Analyse et Traitement des Risques Compétence C1

Simplon
Dr. Toufeik CHOUKRI

Rappel de la Compétence C1

Compétence C1 : évaluation des risques

REFERENTIEL D'ACTIVITES		RÉFÉRENTIEL DE CERTIFICATION		
ACTIVITÉS et TÂCHES	COMPETENCES ASSOCIEES AUX ACTIVITES ET TACHES	COMPETENCES OU CAPACITES EVALUEES	MODALITES D'EVALUATION	CRITÈRES D'ÉVALUATION
A1. Analyse des métiers du commanditaire et évaluation globale de la vulnérabilité de son système d'information				
- Sélection d'une méthodologie d'évaluation du risque - Identification des risques liés aux métiers du commanditaire impactant le système d'information - Élaboration de la liste des incidents redoutés et des impacts associés - Élaboration d'une échelle de gravité des incidents redoutés	C1. Evaluer la criticité des risques liés aux métiers du commanditaire sur le système d'information en exploitant des méthodologies d'identification et de classification des risques.	C1. Evaluer la criticité des risques liés aux métiers du commanditaire sur le système d'information en exploitant des méthodologies d'identification et de classification des risques.	**E1 : Projet professionnel** Le/la candidat(e) doit cartographier les métiers existants au sein de l'organisation. Il/elle doit dresser l'ensemble des risques liés à un métier particulier, résultant de la spécificité des interactions du collaborateur avec le système d'information. A partir de cette analyse, le/la candidat(e) évalue et classifie les risques liés à ces interactions.	Le/la candidat(e) propose une cartographie claire qui identifie l'ensemble des métiers par secteur présents dans l'organisation. Il/elle présente un tableau comprenant l'ensemble des risques liés à chacun des métiers en s'appuyant sur les documents en sa possession, ses connaissances et un état de l'art des incidents opérationnels découlant de sa veille technologique. Il/elle propose une classification des risques cohérente avec leur degré de criticité.
- Analyse de l'architecture réseau	C2. Analyser l'architecture* d'un système d'information et des protocoles de sécurité	C2. Analyser l'architecture* d'un système d'information et des protocoles de sécurité	**E1 : Projet professionnel** Le/la candidat(e) doit réaliser une étude du	Le/la candidat(e) propose une analyse complète du système

Page **4** / **7**

Question préliminaire 1:

Quelles sont, à votre avis, les 3 ou 4 mesures ou recommandations majeures à mettre en place pour sécuriser le SI

Réponse :

Il n’est pas possible de répondre à cette question d’une façon absolue
sans réaliser une évaluation des risques de cybrsécurité du métier et SI concernés

Répondre à la question du **pourquoi**
avant de répondre à la question du **comment**

Question préliminaire 2:

Quelle est la méthode d'analyse et traitement des risques de cybersécurité utilisé par votre entreprise ?

Réponse

Méthodes classiques et standards :

Méthodes usuelles en France
Ebios
Mehari
Standard international
ISO 27005

Notions fondamentales de la sécurité

Question préliminaire 3:

Quelles sont les critères définissant la Sécurité d'un SI (SSI):

- incidents relatifs à la SSI ?
- évènements redoutés relatifs à la SII ?
- risques de cybersécurité ?
- mesures ou contrôles relatifs à la SSI ?
- etc.

Notion 1 : Sécurité d'un S.I.

TCH ©

DÉFINITION DE LA SÉCURITÉ DU SI

- La sécurité d'un S.I. consiste à assurer quatre critères :
  - La **D**isponibilité,
  - L'**I**ntégrité,
  - La **C**onfidentialité,
  - ++ Et les **P**reuves.

  Résumé sous le sigle **D.I.C.P.**

DÉFINITION DES TERMES DICP

- **Disponibilité :**

  Assurer que les utilisateurs autorisés ont accès à l'information et aux actifs associés quand ils en ont besoin et l'usage de ces actifs (ou services).

- **Intégrité :**

  Capacité à maintenir la véracité et la complétude des actifs.

- **Confidentialité :**

  Assurer que l'information n'est accessible qu'aux individus, entités ou processus qui y sont autorisés.

- **Preuves :**

  Garantir la responsabilité et la non-répudiation ainsi que la traçabilité des événements.

Exemples d'évènements/incidents redoutés % DICP

Critère de sécurité impacté	Menaces et évènements redoutés
Disponibilité	Pannes matérielles ou logicielles réseaux Risques d'intrusion sur les réseaux - Interne - externe Attaques par déni de service (DDOS) Attaques en force brute Compromission virale
Confidentialité	Ecoute (ex : logiciel de capture, man in the middle, …)
Intégrité	Erreurs de transmission
Preuve	Manque de traces pour : - Analyser le dysfonctionnement, panne, etc. - Analyser la compromission - Établir les responsabilités

Traitement d'un incident de SSI

Question 4

Quelles sont les informations (ou champs)
à compléter lorsque on enregistre ou traite un incident de SSI (en prenant en compte le DICP)

