CENTRE FOR
CYBER SECURITY
BELGIUM

Comment protéger votre organisation contre un attaque DDoS ?

Quelques conseils pour protéger les petites et moyennes organisations contre les attaques DDoS

Publication – 05/05/2021

Une attaque **Distributed Denial of Service** (DDoS) est une cyberattaque qui entrave le **trafic normal d'un service en particulier.** Dans les organisations et les entreprises, elle peut avoir un impact majeur sur le fonctionnement. Il est donc très important de vous protéger contre ce type d'attaques.

Ces recommandations émanent du **Centre pour la Cybersécurité Belgique (CCB)**.

Le Centre pour la Cybersécurité Belgique (CCB) est l'autorité nationale en charge de la cybersécurité en Belgique. Le CCB a été créé par l'arrêté royal du 10 octobre 2014 et est placé sous l'autorité du Premier ministre. De par sa mission légale, il cherche à informer et à conseiller les organisations sur la protection contre les attaques DDoS.

Une attaque Distributed Denial of Service (DDoS) est une cyberattaque qui entrave le trafic normal d'un service en particulier. Il est probable qu'il soit alors impossible d'en garantir la disponibilité. En d'autres termes, le service est indisponible pendant un certain temps sans qu'il s'agisse d'une effraction ou d'un vol de données. Le phénomène d'attaque *as-a-service*, par lequel des non-techniciens peuvent « commander » des cyberattaques sur le *darkweb*, gagne également en popularité avec le DDoS.

Ce document se veut un guide destiné aux responsables informatiques des petites et moyennes organisations afin de les informer et les conseiller sur les mesures de protection possibles contre une attaque DDoS. L'accent est ici placé sur les attaques DDoS contre le réseau des petites et moyennes organisations, et non contre une plateforme, un site web ou un autre service en ligne spécifique. Ce document n'a pas pour ambition de mettre fin aux attaques DDoS, mais tente de préparer une organisation et de la rendre plus résistante aux attaques DDoS. Ce guide présente des mesures que vous pouvez prendre en tant que responsable informatique d'une petite ou moyenne organisation. La fiche de synthèse propose un résumé efficace. Nous vous recommandons d'imprimer cet aperçu, de le compléter et de l'afficher dans un endroit stratégique afin de pouvoir l'utiliser activement lors d'une attaque DDoS.

CENTRE FOR
CYBER SECURITY BELGIUM
Under the authority of the Prime Minister
Rue de la Loi, 16 - Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CENTRE FOR CYBER SECURITY BELGIUM

Comment protéger mon organisation contre des attaques DDoS ?

Préparation

Maîtrisez votre réseau

Pour vous préparer à une cyberattaque, il importe de bien connaître son réseau. Quel est le mode de connexion à Internet ? S'agit-il d'une connexion directe à l'aide d'un fournisseur d'accès à Internet (FAI, comme Telenet ou Proximus) ou via d'autres organisations ? Quel est votre FAI et quel type de contrat avez-vous conclu ? Quels services sont liés à votre réseau ?

Nous vous conseillons de réaliser au plus vite l'inventaire notamment de vos typologies de réseau, de vos adresses IP internes et externes. Vous pouvez facilement demander vos adresses IP externes via https://whatismyipaddress.com/. Très souvent, cette documentation se révèle essentielle lors d'une attaque. Veillez donc à être en mesure de les obtenir en cas de cyberattaque.

Procédure de réponse aux incidents.

Une procédure de réponse aux incidents vous permet de savoir quoi faire en cas de cyberattaque. Il est essentiel, lors d'une attaque DDoS, de disposer d'un canal de communication hors bande. Il s'agit d'un moyen de communication qui ne nécessite pas le réseau. Quelques exemples : téléphone, WhatsApp, 4G, etc. Il est également important d'établir clairement à l'avance quel groupe communiquera via quel canal. Il est important de disposer d'une liste de contacts hors ligne (imprimée) des personnes qui peuvent vous aider ou que vous devez informer. Il peut s'agir de personnes en interne (direction, élèves, enseignants) ou en externe (FAI, expert en sécurité).

Convenez clairement avec votre FAI de ce qu'il peut faire en cas d'attaque DDoS. Cela pourrait inclure le géo-blocage, la modification d'adresses IP publiques, le *packet scrubbing*, etc. Veillez à examiner les contrats existants avec votre FAI, votre fournisseur d'accès au cloud et votre fournisseur d'hébergement en ce qui concerne la protection DDoS.

