Onglet 1

semaine du 6 au 10 janvier

travaille effectué	lundi	mardi	mercredi	jeudi	vendredi
de 9h à 12h	Travail sur la faille humaine d'une entreprise (Coti Immobilier) en utilisant une attaque par phishing afin de démontrer les problèmes de sécurité liés à la formation des salariés face aux e-mails malveillants. Début du plan d'attaque.	Amélioration finale du plan en rajoutant les parties manquantes comme les techniques utilisées pour contourner les filtres anti-spam et les autres moyens : téléphone ou SMS (ingénierie sociale)	Malade: je suis tombé malade ce jour la je ne suis donc pas aller au stage en prévenant par mail mon tuteur de stage bien évidemment	continuité du code du faux site	malade gastro
de 14h à 17h	Finalisation du plan et des conclusions attendues de cette attaque, afin de la mettre en œuvre sans intention malveillante. https://docs.google.com/document/d/1dUa-0HkWe7pJCzf6PRygWTbqbEIFIFEHA4rLMOadr2o/edit?usp=sharing	Début de la duplication du site web et création d'une adresse e-mail sur ProtonMail pour garantir l'anonymat. Ensuite, en étape finale, héberger le faux lien et envoyer le mail aux employés de Coti Immobilier.	Malade: je suis tombé malade ce jour la je ne suis donc pas aller au stage en prévenant par mail mon tuteur de stage bien évidemment	continuité du code du faux site	pas de travaille le vendredi après midi

semaine du 13 au 17 janvier

travaille effectué	lundi	mardi	mercredi	jeudi	vendredi
de 9h à 12h	Audit et Analyse du Système d'Information de l'Entreprise Influenci à Propriano	pas de travaille tuteur absent pour maladi donc pas de travaille j'ai fais des certification en attendant	nouvelle attaque sur cette fois ci sur costa lucchini habitat pour testé aussi leur réactivite au attaque	continuuité du mercredi et modification du code pour correspondre cette fois si au site de costa lucchini habitat	travaille sur mon portfolio tuteur en déplacement

de 14h à 17h	Audit et Analyse du Système d'Information de l'Entreprise Influenci à Propriano	pas de travaille tuteur absent pour maladi donc pas de travaille j'ai fais des certification en attendant	nouvelle attaque sur cette fois ci sur costa lucchini habitat pour testé aussi leur réactivite au attaque	continuité du mercredi et modification du code pour correspondr e cette fois si au site de costa lucchini habitat	pas de travaille l'apres midi

semaine du 20 au 24 janvier

travaille effectué	lundi	mardi	mercredi	jeudi	vendredi
de 9h à 12h	début audite pour : costa lucchini habitat avec plan déallaié de l'audite et envoie de email pour explication de la procédure	audite évaluation de la Surface d'Attaque: identification des services en ligne utilisés par l'entreprise (emails, sites web, réseaux sociaux)et analyse des informations disponibles publiquement (OSINT).	j'ai activement participé au projet en cours au sein de l'entreprise en contribuant à l'organisation d'un audit pour l'un de nos clients, Costa Lucchini Habitat. L'objectif principal de cette visite sera de réaliser un audit complet de leur réseau informatique, tout en expliquant en détail le plan d'action envisagé pour améliorer leur infrastructure.	j'ai passé la journée à Porto-Vecchio pour effectuer une visite du système informatique de l'entr eprise Costa Lucchini Habitat. L'objectif de cette visite était d'analyser leur infrastructure en détail afin d'identifier d'éventuelles vulnérabilités techniques et organisationne lles.	débute des nouveau mail pour phising
de 14h a 17h	malade gros male de tete pas de travaille l'apres midi	audite évaluation de la Surface d'Attaque: identification des services en ligne utilisés par l'entreprise (emails, sites web, réseaux sociaux)et analyse des informations	j'ai finalisé mon audit du site web de Costa Lucchini Habitat, en identifiant les axes d'amélioration potentiels et en préparant un rapport détaillé. Afin d'assurer	j'ai présenté au dirigeant un premier aperçu du plan d'action envisagé. Cette discussion a permis d'expliquer les différentes	pas de travaille

		disponibles publiquement (OSINT).	une communication efficace lors de la visite de jeudi, j'ai également élaboré un plan structuré pour une présentation qui mettra en avant les résultats de l'audit ainsi que les recommandations adaptées à leurs besoins spécifiques.	étapes prévues pour améliorer la sécurité de leur système, notamment en mettant l'accent sur des tests de vulnérabilité liés aux erreurs humaines. Nous avons abordé plusieurs scénarios de tests visant à évaluer la sensibilisation des employés face aux cybermenaces potentielles, telles que le phishing ou les mauvaises pratiques de gestion des mots de passe.	

