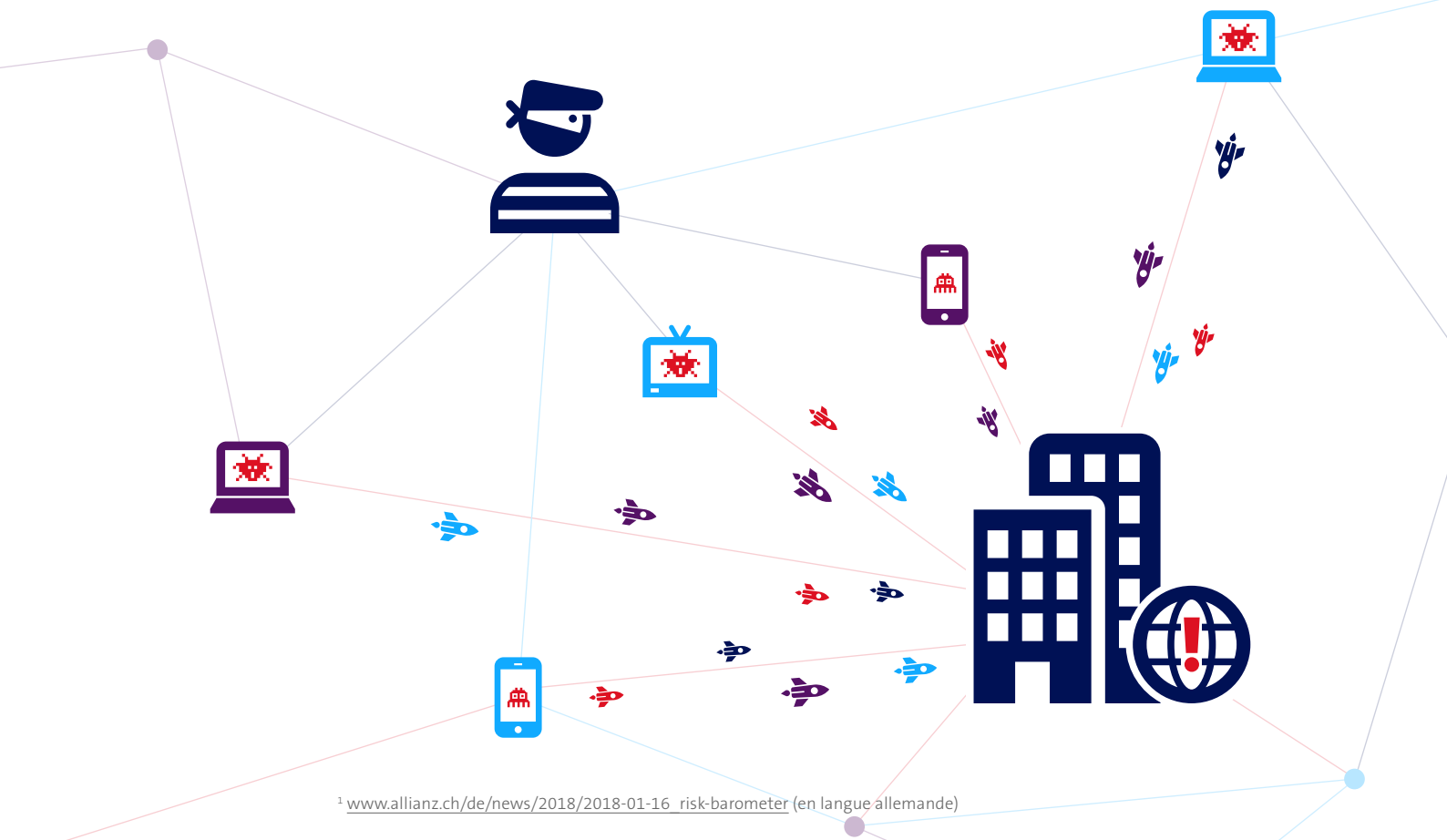
swisscom

SECURITY

Distributed Denial of Service

Les attaques DDoS un risque pour la sécurité IT

Selon le Baromètre des risques d'Allianz[1], les interruptions de l'exploitation constituent, et de loin, les principaux risques pour les entreprises en Suisse. Dans le Baromètre des risques d'Allianz 2018, les cyber-attaques se classent au troisième rang. Dans ce contexte, il ne faut pas oublier que cyber-attaque et interruption de l'exploitation peuvent être étroitement liées.



[1] www.allianz.ch/de/news/2018/2018-01-16_risk-barometer (en langue allemande)

Risque pour l'entreprise: sécurité IT défaillante

Les cyber-attaques et les dysfonctionnements IT peuvent générer des pertes financières massives sans que des installations ou des bâtiments soient endommagés ou détruits.

En conséquence, la protection des actifs immatériels telles que les données, les réseaux ou la propriété intellectuelle devient toujours plus prioritaire. Il faut considérer une sécurité IT défaillante comme un risque d'entreprise si des cyber-attaques paralysent l'exploitation. Dans ce contexte, les attaques Distributed-Denial-of-Service ou attaques DDoS avec lesquelles un système ou un service IT est attaqué simultanément par de nombreux autres systèmes IT, surchargé et poussé à la défaillance, jouent un rôle central.

Surcharge et chantage via Internet

Lorsqu'un site Web, un service en ligne ou un autre service Cloud n'est plus disponible ou joignable, cela peut provenir d'une attaque DDoS. Comme le révèle le dernier rapport semestriel de la centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI)[2], les attaques DDoS comptent parmi les risques Internet majeurs pour les entreprises suisses. MELANI qualifie les attaques DDoS d'outil de choix pour des attaquants aux motivations multiples.

L'ampleur des dommages générés par une attaque DDoS dépend de l'importance des services en ligne pour l'entreprise visée. La digitalisation touche toutes les branches d'activité, les services en ligne deviennent toujours plus importants et critiques, il faut donc considérer les attaques DDoS comme un risque important car elles peuvent causer d'importants dommages dans tous les secteurs.

Il peut y avoir dommage financier pour une entreprise avant même qu'une attaque DDoS ait lieu. MELANI évoque des tentatives de chantage sur Internet, par lesquelles une entreprise se voit menacée d'une attaque DDoS si elle ne paie pas la somme exigée. Les maîtres-chanteurs n'ont pas toujours la possibilité d'exécuter une attaque DDoS. Mais ils espèrent que la menace suffira à déclencher le paiement d'une rançon.

Il est toutefois de plus en plus facile d'exécuter réellement des attaques DDoS. Désormais, des places de marché criminelles proposent sur Internet, moyennant une faible rémunération, d'exécuter des attaques DDoS. Il peut s'agir de Cybercrime as a Service ou de Stress tests. Les attaques DDoS augmenteront encore nettement, car l'accès à ces méthodes est devenu facile et avantageux pour les criminels.

57%

des entreprises ont subi une surcharge de leur bande passante Internet due aux attaques DDoS.

[2] www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2-2017.html

L'Evolution des attaques DDoS et leurs risques

Des rapports comme le «NETSCOUT Arbor 13th annual Worldwide Infrastructure Security Report, 2017»[3] montrent la violence et les graves conséquences des attaques DDoS:

Paysage des menaces

- Le mauvais usage d'appareils IoT et le développement de nouveaux services d'attaques DDoS génèrent des attaques plus fréquentes et plus complexes.
- **Ampleur de la menace:** 57 pour cent des entreprises et 45 pour cent des exploitants de centres de calcul ont subi une surcharge de la bande passante Internet suite à des attaques DDoS.
- **Fréquence:** Selon des données de l'infrastructure NETSCOUT Arbors ATLAS (Active Threat Level Analysis System) qui couvrent environ un tiers du trafic Internet mondial, en 2017, on a observé 7,5 millions d'attaques DDoS.
- **Complexité:** 95 pour cent des fournisseurs de services et 48 pour cent des entreprises ont subi des attaques multi-vecteurs, ce qui correspond à une hausse de 20 pour cent par rapport à l'année précédente. Les attaques multi-vecteurs combinent des floods à grande échelle, des attaques de la couche applicative et des attaques visant l'état d'épuisement TCP en une seule offensive durable, ce qui accroît la difficulté pour mitiger l'attaque et les chances de succès de l'attaquant.