Checklist

La checklist est scindée en deux volets. Le premier compile les actions préparatoires de base recommandées pour toutes les organisations. Le second volet décline des mesures préparatoires plus avancées et de nature plus technique.

- ☐ Divisez le réseau en fonction des applications, activités ou fonctions (services administratifs, systèmes de production, site Internet public, utilisateurs externes, services externes, utilisateurs internes, données d'entreprise internes, etc.). Et ce tant pour le réseau d'entreprise que les services de cloud.
- ☐ Installez un pare-feu réseau et appliquez les règles nécessaires pour l'accès à l'internet (*network-based*).
- ☐ Assurez-vous que les systèmes internes, comme les serveurs et les postes de travail, sont équipés d'un pare-feu actif (*host-based*).
- ☐ Désactivez les services non utilisés ou filtrez-les hors du réseau.
- ☐ Activez les mises à jour automatiques des systèmes d'exploitation, des programmes et des routeurs.

CENTRE FOR
CYBER SECURITY BELGIUM
Under the authority of the Prime Minister
Rue de la Loi, 16 - Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

- ☐ Ne laissez pas le mot de passe défini par défaut sur le routeur Internet et d'autres systèmes.
- ☐ Utilisez si possible les services dans le cloud. Les sites Internet, les services de messagerie ou d'autres plateformes en ligne sont par exemple très vulnérables une fois hébergés localement sur un serveur. Les services dans le cloud sont mieux protégés grâce à leur large disponibilité.
- ☐ Activez l'authentification à deux facteurs (2FA) lorsque c'est possible. Veillez à l'activer pour les comptes admin. et pour les utilisateurs dotés de privilèges supplémentaires ou sensibles qui doivent exécuter des tâches spécifiques, différentes de celles des utilisateurs ordinaires. Pour plus d'informations, cf. : https://www.safeonweb.be/index.php/fr/utilisez-lauthentification-deux-facteurs.

Mesures avancées :

- ☐ Effectuez un scan régulier du réseau : qu'est-ce qui est accessible via Internet ?
- ☐ Activez la fonctionnalité de filtre sur le routeur Internet ou le pare-feu.
- ☐ Validez l'utilisation de plages IP privées : vérifiez si votre réseau scolaire utilise un adressage IP interne valide qui est déterminé globalement (exemple de plages conformes : 192.168.0.0/24 172.16.0.0/16 et 10.0.0.0/8).
- ☐ Empêchez l'usurpation d'adresse IP : l'Unicast Reverse Path Forwarding (uRPF) peut vous y aider. Pour plus d'informations : cf. : https://www.juniper.net/documentation/en_US/junos/topics/concept/unicast-rpf-understanding.html#:~:text=A%20unicast%20reverse%2Dpath%2Dforwarding,and%20checks%20the%20incoming%20interface.
- ☐ N'autorisez que le trafic connu et de bonne qualité : bloquer tout par défaut (*deny all* par défaut), utilisez les listes d'autorisation pour n'autoriser que ce trafic.
- ☐ Consolidez votre routeur autant que possible en désactivant les éléments suivants : adresse IP de diffusion dirigée (*IP directed broadcast*) - Configurations HTTP - Ping ICMP - Routage des sources IP (*IP source routing*).

Identification

Essayez de collecter un maximum d'informations concernant l'attaque. Afin de déterminer l'impact de l'attaque DDoS, il importe de dresser la liste des systèmes impactés. Cet exercice peut reposer sur les plaintes des utilisateurs. Veillez absolument à la **validation technique**. Quelle application, quel élément système ou réseau génèrent un important *workload* et consomme une vaste bande passante ?

Atténuation

Le FAI se révèle un partenaire très important dans l'atténuation des DDoS. Contactez donc le FAI dès que possible après vous être assuré qu'il s'agit bien d'une attaque DDoS. Si vous le souhaitez, vous pouvez également faire appel à un expert en cybersécurité. Le géoblocage au niveau du FAI ou dans des pare-feux plus avancés peut atténuer l'attaque DDoS. Il en va de même pour la modification des adresses IP publiques. Ces actions peuvent être entreprises par le FAI, mais dans le cas d'IP dynamiques, cela peut être fait en désactivant le routeur Internet pendant 15 à 30 minutes.
En cas de dommage, nous vous recommandons de déposer plainte auprès de votre bureau de police local.

CENTRE FOR
CYBER SECURITY BELGIUM
Under the authority of the Prime Minister
Rue de la Loi, 16 - Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

Restauration

Une fois l'attaque DDoS mise à l'arrêt, les services désactivés peuvent être relancés. C'est alors le moment de vérifier que tout est en ordre. Si c'est le cas, communiquez cette information aux utilisateurs.

