Schön und richtig über den Überfluss an Cyberangriffen und Bedrohungen wird in [1] gesagt, wo eine Parallele zu den historischen Schlachten gezogen wird. Keine zwei sind gleich, was in der heutigen Realität wahr ist. Dies bedeutet, dass ähnliche Strategien und Taktiken verwendet werden, da die Personen / Hacker gesehen haben, dass sie effektiv und effizient sind und Zeit sparen. Niemand wird das Rad neu erfinden, es sei denn, dies ist absolut notwendig. Wie in [1] erwähnt, werden sie gängige Techniken verwenden, die mit einer hohen Erfolgsquote eingesetzt wurden, wie Malware, Phising und andere.

Eine weitere Quelle [2] erkennt an, dass hochentwickelte Kriminelle die menschlichen Fehler und die Verwundbarkeit von Computern leicht ausnutzen können. Bei diesen Angriffen können sich die Ergebnisse von Kriminellen unterscheiden, die auf Ihre persönlichen und finanziellen Informationen zugreifen, die Verwendung des Geräts verhindern und viele andere Möglichkeiten, die Sie nur anfällig machen für den Verlust Ihrer Identität. Es gibt bereits ein Strafgesetzbuch aus dem Jahr 1995, aber das Gesetz kann jetzt nur so viel tun, weil es schwierig ist, die verantwortlichen Personen zu finden, die hinter den ähnlichen Taktiken und Strategien stehen.

Angriffe können gestoppt und abgewendet werden, indem Sie einfach eine der zahlreichen Online-Sicherheitsmaßnahmen anwenden, von der Installation von Anti-Malware-Software bis hin zu komplexeren Lösungen.

In Bezug auf die Informationen, die wir gerade aus verschiedenen Quellen gesammelt haben, sind die Angriffe in mindestens zwei Kategorien unterteilt: aktiv und passiv. Wie aus [3] ersichtlich, besteht der Hauptunterschied zwischen diesen beiden Typen darin, dass bei den aktiven Angriffen die Verbindung unterbrochen und die Informationen geändert werden, da bei den passiven Angriffen die Informationen gelesen und analysiert, jedoch nicht modifiziert werden.

**Definition aktiver Angriffe** - sind die Angriffe, bei denen der Angreifer versucht, die Informationen zu ändern oder eine falsche Nachricht zu erstellen, die der Benutzer als echt identifiziert. Um diese Angriffe zu verhindern, hat der Benutzer eine Menge zu tun. Dies ist aufgrund einer Vielzahl möglicher Netzwerk- und Softwareschwachstellen schwierig. Anstelle einer Vorbeugung ist die Erkennung des Angriffs und die Wiederherstellung der Daten von Störungen oder Verzögerungen erwünscht. Diese Angriffe sind meistens in Form von Unterbrechungen, Modifikationen und Fabrikationen.

**Definition passiver Angriffe** – sind die Angriffe, bei denen unbefugtes Abhören, Überwachen der Übertragung oder Sammeln von Informationen auftritt. Beim Lesen der Informationen und Daten findet keine Allteration statt. Daher ist es im Gegensatz zum aktiven Angriff schwieriger zu erkennen. Dies bedeutet, dass der Benutzer den Angriff in seinem System nicht bemerkt. Dies kann verhindert werden, indem die Dateien mit einem komplexen Schlüsselsystem oder mit Zertifikaten verschlüsselt werden, die es anderen Parteien nicht ermöglichen, den Inhalt der Dateien / Daten abzurufen. Bei diesem Typ wird die Prävention eher betont als die Erkennung.

Ein passiver Attck kann in zwei Arten unterteilt werden: die Freigabe des Nachrichteninhalts und die Verkehrsanalyse.

**Die wichtigsten Unterschiede,** die in [3] erwähnt werden, sind wie folgt:

1. Der aktive Angriff bedeutet, dass Nachrichten geändert werden. Andererseits nimmt der Angreifer bei passiven Angriffen keine Änderungen vor.
2. Der aktive Angriff schädigt das System, während der passive Angriff keinen Schaden anrichtet.
3. Ein passiver Angriff gefährdet die Vertraulichkeit von Daten. Wo ein aktiver Angriff die Integrität der Daten gefährdet.
4. Bei aktiven Angriffen ist sich das Opfer des Angriffs bewusst und bei passiven Angriffen ist das Opfer nicht informiert.

Als weitere Quelle [4] heißt es, die Bedrohungen lassen sich in vier Kategorien einteilen: direkt, indirekt, verschleiert und bedingt.

**Direkte Bedrohung** - bezeichnet ein ausgewähltes Ziel, das mit einer bestimmten Handlung angegriffen wird. Der Angriff ist für das Opfer klar und unkompliziert. Diese Kategorie wird nicht nur online verwendet, sondern kann direkt an das Opfer gerichtet werden.

**Indirekte Bedrohung** - bezeichnet eine vage, unklare und mehrdeutige Bedrohung. Jedes Detail aus dem Plan, das Motivationsopfer und mehr werden maskiert und nicht preisgegeben. Es ist möglich aufzutreten, aber nicht garantiert.

**Verschleierte Bedrohung** - wird impliziert, droht jedoch nicht explizit Gewalt. Es ist dem Opfer überlassen, die Bedrohung zu interpretieren und einen Sinn zu geben.

**Bedingte Bedrohung** - Dies ist bei Extrusionsfällen üblich. Eine gewalttätige Handlung findet statt, wenn bestimmte Forderungen oder Bedingungen nicht erfüllt werden.

Alle Angriffe und Bedrohungen können in verschiedene Kategorien eingeteilt werden. Es ist wichtig zu wissen, dass die Trennung auf den Akteuren basiert, entweder dem Opfer oder dem Angreifer. Wenn Sie über diese Angriffe sprechen, denken Sie daran, dass Sie nie genug geschützt sind. Sie finden selbst die kleinste Sicherheitslücke und nutzen sie für ihre Vorteile.