Retour d'expérience
PIRATAGE DE MESSAGERIE

La Mission numérique a été sollicitée par une structure du territoire confrontée à une arnarque au faux ordre de virement, commise suite à un piratage de sa messagerie électronique.

Retour d'expérience suite à l'accompagnement d'un artisan victime de compromission de sa messagerie professionnelle. Dans le cas présent, il s'agît d'une arnaque au Faux Ordre de Virement (FOVI). L'arnaque FOVI permet à l'attaquant de détourner le paiement des travaux facturés par l'artisan à son avantage.

SITUATION

La messagerie de l'artisan a été utilisée par un attaquant pour émettre de faux RIB. L'attaquant a contrefait le RIB de l'entreprise, initialement établi auprès d'une banque française historique (nommons-la « Banque A »), au profit d'un compte détenu auprès d'une néo-banque, BUNQ. Le numéro de l'IBAN indiqué par le pirate est le suivant : FR76 2763 3121 2901 0104 1622 020.
Il est possible d'identifier la banque en testant le numéro IBAN dans l'outil en ligne Iban Calculator (lien ci-après). On s'aperçoit alors que l'entête du RIB, affichant le logo de la Banque A, ne correspond pas à la banque du numéro IBAN.

MODE OPÉRATOIRE

L'attaquant s'est connecté à la messagerie de l'artisan. Il a pu ainsi consulter les courriels présents dans la boîte de réception, les courriels déjà envoyés, les messages présents dans la corbeille, les pièces jointes et autres copies de documents. Il a également eu accès au répertoire des contacts de la messagerie (prospects, clients réguliers, contacts professionnels).

QUELLES FAILLES A-T-IL PU EXPLOITER ?

Pour se connecter en toute discrétion à la messagerie de l'artisan, l'attaquant a tiré profit de l'absence des mesures de sécurité suivantes :

- faiblesse du mot de passe pour se connecter à la messagerie, ici, le mot de passe était facilement devinable ;
- absence de double authentification, aucun avertissement ne pouvait signaler des tentatives de connexion ;
- concentration des données dans la messagerie : la messagerie rassemblait l'intégralité des échanges de l'entreprise.

QUELLES DONNÉES L'ATTAQUANT A-T-IL PU RASSEMBLER ?

En parcourant la messagerie, l'attaquant a pu prendre connaissance de nombreuses informations à caractère personnel ; on peut identifier les types de documents

suivants :

- copies de fiches de paye, documents santé (RIB, numéro de Sécurité sociale, pathologies…),
- devis, factures (nom de clients, travaux demandés, montant des travaux…),
- actes notariés, document de propriété, héritage (accès à des documents confidentiels),
- informations bancaires diverses, RIB, mouvements bancaires (habitudes d'achats, capacité d'investissement etc.),
- signatures dématérialisées, cachets, sceaux (facilite la création de faux documents),
- informations d'ingénierie sociale sur les employés et les clients (facilite et augmente les chances de répliquer et réussir une attaque contre d'autres personnes liées à l'artisan),
- etc.

Les différentes versions numériques de ces documents ont permis à l'attaquant de concevoir des copies réalistes et crédibles du RIB de la société. Il a également pris connaissance des échanges entre l'artisan et ses clients, pour intercepter et détourner les échanges à son profit.

COMMENT SÉCURISER L'ENVIRONNEMENT NUMÉRIQUE ?

- Adopter un mot de passe de messagerie robuste, en s'appuyant sur un coffre-fort numérique,
- Éviter de mélanger les usages :
  - par exemple, séparer la messagerie en deux entités, secrétariat / facturation et prise de contact / devis,
  - séparer les usages personnels et professionnels sur les téléphones ou ordinateurs,
  - réduire les messages reçus dans la messagerie (suppression des abonnements aux newsletters) pour gagner en clarté de lecture
  - sortir les courriels de la messagerie en les archivant, via des fonctionnalités d'exportation. Cela réduira l'impact d'une éventuelle nouvelle compromission.
- activer la double authentification lorsqu'elle est proposée,
- appliquer les mises à jour des logiciels lorsqu'elles sont publiées,
- supprimer les logiciels non utilisés ou obsolètes,
- s'astreindre à une sauvegarde efficace ou opter pour un service de sauvegarde fourni par un prestataire.

LE DÉPÔT DE PLAINTE

Dès que l'attaque est constatée, il est important de porter plainte au plus vite.
La gendarmerie ou le commissariat doivent recueillir votre plainte : munissez-vous de justificatifs (captures d'écran, impressions, photos).

Le dépôt de plainte via le téléservice Thésée est réservé aux particuliers.

Plus de détails :
https://www.service-public.fr/particuliers/vosdroits/F1435

RESSOURCES & LIENS

Iban Calculator – identifier la banque rattachée à un numéro Iban :
https://www.ibancalculator.com/

Numerama – article de recommandations de gestionnaires de mots de passe :
https://www.numerama.com/cyberguerre/1550900-les-meilleurs-gestionnaires-de-mots-de-passe.html

Mobile Connect d'Orange – pour mettre en place une double vérification sur une adresse @orange.fr :
https://assistance.orange.fr/assistance-commerciale/l-identification/mobile-connect/mobile-connect-utiliser_267283-808401

Caractériser la violation de données :
https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles