Jusqu'oú peuvent aller les cyberattaques ?

Aujourd'hui, la quasi totalité données sont informatisées. Celles-ci sont fréquemment mal protégées, ce qui suscite la curiosité de certains individus, appelés "hacker".
Que font ces "hacker" ?
En sécurité informatique, un hacker, francisé hackeur ou hackeuse, est un spécialiste d'informatique, qui recherche les moyens de contourner les protections logicielles et matérielles, généralement pour s'accaparait de données sensibles.
Ces actions sont plus connuement appelées "cyberattaque".

Les différents types d'hacker

Il y trois types d'hackeur, les black Hat hacker, les white hat hacker et les grey hat hacker.
Regardons en quoi ils se différencient.

Les black hat hacker

La plupart du temps, l'objectif du black hat hacker est de gagner de l'argent, en s'en emparant directement ou en le volant, en vendant des informations piratées ou en essayant d'extorquer de l'argent. Mais la plupart du temps, il cherche juste à créer le plus de problèmes possible.

Les white hat hacker

Les white hat hackers, ou pirates éthiques sont l'opposé des black hats. Ils sont tout aussi compétents, mais plutôt que d'appliquer ces compétences dans un but criminel, ils cherchent à aider les entreprises à renforcer leurs systèmes de sécurité informatique. Le white hat hacker essaie intentionnellement d'entrer par effraction dans un système, avec l'autorisation de son propriétaire, afin d'en identifier les points faibles pour pouvoir y remédier. Ce type de travail est appelé « piratage éthique ».

Les grey hat hacker

Alors que les white hat hacker disposent d'une autorisation pour tester les vulnérabilités des systèmes, les grey hat hackers se passent de cette permission.
Certains d'entre eux se comportent comme des mercenaires : après avoir découvert une faille de sécurité, ils contactent l'entreprise concernée pour lui proposer leurs services contre récompense.
D'autres agissent dans le but de forcer une entreprise qui se montre réticente à résoudre une vulnérabilité connue. Un exemple notable de grey hat hacking s'est produit en 2013 et a forcé Facebook à reconnaître une faille de sécurité et à la réparer après avoir ignoré les avertissements du hacker.

Sources : www.avast.com

Maintenant que vous connaissez les différents types d'hackeurs et d'attaques, nous allons entrer dans le vive du sujet et s'intéresser aux conséquences de ces attaques.

01

Les attaques á conséquences financiéres

De plus en plus d'entreprises notamment des PME sont exposées aux cyberattaques. Les conséquences de ces attaques sont nombreuses. Elles peuvent être d'ordre financier .

La rançon

Une attaque informatique peut faire subir á une entreprise des pertes financiéres conséquentes. Ces attaques, de quelque nature qu'elles soient, sont dangereuses, á fortiori, les ransomware. Le ransomware est un programme malveillant qui attaque votre système et vous exige une rançon pour mettre fin á l'attaque. Sous le choc et la menace, certaines entreprises sont tentées de payer la rançon demandée par le hackeur.

Les données

Les autres types d'attaques, tout comme le ransomware, peuvent potentiellement occasionner des conséquences financiéres. Ils donnent un coup d'arrêt aux activités de l'entreprise.
Ces cyberattaques endommagent vos données et peuvent causer un arrêt forcé de tous vos projets. Plus cette attaque (endommagement de vos données) dure, plus vous perdez du temps et de l'argent. C'est d'ailleurs l'exemple du groupe français Saint-Gobain qui a 220 millions d'euros de chiffre d'affaires á cause d'une cyberattaque opérée depuis sa filiale en Ukraine en 2017.

La réparation

Les pertes financiéres peuvent aussi dépendre du montant de la réparation de vos matériels informatiques. En général, De plus, la réparation d'un système informatique est trés onéreuse car certaines attaques affectent tout le réseau informatique de l'entreprise.

Sources : https://www.blank.app

02

Les attaques á conséquences sur la santé et l'intégrité

Sources : www.geostrategia.fr

Les cyberattaques ne sont en effet pas limitées aux menaces informatiques. Ces attaques pourraient aussi avoir de graves conséquences sur la santé et l'intégrité physique des personnes qui travaillent dans les installations sensibles ou qui vivent aux alentours et appellent á des mesures de prévention.
L'impact sur l'outil de production qui pourrait générer des effets dommageables sur l'intégrité physique des hommes ou sur l'environnement naturel n'est quant á lui quasiment jamais pensé. Pour autant, bon nombre d'entreprises disposent d'installations qui stockent, utilisent ou produisent des produits dangereux (gaz naturel, propane, butane, ammoniac, acides, bases, etc...) pouvant être á l'origine d'explosions, d'incendies et/ou de rejets d'effluents toxiques en cas de dysfonctionnements.

Quelques exemples..

En 2000, un ancien employé de la société, ayant installé le SCADA [4] d'une centrale de traitement des eaux usée en Australie, s'est vengé suite á un refus de la société gérant la centrale de l'embaucher. Il a volé un équipement radio de son employeur et a envoyé des commandes au SCADA générant le déversement dans la nature de 800 m3 d'eaux usées.

En 2008, des attaquants ont exploité la vulnérabilité des caméras de surveillance installées le long du pipeline de Baku-Tbilisi- Ceyhan en Turquie pour accéder au serveur de gestion des alarmes et des moyens de communication. Puis, ils se sont rendus physiquement á une station de pompage et ont généré, par l'intermédiaire du système de contrôle local, une montée en pression dans le pipeline qui a entraîné une explosion.

En 2013, des attaquants se sont introduits dans une station d'eau potable en Géorgie (USA) et ont, via le système de supervision, modifié les réglages des taux de fluor et de chlore injectés dans l'eau, la rendant impropre á la consommation et privant ainsi 400 personnes d'eau potable.

03

Les attaques á conséquences étatiques

Les cyberattaques étatiques sont de plus en plus utilisées en temps de paix par les États, pour mener des attaques similaires á des agressions contre d'autres États. Devant ce constat, il apparaît nécessaire de s'interroger sur l'extension de la notion d'agression afin d'y inclure les cyberattaques. En effet, les cyberattaques permettent aujourd'hui aux États d'atteindre les mêmes objectifs que des attaques conventionnelles, et leurs conséquences ainsi que leurs effets peuvent être aussi graves que des agressions par attaque classique.

Sources : dumas.ccsd.cnrs.fr

Conclusion

Après avoir étudié quelques conséquences des cyberattaques, nous pouvons voir qu'elles sont souvent graves voir dramatiques dans certaines situations et qu'elles peuvent aller jusqu'au crime !
Il est très important de se protéger de ces attaques, mais pour quel prix ?
Oh, une question á étudier pour un nouvel article peut-être.. :)