03 juil 2020 -09:53

Le Centre pour la Cybersécurité Belgique met en garde les entreprises contre la fraude aux factures

La fraude aux factures chez les entreprises n'est pas un phénomène nouveau, mais, ces derniers temps, CERT.be, le service opérationnel du Centre pour la Cybersécurité Belgique (CCB), reçoit un nombre accru de signalements de ce procédé d'extorsion. Le CCB alerte également les entreprises pour qu'elles restent vigilantes au moment de procéder à des paiements.

La fraude aux factures est une forme d'extorsion qui consiste pour les cybercriminels à faire modifier le numéro de compte de fournisseurs fixes. Les cybercriminels usurpent l'identité d'un fournisseur et demandent à un collaborateur du service financier ou de la comptabilité de changer le numéro de compte et d'effectuer des versements. Le collaborateur risque alors de ne pas remarquer que la demande ne vient pas du fournisseur et d'effectivement procéder à ces versements sur le compte des criminels.

> "Il semblerait que les cybercriminels tentent toujours plus leur chance en période de vacances. Ils comptent sur un affaiblissement de la vigilance dans le chef des collaborateurs pendant les mois d'été ou espèrent qu'un remplaçant sera moins au courant des procédures en vigueur"
>
> Miguel De Bruycker
> Directeur Centre pour la Cybersécurité Belgique

Une fausse facture peut prendre différentes formes. Les cybercriminels falsifient des factures originales et y changent le numéro de compte bancaire, ou envoient des factures fantôme, c'est-à-dire des factures sans aucune prestation en contrepartie.

Principaux conseils pour s'armer contre la fraude aux factures

Pour le management :

- Prenez contact avec le demandeur en passant par un autre numéro de téléphone ou e-mail que celui fourni dans le message reçu (pour être sûr qu'il s'agit du véritable demandeur). Utilisez par exemple la fonction *Forward* plutôt que *Reply*.

- Veillez à ce que les processus de paiement soient clairs et correctement suivis.
- Instaurez des procédures claires pour vérifier les ordres de paiement ou les demandes d'informations sensibles, surtout lorsqu'ils sont envoyés par e-mail.
- Informez les collaborateurs et veillez à leur fournir une bonne formation pour qu'ils soient en mesure de reconnaître une fraude rapidement et d'y apporter une réponse adéquate.

Pour les collaborateurs :

- Prenez contact avec le demandeur en passant par un autre numéro de téléphone ou e-mail que celui fourni dans le message reçu (pour être sûr qu'il s'agit du véritable demandeur). Utilisez par exemple la fonction *Forward* plutôt que *Reply*.
- Comparez le numéro de compte mentionné sur la facture à vos propres données ;
- Redoublez de vigilance pour les paiements soi-disant urgents qui impliquent d'enfreindre les procédures normales.
- Suivez à la lettre les règles de sécurité et de paiement. Par exemple : faire signer les paiements à partir d'un certain montant par plusieurs collaborateurs.
- Ne décrivez jamais à des inconnus les procédures de paiement dans votre entreprises. Gardez ces procédures pour un usage interne.

Usurpation d'identité commerciale

Dans les cas d'usurpation d'identité commerciale, les cybercriminels agissent au nom de votre entreprise. Cela peut faire suite à un hacking ou à la prise de contrôle d'un compte d'entreprise. Cette manœuvre permet aux cybercriminels de voler de l'argent à vos clients, par exemple.

Recommandations pour prévenir l'usurpation d'identité commerciale

- Utilisez toujours des mots de passe sûrs pour vos comptes
- Utilisez l'authentification multifactorielle (2FA) partout où c'est possible
- Entraînez vos collaborateurs à reconnaître le phishing
- Faites preuve de précautions avec les données de votre entreprise

Centre pour la Cybersécurité Belgique
Rue de la Loi 16
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Andries Bomans
Responsable communication
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien - momenteel in verlof Eggers -momenteel in verlof
Responsable communication
+32 485 76 53 36
katrien.eggers@cert.be