Architecture pour la sécurité des Systèmes d'Information selon le modèle OSI

Yann-Eric DEVARS

Table des matières

Couche 1 : Sécurisation de la couche physique 10

Introduction 10

1. Contrôle d'accès physique..... 11

2. Protection et gestion du câblage..... 16

3. Mesures environnementales 20

4. Sécurité électrique 25

5. Protection des équipements et du matériel 27

6. Surveillances et audits réguliers 30

7. Conclusion 33

Couche 2 : Sécurisation de la couche liaison de données 35

Introduction 35

1. Rappels sur la couche Liaison de données 36

2. Principales menaces à la couche Liaison 39

3. Mesures de base pour la sécurisation de la couche Liaison 41

4. Gestion sécurisée du Spanning Tree 46

5. Sécurisation avancée des VLAN 48

6. Détection et prévention des intrusions au niveau de la couche 2..... 50

7. Sécurité des réseaux sans fil (WLAN) en couche 2 52

8. Procédures d'audit et de test de la sécurité en couche 2 53

9. Bonnes pratiques d'exploitation et d'organisation 56

10. Conclusion 58

Couche 3 : Sécurisation de la couche réseau 60

Introduction 60

1. Rappels sur la couche Réseau 61

2. Principales menaces à la couche Réseau 63

4. Sécurité au niveau des adresses IP et du NAT 71

5. Protocoles sécurisés et tunnels : IPsec, VPN, etc. 73

6. Surveillance et détection des anomalies au niveau Réseau..... 76

7. Audits de la couche Réseau 77

8. Organisation et bonnes pratiques globales..... 80

8. Conclusion 82

Couche 4 : Sécurisation de la couche Transport 84

Introduction 84

1. Rappel sur la couche Transport 85

2. Menaces et vulnérabilités spécifiques à la couche Transport..... 88

3. Mécanismes défensifs intégrés au protocole..... 91

4. Dispositifs de sécurisation complémentaires..... 93

5. Mesures contre les attaques DDoS liées à la couche Transport..... 97

6. Sécurisation des protocoles UDP 98

7. Sécurisation de sessions longues et de flux particuliers 99

8. Audit et tests de la couche Transport 101

9. Exemples concrets de mise en œuvre 103

10. Conclusion 105

Couche 5 : Sécurisation de la couche Session.....107

Introduction 107

1. Rappels et positionnement de la couche Session 109

2. Principales menaces et vulnérabilités liées à la couche Session 113

3. Exemples de protocoles et scénarios concrets ..115

4. Mécanismes de sécurisation dans la couche Session 119

5. Éléments d'infrastructure et d'administration pour sécuriser la couche Session 122

6. Méthodologie d'audit et tests de sécurité 124

7. Études de cas pratiques.....127

8. Bonnes pratiques globales pour la couche Session 129

9. Limites et évolutions 131

10. Conclusion 133

Couche 6 : Sécurisation de la couche Présentation ..136

Introduction 136

1. Rappels sur la couche Présentation.....138

2. Menaces et vulnérabilités liées à la couche Présentation.....141

3. Mécanismes de sécurisation propres à la couche Présentation.....143

4. Cadres d'application et scénarios concrets.....146

5. Outils et technologies de la couche Présentation 151

6. Organisation de la sécurité et bonnes pratiques 152

7. Méthodes d'audit de la couche Présentation 154

8. Tendances actuelles et évolutions.....156

9. Conclusion 158

Couche 7 : Sécurisation de la couche Application 160

Introduction 160

1. Rappels sur la couche Application et ses enjeux162

2. Menaces et vulnérabilités courantes au niveau Application.....164

3. Principaux protocoles et vulnérabilités associées 169

4. Mesures techniques de sécurisation de la couche Application.....172

5. Bonnes pratiques de sécurisation côté développement et administration 175

6. Contrôles de sécurité, audits et tests d'intrusion 177

7. Cas pratiques : panorama d'attaques et de défenses 179

8. Approche organisationnelle et gouvernance 182

9. Perspectives d'avenir et tendances 184

10. Conclusion 185

Le mot de la fin 188

La sécurité des systèmes d'information se retrouve au premier plan des préoccupations des DSI, et elle est désormais l'affaire de tous.