Traitement d’un incident de SSI

TCH ©

Numéro de l'incident (ou Référence)	Description de l'incdient	Activité de l'entreprise impacté	Critère de SSI concerné	Impacts	Gravité de l'impact (Sévérité de l'incident)				Composants du SI	Vulnérabilités Causes	Mesures
					D	I	C	P			
			Disponibilité								
			Confidentialité								
			Intégrité								
			Traçabilité								

Criticité des impacts et évaluation : définition préalable des niveaux d'impacts

IMPACT DU SCENARIO								
Niveau		**Financier**	**Non-conformité légale, réglementaire ou contractuelle,**	**Nombre de processus/fonctions impactés et niveau de besoin**	**Perte d'image de marque**	**Part de marché**	**Satisfaction clients**	**Santé et salariés**
1	**Léger**	< 100 K Euro	Non-conformité mineure Conditions légales, réglementaires et contractuelles respectées Actions internes, litiges	De 2 à 5 processus/fonctions impactée et niveaux de besoin < 3	Quelques usagers isolés Pas de perte d'image Impact sur l''image interne	Baisse < 1% Parc clients	Clients Insatisfaits ≥ 10% Parc clients	Impacts liés à la biologie et à la chimie : catastophes toxique, incendie, explosion, pandémie, endémie
2	**Important**	De 100 K Euro à 300 K €uros	Non-conformité grave, Conditions légales et/ou réglementaires, et/ou contractuelles non respectées	De 5 à 10 fonctions impactées et au moins 3 en besoin sur un des critères	Plus de 30 % des Clients / partenaires Presse locale	Baisse de 1 à 3% Parc clients	Clients Insatisfaits de 3 à 10% Parc clients	Impacts liés à la manutention et à la circulation : Chute, manutention manuelle, mécanisée, circulations/déplacements, effondrements/chutes d'objets Impacts liés aux équipements : Electricité, machines et ouilts
3	**Critique**	> 300 K€ à 10M Euro	Non-conformité légale , mise en question de la structure, Problème concernant tous les contrats.	> 10 fonctions impactées et au moins 3 en besoin sur un des critères	Public - Perte d'image stratégique Tribunal de commerce, presse et média¨ Presse économique	Baisse de 3 à 10% Parc clients	Clients Insatisfaits de 1 à 3% Parc clients	Imapcts liés à l'ambiance : bruit, vibrations, ambiances thermiques, rayonnements, ambiances lumineuses.
4	**Vital**	>10M Euro	Non-conformité légale majeure, fermeture cessation de l'activité, Problème concernant tous les contrats. Dommages et intérêts, RSE	Toutes les fonctions sont impactées	Public - Perte d'image stratégique - atteinte image gouvernementale - International	Baisse ≥ 10% Parc client	Clients Insatisfaits < 1% Parc clients	Impacts liés à l'organisation : Intervention d'une entreprise extérieure, organisation interne du travail

Notions d’analyse et traitement des risques des SSI

Notions d'analyse et traitement des risques des SSI

En plus des notions précédentes concernant l'analyse et le traitement des incidents, il faut rajouter quelques notions complémentaires importantes :

