

ANGLAIS

Je suis un technicien au sein d'une entreprise locale qui fait l'oeuvre de cyber attaque, elle me demande de proposer quelque solution pour faire face à ce type d'attaque.

La première solution serait de mettre en place une zone DMZ qui est une zone dite délimiter qui ne comporte uniquement les serveurs accessibles de l'extérieur. L'intérêt de mettre en place une zone DMZ est qu'elle va isoler le réseau interne des serveurs accessibles de l'extérieur, par exemple le serveur web de la compagnie ou bien un serveur de boîte mail. Le réseau interne comporte les postes utilisateurs et les serveurs uniquement accessibles de l'intérieur et non de l'extérieur. La zone DMZ permet d'éviter une propagation d'une cyber attaque sur l'ensemble du réseau, c'est à dire interne et DMZ, lors d'une cyber attaque uniquement les serveurs présents dans la DMZ seront touchés car des règles de pare-feu ont été mises en place pour que l'attaquant ne puisse en aucun cas accéder au réseau interne. Sans DMZ tout l'ensemble du réseau y compris les postes utilisateurs et tous les serveurs seront touchés par l'attaque.

La deuxième solution serait de mettre en place une campagne de sensibilisation au comportement à avoir face à des types d'attaques par mail, montrer les bons gestes notamment avec le fait de ne pas cliquer sur des liens potentiellement frauduleux qui auront pour but de voler des informations ou d'introduire un virus (ransomiciel par exemple). Vérifier les emails en les comparant avec des emails officiels, prenant l'exemple de la Socredo, être en connaissance de l'email officiel de la Socredo puis le comparer à celui d'un email frauduleux qui incite à rentrer des informations bancaires. Dans ce cas si prendre l'email frauduleux et le comparer avec l'email officiel de la Socredo car un email frauduleux prendra le nom Socredo mais avec une lettre, un caractère ou un chiffre en plus, il s'agit du premier indice pouvant être vu sur un email frauduleux. Deuxième point prévenir son chef ou son informaticien lorsque un mail a l'air suspect afin qu'il puissent examiner en détail le mail.

La troisième solution serait de mettre en place un logiciel anti spam afin d'éviter toute congestion de la boîte mail ou tout type d'attaque visant à saturer la boîte mail de la compagnie.

La quatrième solution serait de mettre en place des règles de pare-feu très concrètes en filtrant le trafic passant du réseau interne au réseau externe (internet). Cela aura pour effet d'avoir moins d'attaques car certains protocoles ou contenus pourront être bloqués ou non. Il est possible également d'analyser en détail le trafic transitant entre le réseau interne et externe afin de détecter toute éventuelle cyber attaque.

I'm a technician at a local company that's been the target of a cyberattack. I've been asked to propose solutions to deal with this type of attack.

The first is to set up a DMZ, a so-called demarcated zone that only contains servers accessible from the outside.

The advantage of a DMZ is that it isolates the internal network from servers accessible from the outside, for example, the company's web server or an email server.

The internal network contains user workstations and servers accessible only from the inside, not from the outside. The DMZ prevents a cyberattack from spreading to the entire network, i.e., both the internal and DMZ.

In the event of a cyberattack, only the servers in the DMZ will be affected, as firewall rules have been implemented to ensure that the attacker cannot access the internal network under any circumstances.

Without DMZ, the entire network, including user workstations and all servers, will be affected by the attack.

The second solution would be to set up awareness campaign about how to behave when faced with a type of email attack, showing the right actions, particularly by not clicking on potentially fraudulent links that could steal information or introduce a virus (ransomware, for example).

Verify emails by comparing them with official emails, taking the example of Socredo, be aware of the official Socredo email and then compare it to that of a fraudulent email that encourages you to enter banking information.

In this case, take the fraudulent email and compare it with the official Socredo email, because a fraudulent email will use the Socredo name but with an additional letter, character, or number; this is the first clue that can be seen in a fraudulent email.

Second point: notify your boss or IT technician when an email looks suspicious so that they can examine it in detail.

The third solution would be to implement anti-spam software to prevent inbox congestion or any type of attack aimed at saturating the company's inbox.

The fourth solution would be to implement very specific firewall rules by filtering traffic passing from the internal network to the external network (internet).

This will reduce the number of attacks because certain protocols or content may or may not be blocked.

It is also possible to analyze in detail the traffic passing between the internal and external networks to detect any potential cyberattacks.

First, there's the first document, a text published on June 10, 2022, which deals with cybersecurity...

Document B, a video published on May 9, 2021, by simplilearn.com, also covers cybersecurity in two minutes.

The third document, a poster published in 2019 bycom, is titled "Don't Get Hooked," which recommends not clicking on links as an awareness campaign.