



RSX112

Sécurité des réseaux

Stéphane LARCHER

Le programme

Introduction à la sécurité et à la gestion des risques informatiques

Concepts de base

Gestion des risques

Primitives Cryptographiques

Cryptographie

Cryptanalyse

Algorithmes de chiffrement

Intégrité et Authentification

Gestion de clés

Le programme

Contrôle d'accès et sécurité de l'information

Authentification

Autorisation

Gestion des identités

Disponibilité et sûreté de fonctionnement

Fiabilité des systèmes

Haute disponibilité

Protocoles de sécurité

Protocoles d'authentification

Sécurité des couches

The background of the image is a composite of financial-themed elements. On the left, there is a grid of numbers in green and red, some with plus and minus signs, resembling stock market data. On the right, a bar chart with vertical bars of varying heights is visible, with some bars colored in a warm orange-gold hue. In the lower right foreground, a pile of various coins is scattered. The overall color palette is dark with blue, green, and orange tones, creating a professional and data-oriented atmosphere.

Des chiffres

Quelques chiffres



2019

- 533 millions de comptes Facebook en 2019
 - Téléphone, identifiant Facebook, nom,
 - localisation, date de naissance, adresse mail,
 - date de création du compte, statut, bio
 - Fichier commercialisé sur le Darknet
 - Puis publication de l'intégralité mi 2021
 - Faille de sécurité :
Fonction import des contacts

2021

- 700 millions de comptes LinkedIn (92% des utilisateurs) en 2021
 - Nom complet, adresse mail, téléphone, employeur, etc.
 - Idem : mise en vente du fichier sur le Darknet
 - Faille de sécurité : XSS (cross-site scripting)

Quelques chiffres

Yahoo
2013-2014

3 milliards de comptes
utilisateurs compromis
leur nom
adresse mail
date de naissance
numéros de téléphone
mot de passe
questions
et réponses de sécurité

Sina Weibo
mars 2020

538 millions de comptes
compromis

Marriott
2014-2018

500 millions de comptes
clients compromis

Starwood hotels

leurs coordonnées, numéro de
passeport
cartes de fidélité
détails de leurs séjours
et autres informations
personnelles
+ 100 millions de numéros de
carte bancaire avec leur date
d'expiration

Quelques chiffres

9,5 trillions \$

- Coût annuel prévu en 2024

90 %

- Signalement de cyber attaques parmi les petites et moyennes entreprises

50 %

- Part du risque des entreprises concernant la cyber sécurité

450 Milliards \$

- Revenus de la cybercriminalité

8,64 Millions \$

- Coût par incident aux U.S.

Quelques chiffres



TOP 10 RISKS IN FRANCE

Source: Allianz Global Corporate & Specialty.

Figures represent how often a risk was selected as a percentage of all responses for that country.

Respondents: 77

Figures don't add up to 100% as up to three risks could be selected.

Rank		Percent	2019 rank	Trend
1	Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)	49%	1 (41%)	=
2	Business interruption (incl. supply chain disruption)	48%	2 (40%)	=
3	Fire, explosion	35%	3 (29%)	=
4	Natural catastrophes (e.g. storm, flood, earthquake)	30%	4 (28%)	=
5	Product recall, quality management, serial defects	18%	8 (12%)	▲
6	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	17%	5 (26%)	▼
7	Political risks and violence (e.g. geopolitical conflict, war, terrorism, civil commotion)	13%	NEW	▲
7	Theft, fraud, corruption	13%	10 (10%)	▲
9	Loss of reputation or brand value	10%	8 (12%)	▼
9	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	10%	6 (18%)	▼

Les risques majeurs pour la France en 2020. Source AOCIS



Concepts de Base de la Sécurité des Réseaux

Concepts de Base de la Sécurité des Réseaux

Confidentialité

Contre l'accès non autorisé
Méthodes de chiffrement

Intégrité

Non modifiées de manière non autorisée
Sommes de contrôle (checksums)
Signatures numériques

Disponibilité

Informations sont disponibles pour les utilisateurs légitimes quand ils en ont besoin
Mesures contre les attaques par déni de service
Plans de continuité d'activité et de reprise après sinistre

Concepts de Base de la Sécurité des Réseaux

Authentification

Vérifie l'identité des utilisateurs et des dispositifs tentant d'accéder au réseau

Seules les entités autorisées peuvent le faire.