1/ Vraisemblance d'un évènement

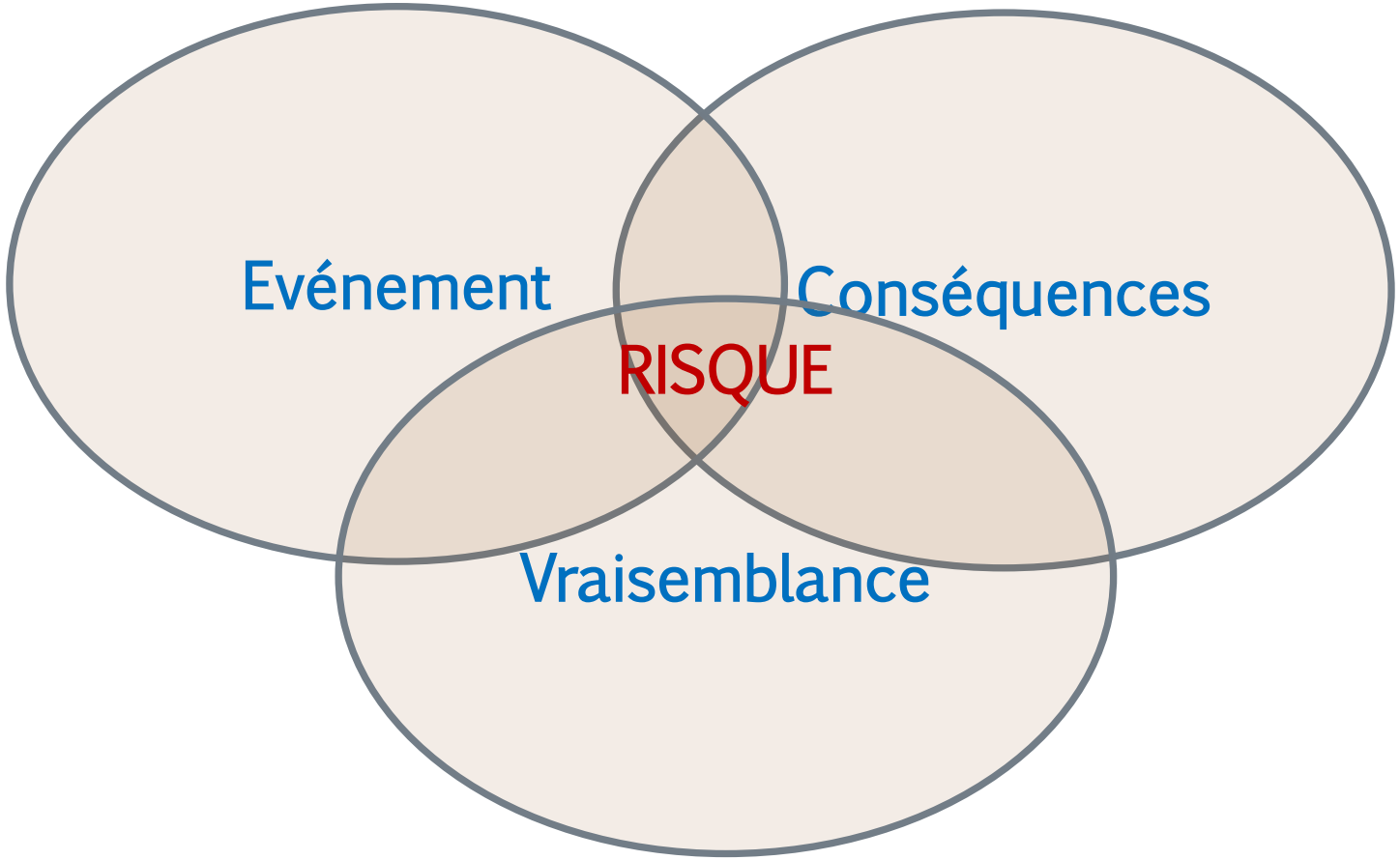
2/ Niveau de risques

Notions de risque

TCH ©

Risque

Combinaison des conséquences d'un évènement et de sa vraisemblance sur un actif de valeur



Criticité des impacts et évaluation : définition préalable des niveaux d'impacts

IMPACT DU SCENARIO								
Niveau		**Financier**	**Non-conformité légale, réglementaire ou contractuelle,**	**Nombre de processus/fonctions impactés et niveau de besoin**	**Perte d'image de marque**	**Part de marché**	**Satisfaction clients**	**Santé et salariés**
1	**Léger**	< 100 K Euro	Non-conformité mineure Conditions légales, réglementaires et contractuelles respectées Actions internes, litiges	De 2 à 5 processus/fonctions impactée et niveaux de besoin < 3	Quelques usagers isolés Pas de perte d'image Impact sur l''image interne	Baisse < 1% Parc clients	Clients Insatisfaits ≥ 10% Parc clients	Impacts liés à la biologie et à la chimie : catastophes toxique, incendie, explosion, pandémie, endémie
2	**Important**	De 100 K Euro à 300 K €uros	Non-conformité grave, Conditions légales et/ou réglementaires, et/ou contractuelles non respectées	De 5 à 10 fonctions impactées et au moins 3 en besoin sur un des critères	Plus de 30 % des Clients / partenaires Presse locale	Baisse de 1 à 3% Parc clients	Clients Insatisfaits de 3 à 10% Parc clients	Impacts liés à la manutention et à la circulation : Chute, manutention manuelle, mécanisée, circulations/déplacements, effondrements/chutes d'objets Impacts liés aux équipements : Electricité, machines et ouilts
3	**Critique**	> 300 K€ à 10M Euro	Non-conformité légale , mise en question de la structure, Problème concernant tous les contrats.	> 10 fonctions impactées et au moins 3 en besoin sur un des critères	Public - Perte d'image stratégique Tribunal de commerce, presse et média¨ Presse économique	Baisse de 3 à 10% Parc clients	Clients Insatisfaits de 1 à 3% Parc clients	Imapcts liés à l'ambiance : bruit, vibrations, ambiances thermiques, rayonnements, ambiances lumineuses.
4	**Vital**	>10M Euro	Non-conformité légale majeure, fermeture cessation de l'activité, Problème concernant tous les contrats. Dommages et intérêts, RSE	Toutes les fonctions sont impactées	Public - Perte d'image stratégique - atteinte image gouvernementale - International	Baisse ≥ 10% Parc client	Clients Insatisfaits < 1% Parc clients	Impacts liés à l'organisation : Intervention d'une entreprise extérieure, organisation interne du travail

Définition préalable des niveaux de vraissemblance

VRAISSEMBLANCE
Rare (0)
Probable (1)
Occasionnel (2)
Certain et/ou Récurrent (3)

Définition préalable des niveaux de risques

VRAISSEMBLANCE	IMPACT			
	Léger	Important	Critique	Vital
Rare (0)	1	2	3	4
Probable (1)	2	3	4	5
Occasionnel (2)	3	4	5	6
Certain et/ou Récurrent (3)	4	5	6	7

Termes et définitions

TCH ©

Risque
Combinaison des conséquences d'un événement et de sa vraisemblance sur un actif de

Actif de valeur

Un équipement ou solution du système d'information qui a de la valeur pour l'activité de l'entreprise, représenté par un propriétaire

Services/Activités

Les services ou les activités supportés par l'actif en question

Evénement (événement redouté)

Occurrence ou changement d'un ensemble particulier de circonstances.