Conséquences

- Les attaques DDoS réussies ont d'importantes conséquences opérationnelles et financières.
- 57 pour cent des victimes ont cité, comme conséquence, des dommages à la réputation de la marque, suivis des coûts d'exploitation.
- 56 pour cent des victimes ont annoncé des conséquences financières se chiffrant entre 10 000 et 100 000 dollars, c'est-à-dire presque le double des chiffres de 2016.
- 48 pour cent des exploitants de centres de calcul ont indiqué que l'exode des clients était un problème central après une attaque réussie.

Défense

- Les équipes réseau et sécurité doivent répondre à un paysage de menaces dynamique et complexe ainsi qu'à des problèmes permanents de personnel.
- 88 pour cent des fournisseurs de services utilisent des solutions de mitigation DDoS, et 36 pour cent utilisent des technologies visant à automatiser la réduction des DDoS.
- La fréquence des attaques augmente aussi la demande de Managed Security Services. 38 pour cent des entreprises se sont appuyées sur des fournisseurs tiers et des services externalisés, ce qui correspond à un bond de 28 pour cent l'année précédente. Seuls 50 pour cent ont mené des exercices, et la part des personnes interrogées menant des exercices au moins une fois par trimestre a chuté de 20 pour cent.
- 45 pour cent des entreprises et 48 pour cent des fournisseurs de services ont des difficultés à embaucher et à garder du personnel qualifié en matière de sécurité.

Attaques DDoS actuelles

Pour visualiser l'ampleur actuelle des attaques DDoS, on peut consulter les cartes des attaques DDoS auprès de fournisseurs tels que NETSCOUT Arbor et Akamai:

Digital Attack Map (Top daily DDoS attacks worldwide) de NETSCOUT Arbor:
www.digitalattackmap.com

Moniteur en temps réel d'Akamai:
www.akamai.com/fr/fr/solutions/intelligent-platform/visualizing-akamai/real-time-web-monitor.jsp

[3] https://www.netscout.com/report (en langue anglaise)

Attaques DDoS en Suisse

Des attaques DDoS ont lieu chaque jour et à toute heure; elles concernent très concrètement des entreprises suisses et les médias s'en font régulièrement les échos. Le nombre d'attaques DDoS contre des entreprises suisses ne cesse de progresser.

Le NETSCOUT Arbor Active Threat Level Analysis System (ATLAS) mentionne par exemple pour mai 2018 qu'en moyenne 227 attaques DDoS par jour contre des entreprises en Suisse ont été constatées. La plus importante attaque en Suisse, en mai 2018, portait sur 10,7 Gbps. L'une des plus importantes attaques observées à ce jour en Suisse avait un volume de 55 Gbps contre une seule entreprise.

Les deux exemples ci-dessous communiqués par des **quotidiens suisses** démontrent les graves conséquences de telles attaques:

- Kriminelle erpressen Schweizer Online-Shops (des criminels font chanter les boutiques en ligne suisses) (NZZ am Sonntag, mars 2016)[4]
- «Grey Hats» greifen SBB-Website an und hacken SVP-Datenbank (Des hackers attaquent le site Web des CFF et piratent la banque de données de l'UDC (Tageswoche, mars 2016)[5]
- Neue Erpresserwelle: Schweizer Online-Shops droht ein Schwarzer Freitag (Une nouvelle vague de racket: menace de vendredi noir pour les boutiques en ligne suisses) (Badener Tagblatt, avril 2016)[6]
- Rechtsradikaler Hacker attackiert linke Websites (Un hacker de la droite radicale attaque des sites Web de gauche) (Aargauer Zeitung, février 2017)[7]

