

Contre les attaques DDoS, un défi toujours plus grand

Internet

Posté par : JulieM

Publié le : 5/5/2021 13:00:00

L'année 2020 aura été particulièrement éprouvante pour l'économie mondiale et aura profondément impacté nombre d'entreprises – bien des regards.

Dans le contexte sanitaire et économique dramatique que nous traversons, nous aurions pu espérer que les hackers, au nom d'une certaine « éthique », observent une trêve pour ne pas asphyxier davantage des entreprises et organisations tentant de survivre ou d'offrir des services essentiels à la population (notamment dans le domaine de la santé et ou de l'éducation).

Mais cela n'a pas été le cas. Bien au contraire, les cyberattaques, notamment les attaques DDoS, ont continué à progresser. Dès le premier trimestre, elles ont bondi de 279 % par rapport à 2019. Cette accélération s'est poursuivie les trimestres suivants.

Le phénomène des attaques DDoS est bien connu par tous, à l'instar de celui des ransomware, est guidé par une logique de chantage consistant à prendre en otage les systèmes informatiques. Ce phénomène est d'autant plus d'actualité que la disponibilité des données est particulièrement cruciale actuellement, et demande une vigilance accrue de la part des DSI et RSSI.

L'année 2021 confirme d'ailleurs cette tendance d'augmentation de la menace, que ce soit à l'encontre des entreprises, des établissements de santé, des dispositifs « domicile », ou bien encore des sites gouvernementaux dédiés aux démarches en ligne.

La situation devrait encore empirer, le recours massif au numérique pour garantir une certaine continuité d'activité dans un contexte de télétravail représentant une aubaine que les cybercriminels ne vont pas manquer de saisir.

L'essor de l'usage du numérique

Déjà largement utilisé, le numérique se positionne aujourd'hui comme central dans le mode de travail des entreprises. En ce sens, la disponibilité des réseaux et des infrastructures est essentielle.

Très sollicités, ces derniers sont plus que jamais exposés et représentent un point de vulnérabilité crucial. Les hackers sont bien conscients de ce phénomène, et ils en tirent profit, dans de nombreux cas d'usage. Les cibles sont en effet multiples et ne concernent pas uniquement les activités stratégiques.

Citons par exemple : le commerce en ligne, l'enseignement, les tournois de jeux vidéo à distance, les attaques sur les objets connectés, etc. L'objectif des attaques est bien sûr de contraindre les entreprises à céder aux exigences financières des hackers qui paralysent leurs activités en s'attaquant massivement à leurs infrastructures.

Finalement, en cumulant la perte de revenu liée à l'indisponibilité des plateformes et les rançons qui peuvent être versées par les entreprises, le coût des attaques DDoS est plus que significatif.

Ceci est aggravé par les avantages présentés par ces attaques : peu coûteuses pour l'attaquant, plus difficile à neutraliser dans un contexte d'afflux de connexions légitimes, relativement insensibles aux dispositifs de protection habituels, et facilement reproductible à l'encontre de cibles visées pratiquement.

Si ce constat est certes alarmant, la bataille n'est pour autant pas perdue. Les entreprises doivent être sensibilisées à ce risque pour mieux s'en prémunir.

Au-delà de cette prise de conscience collective, les acteurs de la cybersécurité doivent aussi s'allier pour proposer des offres combinées qui permettront de lutter plus efficacement contre les attaques DDoS à long terme.

Fabrice Clerc C.E.O. 6cure