Conséquence / impact

Résultat d'un événement affectant les objectifs.

Vraisemblance (probabilité)

La chance que quelque chose se produit.

Termes et définitions

TCH ©

Risque
Combinaison des conséquences d'un événement et de sa vraisemblance sur un actif de

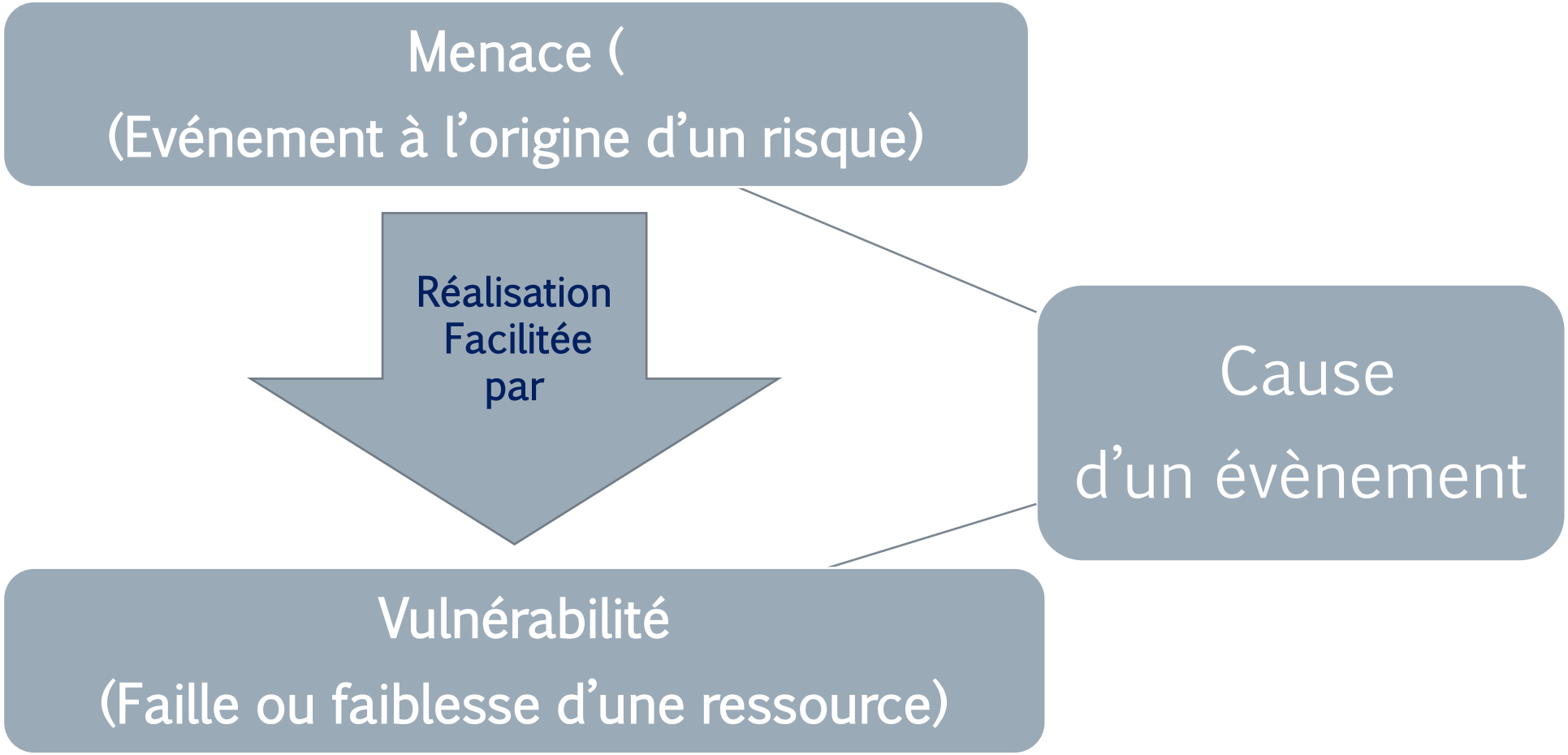
Exemples d'Actif de valeur pour les infrastructures réseaux

- Équipements et services de communications
  - Câblages
  - Switchs
  - Routeurs
- Equipements et services réseaux à valeurs ajoutées
  - Proxies
  - Firewall
  - DNS
  - DHCP
  - VPN
  - PKI
  - Loadpalancer
  - Etc.

Notions de cause d'un évènement: menace et vulnérabilités

TCH ©

Cause d'un évènement



Notions de cause : menace et vulnérabilité

TCH ©

Cause d'un évènement

Menace

Vulnérabilité

Cause

Notions de cause : menace et vulnérabilité

TCH ©

Réduction d'un risque : en réduisant la cause et la vraisemblance

Menace
(Hacker)

Vulnérabilité
(CVE xxxx)

Cause → Impacts

Vraisemblance

Occurrence
d'un Risque

Pour réduire un niveau de risque, il faut réduire un ou plusieurs facteurs du risque :
1/ l'impact
2/ la cause (en réduisant la menace ou la vulnérabilité)
3/ la vraisemblance de l'occurrence de l'événement

Notions d'enjeux et d'impacts

TCH ©

Enjeux et impacts sur l'entreprise (et non sur le SI)

Types d'impacts (vis-à-vis de l'entreprise)	
Financier	Perte de chiffre d'affaires Baisse en bourse Pénalités
Image de marque	Dégradation de l'image de marque Perte de confiance
Légal et réglementaire	RGPD Réglementaire sur le e-commerce Réglementation bancaire Réglementation sur Carte bancaire Réglementation dans le secteur de la santé Etc.
Part de marché	Perte de part de marché suite au désistement des clients, des fournisseurs, etc.

