) (information documentée), généralement implicite (pratique courante) et obligatoire.
Utilisateur	Chaque individu interne ou externe pouvant accéder au système d'information
Compte par défaut	Les comptes qui sont installés par le fournisseur ou le constructeur dans ses produits. Habituellement, ces comptes comportent d'importants privilèges. Les comptes par défaut et leur mot de passe sont habituellement bien connus des hackers (et également disponibles sur Internet).
Système de sécurité des biens et des personnes	Les systèmes de sécurité criminelle sont des systèmes intégrés ou des fonctions d'entreprise visant à protéger les actifs contre les événements criminels. Ces systèmes peuvent regrouper les sous-systèmes de vidéosurveillance, les sous-systèmes anti-intrusion et les sous-systèmes d'accès physique.
Cyber-sécurité/sécurité informatique	Le terme cyber-sécurité est un terme générique pour désigner la sécurité logique des composants informatiques (matériel informatique, micrologiciels, logiciels...).
Système de sureté	Le système de sécurité vise à protéger les actifs contre les événements naturels (exemple : le feu).
Zones informatiques	Les zones hébergeant les composants informatiques. Il peut s'agir de bureaux, de salles informatiques ou de baies de réseau.