Mots de passe

Authentification à deux facteurs

Certificats numériques

Autorisation

Définit et gère les niveaux d'accès aux ressources

Ne peuvent accéder qu'aux données et services pertinents pour leur rôle

Non-répudiation

Empêche les utilisateurs de nier leurs actions

Mécanismes comme les logs d'audit et les signatures numériques aident à assurer la non-répudiation

An aerial photograph of the Chicago skyline, showing a dense cluster of skyscrapers. The Lake Michigan is visible on the left side of the image. The sky is filled with soft, white clouds. The text "Panorama de la cybersécurité" is overlaid in the center of the image.

Panorama de la cybersécurité

Panorama de la cybersécurité

Menaces et Attaques

Inclut tout, des malwares (comme les virus et les ransomwares)

Attaques par déni de service et le phishing

La compréhension des tactiques, techniques, et procédures (TTP) des attaquants est cruciale

Vulnérabilités et Exploits

Les faiblesses dans les systèmes et logiciels peuvent être exploitées par des attaquants

La gestion des vulnérabilités

Evaluation des risques

Application de correctifs

Panorama de la cybersécurité

Stratégies de Défense

Mise en œuvre de couches multiples de mesures de sécurité

Firewalls

Encryptions

Authentification forte

Surveillance des réseaux

Programmes de formation en sensibilisation à la sécurité

Gouvernance et Conformité

Encadre les politiques, les procédures, et les contrôles

Conformité aux réglementations légales et sectorielles

Les impacts



Les impacts

L'obligation légale de notification

Lors d'une fuite de données à caractère personnel joue également un rôle dans la visibilité des cyberattaques.

L'opérationnel

les activités habituelles de l'organisation sont entravées ou rendues impossibles

Impossibilité de soigner les patients dans l'hôpital victime d'un ransomware

Les impacts

L'image

l'image de l'organisation victime est touchée
les clients n'ont plus confiance, et peuvent se tourner vers des concurrents

Financièrement

l'organisation victime peut perdre des parts de marché suite à une attaque

Légalement

Mettent en lumière un non-respect des réglementations et lois, comme l'obligation de sécuriser certains types de données
Le non-respect de ces lois et réglementations peut entraîner des amendes à payer à des régulateurs
La CNIL peut par exemple exiger d'un hôpital victime d'une fuite de données à caractère personnel de verser une amende pour cause de mauvaise sécurisation de son système informatique
L'impact légal peut également concerner le non-respect des engagements contractuels vis-à-vis de tiers, comme des clients



Définitions Clés

Définitions Clés

Cybersécurité

Discipline englobant les technologies, processus, et contrôles conçus pour protéger les systèmes, les réseaux, les programmes, les dispositifs et les données contre les cyberattaques

Cryptographie

Science et pratique du chiffrement et du déchiffrement de l'information. Elle est fondamentale pour de nombreux aspects de la sécurité des réseaux, y compris la confidentialité, l'intégrité, et l'authentification

Gestion des Risques

Processus d'identification, d'évaluation, et de traitement des risques liés à la sécurité des informations. Il vise à minimiser les risques à un niveau acceptable pour l'organisation

Définitions Clés

Sécurité Physique

Bien que souvent considérée comme distincte, la sécurité physique des dispositifs et infrastructures réseau est une composante essentielle de la cybersécurité

Intrusion Detection System (IDS) et Intrusion Prevention System (IPS)

Systèmes conçus pour détecter et, dans le cas d'IPS, prendre des mesures préventives contre les activités malveillantes dans les réseaux

Darknet

Accès via des navigateur spécifiques
(Tor : The Onion Router)

Anonymat et cryptage des échanges

Utilisations

- Cybercriminalité

- Journalisme

- Activisme politique

La vulnérabilité



La vulnérabilité

Une **vulnérabilité** (“faille”)

Faiblesse dans le système d'information
qui, si elle est connue
peut être utilisée pour lancer une
attaque

