Information presse

Rubriques : Sécurité/Etudes

Priorité à la protection contre les DDoS pour 89% des prestataires !

C'est ce que révèle une étude menée à l'initiative de Corero par Megabuyte Research auprès des data centers, des hébergeurs et des fournisseurs de services aux réseaux

Megabuyte Research évalue l'impact, la sensibilisation et les attitudes adoptées envers la sécurité contre les DDoS dans les Data Centers

Paris, le 23 octobre 2014 - Corerro Network Security (LSE: CNS), leader mondial des solutions de sécurité contre les attaques par DDoS avec Première Ligne de Défense®, annonce les résultats de sa collaboration avec Megabuyte, l'une des principales firmes européennes d'intelligence économique dans le secteur de la technologie. Megabuyte publie son rapport 2014, "Security in the Data Center: DDoS Impact, Awareness & Attitudes." Le rapport s'appuie sur une enquête réalisée auprès de dirigeants d'entreprises de services basées au Royaume-Uni. Il analyse la capacité des fournisseurs de services à se défendre et à répondre aux attaques par DDoS.

Aujourd'hui, dans les entreprises axées sur Internet, toute dégradation du service ou toute panne causée par une attaque DDoS peut avoir un impact négatif sur la marque, la fidélisation de la clientèle et, finalement, l'entreprise toute entière. Pour comprendre comment les data centers, les hébergeurs, les fournisseurs de services réseau et de services Internet répondent aux menaces DDoS, Megabuyte a recueilli leur avis sur l'impact des attaques DDoS, les stratégies de mitigation disponibles et leur attitude envers celles-ci. Les principales conclusions, à l'issue des entretiens menés avec un grand nombre de cadres au sein de ces entreprises, sont édifiantes sur leur motivation face aux DDoS :

- 89% des prestataires participant à cette étude se sentent responsables de la mise en œuvre de la protection contre les DDoS, que ce soit la protection de leurs clients ou leur propre protection, en dépit du fait qu'ils croient que leurs clients sont plus touchés par les DDoS que leurs propres réseaux.
- Les outils de mitigation des DDoS aident à détecter les attaques par DDoS ; mais ce sont les plaintes des clients à propos des problèmes de service qui demeurent, pour les prestataires, l'un des principaux indicateurs d'une attaque en cours. Près de la moitié des participants, victimes d'une attaque l'année dernière les ont citées comme le principal moyen d'alerte.
- Plus de 80% des participants ont exprimé que leur défense anti-DDoS est plus importante ou d'égale importance par rapport aux autres types de défense en sécurité, que cela soit pour eux-mêmes ou pour leurs clients.

Philip Carse, associé et analyste principal pour Megabuyte, souligne *« La prise de conscience globale et de plus en plus fréquente que les attaques par DDOS sont en hausse et la majorité des entretiens que nous avons menés indiquent qu'ils doutent désormais, plus que jamais, de leurs initiatives actuelles de défense contre les DDoS et de leur stratégie de protection de leur propre entreprise et des entreprises de leurs clients. »*

La croissance visible du nombre et de la sophistication des attaques par DDoS s'explique en particulier par le potentiel de gains de la criminalité liée à cette méthode d'attaque. L'utilisation de DDoS comme écran de fumée permet aussi de lancer un plus grand exploit ou d'ouvrir une brèche dans l'entreprise-victime ciblée. Ceci signifie qu'un plus large spectre d'entreprises risque d'en souffrir à l'avenir car elles sont les victimes potentielles de cette tendance. A leur tour, les entreprises et les administrations demandent à leurs fournisseurs de services de les aider à lutter contre les attaques DDoS malveillantes.

« Bien que cette enquête ait porté sur des fournisseurs basés au Royaume-Uni, je suis vraiment persuadé que nous observerions des résultats similaires dans le monde entier - les attaques DDoS, par nature, ne connaissent pas les frontières géographiques », déclare **Ashley Stephenson**, CEO de Corero Network Security. *« Les conclusions de ce rapport soulignent avec force l'importance d'inclure une Première Ligne de Défense contre les attaques DDoS comme composante essentielle de l'architecture sécurité du réseau. La totale visibilité des événements de sécurité liés aux DDoS qui ont lieu sur le réseau et la capacité des fournisseurs à réagir en temps réel pour les bloquer, les rend proactifs, protégeant leurs clients d'une autre catégorie de cyber-menaces néfastes visant leur réseau et les services destinés à leurs clients. »*

Pour accéder au rapport "Security in the Data Center: DDoS Impact, Awareness & Attitudes " de Megabuyte : http://www.corero.com/megabuyte-security-in-the-data-centre

A propos de Megabuyte

Megabuyte est un fournisseur indépendant de recherche, suivant le monde des affaires institutionnelles et financières de quelques 1000 entreprises publiques et privées en Europe dans le secteur des services ICT et du logiciel. Le fondateur de Megabuyte, Ian Spence, est l'un des analystes financiers les plus établis et respectés du secteur de la technologie au Royaume-Uni. Il a été récemment reconnu par le Debrett's et Le Sunday Times comme l'une des 20 personnalités les plus influentes du secteur de la technologie au Royaume-Uni.

Pour plus d'informations : www.megabuyte.com

A propos de Corero Network Security

Corero Network Security, Première Ligne de Défense® des entreprises et des administrations contre les attaques DDoS et les cyber-menaces, est un pionnier de la sécurité globale du réseau. Les produits et services Corero offrent aux entreprises en ligne, aux fournisseurs de services, aux hébergeurs et aux fournisseurs de services managés de sécurité une couche supplémentaire de sécurité, capable d'inspecter le trafic Internet et de faire respecter l'accès en temps réel et le suivi des politiques visant à répondre aux besoins de l'entreprise protégée. La technologie Corero améliore l'ensemble de l'architecture de sécurité grâce à une défense en profondeur, évolutive, flexible et réactive contre les attaques par DDoS et les cyber-menaces avant qu'elles n'atteignent l'infrastructure informatique ciblée, permettant ainsi aux services en ligne d'opérer comme prévu.

Pour plus d'informations : www.corero.com

Contact Presse

Migé Gauchet - 06 84 77 31 74 - mige.gauchet@free.fr