Présentation de la chaîne de la mort « kill chain » relative à la sécurité des réseaux

Gestion des vulnérabilités techniques
Selon la chaîne de la mort « Kill Chain »

En attaque	En défense
Etape 1 : Détection des vulnérabilités	1- Gestion des vulnérabilités : - Détection et enregistrement pour le suivi - Traitement des vulnérabilités par ordre de priorité (élimination ou contournement-rustine) - Revérification 2- IPS/IDS 3- Filtrage des flux entrants
Etape 2 : Vérification des vulnérabilités exploitables	
Etape 3 : Choix des vulnérabilités à essayer d'exploiter	
Etape 4 : Réalisation des différentes tentatives	
Réalisation de l'exploit (intrusion)	
Etape 5 : Installation et mise en place du flux de communication de commande (CC)	Filtrage des flux sortants (et entrants)
Etape 6 : Mouvements latéraux (compromission d'autres systèmes)	Cloisonnement des réseaux
Etape 7 : Exploitation du méfait (Ransmware, détournement, fraude, …)	Mesures spécifiques : Ransmware : PCA Fraude : outil de détection de fraude Etc.

Rétro-analyse de la kill chain d'un incident d'intrusion

TCH ©

Mitsubishi Electric discloses security breach, China is main suspect

Mitsubishi Electric says hackers did not obtain sensitive information about defense contracts.

In a short statement published today on its website, Mitsubishi Electric, one of the world's largest electronics and electrical equipment manufacturing firms, disclosed a major security breach.

10 dangerous app vulnerabilities to watch out for (free PDF)

Although the breach occurred last year, on June 28, and an official internal i[illegible] began in September, the Tokyo-based corporation disclosed the security incident today, only after two local newspapers, the Asahi Shimbun and Nikkei, published stories about the hack.

Both publications blamed the intrusion on a Chinese-linked cyber-espionage group named Tick (or Bronze Butler), known to the cyber-security industry for [illegible] past few years [1, 2, 3, 4, 5, 6, 7, 8, 9, 10].

Enjeux industriels (espionnage industriel)

Entre l'intrusion et la découverte, 2 à 3 mois

Menace : équipe de hacker professionnelle

Référence :
https://www.zdnet.com/article/mitsubishi-electric-discloses-security-breach-china-is-main-suspect/

Rétro-analyse de la kill chain d'un incident d'intrusion

TCH ©

Mitsubishi Electric discloses security breach, China is main suspect

Mitsubishi Electric says hackers did not obtain sensitive information about defense contracts.

HACK ORIGINATED FROM A CHINESE AFFILIATE

According to the reports in local media, the intrusion was detected after Mitsubishi Electric staff found a suspicious file on one of the company's servers.

"Unauthorized access began with affiliates in China and spread to bases in Japan," Asahi reported.

The newspaper said hackers escalated their access from this initial entry point to Mitsubishi Electric's internal systems, gaining access to the networks of around 14 company departments, such as sales and the head administrative office.

The two newspapers reported that hackers stole sensitive data from the company's internal network. In particular, Nikkei reported that hackers compromised "ten of [illegible] Japan and overseas," from where they stole around 200 MB of files, mostly business documents.

Mitsubishi Electric did not deny that data exfiltration took place, but only denied that the intruders stole data on its business partners and defense contracts.

The company said it's still investigating the incident, but according to open-source reporting the attackers appeared to have deleted access logs, slowing down investigators.

Mouvements latéraux

Entre l'intrusion et la découverte, 2 à 3 mois

Vol d'information sensible

Investigation : besoin de SIEM

Référence :
https://www.zdnet.com/article/mitsubishi-electric-discloses-security-breach-china-is-main-suspect/

Rétro-analyse de la kill chain d'un incident d'intrusion

TCH ©

Mitsubishi Electric discloses security breach, China is main suspect

Mitsubishi Electric says hackers did not obtain sensitive information about defense contracts.

MAJOR SECURITY BREACH IN JAPAN

In Japan, the incident is being treated with the utmost severity. Mitsubishi Electric is one of Japan's biggest defense and infrastructure contractors, with active projects within the Japanese military, but also telecommunications, railways, and the electrical grid.

Before going public with the news today, Mitsubishi Electric had also notified members of the Japanese government and Ministry of Defense, according to local newspaper Mainichi.

Enjeux plus important

Référence :
https://www.zdnet.com/article/mitsubishi-electric-discloses-security-breach-china-is-main-suspect/

Rétro-analyse de la kill chain d'un incident d'intrusion

TCH ©

Mitsubishi Electric discloses security breach, China is main suspect

Mitsubishi Electric says hackers did not obtain sensitive information about defense contracts.