Les menaces qui ciblent les réseaux et les applications ne cessent de croître en sophistication, tout comme les exigences réglementaires.

Un solide socle de connaissances s'avère indispensable pour bâtir et maintenir un système d'information résilient.

Cet ouvrage s'adresse à un lectorat varié : architectes du SI, responsables de la sécurité, directeurs techniques, chefs de projet et toute personne soucieuse d'assurer la robustesse de son infrastructure au sens large.

L'objectif est de fournir une approche complète, organisée autour du modèle OSI, permettant d'appréhender la sécurité sous toutes ses facettes, du câblage jusqu'à la couche applicative.

Le choix de structurer les chapitres selon le modèle OSI découle d'un constat simple : une faille à un seul niveau peut compromettre l'ensemble du dispositif.

Attention tout de même, sans se limiter à une simple vulgarisation, ceci n'est pas un référentiel complet des composantes techniques afin de sécuriser un Système d'Information, les exemples techniques ne servant que d'illustration.

Vous devrez vous renseigner précisément sur chaque sujet technique pour être le plus pertinent possible ***d'après votre organisation*.**

Au fil des pages, le lecteur découvrira aussi qu'une stratégie de défense efficace ne se limite pas à l'aspect purement technique : elle implique la sensibilisation des acteurs, la gouvernance, la veille continue et une gestion rigoureuse des risques.

Au-delà de la théorie, vous trouverez des conseils pragmatiques, des retours d'expérience et des études de cas concrets.

Chacun des chapitres est conçu pour éclairer les problématiques rencontrées au quotidien par les équipes de conception, les opérationnels et les décideurs.

Qu'il s'agisse de sécuriser un réseau local, de déployer une architecture multicloud ou de protéger une application métier, la démarche reste la même : comprendre les vulnérabilités possibles, mettre en place des parades adaptées et maintenir une veille active sur l'évolution des menaces et des standards de sécurité.

Bonne lecture

Yann-Eric DEVARS, fondateur de DYNAMAP.


DYNAMAP


7
Application
Présentation
6
5
Session
Transport
4
3
Réseau
Liaison de données
2
1
Physique

Couche 1 : Sécurisation de la couche physique

Introduction

La **couche physique** du modèle OSI (Open Systems Interconnection) représente la base sur laquelle reposent toutes les communications réseau.

C'est à ce niveau que transitent les signaux électriques, optiques ou radio, permettant la transmission de données d'un point à un autre.

On y définit les normes matérielles (câbles, connecteurs, fréquences radio, etc.), les caractéristiques électriques (tension, signal, modulation) et mécaniques (type de connecteurs, format des câbles, disposition physique des équipements).

Dans de nombreux projets, la sécurisation des couches supérieures (logicielles, protocolaires) est considérée comme prioritaire, pourtant, négliger la protection de la couche physique peut provoquer des compromissions graves et parfois difficiles à détecter.

Une simple interruption, une dérivation clandestine du câble ou l'insertion d'un dispositif malveillant sur le chemin physique peuvent aboutir à la perte, la manipulation ou l'espionnage de données critiques.

La mise en place de mesures de sécurité physiques exige une vision d'ensemble : contrôle des accès au bâtiment, surveillance des locaux, gestion des câbles et des points de terminaison, maîtrise des conditions environnementales (température, humidité, prévention incendie), protection de l'alimentation électrique, etc.

Ce chapitre propose donc une analyse détaillée de chaque élément, en insistant sur les bonnes pratiques, la méthodologie et les retours d'expérience du terrain.

1. Contrôle d'accès physique

1.1. Gestion des accès aux bâtiments et aux locaux sensibles

Le point de départ pour sécuriser la couche physique consiste à contrôler rigoureusement l'accès aux infrastructures où se situent les équipements informatiques critiques (centres de données, salles serveurs, zones de câblage).

Ces espaces renferment les composants et connexions indispensables au fonctionnement de tout le système d'information.

- **Systèmes de verrouillage** : La première barrière pour éviter les intrusions est la présence de portes solides, équipées de serrures de haute sécurité ou de dispositifs électroniques (clavier à

code, badges RFID*, badges magnétiques, solutions biométriques).