Évaluation

Faites le point sur ce qui s'est bien passé et ce qui s'est moins bien passé. Tentez de traduire les points d'action en actions concrètes dans la phase préparatoire.

Les questions suivantes peuvent servir de fil rouge à cet égard :

- Quelles étapes préparatoires sont nécessaires pour réagir de manière plus rapide et plus efficace ?
- Les canaux de communication nécessaires (internes et externes) étaient-ils disponibles ?
- Les canaux de communication (internes et externes) étaient-ils connus et ont-ils été utilisés ?
- À quels mécanismes de défense vous attendez-vous pour empêcher une attaque DDoS ?
- Qu'est-ce qui a provoqué l'incident et étiez-vous en mesure de réagir plus rapidement ?
- Quelles étapes avez-vous entreprises pour contenir l'incident et en limiter l'impact au mieux ?
- Quelles étapes avez-vous entreprises pour éviter toute répétition ?
- Quels furent les principaux obstacles lors de l'incident ?
- Quelles relations externes et internes peuvent être utiles si d'autres incidents surviennent à l'avenir ?

CENTRE FOR
CYBER SECURITY BELGIUM
Under the authority of the Prime Minister
Rue de la Loi, 16 – Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

Pour plus d'informations

Centre pour la Cybersécurité Belgique :
https://ccb.belgium.be/fr

Cyberguide :
https://cyberguide.ccb.belgium.be/fr

Différents types d'attaques DDoS :
https://www.enisa.europa.eu/publications/info-notes/dns-ddos-attack-protections

Vidéo sur les DDoS :
https://www.youtube.com/watch?v=E6t_jrk3LUs

Disclaimer

Ce document a été rédigé par le Centre pour la Cybersécurité Belgique (CCB), une administration fédérale créée par l'arrêté royal du 10 octobre 2014 et placée sous l'autorité du Premier ministre.

La CCB décline toute responsabilité quant au contenu de ce document.

Les informations fournies :

- sont de nature purement générale et ne sont pas destinées à couvrir toutes les situations spécifiques;
- ne sont pas nécessairement complètes, exactes ou actualisées à tous égards.

Le CCB met tout en œuvre pour assurer au mieux l'actualisation, l'accessibilité, l'exactitude et l'exhaustivité du contenu et des mises à jour publiés sur ce site. En cas de modification, une nouvelle version sera publiée le cas échéant.

La présente note contient des liens vers des sites publiés par des tiers et qui ne relèvent pas de la gestion du CCB. Ces informations sont également susceptibles de changer à tout moment.

Le CCB ne peut être tenu responsable de tout dommage causé par l'utilisation de ces informations. En outre, aucun droit ne peut dériver des informations fournies par des tiers.

CENTRE FOR
CYBER SECURITY BELGIUM
Under the authority of the Prime Minister
Rue de la Loi, 16 - Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

Préparation

RÉSEAU

Accès à Internet :
directement/par d'autres, à savoir ……..

FAI : ……

Contrat : ……

Adresses IP: ……..

Services sur le réseau : ……

PROCÉDURE DE RÉPONSE À UN INCIDENT

Communication + coordonnées hors bande

Interne :

- Direction : ……
- Service IT : ……..
- Collaborateurs : ……

Externe :

- FAI : ……
- Expert en sécurité :……
- Clients :……..

Accords avec les FAI

- Géoblocage/switch IP publiques/packet scrubbing/autres
  ……

Identification

- Collecter les infos
- Déterminer l'impact de l'attaque
- Validation technique

Atténuation

- Impliquer le FAI
- Géoblocage
- IP switch
- Plainte à la police

Restauration

- Relancer les services
- Vérifier statut normal

Évaluation

- Tirer des leçons
- Appréhender les points d'action

Checklist préparation

- ☐ Réseau distinct
- ☐ Pare-feu réseau + host based
- ☐ Désactivation services inutilisés
- ☐ Mises à jour automatiques
- ☐ Pas de mot de passe par défaut
- ☐ Services dans le Cloud
- ☐ 2FA si possible

Mesures avancées :

- ☐ Scan régulier du réseau
- ☐ Fonctionnalité de filtre active sur le routeur
- ☐ Plages IP privées
- ☐ Empêcher l'usurpation IP
- ☐ N'autoriser que le trafic connu et de bonne qualité
- ☐ Désactiver : IP directed broadcast – configurations HTTP - ICMP ping - IP source routing