

Escape Room pour la sécurité : sensibilisation à la sécurité informatique

Projet issu de la recherche avec l'appui des chercheurs cybersécurité LAAS/CNRS
Vincent Nicomette et Eric Alata


Erwan Béguin : beguin@toulouse-tech-transfer.com
06 86 05 98 65

◎ 80% des entreprises françaises estiment avoir été attaquées

◎ 800 000€ de pertes en moyenne



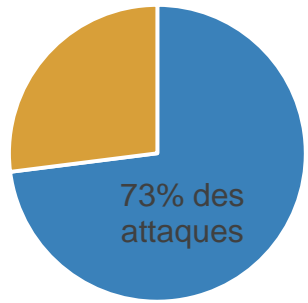
Plan

- © **I. Le risque humain**
 - © **II. Les méthodes de sensibilisations**
 - © **III. Pourquoi une escape room?**
- 

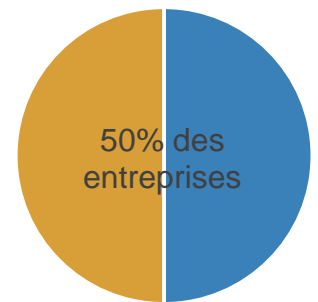
a. Répartition des attaques informatiques

🎯 La principale vulnérabilité est humaine

Phishing et spear phishing



Attaques au président



- Intrusion par mot de passe faible
- Intrusion sur les lieux de travail
- Clefs usb piégées
- ...



Regain d'intérêt pour l'ingénierie sociale

◎ Données professionnelles/privées

- Prise d'informations ciblées sur les réseaux sociaux
- Stratégie d'attaque influencées par les informations collectées
- Spear phishing et ingénierie sociale personnalisées

Diversification des risques

◎ Objets connectées

- Multiplication des points d'entrés
- Mots de passe par défauts
- Protocoles faibles

◎ Environnement de travail

- Baies de brassages
- Cloud

b. Conséquences des attaques liées à l'humain

b.1 Risques financiers

◎ Paralysies

- Gel des activités
- Chiffrement des données

◎ Rançons

- Ransomware

◎ Espionnage

b. Conséquences des attaques liées à l'humain

b.2 Risques d'image

⊙ Crédibilité des entreprises

- Données personnelles
- Sécurité des utilisateurs

⊙ Crédibilité des OIV

b. Conséquences des attaques liées à l'humain

b.3 Risques humains

◎ Vol de données personnelles

- Données bancaires
- Données privées

◎ Fautes graves

c. Interêt de la sensibilisation

- ◎ La majorité des risques sont humains
 - La sensibilisation est la manière la plus simple de réduire les risques
 - Doit être mise en place avec des solutions techniques

II. Les différentes méthodes de sensibilisation

⊙ Doit répondre à plusieurs critères

- Facilité de mise en place
- Efficacité (dans le temps)
- Mesurable

a. La sensibilisation par l'explication

◎ Cours en petits/grands comités

- Facilité de mise en place
- Permet de sensibiliser un grand nombre
- Temps d'attention humain minimal (25 min)
- Manque de mise en contexte

b. La sensibilisation par la démonstration

◎ Campagne de phishing, red team...

- Efficace pour l'évaluation des risques
- Ethiquement discutable
- Délaisse la mise en pratique des bons réflexes

a. La sensibilisation par la pratique

◎ Serious game, CTF, jeux de rôles

- Gamification bénéfique :
 - ◎ Compétitivité
 - ◎ Scoring (+ données d'observation)
 - ◎ Engagement des participants
- Ne doit pas être trop technique

III. Pourquoi utiliser une escape room comme outil pédagogique ?

- ⊙ **Jeu d'évasion** dans une salle en équipe avec énigmes et temps limité
- ⊙ **Attractif**, populaire
- ⊙ Apprentissage par **action et réflexion**
- ⊙ Simulation de **situations réalistes**



Quels objectifs pour quel public cible ?

Public cible : **utilisateurs quotidiens** de l'outil informatique **sans formation** en sécurité

Objectifs :

- Apprendre les **réflexes de base** en sécurité informatique
- Reconnaître et se protéger contre des **attaques d'ingénierie sociale**

Scénarios

Scénario défense

Les participants jouent le rôle de 4 employés d'une entreprise sous menace d'une cyber attaque.

Ils ont une heure pour sécuriser la salle et trouver qui est le hacker sans tomber dans ses pièges.