Tick's favored method of operation begins by stealing email accounts belonging to private market research firms. The hackers then send emails to Chinese subsidiaries of target corporations in the guise of the research firms

The emails contain malware that can be controlled remotely by Tick. Using the subsidiary's computer system as a steppingstone, the hackers can gain access to the parent company's networks and steal sensitive information.

Méthode Phishing

The latest attack was reported Monday by Japan's Mitsubishi Electric. Cyberthieves may have gained access to more than 8 [illegible] information, the company said, but reported that no highly sensitive information had been compromised.

RGPD

Référence :
https://www.zdnet.com/article/mitsubishi-electric-discloses-security-breach-china-is-main-suspect/

Rétro-analyse de la kill chain d'un incident d'intrusion

TCH ©

Mitsubishi Electric discloses security breach, China is main suspect

Mitsubishi Electric says hackers did not obtain sensitive information about defense contracts.

MAJOR SECURITY BREACH IN JAPAN

In Japan, the incident is being treated with the utmost severity. Mitsubishi Electric is one of Japan's biggest defense and infrastructure contractors, with active projects within the Japanese military, but also telecommunications, railways, and the electrical grid.

Before going public with the news today, Mitsubishi Electric had also notified members of the Japanese government and Ministry of Defense, according to local newspaper Mainichi.

Enjeux plus important

Référence :
https://www.zdnet.com/article/mitsubishi-electric-discloses-security-breach-china-is-main-suspect/

Synthèse de la kill chain relatif à cet incident

TCH ©

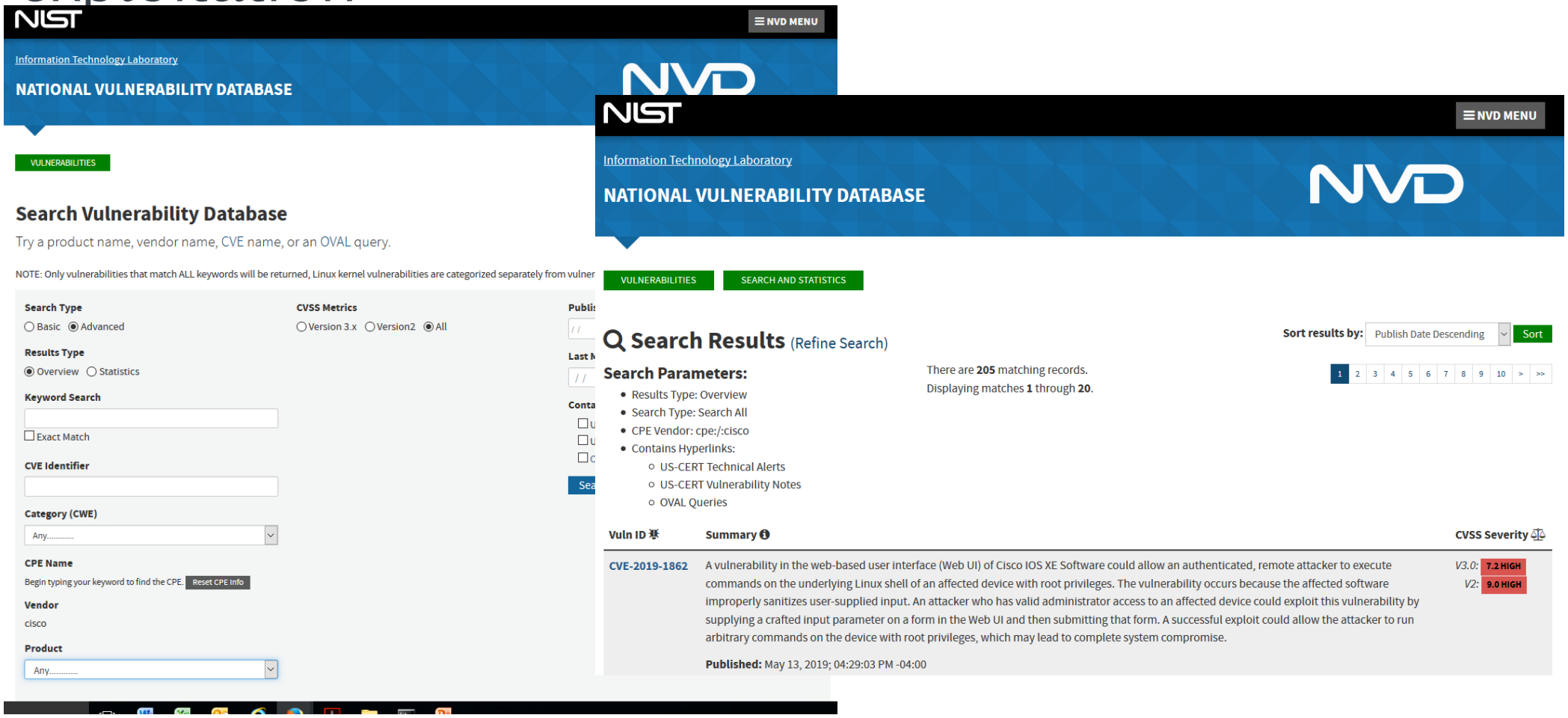
En attaque (Cas de Mitsubishi Electric.)	En défense (Cas de Mitsubishi Electric.)
Détection des vulnérabilités (Dans la messagerie)	1- Vulnérabilités au niveau de la sensibilisation des RH vis-à-vis du phishing (dans une filiale) 2- Vulnérabilités techniques dans les outils de messagerie par rapport au phishing 3- Vulnérabilités techniques sur les postes de travail 4- manquement de l'IPS/IDS 5- manquement dans le Filtrage des flux entrants
Vérification des vulnérabilités exploitables (Tentative de phishing dans la filiale en chine)	
Choix des vulnérabilités à essayer d'exploiter (Méthode utilisé phishing)	
Réalisation des différentes tentatives	
Réalisation de l'exploit (intrusion) **(Intrusion dans la filiale en chine)**	
Installation et mise en place du flux de communication de commande (CC) (installation et CC à partir de la filiale)	Filtrage des flux sortants (et entrants)
Mouvements latéraux (compromission d'autres systèmes) Passage de la filiale à 14 autres départements au niveaux international (au moins) pendant 2 à 3 mois	Cloisonnement des réseaux entre les filiales et entre les départements
Exploitation du méfait (Ransmware, détournement, fraude, …) Vol de données sensible (au moins)	Mesures spécifiques : Ransmware : PCA Fraude : outil de détection de fraude Etc. Pas d'outil DLP Pas de SIEM efficace

