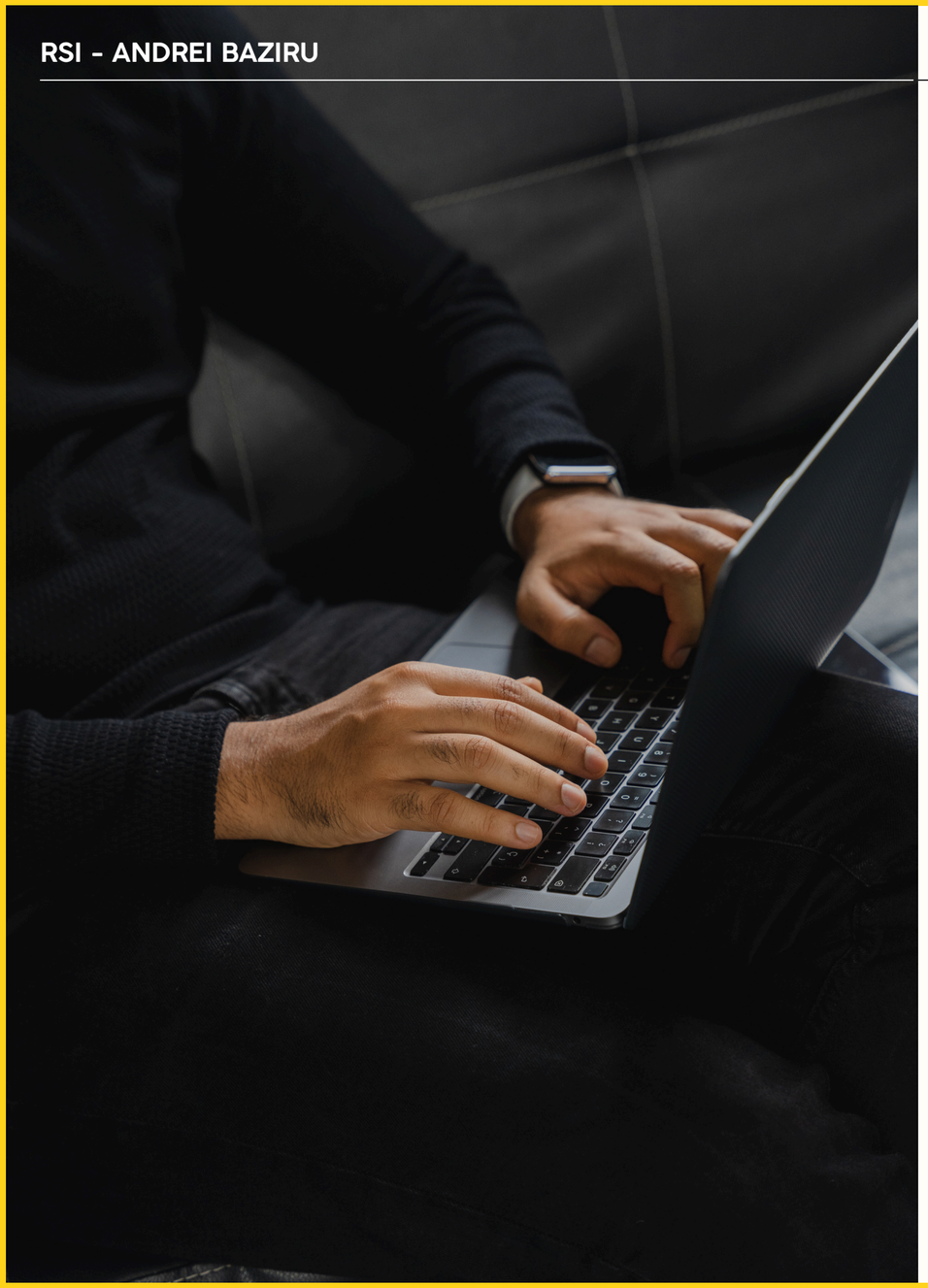
PRÉSENTATION

SENSIBILISATION SUR L'HYGIÈNE INFORMATIQUE



INTRODUCTION

Etudes :
->Verizon Data Breach Investigations Report 2023 (phishing)
-> Université de l'Illinois, de Michigan et Google (clé USB)

Ces Etudes présentent les principales cyber menaces sur les entreprises. Nous allons donc les aborder afin d'éviter de compromettre nos données à cause de cela.