L'**Office fédéral de la police (Fedpol)** a signalé des tentatives d'extorsion au moyen de DDoS (Distributed Denial of Service). Derrière les attaques DDoS, on trouve par exemple un groupe nommé Lizard Squad:

- Ses victimes ont reçu un e-mail rédigé en anglais avec pour expéditeur lizardlands@lizardsquad.net. Dans l'e-mail, les victimes étaient sommées de payer 10 Bitcoins (environ CHF 6280) avant une certaine date. Les maîtres-chanteurs menaçaient, si l'on ne leur donnait pas satisfaction, d'exécuter une attaque DDoS contre le système informatique de la victime.

[4] https://www.nzz.ch/nzzas/nzz-am-sonntag/cyber-attacken-kriminelle-erpressen-schweizer-online-shops-ld.9083

[5] https://tageswoche.ch/allgemein/grey-hats-greifen-sbb-website-an-und-hacken-svp-datenbank

[6] https://www.badenertagblatt.ch/wirtschaft/neue-erpresserwelle-schweizer-online-shops-droht-ein-schwarzer-freitag-130227864

[7] https://www.aargauerzeitung.ch/schweiz/rechtsradikaler-hacker-attackiert-linke-websites-130956850

(toutes les sources en langue allemande)

La **Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI** a souvent rapporté de telles attaques, et les chantages correspondants des groupes Armada Collective et DD4BC qui ont attiré l'attention des médias en Suisse. MELANI déconseille fortement de répondre aux exigences de telles bandes d'escrocs:

- Sous la pression d'une menace d'impossibilité de connexion sur son propre site Web et dans l'espoir d'une solution «rapide», certaines entreprises envisagent de payer les maîtres-chanteurs. En payant, non seulement on offre aux malfaiteurs une victoire facile, mais on leur donne aussi les moyens financiers pour renforcer leur infrastructure d'attaque et intensifier leurs actions.
- Souvent, les attaquants utilisent des services Booter ou Stresser, explique MELANI. Il s'agit d'outils déclenchant des attaques DDoS contre paiement («DDoS as a Service»). Plus les attaquants ont d'argent, plus le volume d'attaques (en termes d'intensité et de durée) qu'ils peuvent acquérir auprès d'un fournisseur de services criminels est important. Si les rançons ne sont pas payées, le modèle commercial des délinquants échoue. C'est pourquoi MELANI déconseille le paiement.

Le **Service de renseignement de la Confédération (SRC)** évoque dans son dernier rapport de la situation 2018 (La sécurité en Suisse) des attaques DDoS en liaison avec l'Internet des objets (IoT)[8]:

- Les attaquants utilisent l'IoT en se servant d'appareils insuffisamment protégés, par exemple des webcams, des babyphones ou des systèmes Smart TV pour leurs attaques. Il faut mentionner dans ce contexte le botnet Mirai sur le prestataire de services Internet Dyn, connu depuis l'attaque, qui infecte des appareils de l'Internet des objets. Mirai est un logiciel malveillant contre le système d'exploitation Linux, utilisé surtout dans des appareils de l'Internet des objets.

A l'**Assemblée fédérale** également, des attaques DDoS ont déjà fait l'objet d'une question sur la manière dont la Confédération soutient les cantons dans les poursuites pénales après des attaques, en cas de manque de savoir-faire.[9]

227

attaques par jour ont été lancées en moyenne contre des entreprises en Suisse en mai 2018.

[8] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-70611.html

[9] https://www.parlament.ch/fr/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=38493

Attaques DDoS: plus simples mais plus complexes aussi

Suite à diverses évolutions dans le domaine du cyber-crime, des attaques DDoS font augmenter encore le risque déjà important.