semaine du 27 au 31 janvier

travaille effectué	lundi	mardi	mercredi	jeudi	vendredi
de 9h a 12h	malade je suis tombé malade	malade je suis tombé malade	envoie des email et sms et analyse des résulta	envoie des email et sms et analyse des résulta	conclusion sur l'attaque
de 14h a 17h	malade je suis tombé malade	malade je suis tombé malade	envoie des email et sms et analyse des résulta	envoie des email et sms et analyse des résultats	ne travaille pas le vendredi après midi

semaine 3 février aux 7 février

travaille efectué	lundi	mardi	mercredi	jeudi	vendredi
de 9h a 12h	pas de projet particulier j'ai surtout aidé l'entreprise	aide au développement d'un site web pour une entreprise de fleure	aide au développement d'un site web pour une entreprise de fleure		rien a faire
de 14h a 17h	pareil pour l'apres midi	aide au développement d'un site web pour une entreprise de fleure	aide au développement d'un site web pour une entreprise de fleure		fermé le vendredi apres midi

travaille efectué	lundi	mardi	mercredi	jeudi	vendredi
de 9h a 12h	malade pas de travaille				
de 14h a 17h	malade pas de travaille				

Audit Cybersécurité – Présentation et Plan d'Action

✦ Résumer cet e-mail

B

Baptiste Hilmi <baptiste@influenci.com> 09:07 (il y a 1 heure)

À b.costa@cl-habitat.fr

Bonjour M. Costa,

Je vous transmets ci-joint le document présentant les différentes étapes de l'audit de cybersécurité que nous envisageons pour Costa Lucchini Habitat. Cet audit permettra d'identifier les vulnérabilités potentielles, notamment celles liées au facteur humain, et de proposer des solutions adaptées pour renforcer la sécurité de votre entreprise.

N'hésitez pas à me faire part de vos retours ou de vos disponibilités pour échanger sur le sujet.

Cordialement,

Baptiste Hilmi

stagiaire Influenci

numéro perso : 06 02 72 06 55

1 pièce jointe • Analyse effectuée par Gmail

Répondre Transférer

Onglet 2

Attaques par phishing pour le site de Coti Immobilier.

---

1. Description du contexte de réalisation

a. Contexte de réalisation

Dans le cadre d'une formation sur la cybersécurité, j'ai réalisé une attaque par phishing ciblant l'entreprise Coti Immobilier. Cette simulation visait à démontrer les vulnérabilités potentielles des employés face à des attaques sociales et à développer des compétences en cybersécurité défensive.

b. Présentation de l'organisation cliente

Coti Immobilier est une agence immobilière dotée d'une infrastructure numérique reposant sur un site web principal (http://www.cotiimmobilier.com) et une plateforme d'administration accessible à l'adresse http://www.cotiimmobilier.com/admin/. L'organisation utilise plusieurs adresses email professionnelles pour ses employés, ce qui constitue une surface d'attaque exploitable.

c. Impact attendu

L'objectif final était de sensibiliser les employés de l'organisation aux risques de phishing, de tester les défenses existantes, et de renforcer la sécurité informatique via des recommandations adaptées. Une meilleure prise de conscience des menaces améliorerait la résilience de l'organisation face à de potentielles attaques réelles.

---

2. Actions réalisées

a. Ressources mises à disposition

- Adresses emails professionnelles fournies par l'entreprise (liste des employés).
- Logiciels pour la simulation : outils de création d'emails anonymes (ProtonMail, GuerrillaMail).
- Environnement de développement local pour la création d'un site répliqué (XAMPP).