1. PHISHING
2. ATTAQUE PAR CLÉ USB
3. GESTES BARRIERES : UNE SÉCURITÉ OPTIMALE

1. PHISHING

Le phishing est une méthode qui repose sur l'ingénierie sociale, elle est utilisée par les cybercriminels pour tromper les gens et leur voler des informations confidentielles (mots de passes, fichiers, données bancaires etc...). Elles peuvent être retrouvées par mail, sms ou encore les réseaux sociaux.

COMMENT ÇA FONCTIONNE ?

1 - Leurre

RECEPTION D'UN MESSAGE SEMBLANT VENIR D'UNE SOURCE DE CONFIANCE.

EXEMPLE :
RECEPTION D'UN MESSAGE DE VOTRE BANQUE DISANT QU'IL Y A UN PROBLÈME AVEC VOTRE COMPTE

OU

RECEPTION D'UN MESSAGE DE VOTRE MANAGER INDIQUANT UNE ERREUR SUR UN DOSSIER

2 - Appat

DEMANDE DE CLIQUER SUR UN LIEN OU DE TÉLÉCHARGER UN DOCUMENT

EXEMPLE :
ACCÈDER DIRECTEMENT À SON COMPTE BANCAIRE DEPUIS LE LIEN DU MAIL (LIEN MALVEILLANT)

OU

TÉLÉCHARGER LE DOCUMENT ÉRRONÉ EN QUESTION
(FICHIER MALVEILLANT)

3 - Action

ACCÈS À UN ENVIRONNEMENT À L'IMAGE LÉGITIME DEMANDANT SOUVENT LA SAISIE D'INFORMATIONS

EXEMPLE :
FAUX SITE IMITANT CELUI DE LA BANQUE ET INCITANT À LA SAISIE DE SES INFORMATIONS BANCAIRES

OU

TÉLÉCHARGEMENT D'UN FICHIER AYANT UN IMPACT DIRECT SUR LA SÉCURITÉ DE L'ENVIRONNEMENT NUMÉRIQUE

4 - Attaque

REMPLIR CES INFORMATIONS OU TÉLÉCHARGER UN FICHIER DEPUIS UNE SOURCE MALVEILLANTE MÈNE DIRECTEMENT À LA COMPROMISSION DE L'ENTREPRISE

EXEMPLE :
LES INFORMATIONS BANCAIRES SONT DIRECTEMENT ENVOYÉES À L'ATTAQUANT

OU

VOL DES DONNÉES DE L'ENTREPRISE
ESPIONNAGE / DEMANDE DE RANÇON

COMMENT SE PROTEGER ?

Vérifier l'expéditeur

BIEN S'ASSURER QUE L'EXPÉDITEUR EST UNE SOURCE CONNUE

SI CELLE CI SEMBLE ETRANGE = MEFIANCE

Faire attention aux liens

NE PAS CLIQUER SANS VÉRIFIER LE LIEN, SI L'ADRESSE SEMBLE SUSPECTE OU NE CORRESPOND PAS AU VRAI SITE = FRAUDE

Ne jamais renseigner des infos personnelles

DE LA MÊME MANIÈRE, SI UN SITE VOUS DEMANDE DE RENSEIGNER DES INFOS PERSONNELLES DEMANDEZ VIS SI C'EST NORMAL ET LÉGITIME

Ne pas céder à la pression

SOUVENT, LES FRAUDES AJOUTENT UNE FORME DE PRESSION DU TYPE "VOTRE COMPTE SERA SUSPENDU SI ..."

NE VOUS LAISSEZ PAS INFLUENCER PAR CE TON URGENT ET FAITES LES VÉRIFICATIONS NÉCEÉSSAIRES

2. ATTAQUES PAR CLÉ USB

Les attaques par clé USB sont utilisées par les cybercriminels afin d'infecter des ordinateurs ou des réseau informatiques en utilisant seulement une clé USB. Cette méthode consiste à faire en sorte qu'un employé insère une clé USB infectée dans un ordinateur , par curiosité ou altruisme. Le problème étant que lors de l'insertion plusieurs attaques sont possibles.

QUELLES SONT LES ATTAQUES POSSIBLES ?

VOICI DEUX ATTAQUES BEAUCOUP UTILISÉES

HID SPOOFING
(HUMAN INTERFACE DEVICE SPOOFING)

- CONFIGURATION
- IMITATION DE PÉRIPHÉRIQUE
- SAISIE MALVEILLANTE
- ATTAQUE

USB KILLER

- CONFIGURATION
- CHARGE DE HAUTE TENSION
- DÉCHARGE
- DOMMAGES MATERIEL

COMMENT SE PROTEGER ?