- Il est relativement simple démarrer une attaque DDoS, on peut les commander sur des places de marché en ligne et les payer avec des données de cartes de crédit volées. Il n'est plus nécessaire d'être un expert IT pour les réaliser. N'importe quel criminel peut, moyennant une faible rémunération, commander les attaques souhaitées et les faire exécuter par des fournisseurs de service DDoS criminels.
- Les attaques DDoS sont ciblées. Elles ne sont pas lancées au hasard. Elles suivent un objectif précis, par exemple paralyser le site Web d'une entreprise. Le client peut par exemple être un concurrent de la victime.
- Si l'on s'aperçoit rapidement des effets d'une attaque DDoS, par exemple parce qu'il est impossible de consulter le site Web de l'entreprise concernée, il est difficile par contre d'identifier les sources et le donneur d'ordre de l'attaque, et donc de mettre un terme à leur activité.

En conséquence, si les attaques DDoS sont simples, la défense à mettre en place est complexe.

Pourquoi et comment des attaques DDoS sont exécutées

Comme l'explique MELANI, à l'origine des attaques DDoS il y a diverses motivations. Il peut s'agir souvent d'activisme politique, de chantage ou de la volonté de porter préjudice à un concurrent ou à sa réputation:

- S'il est impossible d'accéder à un site Web, le propriétaire peut subir une importante perte de bénéfices et de réputation, en particulier si le service attaqué est de nature commerciale.
- Souvent, une attaque DDoS est accompagnée d'une demande d'argent. Le maître-chanteur exige de l'argent pour mettre un terme à une attaque déjà lancée où renoncer à en lancer une. Les attaquants espèrent que la victime paiera pour ne pas subir les conséquences négatives d'une telle attaque.
- On peut aussi utiliser l'attaque DDoS pour détourner l'attention d'un vol de données se déroulant en parallèle ou d'un hacking du système.

L'éventail des motivations montre clairement que les attaques DDoS peuvent frapper n'importe quelle entreprise et n'importe quelle organisation.

Exemple d'Europol

Europol, l'agence européenne de police criminelle, qui coopère avec Fedpol a récemment fait état d'une place de marché DDoS. Le rapport d'Europol présente le mode de fonctionnement de ces places de marché, et illustre le risque important généré par l'accès simple et avantageux à des attaques DDoS pour des criminels, même s'ils n'ont aucune connaissance en IT:

- Les administrateurs de la place de marché DDoS webstresser.org ont été arrêtés le 24 avril 2018 suite à l'opération Power Off, une enquête complexe menée par la police néerlandaise et la National Crime Agency britannique, avec le soutien d'Europol et d'environ une douzaine d'organismes chargés de l'application de la loi. Le service illégal a été arrêté et son infrastructure saisie.
- Jusqu'en avril 2018, webstresser.org était considéré comme la plus importante place de marché du monde pour les services DDoS, avec plus de 136 000 utilisateurs enregistrés et quatre millions d'attaques. Les attaques orchestrées visaient des services en ligne critiques de banques, d'institutions gouvernementales et la police ainsi que l'industrie du jeu.
- Dans le temps, pour lancer une attaque DDoS, il fallait avoir d'assez bonnes connaissances de la technologie Internet, aujourd'hui ce n'est plus nécessaire. Chez webstresser.org, les coûts d'un mandat d'attaque DDoS étaient de seulement 15 euros par mois. Des personnes ayant des moyens financiers réduits et ne disposant d'aucune connaissance technique pouvaient ainsi lancer des attaques DDoS dangereuses.

Europol conclut[10]:
Les criminels utilisent des attaques DDoS comme moyen contre des entreprises privées et le secteur public. De telles attaques servent non seulement à obtenir des bénéfices financiers mais aussi à favoriser des buts idéologiques, politiques ou juste malveillants. Ce type d'attaque est non seulement l'un des plus fréquents, mais de plus, elles sont d'accès facile, avantageuses et sans trop de risques pour les attaquants et leurs clients.

15 euros
par mois étaient les tarifs sur webstresser.org pour commander des attaques DDoS.