b. Méthodes suivies et technologies utilisées

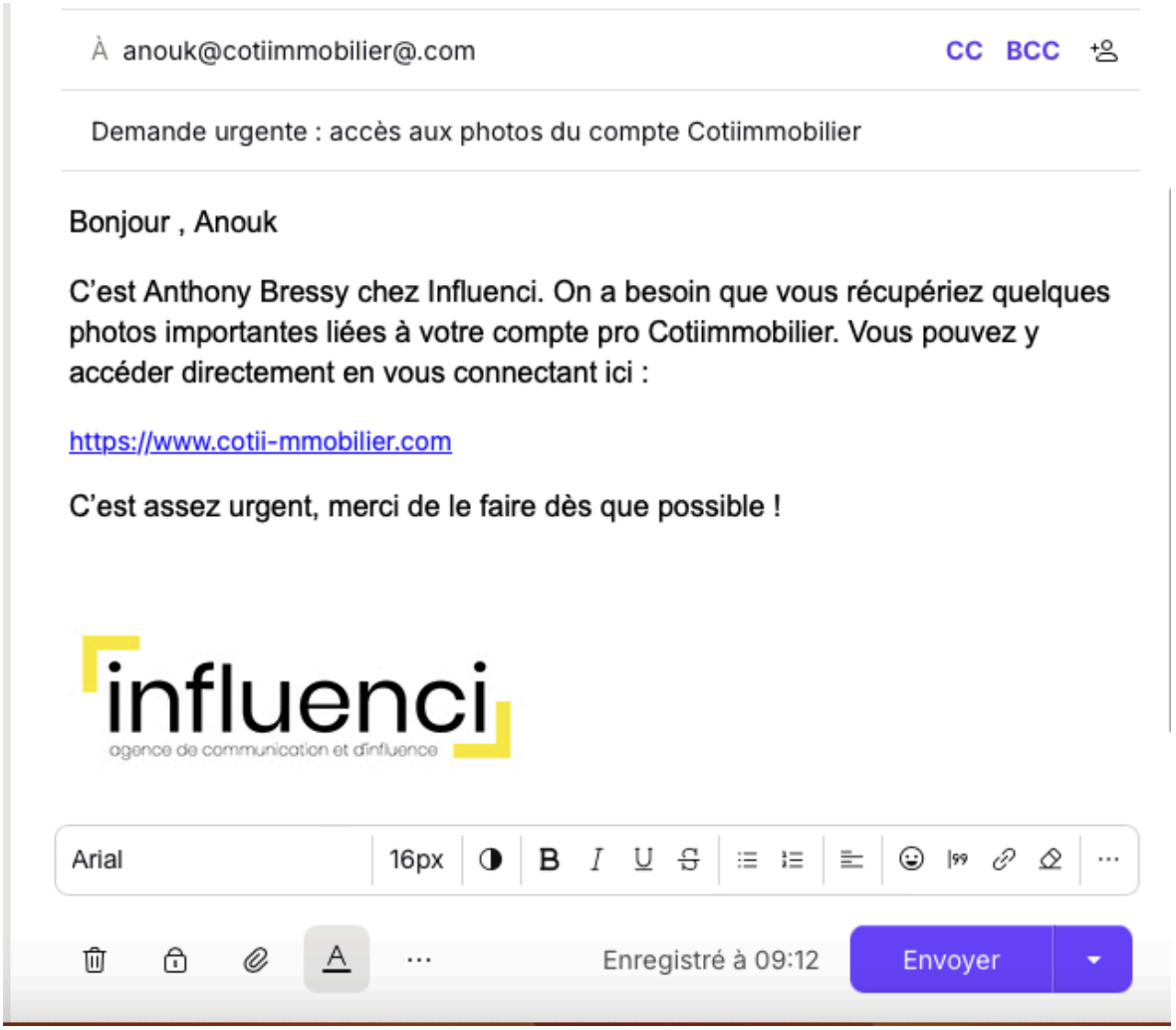
1. **Analyse des vulnérabilités potentielles :**
    - Recensement des adresses email.
    - Identification des employés potentiellement vulnérables (par exemple, moins sensibilisés à la cybersécurité).

2. **Création d’un email de phishing :**
    - Utilisation d’un service d'email anonyme (ProtonMail) pour simuler une communication légitime.
    - Rédaction d’un message convaincant avec un lien menant à un site répliqué.
3. **Réplication du site web cible :**
    - Extraction du code HTML et CSS via les outils de développement de navigateur.
    - Modification des formulaires de connexion pour collecter les données soumises.
4. **Lancement de la campagne de phishing :**
    - Envoi des emails de phishing avec un lien vers le site répliqué.
    - Suivi des taux d’ouverture, de clic, et de soumission des informations.
5. **Techniques utilisées pour contourner les filtres anti-spam :**
    - Création d’adresses email proches des adresses légitimes.
    - Inclusion de contenus personnalisés (nom des employés, projets spécifiques).

---

3. Description des documents produits (à compléter)

- **Modèle d'email de phishing** : conçu pour imiter les communications officielles de l’entreprise.



- **Site web répliqué** : une copie fidèle du site original, permettant de capturer les identifiants soumis.(à était supprimé après l'attaque)
- **Rapport d'analyse post-simulation** : présentant les résultats, incluant le taux de clics sur le lien et les informations soumises par les employés. : https://docs.google.com/document/d/1oG-a1eKl3JrE2DKzhwxsI5k--kPqnsFsXeDApv6lboU/edit?usp=sharing

Ces documents ont servi à démontrer les vulnérabilités et à constituer les preuves nécessaires pour proposer des solutions adaptées.

---

4. Organisation mise en place

- **Planification des étapes** :
  Une structure claire a été suivie, comprenant les phases d'analyse, de

conception, de test, et d'exécution de la simulation. Chaque étape a été définie avec des objectifs précis pour assurer une progression méthodique.

- **Méthodologie suivie** :
  Une approche par simulation réaliste a été adoptée, s'inspirant des techniques couramment utilisées par les attaquants.