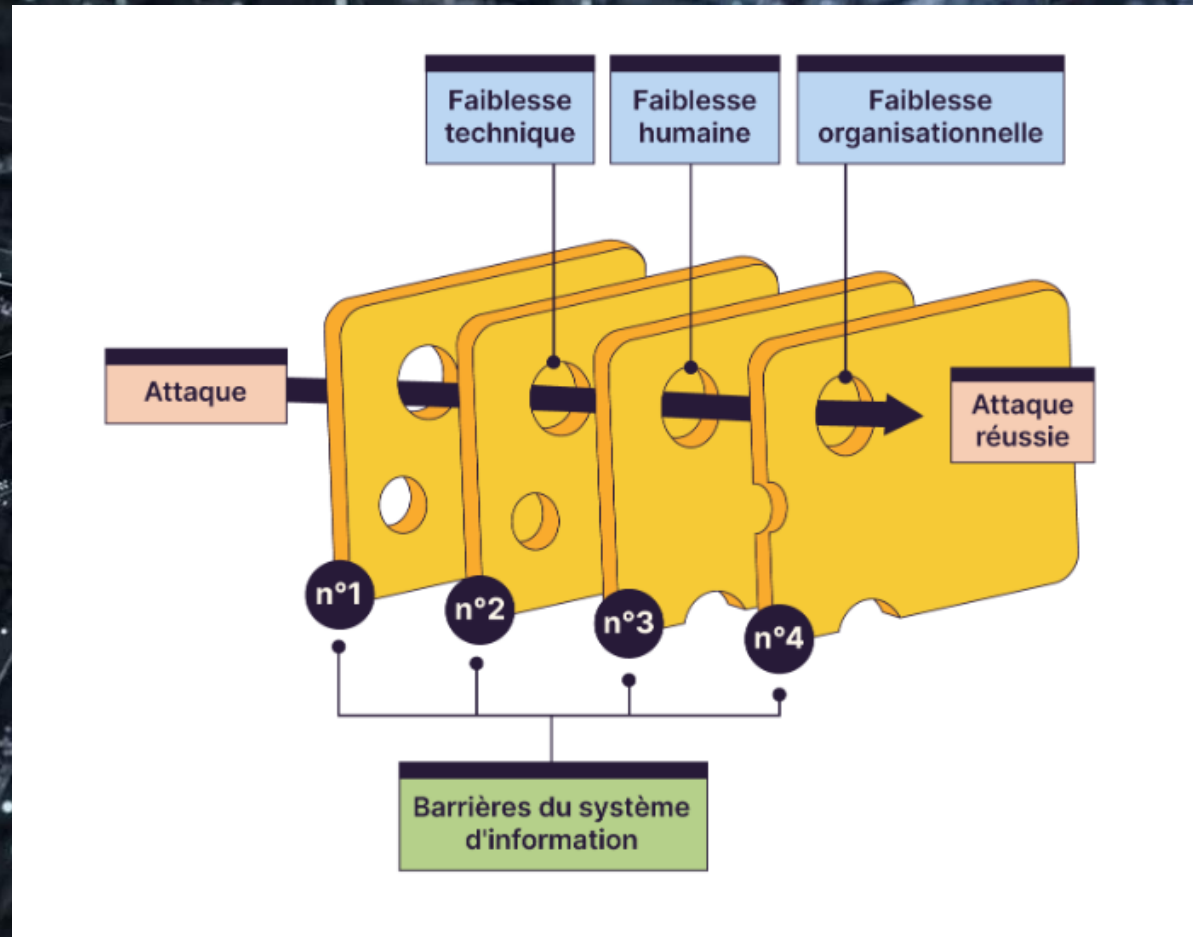
On parle alors
d'exploitation de la
vulnérabilité


Une vulnérabilité résulte d'une
erreur ou d'une malveillance
lors de la conception, de
l'installation ou de l'utilisation
d'un système d'information

Mot de passe faible peut constituer
une vulnérabilité.

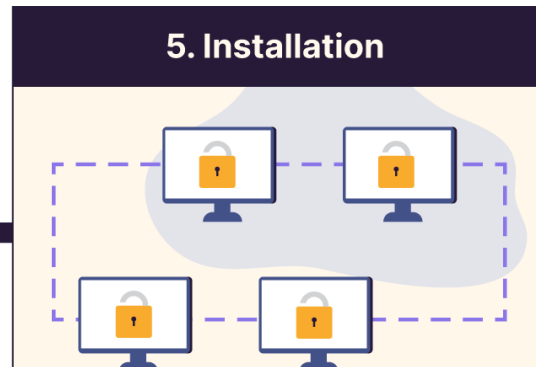
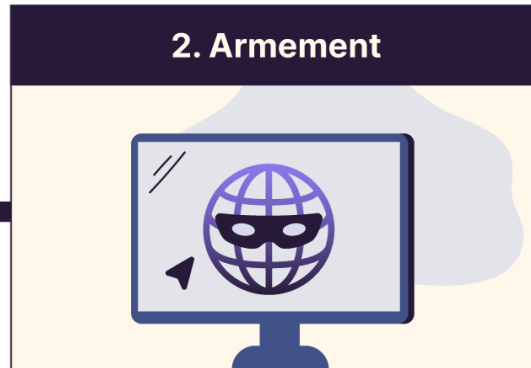
La vulnérabilité

Le modèle du fromage suisse "Swiss Cheese Model"



A person wearing a Guy Fawkes mask and a dark hoodie is shown from the chest up. They are sitting in front of a laptop. The laptop screen displays a terminal window with green text on a black background, resembling a command prompt or a code editor. The text on the screen is partially legible and appears to be a mix of letters and numbers. The overall scene is dimly lit, with the primary light source being the laptop screen.