[10] https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018 (en langue anglaise)

Conséquences d'attaques DDoS

Pour évaluer les risques et pouvoir prendre des mesures de protection appropriées à la menace, il est important de se donner une vue d'ensemble des conséquences possibles: les entreprises victimes d'une attaque DDoS réussie subissent des dommages multiples, tant sur les systèmes IT concernés que pour l'entreprise dans son ensemble.

Dommages sur les systèmes IT

Systèmes attaqués	Les serveurs, réseaux, systèmes d'exploitation et applications sont surchargés jusqu'à ce qu'une panne se produise.	La communication de données peut être arrêtée, les services en ligne et les systèmes internes sont inutilisables.
Systèmes utilisés de manière abusive pour l'attaque	Les serveurs, terminaux et appareils IoT sont infectés avec un logiciel malveillant (bot) et deviennent une partie du réseau bot (botnet). Outre les ordinateurs, des appareils connectés tels que les téléviseurs compatibles Internet, les caméras de surveillance, les routeurs ou les Set-Top box peuvent également être utilisés pour des réseaux bot ou des attaques DDoS. Les experts en sécurité soulignent que, selon le type de l'attaque et l'entreprise victime, quelques douzaines d'appareils (bots) suffiraient pour exécuter avec succès une attaque DDoS.	Les attaquants (bot-master) commandent les systèmes à distances. Souvent, les utilisateurs ne remarquent pas que leur système fait partie d'un botnet.

Des dommages pour l'ensemble de l'entreprise

Perte de chiffre d'affaires	Les sites Web et d'autres services en ligne ne sont plus disponibles pour les clients et les partenaires. Il n'est plus possible de passer des commandes ou d'effectuer des réservations ou d'autres transactions.
Atteinte à la réputation	Les clients et partenaires sont irrités et passent souvent à la concurrence.
Perte de données	Des données sont perdues, manipulées ou supprimées.
Hausse des coûts, baisse de la productivité	La charge augmente nettement pour le service informatique, le support, le service client et aussi le service juridique, à cause de clients et partenaires furieux, d'appels à l'hotline et de possibles plaintes pour non-exécution de contrats. Dans le même temps, la productivité diminue, car les collaborateurs n'arrivent plus à exécuter leurs activités en ligne.

La multiplicité des attaques DDoS

Afin de pouvoir mieux comprendre le risque et développer une stratégie de défense, il est important de comprendre les divers types d'attaques DDoS.

Les divers types d'attaques DDoS

DoS vs. DDoS vs. DRDoS Attacks

Les attaques «Denial-of-Service»-**(DoS)** génèrent une restriction massive de la disponibilité de systèmes et/ou de services en ligne déterminés, ou l'impossibilité totale d'accès à ceux-ci.

Avec les attaques «Distributed Denial-of-Service» **(DDoS)**, l'attaquant utilise la puissance de plusieurs systèmes de manière abusive (botnet). Dans ce contexte, le nombre de systèmes impliqués (PC, smartphones, appareils IoT) peut varier de quelques centaines à plus de 100 000 systèmes attaquants en même temps. En conséquence, il est possible de perturber avec succès même des systèmes en ligne très performants avec des lignes à très haut débit.

Avec une attaque «Distributed Reflected Denial of Service» **(DRDoS),** la procédure est indirecte. L'attaquant n'envoie pas ses paquets de données directement à la victime, mais à des services Internet. Toutefois, il indique l'adresse IP de la victime comme adresse d'expéditeur. Il devient alors pratiquement impossible de déterminer la source de l'attaque («IP-Spoofing»). La réponse aux paquets de données par le service Internet et la surcharge du système qui en résulte chez la victime représentent l'attaque DoS indirecte.

Volume Based Attacks

Avec les **Volume Based Attacks,** les attaquants inondent un site Web de trafic, afin que la largeur de bande disponible de celui-ci soit totalement utilisée. En conséquence, le trafic de données légitime ne peut plus passer et le site n'est plus disponible pour les utilisateurs légitimes.