Outils utilisés pour les échanges et validations :

- **Google Docs** : Utilisé pour rédiger, partager et collaborer sur les documents nécessaires au projet.
- **Emails** : Principal moyen de communication pour partager les documents et recueillir les retours du patron à chaque étape.

---

5. Contraintes et difficultés rencontrées

- **Techniques de détection des filtres anti-spam :** certains emails ont été bloqués ou marqués comme indésirables.
- **Conception réaliste du site répliqué :** le site devait être suffisamment crédible pour tromper les utilisateurs.
- **Sensibilisation des cibles :** certains employés étaient déjà bien informés sur les attaques par phishing, réduisant le taux de succès.

---

6. Conclusion / Bilan : réalisations et acquis personnels liés à la mission ou au projet

a. Réalisations professionnelles

Cette mission a permis de faire une attaque de phishing réaliste et de mettre en lumière les vulnérabilités potentielles au sein des systèmes numériques et des pratiques des employés de Coti Immobilier. La campagne de phishing élaborée a mis en évidence :

- Les comportements des employés face à des emails frauduleux, notamment leur propension à cliquer sur des liens ou à fournir des informations sensibles.
- Les faiblesses structurelles dans la sécurisation des accès administratifs et la gestion des mots de passe.
- Les limites des mesures anti-phishing en place, telles que les filtres anti-spam ou les protections du site web.

b. Acquis personnels
Cette réalisation m'a apporté plusieurs compétences techniques et méthodologiques précieuses :

1. **Compétences techniques en cybersécurité :**
    - J'ai perfectionné mes connaissances sur les outils nécessaires à la création de campagnes de phishing, comme la conception de sites répliqués ou l'utilisation de services d'emails temporaires.
    - J'ai renforcé mes compétences en analyse des vulnérabilités humaines et techniques, notamment en matière d'ingénierie sociale.
2. **Capacité à adopter une démarche critique et analytique :**
    - L'évaluation des résultats de l'attaque m'a permis de comprendre les points faibles dans la stratégie de cybersécurité de l'entreprise, et d'en proposer des solutions concrètes.
    - J'ai appris à analyser les taux de succès et d'échec d'une attaque simulée pour en déduire des enseignements applicables dans des contextes réels.
3. **Sensibilisation et pédagogie :**
    - J'ai réalisé l'importance de la sensibilisation continue des équipes aux enjeux de la cybersécurité.

c. Apports pour l'entreprise cliente

- **Amélioration de la sensibilisation :** Les résultats de cette attaque ont montré l'urgence de former les employés à reconnaître les signes d'une tentative de phishing.
- **Renforcement des mesures de sécurité :** La nécessité de mettre en place une authentification à deux facteurs (2FA), des filtres anti-phishing plus performants, et des audits réguliers a été identifiée.
- **Valorisation des actions préventives :** L'analyse critique de la simulation a permis d'orienter les recommandations vers des solutions concrètes et adaptées, comme l'utilisation de gestionnaires de mots de passe et la mise en place de campagnes de sensibilisation régulières.

d. Réflexion critique sur la démarche
Bien que l'attaque ait révélé des points d'amélioration, certains aspects pourraient être optimisés à l'avenir :

- La diversification des scénarios de phishing pour inclure des approches plus subtiles, comme les attaques via SMS ou réseaux sociaux.
- Une analyse plus approfondie des comportements des utilisateurs après la simulation, avec des entretiens pour recueillir leurs impressions et lacunes.
- L'intégration de tests de pénétration plus complets, ciblant à la fois les systèmes techniques et humains.

Onglet 3

Audit et Analyse du Système d’Information de l’Entreprise Influenci à Propriano

1. Présentation de l'entreprise et de son SI

- **Effectif** : 4 employés.
- **Équipement** : Chaque employé dispose d'un Mac avec un compte professionnel personnalisé et des droits d'accès adaptés à ses besoins.
- **Connexion Internet** : Accès à la fibre optique.
- **Messagerie** : Utilisation de boîtes mail professionnelles se terminant par @influenci.com.
- **Sauvegarde des données** :
    - Données stockées sur les ordinateurs et un serveur local.
    - Réplication et sauvegarde sur un cloud pour prévenir la perte de données.
- **Applications utilisées** : Outils de développement tels que Visual Studio Code (VSCode).

---

2. Évaluation des composantes du SI

A. Infrastructure IT

- **Matériel** : Les Mac utilisés semblent adaptés aux besoins des employés. Il serait pertinent de vérifier régulièrement leur état et de planifier des mises à jour matérielles si nécessaire.
- **Réseau** : L'accès à la fibre offre une connexion rapide et stable. Il est recommandé de s'assurer que le réseau interne est correctement configuré pour optimiser les performances et la sécurité.