Le contrôle d'accès peut être géré par un système centralisé, qui enregistre les identifiants des utilisateurs, les heures d'entrée et de sortie, et qui peut être paramétré pour limiter les accès à certaines plages horaires ou selon les besoins de l'activité : urgences, maintenance programmée etc.

- **Badges nominatifs et authentification** : L'émission de badges nominatifs, attribués de façon individuelle et personnelle à chaque collaborateur ou prestataire, constitue un moyen efficace pour tracer les allées et venues.

  On peut coupler ce badge à un code PIN ou à un système biométrique (empreinte digitale, reconnaissance faciale, etc.) pour renforcer l'authentification.

  Dans ce contexte, la gestion du cycle de vie des badges (création, attribution, renouvellement, révocation) doit être rigoureuse.

- **Gestion des visiteurs et des prestataires** : Les personnes extérieures (livreurs, auditeurs, prestataires de maintenance) ne doivent pas accéder librement aux salles sensibles.

RFID* : Méthode d'identification à distance à l'aide de marqueurs et de lecteurs de radiofréquences.

Elles devront être accompagnées, enregistrées et munies d'un badge temporaire ou limité à une zone spécifique.

Une bonne pratique consiste à consigner leur entrée et leur sortie dans un registre (papier ou numérique), et à recueillir leur signature pour attester de leur passage.

- **Sécurisation multi-niveau** : Dans un centre de données de grande envergure, plusieurs niveaux de filtrage se succèdent : l'entrée générale du bâtiment, l'accès à l'étage ou la zone technique, puis l'accès à la salle serveurs proprement dite.

  À chaque niveau, des contrôles d'accès distincts peuvent exiger des méthodes d'authentification différentes, renforçant la sécurité globale.

1.2. Vidéosurveillance et dispositifs de dissuasion

La vidéosurveillance est un élément indispensable pour compléter le dispositif de verrouillage.

Les caméras, idéalement placées à chaque point d'entrée, permettent de détecter rapidement toute présence suspecte et d'enregistrer des preuves visuelles en cas d'incident.

- **Position stratégique des caméras** : Les caméras doivent couvrir les zones les plus importantes (accès principal, locaux techniques,

issues de secours, couloirs menant aux salles informatiques, etc.).

Il est recommandé de limiter les angles morts et de privilégier des caméras haute résolution.

- **Stockage et rétention des enregistrements** : Les images enregistrées doivent être conservées selon une politique de rétention adaptée au risque (plusieurs jours, semaines ou mois).

  Les dispositifs de stockage peuvent être localisés sur un serveur NAS/RAID* à l'extérieur de la pièce surveillée, afin de prévenir la destruction des preuves en cas de sabotage physique.

- **Surveillance active ou passive** : Dans certains environnements critiques (banques, organismes gouvernementaux, sites industriels stratégiques), un service de sécurité peut assurer une surveillance en temps réel des caméras.

  Dans d'autres contextes, on se contente d'une surveillance passive, où les enregistrements ne sont consultés qu'a posteriori pour enquêter sur un incident.

NAS/RAID* : Systèmes de stockage avec une intelligence pour le partage et parfois la classification

- **Signalétique et effet dissuasif** : L'affichage de panneaux indiquant la présence d'un dispositif de vidéosurveillance constitue souvent un moyen de dissuasion efficace.

  Les intrus potentiels savent qu'ils pourront être filmés et identifiés.

1.3. Présence d'un service de sécurité sur site

Dans les structures de grande taille ou sensibles, une équipe de sécurité (agents, vigiles) peut être chargée de contrôler physiquement les accès et de patrouiller dans les zones sensibles.

Leur rôle est d'intervenir rapidement en cas de comportements suspects, de vérifier que les portes ne sont pas laissées ouvertes, d'empêcher l'introduction d'objets illicites, etc.

- **Contrôle manuel des badges et identité** : Les agents peuvent demander l'identité et les justificatifs des personnes entrant dans une salle serveurs.

  En cas de doute, ils peuvent contacter les responsables internes pour obtenir une confirmation.

- **Gestion des livraisons et du matériel entrant** : Tout matériel (serveurs, équipements réseau) livré sur site doit être inspecté.