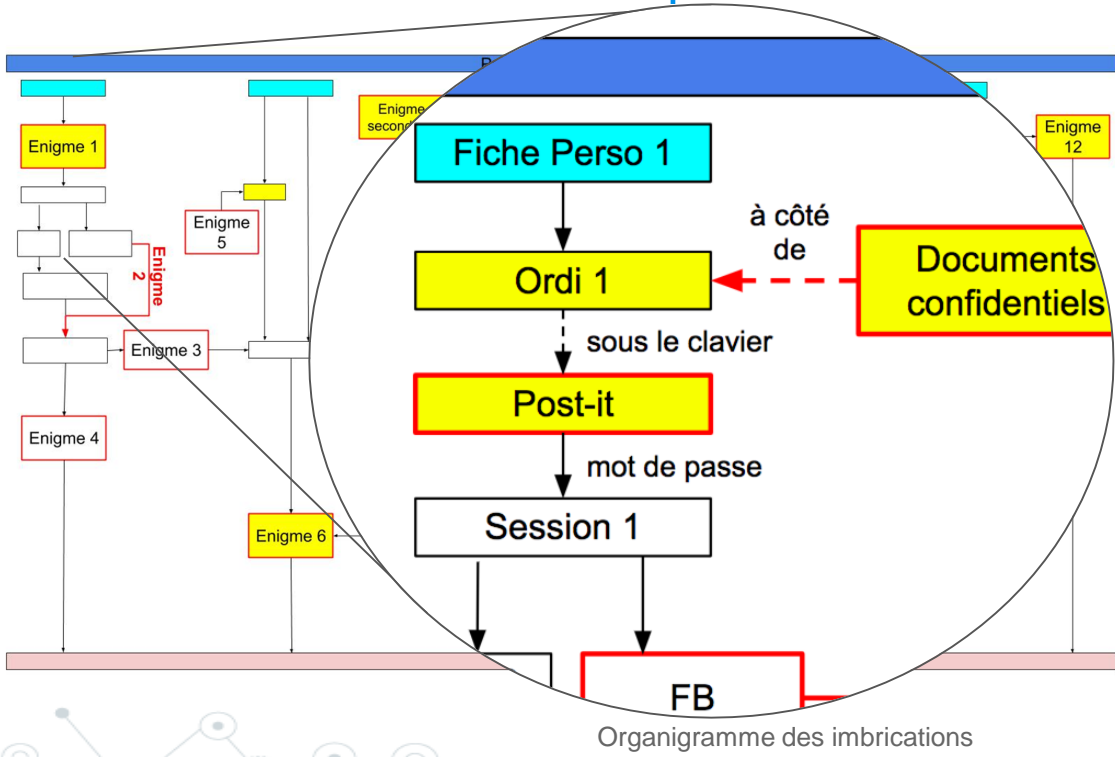
Scénario attaque

Les 3 participants ont été engagés par le maître du jeu pour récupérer des documents compromettants d'une entreprise concurrente.

Ils ont une heure pour tenter d'élever leurs privilèges afin de devenir administrateur et de récupérer ces documents.



