|  |  |
| --- | --- |
| **Angriffsbeschreibung** | |
| **Name:** DOS Angriff | **Hauptverantwortliche**: Devin-A. Meier, Martin Ziel |
| **Ziel des Angriffs**: Lahmlegen einer Webseite, Server etc. | **Gefährdete Personengruppen**: Alle |
| **Beispiel eines Angriffsszenarios** | |
| Akteure : Firma Ebuy, Firma Bmazon, Herr Itsich **Fallbeschreibung**:  Die Firma Ebuy will aufgrund eines schlechten Weihnachtsgeschäftes im letzten Jahr dem Konkurenten Bmazon das Weihnachtsgeschäft diesen Jahres vermiesen. Also beauftragt der Vorstand der Firma Ebuy, Herrn Itsich, den IT Sicherheitsbeauftraten der Firma damit einen solchen Angriff im Geheimen zu planen. Herr Itsich überlegt welches der einfachste aber auch effektiveste Angriff ist und entscheidet sich für einen DOS-Angriff. Er überwacht den traffic der Firma Bmazon und entscheidet so, wann die meisten Leute auf der Seite einkaufen. Diesen Zeitpunkt möchtet er ausnutzen um dann mit einem DOS-Angriff die Seite von Bmazon lahmzulegen, damit deren Kunden dort nicht vernünftig einkaufen können und die Firma einen großen Verlust macht. Herr Itsich entscheidet sich für den Angriff das Programm LOIC zu benutzen. | |
| *1 . Herr Itsich stezt eine VirtualMachine mit KaliLinux auf und auf dieser LOIC:* | |

|  |
| --- |
| *2. Herr Itsich kümmert sich nun um die IP Adresse des Servers der Website* [*www.Bmazon.de*](http://www.Bmazon.de/) *und trägt diese in LOIC ein :* |

|  |
| --- |
| Nun kann Herr Itsich noch gewünschte Einstellungen vornehmen, wie zum Beispiel: Erhöhen der Threads, Schnelligkeit der Anfragen, eine Nachricht eintragen, die über TCP gesendet wird usw., um so einen stärkeren Angriff oder einen nicht so starken Angriff auszuführen. Nachdem alles eingestellt ist, startet er den Angriff zum geplanten Zeitpunkt. |
| *3. Angriff starten:* |

|  |
| --- |
| *4. Nun wird der Server von Bmazon mit Anfragen „überflutet“ und somit lädt die Webseite langsamer, dies führt dazu, das Kunden nur vereinzelt auf die Seite kommen und deshalb Bmazon großen Verlust macht:* |

|  |
| --- |
| **Fazit:** Einen DOS-Angiff auszuführen ist ziemlich einfach. Mit wenigen IT-Kenntnissen und den nötigen Informationen kann man jede IP Adresse angreifen. |

|  |
| --- |
| **Verteidigunsbeschreibung** |
| Selbstverständlich ist einem Unternehmen wie Bmazon diese Art eines Angriffs schon bekannt.Deshalb haben Sie schon im Vorraus einen Vertrag mit einem darauf spezialisierten IT-Unternehmen abgeschlossen, welche den Zugang zu der Webseite aufrecht erhalten sollen. |
| ***Prävention:*** |
| Das beauftragte IT-Unternehmen macht sich gedanken, wie im Falle eines DOS-Angriffs der Ausfall des Onlinedienstes möchglist verhindert oder verzögert werden kann. Sie entscheiden sich die Server auf mehrere Standorte aufzuteilen, so dass im Falle eines Angriffs auf eine Schwachstelle in einem der Standorte die anderen unbetroffen bleiben.Außerdem weisen Sie den Servern weit mehr als die typisch benötigten Resourcen zu, damit diese nicht schon zu Beginn in die Knie gehen. |
| ***Erkennung****:* |
| Im Falle eines DOS Angriffs gehen von einem Angreifer eine stark erhöhte Anzahl von Anfragen an den Server welches sich durch ein simples Analysetool, wie Snort + Sguil, feststellen lässt. Falls es sich jedoch um einen DDOS Angriff handelt, ist, ab einer gewissen Größe, der normale Nutzer kaum von einem einem Angreiffer zu unterscheiden. Hier werden dann komplexere Tools und Mechanismen angewendet, welche das gesamte Surfverhalten der Nutzer in Betracht ziehen, zum Beispiel werden Nutzer, die regelmäßig diesen Dienst beanspruchen eher nicht blockiert. Die genauen Regeln und Filter sind Firmengeheimnis des IT-Unternehmens. |
| ***Aktion****:* |
| Anfragen die als Angriff identifiziert werden, werden in einem möglichst frühen Stadium blockiert. So kann das IT-Unternehmen zum Beispiel mit dem Netzbetreiber zusammenarbeiten um die IPs im kompletten Netz des Betreibers für einen Zeitraum zu blockieren. Um einen einfachen Nutzer gegen einen DOS Angriff zu schützen ist es in der Regel ausreichend die IP-Adresse des Angreifers in der Firewall des Opfers zu sperren.Falls es nicht möglich sein sollte Angreifer von normalen Nutzern zu unterscheiden, bleibt nichts anderes übrig, als die Server für einen Zeitraum vom Netz zu nehmen, damit diese nicht beschädigt werden. |