Retour d'expérience

PIRATAGE DE MESSAGERIE

La Mission numérique du Pays Auxois Morvan a été sollicitée par une adjointe au maire d'une commune du territoire, pour une arnaque au faux ordre de virement, commise suite à un piratage de la messagerie électronique.

Dans le cadre de sa mission d'appui des collectivités, Alexandre GARDAVOT, Chargé de mission développement des usages numériques, est intervenu pour accompagner une collectivité et un artisan victimes d'une compromission. Dans le cas présent, il s'agissait d'une arnaque au Faux Ordre de Virement (FOVI). L'arnaque FOVI a permis 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, messagerie également utilisée par l'épouse, adjointe au maire, dans le cadre de son mandat. Le pirate ainsi pu 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), **menaçant ainsi la sécurité de la collectivité**.

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 et de l'adjointe de la commune.

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

En parcourant la messagerie, l'attaquant a pris 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),
- **échanges de courriels relatifs aux affaires de la commune**.

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,
- Séparer les usages professionnels et personnels :
  - conserver la messagerie de l'entreprise et créer une messagerie dédiée au mandat,
  - **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 réagir au plus vite. En effet, selon la portée de l'attaque, un délai peut s'appliquer : dans le cas d'une fuite de données à caractère personnel, vous devrez contacter la CNIL dans un délai de 72h.

Concernant les communes et les collectivités, la Gendarmerie ou le commissariat doivent recueillir la plainte : il faudra alors fournir des justificatifs (captures d'écran, impressions, photos).

Attention, pour les particuliers, le dépôt de plainte doit se faire via le téléservice Thésée.

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

17 CYBER

Mon assistance en ligne

LE 17CYBER VOUS GUIDE

Afin d'aider les victimes à identifier le service auprès duquel porter plainte, la Police Nationale, la Gendarmerie Nationale et Cybermalveillance.gouv.fr ont développé un service d'assistance en ligne.

Celui-ci, disponible à l'adresse https://17cyber.gouv.fr/ permet de rediriger, après un court questionnaire, la victime vers le service adéquat.

En cas d'attaque, contactez le centre de réponse à incident cyber :
CSIRT BFC au 0 970 609 909

CSIRT
BOURGOGNE-FRANCHE-COMTÉ

RESSOURCES & LIENS

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

UpSignOn, le coffre-fort numérique proposé par l'ARNia : https://www.ternum-bfc.fr/services/cybersecurite/coffre-fort-de-mot-de-passe

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://mc.orange.fr/