Cartes Attaques

CARTE A1 :

En se plaçant sur mon réseau wifi qui avait un mot de passe trop faible (clé wep facilement piratable) (BP5/NS* du WIFI de 2), l'attaquant observe les données que j'échange avec un ami via un message électronique non chiffré (BP8/NS de la messagerie de 3). L'attaquant possède alors des informations personnelles compromettantes (BP12/NS « identité numérique » de 2).

CARTE A2 :

Un forum amateur a été compromis par un attaquant à l'aide d'un XSS ou cross-Site scripting et l'a utilisé sur un site de commerce en ligne pour lequel j'utilisais le même mot de passe (BP1/NS de « mot de passe » de 3). Il a ensuite pu se connecter à ma messagerie pour laquelle j'utilisais le même identifiant utilisateur et le même mot de passe (BP8/NS « prudence messagerie » de 3), et il a finalement envoyé à l'ensemble de mes contacts professionnels et personnels (BP11/NS «séparation des usages » de 2) un mail frauduleux.

CARTE A3 :

Un attaquant est parvenu à se connecter à ma messagerie électronique professionnelle (BP11/ NS « séparation des usages de 2) après avoir obtenu la réponse à ma question secrète par le biais de ses recherches sur les réseaux sociaux (BP12/ NS « Identité numérique » de 3). Il a ensuite envoyé un lien vers un fichier exécutable contenant un Cheval de Troie à l'ensemble de mes collaborateurs (BP8/NS « prudence messagerie » de 3).

CARTE A4 :

Lors d'un déplacement professionnel, je m'absente 10 min laissant mon ordinateur portable déverrouillé, sans surveillance (BP7/NS « déplacement » de 2). Un attaquant profite alors de l'opportunité pour récupérer des informations confidentielles sur des clients de mon entreprise, travaillant directement depuis un compte administrateur (BP3/NS « Connaissance des utilisateurs » de 3), il parvient sans difficulté à récupérer ces dossiers. Il en profite ensuite pour télécharger des logiciels espions sur mon PC (BP9/NS « téléchargement de programmes » de 2).

CARTE A5 : Injection SQL

Le SI dispose d'un site pour présenter l'entreprise. Sur celui-ci il est possible de s'identifier pour candidater à des offres d'emplois notamment. Un attaquant est parvenu à injecter des requêtes sql pour extraire des données de la base de données. La BDD est entièrement compromise. Il faut avertir les utilisateurs de la compromission de leurs données. Attaque irréversible. BP ciblée 1: choisir avec soins ses mots de passes car les utilisateurs doivent à tout prix avoir des mdp différents pour des services différents (NS = 3). BP ciblée 12 : identité numérique. Sur ce site les utilisateurs disposent leur CV et lettre de motivation et donc publient leur identité professionnelle (NS = 3). BP ciblée 3 : bien connaître les utilisateurs du SI et la sensibilité des données (NS = 2).

CARTE A6 : Ransomware (rançongiciel)

Un utilisateur du SI, peu au fait des bonnes pratiques et des recommandations de l'ANSSI, reçoit un mail fallacieux avec un lien cliquable. En cliquant, il active un ransomware (rançongiciel) qui chiffre ses données (du moins c'est ce qui est annoncé) et qui réclame une rançon en échange de la restitution de la clé privée pour déchiffrer les données. BP ciblée 4 : effectuer des sauvegardes régulières (NS = 2 car seul l'ordinateur du collaborateur est affecté). BP ciblée 8 (NS = 3) : être prudent lors de l'utilisation de la messagerie. BP ciblée 12 (NS = 2 car les données ne peuvent être exploitées par l'attaquant). Identité numérique.

CARTE A7 : Phishing & Spearphishing (hameçonnage ciblé)

L'utilisateur du SI, fatigué par une longue matinée de travail ouvre ses mails persos pour faire une petite pause. Il reçoit un mail provenant d'un réseau social qu'il connaît, lui demandant de confirmer son identifiant et mot de passe. En réalité, il s'agit d'un site vitrine disposant du même affichage que le réseau social afin de tromper l'utilisateur. Il entre alors les données demandées sans faire attention aux fins détails qui diffèrent du véritable réseau social. Il les divulgue donc au hacker. BP ciblée 8 (N.S = 2) Prudence lors de l'utilisation de la messagerie. BP ciblée 11 (N.S = 2) : séparer l'usage professionnel et personnel. BP ciblée 12 (N.S = 3) : prendre soin de son identité numérique.

CARTE A8 : ATTAQUE WIFI

En déplacement, vous vous trouvez à une enseigne de café connue à l'emblème vert. Il y a une borne wifi gratuite sans protection et décidez de commander un cadeau à votre meilleur ami(e). Mais vous ignoriez que la borne wifi n'appartient pas au café mais à un attaquant assis deux places plus loin, entre vous et le comptoir. Celui-ci analyse les paquets (sniffing) et parvient à extraire les données bancaires que vous avez transmises pour l'achat. De plus, il accède également au contenu et à la pièce jointe du mail professionnel que vous avez envoyé. Ce sont des informations sur la stratégie d'entreprise qu'il peut transmettre à la concurrence. BP ciblée 5 (N.S = 2) : toujours se connecter à un wifi sécurisé, surtout lors de l'utilisations de données sensibles. BP ciblée 10 (N.S = 3) : vigilance lors de l'achat sur internet. BP ciblée 11 (N.S = 3) : séparation usages

CARTE A9 : Faille d'un logiciel non à jour + Privilèges accordés à des utilisateurs autre que le service informatique

Certains des logiciels installés par un employé ne sont plus à jour. Un attaquant a pu, à l'aide encore une fois d'une pièce jointe piégée, exploiter une faille d'un de vos logiciels afin d'installer un keylogger et surveiller l'activité de l'entreprise. BP ciblée 2 (NS = 3) Mettre à jour les logiciels. BP ciblée 3 (N.S = 2) Bien connaître ses utilisateurs. BP ciblée 8 (N.S = 3). Prudence messagerie.

CARTE A10 : Password attack (brute force, dictionnaire) + vol -> perte de fichier si non sauvegardés, vol de données si disque dur non chiffré

En weekend dans votre maison de campagne, vous prenez avec vous votre ordinateur pour rédiger 2,3 mails. Un bon matin, vous vous réveillez et vous constatez à votre grand désarroi que vous avez été cambriolé. Votre ordinateur a disparu. De plus, l'attaquant est parvenu à s'authentifier à l'aide d'une attaque brute force et a accès à toutes vos données personnelles et professionnelles car votre disque dur n'est pas chiffré. BP ciblée 4 : sauvegardes régulières (NS=3). BP ciblée 6 : être prudent avec son ordinateur (NS=2). BP ciblée 11 : séparer usage pro et perso (NS =3).

CARTE A11 : Installation application espion

Au cours d'un déplacement dans un vaste pays asiatique densément peuplé, vous êtes abordé par un individu charismatique, souriant et drôle qui a besoin d'effectuer un appel avec votre portable, le sien étant à cours de batterie. Il vous remercie et vous rend le portable. Rien ne semble avoir changé mais en réalité il a installé un profil de configuration qui ne se voit que dans les réglages et capable d'accéder à l'ensemble de vos données (mail, photos, documents, sms…) et de les envoyer à un destinataire particulier. Bien entendu, il vous a vu préalablement composé votre mot de passe de 4 chiffres pour déverrouiller votre smartphone. Bienvenue dans le monde de l'espionnage industriel. BP ciblée 6 : protection smartphone (NS=3). BP ciblée 7 déplacements (NS=3). BP ciblée 11 : séparations usage professionnel et personnel (NS=3).