B. Sécurité

- **Comptes utilisateurs** : La création de comptes professionnels avec des droits spécifiques est une bonne pratique. Il est essentiel de s'assurer que les droits sont régulièrement revus et ajustés en fonction des besoins.
- **Sauvegardes** : La stratégie de sauvegarde locale et cloud est judicieuse. Il est important de tester périodiquement la restauration des sauvegardes pour garantir leur efficacité.
- **Protection des terminaux** : Il est recommandé de vérifier la présence et la mise à jour régulière de logiciels de sécurité (antivirus, pare-feu) sur chaque Mac.

C. Applications et logiciels

- **Outils de développement** : VSCode est un choix populaire et efficace pour le développement. Il est conseillé de maintenir les applications à jour pour bénéficier des dernières fonctionnalités et correctifs de sécurité.

- **Gestion des licences** : Assurez-vous que toutes les applications utilisées disposent de licences valides et conformes aux conditions d'utilisation.

D. Gouvernance IT

- **Politiques internes** : Il serait bénéfique de formaliser des politiques concernant l'utilisation des ressources IT, la gestion des mots de passe, et la formation des employés à la sécurité informatique.
- **Plan de continuité** : Bien que des sauvegardes soient en place, il est recommandé de développer un plan de continuité d'activité (PCA) pour faire face à des incidents majeurs.

---

3. Recommandations

1. **Sécurité des données** :
    - Mettre en place une politique de gestion des mots de passe robustes et encourager leur renouvellement régulier.
    - Former les employés aux bonnes pratiques en matière de sécurité informatique, notamment la reconnaissance des tentatives de phishing.
2. **Sauvegardes** :
    - Tester régulièrement les procédures de restauration des données pour s'assurer de leur efficacité.
    - Vérifier la conformité des sauvegardes avec les réglementations en vigueur, notamment en matière de protection des données personnelles.
3. **Mises à jour et maintenance** :
    - Mettre en place un calendrier de maintenance pour les mises à jour des systèmes d'exploitation, des applications et des dispositifs de sécurité.
    - Surveiller l'état des équipements et planifier leur renouvellement en fonction de leur cycle de vie.
4. **Documentation et procédures** :
    - Documenter les procédures IT, y compris les configurations système, les plans de sauvegarde, et les protocoles de sécurité.
    - Établir des procédures claires pour la gestion des incidents et des pannes.
5. **Conformité** :
    - S'assurer que les pratiques de l'entreprise sont conformes aux réglementations locales et internationales, notamment le Règlement Général sur la Protection des Données (RGPD).

Points Négatifs et Améliorations du SI de l’entreprise Influenci

1. **Gestion des Comptes Utilisateurs**
    - **Problème** : Droits d'accès non revus régulièrement.

    - **Solution** : Instaurer une revue périodique des droits et activer la double authentification (2FA).
2. **Sécurité des Données**
    - **Problème** : Dépendance au cloud et absence de mention explicite de cryptage.
    - **Solution** : Chiffrer les données et diversifier les sauvegardes (ex. : sauvegarde hors ligne).
3. **Sécurité des Postes de Travail**
    - **Problème** : Pas d'antivirus ou pare-feu mentionnés.
    - **Solution** : Installer un antivirus, configurer un pare-feu, et automatiser les mises à jour.
4. **Réseau et Connectivité**
    - **Problème** : Sécurité réseau non audité et absence de segmentation.
    - **Solution** : Segmenter le réseau et effectuer un audit de sécurité.
5. **Formation des Employés**
    - **Problème** : Manque de sensibilisation aux cybermenaces.
    - **Solution** : Former les employés sur la sécurité et instaurer des règles d'utilisation claires.
6. **Plan de Continuité**
    - **Problème** : Pas de PCA/PRA documenté ni testé.
    - **Solution** : Élaborer un plan de continuité d'activité et tester les sauvegardes.
7. **Conformité RGPD**
    - **Problème** : Absence d'audit sur la gestion des données personnelles.
    - **Solution** : Effectuer un audit RGPD et définir une politique de confidentialité.

En appliquant ces recommandations, l'entreprise Influenci pourra renforcer la sécurité et l'efficacité de son système d'information, tout en se préparant aux défis futurs liés à l'évolution technologique et aux menaces potentielles.

Onglet 4

RA : Rapport d'Activité

1.1 Présentation du contexte et du sujet

Contexte organisationnel :

Mon stage se déroule chez **Influenci**, une entreprise située à Propriano en Corse, spécialisée principalement dans le développement et le marketing. Actuellement, Influenci cherche à se développer dans le domaine de la cybersécurité, ce qui représente une opportunité stratégique majeure pour diversifier ses services. Au cours de mon stage, mes missions se concentrent principalement sur des activités liées à la cybersécurité, notamment des audits de sécurité et des simulations d'attaques par phishing.

