**Definition IDS**

Ein Intrusion Detection System (IDS) ist ein Gerät oder eine Softwareanwendung, das bzw. die ein Netzwerk auf böswillige Aktivitäten oder Richtlinienverstöße hin überwacht. Jede böswillige Aktivität oder Sicherheitsverletzung wird normalerweise zentral mithilfe eines Sicherheitsinformations- und Ereignisverwaltungssystems gemeldet oder erfasst.

Es gibt viele verschiedene Arten, von Antivirensoftware bis hin zu mehrstufigen Überwachungssystemen, die den Datenverkehr im gesamten Netzwerk überwachen. Die häufigsten **Arten** sind:

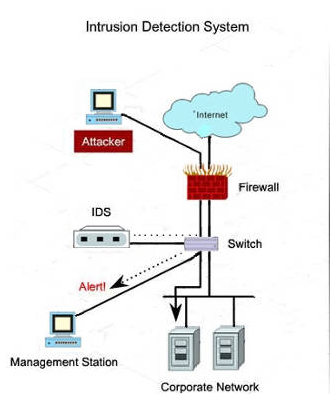
* Network Intrusion Detection System (NIDS): Ein System, das eingehenden Netzwerk-Datenverkehr untersucht.
* Host-basierte Intrusion Detection System (HIDS): Ein System, das wichtige Betriebssystemdateien überwacht.

Es gibt auch eine **Untergruppe von IDS-Arten**. Die gängigsten Varianten basieren auf Signatur- bzw. Anomalie Erkennung.

* Signaturbasiert:
  + erkennt mögliche Bedrohungen, indem es nach bestimmten Mustern sucht, z. B. nach Byte-Sequenzen im Netzwerkverkehr oder nach bekannten böswilligen Anweisungssequenzen, die von Malware verwendet werden
  + diese Terminologie stammt von der Antivirensoftware, bei der diese erkannten Muster als Signaturen bezeichnet werden
  + Obwohl bekannte Angriffe leicht erkennbar, ist es unmöglich, neue Angriffe zu erkennen, für die noch kein Muster vorliegt
* Auf Anomalien basierend
  + neuere Technologie zur Erkennung und Anpassung an unbekannte Angriffe, hauptsächlich aufgrund der explosiven Zunahme von Malware
  + diese Erkennungsmethode verwendet maschinelles Lernen, um ein definiertes Modell vertrauenswürdiger Aktivitäten zu erstellen und dann neues Verhalten mit diesem Vertrauensmodell zu vergleichen
  + Auch wenn Erkennung bisher unbekannter Angriffe möglich, besteht die Gefahr, dass bisher legitime Aktivitäten irrtümlicherweise als bösartig eingestuft werden (sogenannte „False Positives“)

**Umgehungsmethoden**

* **Fragmentierung:** Beim Senden fragmentierter Pakete kann der Angreifer unentdeckt bleiben, indem er die Systeme zur Erkennung von Angriffssignaturen umgeht.
* Vermeidung von Standardeinstellungen: Ein von einem Protokoll verwendeter Port liefert nicht immer einen Hinweis auf das zu transportierende Protokoll. Wenn ein Angreifer es für die Verwendung eines anderen Ports neu konfiguriert hat, kann es passieren, dass ein IDS einen möglicherweise vorhandenen Trojaner nicht erkennt.
* **Koordinierte Angriffe mit geringer Bandbreite:** Hierbei handelt es sich um einen koordinierten Scan, der sich auf unzählige Angreifer aufteilt. Dies kann sogar das Zuweisen unterschiedlicher Ports oder Hosts auf verschiedene Angreifer umfassen. So wird es für das IDS schwierig, die erfassten Pakete zuzuordnen und daraus zu schließen, dass gerade ein Netzwerkscan durchgeführt wird.
* **Adress-Spoofing/Proxying:** Angreifer können die Quelle des Angriffs verschleiern, indem sie schlecht gesicherte oder falsch konfigurierte Proxyserver verwenden, um einen Angriff zu starten. Wenn die Quelle gefälscht und von einem Server als Bounce-Nachricht zurückgegeben wird, ist eine Erkennung sehr schwierig.
* **Umgehung durch Musteränderungen:** IDS verlassen sich auf den Abgleich von Mustern, um Angriffe zu erkennen. Durch geringfügige Anpassungen an die Angriffsarchitektur kann die Erkennung vermieden werden.



**IDS-Nutzung in Netzwerken**

Wenn ein IDS an einem strategischen Punkt oder mehreren Punkten innerhalb eines Netzwerks eingesetzt wird, um den Datenverkehr zu und von allen Geräten im Netzwerk zu überwachen, führt es eine Analyse des weitergeleiteten Traffics durch und gleicht den Traffic, der an die Subnetze weitergeleitet wird, mit der Bibliothek bekannter Angriffe ab. Sobald ein Angriff erkannt oder ein unnormales Verhalten festgestellt wurde, kann die Warnung an den Administrator (Management Station) gesendet werden.

http://www.was-ist-malware.de/it-sicherheit/intrusion-prevention-system/

https://de.barracuda.com/glossary/intrusion-detection-system