الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

Comment se protéger des attaques BEC* ?

*Business Email Compromise

tunCERT

Tunisian Computer Emergency ResponseTeam

Business Email Compromise

C'est quoi une attaque BEC ?

Les attaques par compromission d'emails professionnels (BEC) représentent la menace la plus coûteuse parmi toutes les cyber-attaques visant les entreprises ou les organisations. Ce type d'attaque consiste à envoyer des emails de type BEC donnant l'impression d'émaner de personnes de confiance, et inciter les victimes à envoyer de l'argent ou des informations sensibles de l'entreprise à des cybercriminels, ou encore cliquer sur des liens douteux engendrant des actions malveillantes (Phishing, infections ransomwares, etc ...)

Étant donné que ce type de menace s'appuie davantage sur la technique d'ingénierie sociale que sur les logiciels malveillants, le courrier électronique frauduleux parvient souvent de dérouter les solutions de sécurité des emails, qui ne recherchent que les contenus ou les comportements malveillants.

Les attaques par compromission d'emails professionnels (BEC) ciblent, principalement,les grandes entreprises notamment les directeurs et les décideurs.

Comment se protéger des attaques BEC ?

Protéger ses identifiants et paramètres d'accès et veiller à ne pas utiliser les mêmes pour différents comptes (réseaux sociaux, e-mail, etc...).

Vérifier la concordance des adresses emails de l'émetteur et du récepteur avant de répondre aux courriers : certaines adresses peuvent utiliser des noms de domaine qui peuvent tromper le destinataire au premier coup d'œil et vice versa.

Vérifier la date, le format des dates ainsi que la langue utilisée dans le corps de l'e-mail (termes familiers, fautes d'orthographe). On reconnait généralement, le style de rédaction de l'un de nos contacts ou encore la présence de formats de date différentes. Ceci est très courant dans ce type d'attaque.

Se méfier des e-mails qui contournent les circuits habituels : (un devis en pièce jointe qui parvient au courrier du DG au lieu de celui du comptable, etc...)

Mettre à jour la liste des contacts (suppression des adresses inactives, fusionner les contacts, etc...)

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency ResponseTeam

Comment se protéger des attaques BEC ?

Scanner les pièces jointes avec un antivirus mis à jour avant de les ouvrir, même si ça provient de l'un de vos contacts. En cas de doute quant à la source ou la véracité de l'identité de l'expéditeur, ne pas ouvrir la pièce jointe et vérifier directement auprès de l'émetteur.

Prendre son temps et ne pas répondre à un email urgent : en effet, ces emails visent à manipuler la victime pour qu'elle réponde vite.

En cas d'attaque, vous pouvez contacter l'ANSI et déclarer vos incidents via :

incident@ansi.tn

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency ResponseTeam

tunCERT
Tunisian Computer Emergency ResponseTeam

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

Votre partenaire en sécurité de l'information...

CONTACTEZ-NOUS !

https://www.facebook.com/ansitn/

https://www.linkedin.com/in/ansi-tuncert-80bb4b172/

www.ansi.tn

ansi@ansi.tn

71 846 020

49, Avenue Jean Jaurès, 1000 Tunis