Le scénario



L'attaque

The background of the slide is a dark, textured image. In the center, there is a Guy Fawkes mask, a symbol often associated with hacktivism. The mask is light-colored with a stylized face. Surrounding the mask and filling the background are faint, glowing patterns of binary code (0s and 1s) in a light blue or green color, giving it a digital or cyber-themed appearance.

Étape 1 - Reconnaissance

L'attaquant recherche et identifie sa cible

Collecter des informations sur la cible, telles que les détails du réseau, les systèmes d'exploitation utilisés, et les failles potentielles

Utilisation d'outils de balayage de ports et de réseaux sociaux pour identifier les employés clés.

L'attaque

The background of the slide is a dark, textured image. In the center, there is a Guy Fawkes mask, a symbol often associated with hacktivism. The mask is light-colored with a stylized face. Surrounding the mask and filling the background are streams of binary code (0s and 1s) in a light green or yellow color, giving it a digital or cyber-themed appearance.

Étape 2 - Armement

Attaquant crée ou achète son outil d'intrusion (un logiciel malveillant, ou malware) sur le dark web

Ce malware exploite une ou plusieurs vulnérabilités dans le système d'information cible

Phishing

L'attaque peut commencer par une campagne de phishing ciblant le personnel de l'hôpital. Un courriel, apparemment légitime, incite le personnel à cliquer sur un lien ou à ouvrir une pièce jointe qui installe un malware sur le réseau de l'hôpital.

Exploitation de vulnérabilités :

Les attaquants peuvent également exploiter des vulnérabilités connues dans des logiciels non mis à jour utilisés par l'hôpital pour gagner un accès non autorisé

L'attaque

The background of the slide features a Guy Fawkes mask, a symbol often associated with hacktivism, set against a dark background with a faint, glowing binary code pattern.

Étape 3 : Livraison

Le logiciel malveillant est transmis à la cible

Pièce jointe d'un mail ou via une clé USB...

Installation de logiciels malveillants

Une fois dans le réseau, les attaquants peuvent installer des logiciels malveillants supplémentaires pour maintenir l'accès, collecter des informations supplémentaires, ou se déplacer latéralement dans le réseau.

Mouvement latéral

Les attaquants cherchent à accéder à d'autres systèmes dans le réseau, souvent à la recherche de données sensibles ou de systèmes critiques pour les opérations de l'hôpital

L'attaque

The background of the slide is a dark, textured image. In the center, there is a Guy Fawkes mask, a symbol often associated with hacktivism. The mask is light-colored with a stylized face. Surrounding the mask and filling the background are streams of binary code (0s and 1s) in a light green or yellow color, giving it a digital or cyber-themed appearance.

Étape 4 : Exploitation

le logiciel malveillant exploite la vulnérabilité identifiée au préalable
c'est-à-dire qu'il tire parti des faiblesses du système d'information cible.

Déploiement de ransomware

Dans de nombreux cas, l'objectif est de déployer un ransomware pour chiffrer des fichiers critiques, paralysant ainsi les opérations de l'hôpital et exigeant une rançon pour le déchiffrement.

Exfiltration de données

Les attaquants peuvent également chercher à voler des données sensibles, telles que des informations sur les patients ou des données de recherche, avant de procéder à l'attaque de ransomware

L'attaque



Étape 5 : Commandement et contrôle

Commandement et contrôle

l'attaquant s'installe de façon permanente dans le système d'information cible

L'attaque



Étape 6 : Action sur l'objectif

l'attaquant réalise ses objectifs initiaux, tels que le vol de données, la destruction de données, ou le chiffrement pour demander une rançon

Demande de rançon

L'hôpital se retrouve face à une demande de rançon pour restaurer l'accès à ses systèmes et données. La décision de payer ou non la rançon implique des considérations éthiques, légales, et pratiques complexes.