NE PAS BRANCHER DES CLÉS USB INCONNUES !

UTILISER LES PORTS USB SÉCURISÉS PAR L'ANTIVIRUS DE L'ENTREPRISE

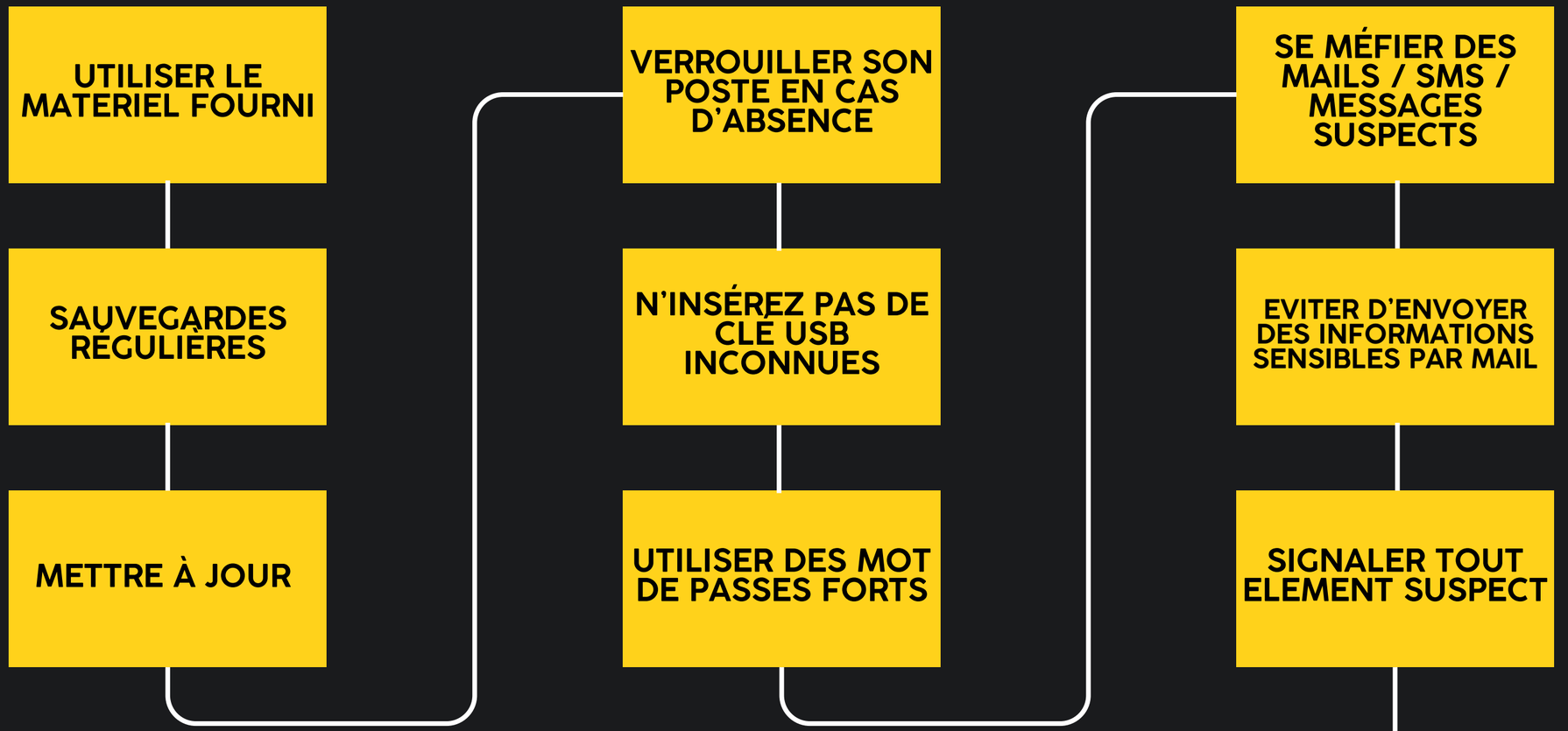
EN CAS DE BRANCHEMENT D'UNE CLÉ MALVEILLANTE :

- DÉCONNECTEZ L'ORDINATEUR DU RÉSEAU
- CONTACTEZ LE SERVICE INFORMATIQUE

3. GESTES BARRIERES

Voici une liste de certains gestes à appliquer afin de ne pas compromettre l'entreprise

LES GESTES À CONNAITRES



SECURITÉ OPTIMALE

MERCI POUR L'ÉCOUTE

AVEZ VOUS DES QUESTIONS ?