Fraude au prÃ©sident : Arnaque de lâ□□essor du tÃ©lÃ©travail
Internet
PostÃ© par : JPilo
PubliÃ©e le : 24/11/2021 15:00:00

Selon le baromÃ¨tre 2020 â□□Etude sur la fraudeâ□□ du cabinet Euler Hermes, la fraude au prÃ©sident est devenue lâ□□une des principales cyberattaques dans le monde (la troisiÃ¨me dâ□□aprÃ¨s le cabinet). Cette escroquerie, qui a recours Ã lâ□□usurpation dâ□□identitÃ© des dirigeants dâ□□entreprise, est en hausse notable et est mentionnÃ©e par 38% des entreprises ayant rÃ©pondu Ã lâ□□Ã©tude.

Tout comme les ranÃ§ongiciels, la fraude au prÃ©sident a profitÃ© de lâ□□essor massif du tÃ©lÃ©travail en 2020 pour se dÃ©velopper. Si, dans le cas des ranÃ§ongiciels, ce sont les technologies dâ□□accÃ¨s Ã distance qui ne sont pas adaptÃ©es au tÃ©lÃ©travail, ici câ□□est le manque dâ□□interactions sociales en prÃ©sentiel et de communication qui est lâ□□une des causes majeures de la multiplication de ce type dâ□□arnaque.

Comment se dÃ©roule une fraude au prÃ©sident ?

Dans le cadre de la fraude au prÃ©sident, un escroc qui a prÃ©alablement fait des recherches sur lâ□□entreprise cible se fait passer pour le PDG ou pour un administrateur pour demander, par e-mail, au comptable de la sociÃ©tÃ©, un virement bancaire pour une opÃ©ration confidentielle et urgente.

Cet escroc usurpe ainsi lâ□□identitÃ© dâ□□une personne de confiance, via une adresse e-mail crÃ©Ã©e pour lâ□□occasion, et sâ□□adresse directement au bon interlocuteur (le comptable). Cette tÃ¢che apparaissant comme urgente, la personne contactÃ©e va parfois sâ□□exÃ©cuter sans prendre le temps de la rÃ©flexion et, puisquâ□□il sâ□□agit dâ□□une opÃ©ration confidentielle, elle nâ□□en parlera pas Ã ses collÃ¨gues et nâ□□Ã©veillera donc pas les soupÃ§ons.

En dÃ©cembre 2020, le CDER, lâ□□une des associations de gestion et comptabilitÃ© les plus importantes en France, a subi une attaque de ce type avec un prÃ©judice annoncÃ© de 14,76 Mâ□¬ (source : Lâ□□Union). La comptable de lâ□□association a Ã©tÃ© licenciÃ©e pour faute grave pour avoir â□□contournÃ© les procÃ©dures internesâ□□.

â□□Suite Ã la pandÃ©mie et la mise en place du tÃ©lÃ©travail au sein des organisations, de nombreux collaborateurs travaillent depuis chez eux au moins une partie de la semaine. En consÃ©quence, une forte diminution voire une absence dâ□□intÃ©ractions et de discussions de vive voix avec les dirigeants et administrateurs.

Les Ã©changes Ã distance se sont multipliÃ©s et les opÃ©rations qui avaient pour habitude dâ□□Ãªtre confirmÃ©es ou Ã©voquÃ©es en prÃ©sentiel ont fait place Ã des rÃ©ponses par simples emails qui, dans le cas d'une fraude au prÃ©sident rÃ©ussie, engendrent des dommages irrÃ©versiblesâ□□, explique Christophe Corne, PrÃ©sident du Directoire de Systancia.

Quelques bonnes pratiques pour sâ□□en prÃ©munir

Pour les entreprises, la fraude au prÃ©sident est loin dâ□□Ãªtre une fatalitÃ©. Plusieurs actions peuvent en effet Ãªtre mises en place pour limiter drastiquement le risque quâ□□une telle arnaque aille Ã son terme.

Dans un premier temps, il est indispensable de sensibiliser les comptables Ã ce type de fraude puisque ce sont eux qui sont spÃ©cifiquement visÃ©s. Deux Ã©lÃ©ments doivent les alerter : les caractÃ¨res urgents et confidentiels de lâ□□opÃ©ration. En cas de doute, il conviendra alors de contacter le prÃ©sident par tÃ©lÃ©phone pour valider cette opÃ©ration de vive voix.

Cependant, si ce type de vÃ©rification est faisable au sein des PMEs, lorsquâ□□il sâ□□agit dâ□□une grande entreprise, il est parfois plus compliquÃ© dâ□□obtenir une confirmation orale.

Câ□□est dans ce cas quâ□□une fonctionnalitÃ© telle que la sÃ©paration des tÃ¢ches (SoD â□□ Segregation of Duties) prend tout son sens. IntÃ©grÃ©e aux solutions dâ□□identitÃ©s des utilisateurs et de leurs habilitations, telle que Systancia Identity, cette fonctionnalitÃ© rend nÃ©cessaire le fait dâ□□avoir deux personnes pour rÃ©aliser certaines tÃ¢ches considÃ©rÃ©es comme critiques.

Les virements bancaires Ã©tant, en tout Ã©tat de cause, critiques pour toute organisation, ceux-ci doivent Ãªtre soumis Ã un mÃ©canisme de SoD pour tout virement non rÃ©current ainsi que lors de la mise en place dâ□□un virement rÃ©current.

La rÃ©alisation dâ□□un virement bancaire par le comptable serait soumise Ã une validation Ã©lectronique dâ□□un administrateur de la sociÃ©tÃ© ou de tout autre personne habilitÃ©e Ã valider ce type dâ□□opÃ©ration. Ainsi, si le virement semble suspect, celui-ci sera investiguÃ© et stoppÃ© avant mÃªme que le virement ne soit effectuÃ©.

Dans son rapport d'Ã©tat de la menace ranÃ§ongicielle en France en 2020, l'Agence nationale de la sÃ©curitÃ© des systÃ¨mes d'information (ANSSI) pointe une hausse des signalements d'attaque de 255 % par rapport Ã 2019. En 2020, l'agence estime que le nombre de ranÃ§ongiciels a quadruplÃ© (source SÃ©nat).

La fraude au prÃ©sident, comme tout autres principales cybermenaces, doit Ãªtre intÃ©grÃ©e aux actions de sensibilisation Ã la cybersÃ©curitÃ© dispensÃ©es par les organisations. Il sâ□□agit lÃ de la premiÃ¨re barriÃ¨re face aux cyberattaques et parfois la seule disponible, dÃ¨s lors quâ□□une sociÃ©tÃ© ne dispose pas de solutions de cybersÃ©curitÃ© adÃ©quates face aux diffÃ©rentes menaces qui pÃ¨sent sur les systÃ¨mes dâ□□information.

â□□Les collaborateurs sont en premiÃ¨re ligne face aux cyberattaques et doivent donc Ãªtre au cÅ□ur de la stratÃ©gie de sÃ©curisation des systÃ¨mes. Un collaborateur formÃ© et informÃ© voit son statut passer de celui de faille Ã celui de maillon fort de lâ□□organisation,â□□ conclut Christophe Corne.Â