Il arrive que des dispositifs malveillants soient introduits sous couvert de matériel légitime.

- **Rondes et inspections** : Des rondes régulières, à horaires aléatoires, permettent de vérifier l'intégrité des portes, des baies de brassage, et de repérer d'éventuels signaux d'alerte (câbles débranchés, odeur de brûlé, etc.).
  Des formations sont parfois nécessaires sur les modifications de configuration pour les gardiens ainsi que la planification des revues de check-lists.

2. Protection et gestion du câblage

2.1. Organisation et documentation du câblage

Le câblage réseau, qu'il soit cuivre ou fibre optique, représente la colonne vertébrale de la couche physique.

Sa protection contre le sabotage, le branchement non autorisé ou l'interception des signaux est donc nécessaire.

- **Plan de câblage documenté** : Chaque connexion, chaque route de câble, chaque prise réseau doit être rigoureusement répertoriée.

  On établit généralement un schéma de câblage (ou plan de brassage) décrivant l'emplacement et l'identifiant de chaque point de terminaison.

***Cette documentation facilite la maintenance et l'audit*.**

- **Étiquetage clair et cohérent** : Les câbles (RJ45, fibre) et les panneaux de brassage sont souvent munis d'étiquettes indiquant la destination et l'origine.

  Une nomenclature cohérente (ex. Bâtiment/Étage/Salle-Baie/Port) réduit le risque d'erreur lors des interventions et contribue à repérer rapidement un câble défectueux ou mal branché.

2.2. Chemins de câbles sécurisés et inaccessibles

- **Goulottes, conduits et faux planchers** : Pour empêcher qu'un individu malintentionné n'accède facilement aux câbles, on recourt à des chemins protégés.

  Les goulottes métalliques fermées, les conduits enterrés ou les faux planchers limitent la manipulation directe des liaisons.

  Dans certaines configurations, on installe des barrières infra-rouges ou des détecteurs de vibrations dans ces passages pour signaler toute ouverture ou intrusion.

- **Consolidation des points de brassage** : Il est préférable de centraliser les points de

distribution réseau dans des armoires verrouillables.

Les salles de brassage intermédiaires, souvent situées à différents étages, doivent également être sécurisées par un contrôle d'accès (serrure à clé ou badge).

- **Éviter les trajets non contrôlés** : Les câbles ne devraient pas passer par des zones où circulent du public ou des tiers non autorisés.

  En cas d'impossibilité, il est alors essentiel de recourir à des solutions de blindage et de surveillance régulière.

2.3. Blindage et isolation des câbles

La transmission de données sur un support cuivre (paires torsadées, coaxial) est sensible aux interférences électromagnétiques (EMI) et peut être sujette à des écoutes clandestines.

Pour pallier ces risques :

- **Câbles blindés (STP, FTP, S/FTP*)** : Le blindage (Feuille, Tresse, etc.) réduit grandement les perturbations électromagnétiques.

  Il est particulièrement recommandé dans les environnements industriels ou lorsqu'on craint la proximité de câbles haute tension.

STP, FTP, S/FTP* : Câbles blindés (feuilles, tresses etc.)

- **Fibre optique** : La fibre optique est à la fois plus rapide et plus sûre contre l'écoute passive (par induction ou rayonnement).

  Extraire le signal optique requiert un équipement spécialisé et implique souvent de rompre le câble, ce qui est plus facilement détectable.

  Attention tout de même aux Etats ennemis qui possèdent des moyens capables d'écoutes de proximité sur les fibres optiques.

- **Distance de sécurité** : On évite de faire circuler les câbles réseau parallèlement à des conduites électriques fortes ou des dispositifs générant un champ électromagnétique important.

  Des réglementations (comme celles de la TIA/EIA*) indiquent les distances minimales ou les séparations requises.

2.4. Sécurisation des points de terminaison

- **Boîtiers et verrous de prises RJ45** : Les points d'accès muraux peuvent être protégés par des boîtiers verrouillables, empêchant le branchement arbitraire d'un périphérique.

  Il existe également des bloque-port (port lock) qui se clipsent sur la prise RJ45 pour la rendre inopérante.

TIA/EIA* : Standards de réseau