Contexte technique :

Chez **Influenci**, le matériel utilisé est principalement composé d'ordinateurs Mac. Ces machines offrent un environnement stable et adapté aux besoins de l'entreprise, bien que leur utilisation en cybersécurité nécessite parfois des ajustements ou l'installation d'outils spécifiques pour mener des analyses techniques. Les tests de sécurité et les audits que je réalise s'appuient sur des outils adaptés à cet environnement macOS, garantissant une compatibilité optimale avec les projets en cours.

Objectifs du stage :

L'objectif principal du stage est d'évaluer la réactivité de diverses entreprises face aux attaques de phishing en utilisant des techniques d'ingénierie sociale. Il s'agit aussi d'auditer le système d'information de **Influenci** pour identifier des failles potentielles. Le travail consiste également à améliorer mes compétences pratiques en cybersécurité et à produire des livrables pour l'entreprise.

1.2 Les activités quotidiennes

Semaine du 6 au 10 janvier

- **Lundi :** J'ai travaillé sur l'analyse des failles humaines d'une entreprise cliente, **Coti Immobilier**, en menant une simulation d'attaque par phishing. Le but était de démontrer les risques liés à une formation insuffisante des employés face aux e-mails malveillants. Un plan d'attaque a été préparé, comprenant les techniques à utiliser, ainsi que l'importance d'adopter une approche éthique dans la mise en œuvre de cette simulation

- **Mardi :** Finalisation du plan d'attaque, ajoutant des stratégies pour contourner les filtres anti-spam, et la création de failles supplémentaires via des moyens alternatifs

comme le téléphone et le SMS. Le but était de compléter l'analyse en diversifiant les vecteurs d'attaque.

- **Mercredi :** Je me suis concentré sur la continuité du développement d'un faux site web pour l'attaque par phishing. Ce site devait être conçu pour tromper les employés de **Coti Immobilier** en simulant une page de connexion légitime.

- **Jeudi :** Le travail a continué sur la création et l'hébergement du faux site web. Une adresse email a été créée sur ProtonMail pour garantir l'anonymat de l'attaque. Le plan a été peaufiné, et les outils nécessaires pour envoyer des mails de phishing aux employés ont été mis en place.

- **Vendredi :** Absence due à une maladie.

Semaine du 13 au 17 janvier

- **Lundi :** J'ai débuté l'audit du système d'information de **Influenci** à Propriano. Il s'agissait d'analyser l'architecture réseau et de détecter des vulnérabilités potentielles dans les outils utilisés par l'entreprise.

- **Mardi :** La matinée a été consacrée à une nouvelle attaque, cette fois-ci sur l'entreprise **Costa Lucchini Habitat**, dans le but de tester leur réactivité face aux tentatives de phishing. Le code du faux site a été adapté pour imiter le site web de l'entreprise cible.

- **Mercredi :** Poursuite des travaux sur l'attaque contre **Costa Lucchini Habitat**, avec des ajustements supplémentaires au niveau du site frauduleux pour mieux correspondre au site réel de l'entreprise.

- **Jeudi :** Reprise de l'audit du système d'information d'Influenci et poursuite de l'adaptation du faux site pour l'attaque (tuteur en déplacement)

- **Vendredi :** Temps consacré à la mise à jour de mon portfolio personnel (tuteur en déplacement)

1.3 Conclusion ⇒ Enseignements à tirer

Mon stage m’a permis de renforcer mes compétences pratiques en cybersécurité et en gestion de projet. J'ai appris à travailler de manière autonome, à gérer mon temps efficacement et à m’adapter aux imprévus. Les attaques par phishing que j'ai réalisées m'ont permis de mieux comprendre l'importance de la formation des employés et des tests de pénétration.

Points forts :

- Approfondissement des connaissances en cybersécurité, notamment sur les attaques par phishing.
- Adaptabilité face aux absences et aux changements de plan.
- Création d’un plan d’attaque structuré et éthique.

Onglet 5

Questionnaire d'aide à la découverte de l'environnement

Existe-t-il un logiciel d'inventaire des éléments informatiques dans l'organisation ? Si oui, lequel ?

Nous utilisons **GLPI** pour l'inventaire des éléments informatiques. Cet outil nous permet de suivre tous nos équipements, notamment les Mac et autres périphériques, et de gérer les configurations de manière centralisée. GLPI est essentiel pour assurer une bonne gestion de notre système informatique et pour planifier la maintenance ou le remplacement des équipements.

Existe-t-il un outil de gestion des configurations ? Si oui, lequel ? Quel aspect des configurations sont gérés par ce mécanisme ?