Formalisme de conception



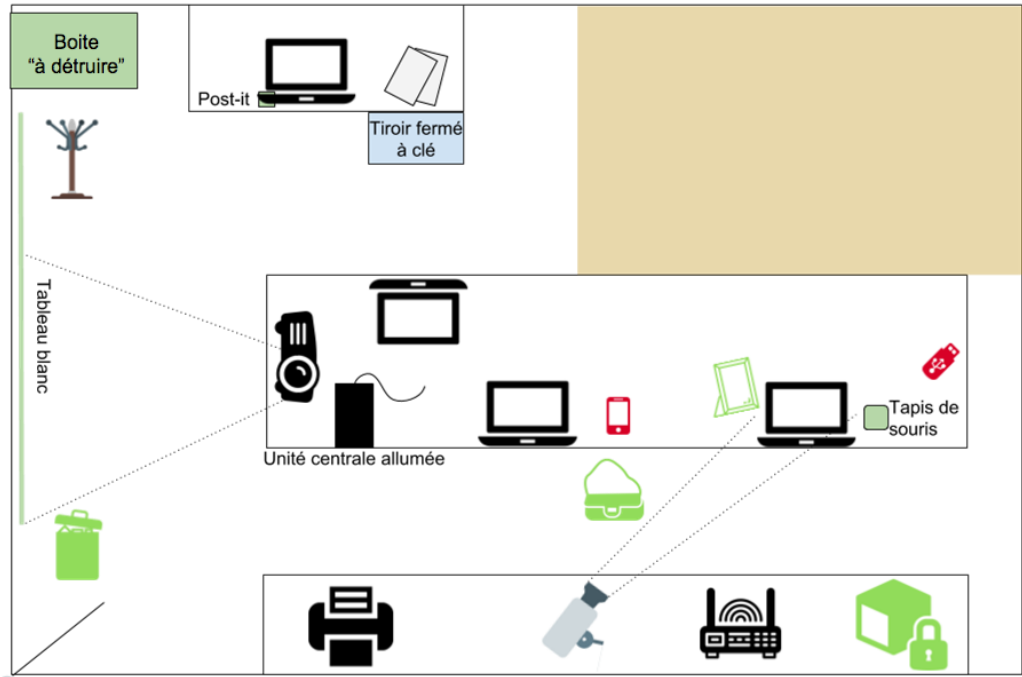
Fiches énigmes

ÉNIGME N° X - TITRE

-  Description de l'énigme
-  Solution de l'énigme
-  Dépendances avec les autres énigmes
-  Apports pour les énigmes suivantes
-  Indices ou coups de pouce si les joueurs sont bloqués
-  Aspect de sécurité informatique concerné



Les ingrédients d'une bonne escape room en sécurité informatique



Plan de la salle

⊙ Défis informatiques techniques

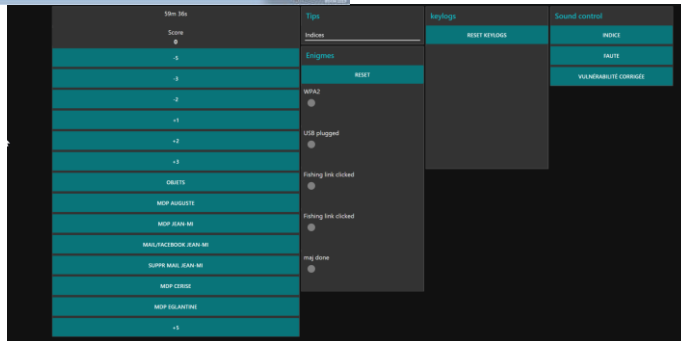
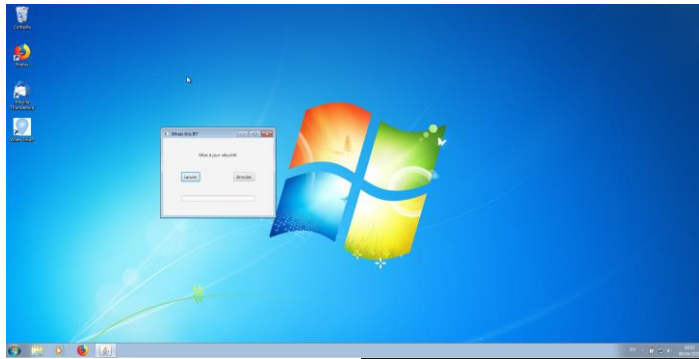
⊙ Ingénierie sociale

⊙ Objets matériels

⊙ Debriefing



Réalisation technique de l'escape room



⊙ Machine virtuelles
Windows

⊙ Scripts et software
additionnels

⊙ API Rest

⊙ Serveur node-red

“Merci à vous pour cet escape game !

C'était à la fois **amusant et instructif** !

On ne pense pas toujours à **l'aspect humain comme faille**, et on a plus **l'image technique** en tête, mais **j'ai changé d'avis grâce à vous !**”

Christophe

“**Vraiment cool** votre escape game, je ne regrette pas que ce soit ma première expérience !!”

Délia

“

“Merci à toute l'équipe pour cet escape game il est **trop top** ! :-)”

Jean

“Honnêtement, j'ai trouvé votre Escape Room vraiment géniale !!

Très bien organisée, avec les petits sons,

le coup de fil, le scénario, tout, vraiment chapeau !”

Aubin

Analyse comportementale

- ⊙ La majorité des participants doute encore qu'il faille faire les **mise à jour** rapidement
- ⊙ L'attitude face à la **clé USB** dépend de l'avancée dans le jeu
- ⊙ Une **personne avertie** suffit pour convaincre



Conclusion

- ◎ La sensibilisation est primordiale
- ◎ Il faut des méthodes efficaces
- ◎ Nous proposons notre escape room aux professionnels