Présentation de la gestion des vulnérabilités de la sécurité des réseaux

Analyse des vulnérabilités réseaux

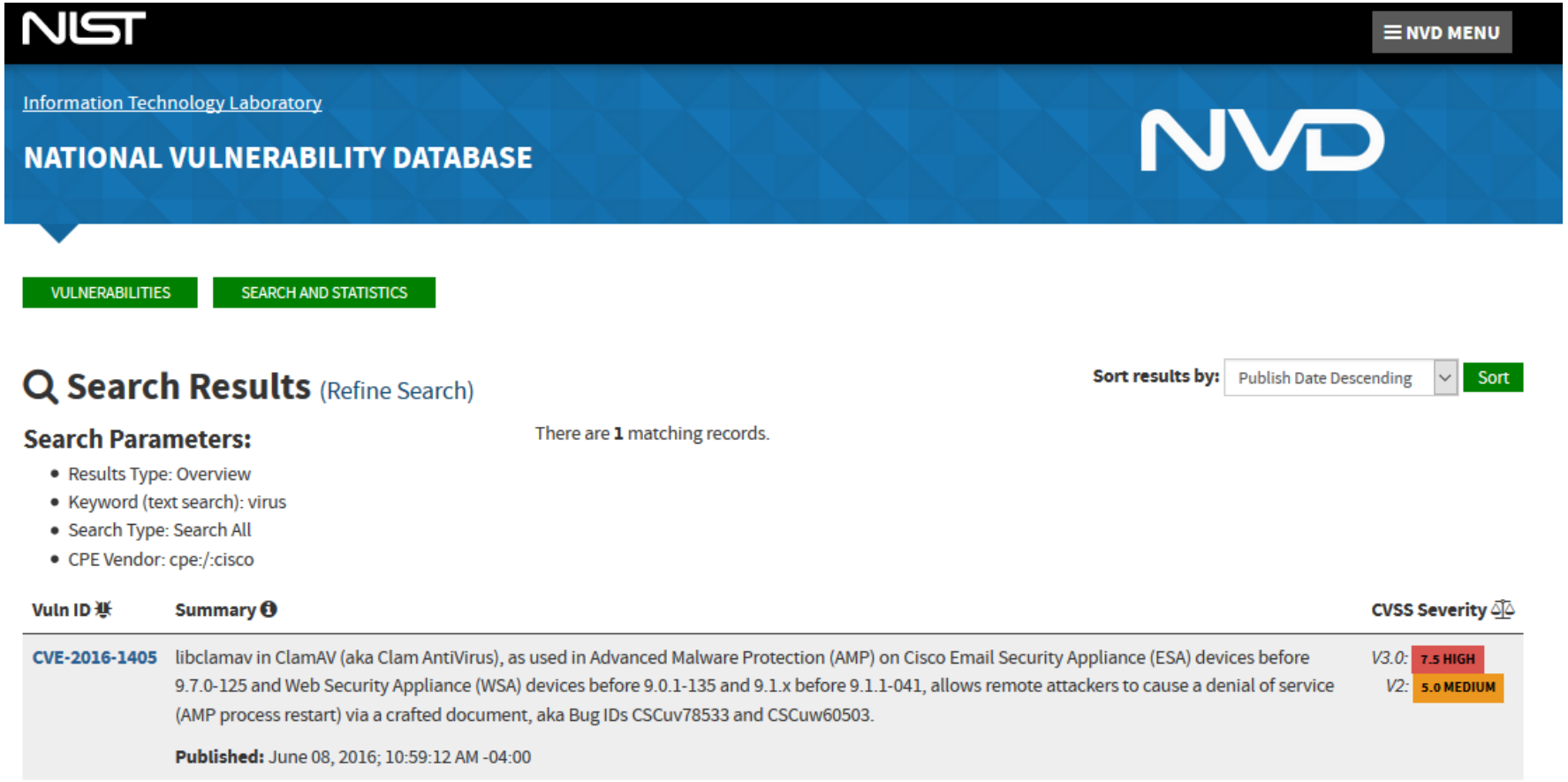
1. Vulnérabilités techniques (CVE ou autres)
2. Vulnérabilités d’architecture
3. Vulnérabilités d’installation et de configuration
4. Vulnérabilités d’exploitation