Oui, nous avons un outil de gestion des configurations qui nous permet de créer et configurer les comptes sur les Mac des employés. Cet outil automatise la configuration des postes de travail selon les rôles spécifiques de chaque utilisateur, assurant ainsi une gestion cohérente et efficace des configurations sur plusieurs machines. Cela facilite également la maintenance et l'administration des systèmes, notamment la mise à jour des configurations en fonction des besoins des utilisateurs.

Existe-t-il un logiciel de gestion des incidents ? Si oui, lequel ?

Nous n'utilisons pas de logiciel spécifique pour la gestion des incidents. Lorsque des problèmes surviennent, les utilisateurs contactent directement l’équipe informatique via téléphone. En fonction de la nature et de la gravité de l'incident, l’équipe prend les mesures nécessaires pour résoudre le problème.

Existe-t-il une cellule dédiée à la résolution des incidents dans l'organisation ? Comment se passent les niveaux 1, 2 et 3 de résolution des incidents ? Quels sont les acteurs concernés et les circuits ?

Il n’y a pas de cellule dédiée à la gestion des incidents dans l'entreprise. L’équipe informatique composée de 5 personnes et de 2 stagiaires gère les incidents au fur et à mesure. Les utilisateurs signalent les problèmes par téléphone, et l’équipe résout les incidents en fonction de leur priorité et de leur complexité. Nous n’avons pas de classification formelle des niveaux d'incidents, mais la résolution est effectuée par l’équipe, avec l’assistance des stagiaires lorsque nécessaire.

Comment les sauvegardes sont-elles réalisées ? Quel type de sauvegarde ? Quelle est leur régularité ? Avec quel outil ? Sur quel support ? Comment vérifier que les sauvegardes se passent correctement ?

Nos sauvegardes sont réalisées par la réplique de toutes les données sur le cloud. Cela sert de mécanisme de sauvegarde pour garantir la continuité des activités en cas de panne du serveur local. Nous n’utilisons pas d’outil spécifique pour gérer les sauvegardes locales, mais la réplication dans le cloud nous assure une forme de sécurité. La régularité des sauvegardes est automatique via le cloud, ce qui garantit que les données sont sauvegardées en temps réel.

Les serveurs de l'organisation sont-ils virtualisés ? Si oui, avec quel logiciel ?

Non, nos serveurs ne sont pas virtualisés. Nous utilisons un seul serveur physique sur lequel toutes les données sont stockées et répliquées dans le cloud pour la continuité des activités.

Y a-t-il un serveur d'annuaire LDAP ? Si oui, lequel ? Quelle en est la structure (ou un extrait) ?

Non, nous n’utilisons pas de serveur d’annuaire LDAP. La gestion des utilisateurs se fait directement via les outils macOS, où chaque compte est configuré selon les rôles des utilisateurs au sein de l'entreprise.

Quel système de gestion de base de données (SGBD) est utilisé?

Nous utilisons **MySQL** pour gérer nos bases de données. C’est notre solution principale pour stocker et gérer les informations liées à nos activités.

Y a-t-il un PRA (plan de reprise d'activité), un PCA (plan de continuité d'activité) ?

Oui, nous avons un **PCA** en répliquant nos données sur le cloud. Cela nous assure que, en cas de panne du serveur local, nous pourrons toujours accéder aux données essentielles pour la continuité de nos activités. Cependant, nous n’avons pas de PRA formalisé au-delà de cette réplique dans le cloud.

Quelle est l'organisation du service informatique ?

Il n'y a pas vraiment d'organisation formelle dans notre service informatique. Chacun prend en charge les tâches selon les besoins du moment

Quels outils ou mécanismes de veille sont mis en place dans l'organisation ? Qui utilise ces outils ? Pour quoi faire ?

Nous utilisons principalement **Google Docs** et **Microsoft Teams** pour la collaboration sur les projets en cours. Pour la veille technologique, les membres de l’équipe informatique sont responsables de la recherche d'informations et de la mise à jour de nos pratiques, notamment via des alertes Google et des discussions régulières.

Comment travaille-t-on en mode projet ?

Le mode de travail est informel pour la plupart des projets. Nous utilisons **Google Docs** pour partager des informations et **Microsoft Teams** pour la gestion des communications entre les membres de l'équipe. Nous n'avons pas de planification formelle de projet comme dans des méthodologies agiles, mais nous nous adaptons aux besoins des projets au fur et à mesure.

l'infrastructure réseau .

Nous n'avons pas de schéma détaillé de l'infrastructure réseau. Notre réseau est relativement simple, avec un pare-feu pour la sécurité, un accès Wi-Fi pour les employés, et un serveur central pour le stockage des données.

Concernant les postes de travail, quelle est la description précise matérielle et logicielle de la machine (ou des machines) que vous utilisez ?

Tous les postes de travail sont des **Mac**. Les utilisateurs disposent d'un Mac adapté à leurs besoins professionnels. chaque poste est configuré en fonction des tâches spécifiques de l'utilisateur, via un compte créé avec des droits d'accès adaptés.