Avec les attaques volumétriques, un botnet peut envoyer plusieurs Gbps en quelques secondes et surcharger la ligne ou le pare-feu.

Application Layer Attacks

Les **Application Layer Attacks** visent les failles de sécurité dans des applications comme Apache, Windows et OpenBSD. Les attaques Application-Layer mettent le serveur en panne en lançant un grand nombre de demandes à une application, qui semblent tout d'abord légitimes car elles imitent le comportement d'un utilisateur.

Protocol Attacks (comme SYN-Flooding, ICMP Flooding, HTTP Flooding)

Les **Protocol Attacks** visent à utiliser les ressources d'un serveur.

Avec le **SYN-Flooding,** l'attaquant envoie un paquet de données pour établir une connexion au système visé. Ce dernier réserve un port et renvoie un paquet de données. Toutefois, comme l'attaquant n'emploie pas sa propre adresse IP, l'expéditeur ne reçoit pas de confirmation. Le système victime répète son envoi et écarte définitivement la connexion réservée après une durée prédéfinie qui peut être de plusieurs minutes selon le système d'exploitation. Si cet établissement de la liaison est effectué non pas une fois, mais très souvent en parallèle, il en résulte que l'ordinateur est surchargé par la réponse aux demandes et s'en trouve pratiquement bloqué.

Avec l'**ICMP Flooding** ou le **Ping Flooding,** le système de la victime est inondé de paquets de demandes d'écho ICMP (Ping). Ce type d'attaque peut solliciter la bande passante entrante et sortante car les systèmes de la victime s'efforcent de répondre par des paquets ICMP Echo Reply ce qui génère un fort ralentissement de l'ensemble du système.

Avec les **HTTP-Floods,** l'attaquant utilise des commandes HTTP-GET ou POST apparemment légitimes pour surcharger un serveur Web ou une application.

DNS Attacks

Avec un **DNS-Flood,** l'attaquant vise un ou plusieurs serveurs DNS (Domain Name System) d'une zone déterminée. Il essaie de bloquer la résolution de ressources de cette zone et de ses sous-zones en surchargeant les serveurs DNS.

Avec la **DNS Amplification,** l'attaquant exploite les failles de sécurité de serveurs DNS pour transformer de petites demandes initiales en charges utiles bien plus importantes qui sont utilisées pour faire planter le serveur de la victime.

100 – 100 000

périphériques en exploitation (PC, smartphones, appareils IoT) peuvent être utilisés simultanément comme systèmes attaquants.

Défense contre les attaques DDoS et réduction de leurs effets

Pour se défendre et réduire les effets des attaques DDoS (mitigation), on utilise et propose diverses procédures. Il est clair dans ce contexte que la lutte la plus efficace contre des flux de données non souhaités devrait idéalement avoir lieu dans le Backbone d'un fournisseur d'accès à Internet (ISP) et non au point final susceptible d'être surchargé par l'attaque.

Procédures pour repousser ou réduire (mitigation) des attaques DDoS

Black-hole

Avec la méthode de Black-hole, les flux de données non souhaités sont déroutés en totalité (sur les ports du routeur des transitions du réseau central), et rendus inoffensifs.

Remarque: La technique Blackhole n'apporte qu'une protection limitée à l'infrastructure Web.

Tous les flux de données sont supprimés, avec pour conséquence que l'entreprise ne peut plus recevoir certains secteurs du réseau ou certaines régions, même si le trafic de données est légitime et voulu.

Active DDoS Filtering (détection d'anomalies)

Les flux de trafic sont surveillés en permanence (dans le Backbone). Si un écart survient par rapport à la Baseline (= évolution de largeur de bande enregistrée en permanence pendant 24 heures), une alarme est lancée en fonction de l'écart, de manière proactive, et/ou un filtrage automatique est lancé. Sur la base des informations de l'alerte, l'entreprise peut contrer ou faire contrer les attaques DDoS de manière ciblée.