Veille sur les vulnérabilités techniques et exploitation



Selon les équipements et solutions réseaux mises en place, il est important de suivre régulièrement les vulnérabilités du réseau en consultant les bases de vulnérabilités publiées.

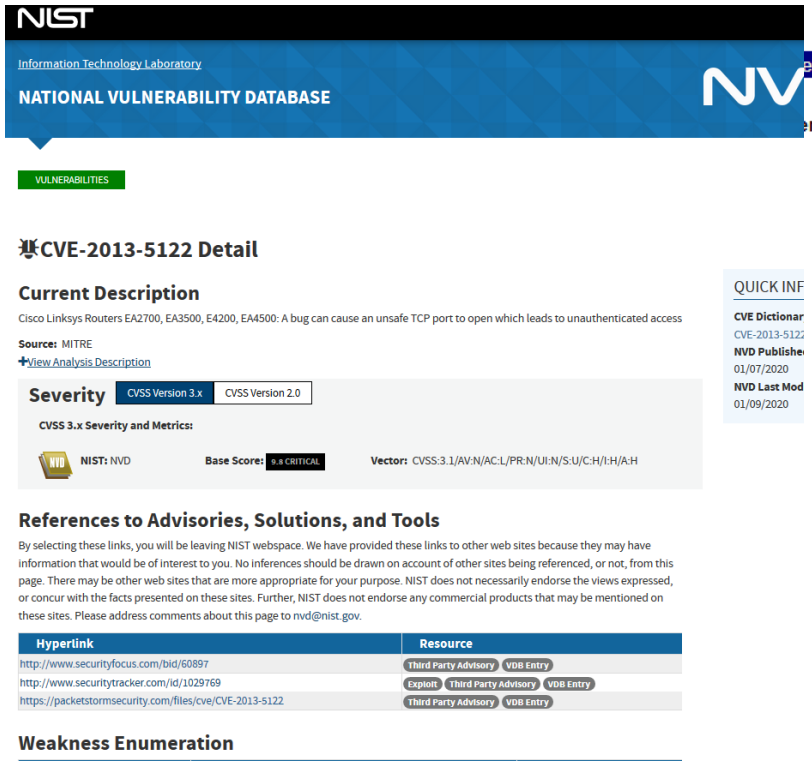
Veille sur les vulnérabilités techniques et exploitation



Pour évaluer les vulnérabilités des infrastructures, il faut prendre en considération la sévérité de chaque vulnérabilité détectée dans le réseau

Veille sur les vulnérabilités techniques et exploitation

TCH ©



NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2013-5122 Detail

Current Description

Cisco Linksys Routers EA2700, EA3500, E4200, EA4500: A bug can cause an unsafe TCP port to open which leads to unauthenticated access

Source: MITRE

View Analysis Description

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://www.securityfocus.com/bid/60897	Third Party Advisory, VDB Entry
http://www.securitytracker.com/id/1029769	Exploit, Third Party Advisory, VDB Entry
https://packetstormsecurity.com/files/cve/CVE-2013-5122	Third Party Advisory, VDB Entry

Weakness Enumeration

QUICK INF

CVE Dictionar

CVE-2013-5122

NVD Publishe

01/07/2020

NVD Last Mod

01/09/2020

Security tracker

ew Topics | Search | Contact Us |

Category: Device (Router/Bridge/Hub) > Linksys Router

Vendors: Linksys

Linksys Router Installation/Upgrade Flaw Lets Remote Users Gain Administrative Access

SecurityTracker Alert ID: 1029769

SecurityTracker URL: http://securitytracker.com/id/1029769

CVE Reference: CVE-2013-5122 *(Links to External Site)*

Date: Feb 17 2014

Impact: User access via network

Exploit Included: Yes

Version(s): EA2700, EA3500, E4200, EA4500

Description: A vulnerability was reported in some Linksys Routers. A remote user can gain administrative access to the target system.

During the installation and upgrade process, a remote user can connect to TCP port 8083 on the WAN interface to access portions of the administrative interface even though the console indicates that remote access is disabled.

On some systems, TCP port 443 may also be open.

The vendor was notified in July 2013.

Kyle Lovett and Matt Claunch reported this vulnerability.

Impact: A remote user can gain administrative access on the target system.

Solution: No solution was available at the time of this entry.

Vendor URL: www.linksys.com/ *(Links to External Site)*

Cause: Access control error

Message History: None.

En plus de l'évaluation de chaque vulnérabilité détecté (en prenant compte le niveau de sévérité) Vous pouvez vérifier l'exploitabilité de la vulnérabilité