Modèle : Mac mini

Puce : Apple M1 (8 cœurs, 4 pour la performance et 4 pour l'efficacité)

Mémoire : 8 Go

Stockage : SSD de 256 Go (Apple SSD AP0256Q)

Version du système d'exploitation : macOS avec la dernière mise à jour du programme interne et du chargeur de système d'exploitation.

Comment l'organisation procède-t-elle pour installer de nouveaux postes de travail ? Existe-t-il des mécanismes d'automatisation des installations ? Si oui, lesquels ? Existe-t-il des procédures ? Si oui, lesquelles ?

L'installation de nouveaux postes se fait manuellement . Nous avons des procédures simples pour configurer les nouveaux postes en fonction des rôles des utilisateurs, assurant ainsi leur mise en service rapide et efficace.

Quel(s) antivirus sont mis en place ? Comment sont gérées les mises à jour et les analyses d’ antivirus ?

Nous n’utilisons pas d’antivirus spécifique. Les Mac bénéficient de la protection intégrée de macOS, qui assure une sécurité de base contre les menaces courantes. Les mises à jour de sécurité et les analyses sont gérées automatiquement par macOS.

Onglet 6

RAPPORT D'ACTIVITÉS

Semaine du 20 au 24 janvier

Contexte

J'ai participé a une audit pour l'entreprise **Costa Lucchini Habitat**, spécialisée dans la gestion immobilière. Cet audit faisait partie d'une mission pour évaluer la sécurité de leur réseau informatique et de leurs services en ligne. L'objectif était d'identifier les vulnérabilités et de proposer des solutions pour améliorer leur infrastructure et leur sensibilisation à la cybersécurité.

Travail effectué :

- **Lundi 20 janvier :**
    - Début de l'audit pour Costa Lucchini Habitat avec un plan détaillé de l'audit.
    - Envoi d'emails expliquant la procédure de l'audit et les attentes.
    - Participation active à l'élaboration du plan d'action pour l'audit.
    - Identification des services en ligne utilisés par l'entreprise et analyse des informations disponibles publiquement (OSINT).

- **Mardi 21 janvier :**
    - Continuation de l'audit avec l'évaluation de la surface d'attaque.
    - Finalisation de l'audit du site web de Costa Lucchini Habitat, identification des points faibles.
    - Élaboration d'un rapport détaillé et préparation d'une présentation pour le dirigeant.
    - Discussion avec le dirigeant pour présenter un aperçu du plan d'action, incluant des tests de vulnérabilité sur les erreurs humaines, telles que les attaques de phishing et la gestion des mots de passe.

- **Mercredi 22 janvier :**
    - Début d'une nouvelle campagne de phishing par email pour tester la sensibilisation des employés.
    - Temps de travail perturbé par un mal de tête important, absence l'après-midi.

- **Jeudi 23 janvier :**
    - Réalisation de la visite à Porto-Vecchio pour analyser l'infrastructure informatique de l'entreprise et identifier d'éventuelles vulnérabilités.
    - Finalisation de la présentation pour le dirigeant, en mettant l'accent sur les résultats de l'audit et les recommandations pour améliorer la sécurité.

- **Vendredi 24 janvier :**
    - Absence pour cause de maladie.

Semaine du 27 au 31 janvier

Contexte

La semaine a été marquée par l'envoi de nouveaux emails et SMS dans le cadre de l'attaque de phishing, et l'analyse des résultats de ces attaques.

Travail effectué :

- **Lundi 27 janvier**
    - Absence en raison de maladie, aucune tâche réalisée.

- **Mardi 28 janvier :**
    - Absence en raison de maladie, aucune tâche réalisée.

- **Mercredi 29 janvier :**
    - Reprise du travail après la maladie.
    - Envoi d'emails et SMS pour l'attaque de phishing.

    - Analyse des résultats des campagnes précédentes, en évaluant leur impact et en planifiant les prochaines étapes.

- **Jeudi 30 janvier :**
    - Finalisation de l’analyse des résultats des campagnes de phishing et proposition d’améliorations sur la sensibilisation des employés.

- **Vendredi 31 janvier :**
    - Travail effectué le matin.
    - L'entreprise ferme l'après-midi.

Conclusion

Cette période d'activité a permis d'avancer dans l'évaluation des risques pour Costa Lucchini Habitat, notamment en analysant l'exposition de l'entreprise aux cybermenaces, à travers des tests de phishing et des audits de sécurité. J'ai pu identifier des axes d'amélioration pour leur infrastructure et leur stratégie de sécurité. L'objectif à long terme est de renforcer leur résilience face aux attaques et de sensibiliser leurs employés aux risques liés aux cybermenaces.