Remarque: Des connaissances approfondies sont nécessaires pour évaluer les anomalies. Si celles-ci ne sont pas disponibles, il serait opportun d'évaluer le recours à un prestataire de services avec un Backbone performant, protégé contre les attaques DDoS.

Malicious Traffic Rerouting/ Legitimated Traffic forwarding

Une solution de Threat Intelligence/Security Intelligence analyse le trafic de données et peut distinguer et filtrer le trafic bénin du trafic malveillant. Le trafic filtré et donc autorisé sera ensuite transféré à sa destination d'origine alors que le trafic de données malveillant sera détourné et écarté.

Remarque: L'activation d'une telle fonction de filtre devrait être initialisée par l'entreprise même si elle n'a recours à aucun prestataire de services. Bien connaître l'exploitation de son réseau permet d'éviter les fausses alertes qui pourraient se déclencher par exemple en raison d'une mise à jour logicielle prévue.

Conclusion

Lors de l'évaluation des risques d'entreprise, les cyber-risques deviennent toujours plus importants en raison de la digitalisation des processus commerciaux. Les cyber-attaques telles que les attaques DDoS font partie dès à présent des causes les plus importantes et les plus dangereuses qui peuvent causer l'interruption de l'exploitation.

De nombreux incidents en Suisse montrent concrètement quels sont les risques d'attaques DDoS pour les entreprises suisses. Les autorités en charge de la sécurité en Suisse sont alertées et informent en détail sur les attaques DDoS et les mesures nécessaires pour s'en protéger. Les dommages possibles pour les entreprises suisses concernent la perte de données, la perte de chiffre d'affaires, l'atteinte à la réputation et la violation de contrat car des prestations garanties envers un client ne peuvent pas être fournies si les services en ligne nécessaires sont défaillants.

Les attaques DDoS peuvent désormais être effectuées très simplement. Les attaquants peuvent utiliser les services de criminels et n'ont plus besoin d'être eux-mêmes des pirates. Ils peuvent ainsi, à peu de frais, causer de graves dommages. Les motivations des assaillants sont complexes et les attaques sont très ciblées. Elles utilisent divers points faibles et goulots d'étranglement, dans la largeur de bande Internet, des applications et des protocoles de communication. La détection et la défense deviennent toujours plus complexes, le besoin d'agir pour la protection DDoS est fort.

La centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI souligne qu'une attaque DDoS peut frapper n'importe quelle organisation et que la victime subit alors des conséquences économiques lourdes. En conséquence, les entreprises doivent prendre des mesures pour se protéger contre de possible attaques DDoS.

Selon MELANI, en cas de menace (situation de chantage), il est recommandé de prendre des mesures techniques avec l'hébergeur/le fournisseur d'accès, afin de se préparer à une éventuelle attaque. Mais même si une entreprise n'est pas menacée pour l'instant, si les services en ligne sont essentiels pour son fonctionnement, des mesures de protection préventives sont de mise.

La progression de la digitalisation dans les entreprises suisses rend pertinente pour chacune cette recommandation de MELANI: les mesures de protection contre de possibles attaques DDoS ne doivent pas être prises uniquement lorsqu'elle se produit ou lorsqu'une menace proférée. Dans ce cas, comme dans tous les domaines, mieux vaut prévenir que guérir. La présence en ligne et l'utilisation d'Internet sans une protection proactive contre les attaques DDoS n'est plus possible pour une entreprise.

Agissez dès maintenant!

Protégez efficacement vos réseaux et votre infrastructure Internet contre les attaques DDoS. Nous sommes à votre entière disposition pour vous conseiller!

Des questions? Contactez
Duilio Hochstrasser et le Security Product Management Team
productmanagement.security@swisscom.com

Pour davantage d'informations sur le service DDoS, consultez www.swisscom.ch/ddos

Vous trouverez plus d'informations sur la cyber-sécurité sur www.swisscom.ch/security

Ce document et son contenu sont protégés par le droit d'auteur. Une utilisation qui déborde le cadre privé doit faire l'objet d'une autorisation écrite préalable de Swisscom.