ANGLAIS

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

La premiere serrais de mettre en place une zone DMZ qui est une zone dite delimitariser qui ne comporte uniquement les serveur accessible de l'extérieur. L'intérêt de mettre en place une zone DNZ est qu'elle va isoler le réseaux interne des serveur accessible de l'extérieur, par exemple le serveur web de la compagnie ou bien un serveur de boite mail. Le réseau interne comporte les postes utilisateur et les serveur uniquement accessible 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 a dire interne et DMZ, lors d'une cyber attaque uniquement les serveur présent dans la DMZ seront toucher car des règle de par feu en été mis en place pour que l'attaquant ne puissent en aucun cas accéder au réseaux interne. Sans DMZ tout l'ensemble du réseaux y compris les poste utilisateur et tout les serveurs seront touché par l'attaque.

La deuxième solution serrait de mettre en place une compagne de sensibilisation au comportement a avoir face a des type d'attaque par mail, montrer les bon geste notamment avec le fait de ne pas cliquer sur des lien potentiellement froduleux qui auront pour but de voler des information ou d'introduire un virus (rançongiciel par exemple). Verifier les email en les comparent avec des email officiel, prenant l'exemple de la Socredo, être en connaissance de l'email officiel de la Socredo puis le comparer a celui d'un email frauduleux qui incite a rentrer des information 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 vue sur un email frauduleux. Deuxieme point prévenir sont chef ou son informaticien lorsque un mail a l'air suspect afin qu'il puissent examiner en detail le mail.

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

La quatrième solution serait de mettre en place des règle de par feu très concrete en filtrant le trafic passant du réseaux interne au réseaux externe (internet). Cela aura pour effet d'avoir moins d'attaque car certain protocole ou contenu pourront être bloquer ou non. Il est possible également d'analyser en detail le traffic transitant entre le réseaux 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 compaign 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.