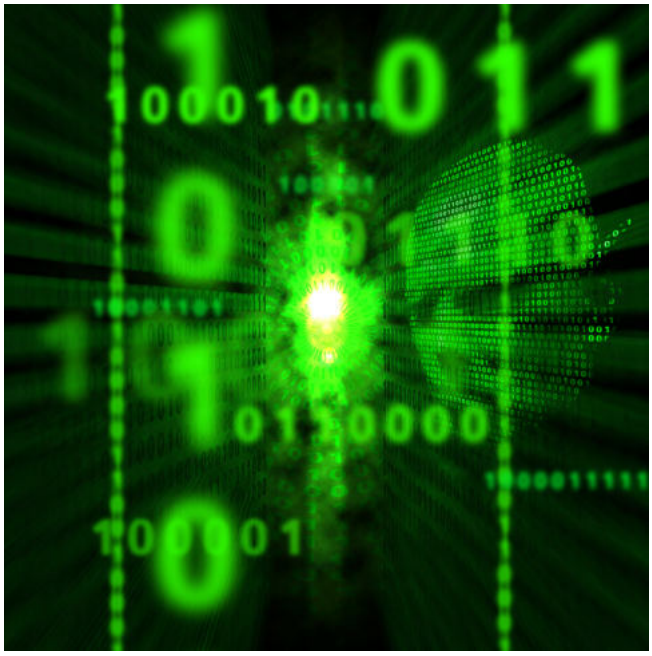
VIRTUELLE KÄMPFE

1. Einführung



Personen, die in Computersysteme eindringen, werden Hacker oder Cracker genannt. Das illegale Eindringen wird als Cracken bezeichnet, umgangssprachlich aber häufig mit hacken wiedergegeben. Virtuelle Angriffe können mit Hilfe von Computern, wie Pulsatoren durchgeführt werden und gelangen über Kom-Wellen über das Hyper-Net oder auf gewisse Distanzen direkt in alle möglichen technischen Instrumente, ob das nun ein gegnerischer Pulsator ist, ein Firmencomputer, die Brücke eines Raumschiffs, ein Terminal, ein Phaser usw. Systeme werden dadurch ausspioniert, durch Viren unterwandert, lahmgelegt oder der Angreifer verwendet das System auf seine Weise. Virtuelle Angriffe sind strafbar und Netzwächter und Firewalls sollen virtuelle Angriffe verhindern und die Hacker ausfindig machen.

- Um einen virtuellen Angriff durchzuführen, benötigt der Charakter in INF mind. den Wert 9.
- Zum Hacken ist ein Hacker-Modul (bzw. eine Hacker-Software) erforderlich.
- Humanoiden, die gedanklich in ein System eindringen können, z. B. Personen mit der Psinetik Neuralinkinese oder der Scitech-Fähigkeit Neuronalik, verwenden ihre WS.
- Ein Hacker benötigt mit einem Computer dafür eine Handlung.
- Ein Hacker, der gedanklich hacken kann, benötigt dafür eine Kognition.
- Das System verteidigt sich mit einer Firewall, wofür das Talent WS genutzt wird.
- Die Reichweite eines Hacker-Moduls beträgt bei Direktübertragung bis zu 100 m.
- Die Reichweite durch die Scitech-Fähigkeit Neuronalik beträgt bei Direktübertragung 100 m.
- Die Reichweite durch die Psinetik Neuralinkinese beträgt 10 m Sichtweite.
    - Wird das Ziel von Wänden abgeschirmt, beträgt die Reichweite 10 m.
    - Wird das Ziel von massivem Mauerwerk oder Metallwänden abgeschirmt, ist ein durchdringen unmöglich.
    - Wird der Computer durch einen Störsender aktiv geschützt, kann man sich nicht ohne Kabelverbindung in das Netzwerk hineinbegeben, weil der Störsender fremde Kom-Wellen abschirmt.
    - Die Systeme können auch direkt per Drahtverbindung angeschlossen werden.
    - Der Systemzugriff kann auch über das Hypernet erfolgen, wenn die Systeme dort vernetzt sind. Dafür ist ein funktionierendes orbitales Hypernet-Satelliten-Netzwerk nötig.
- Die Hacker-Module eines Raumschiffs können bis zu 10 Felder weit im Weltall virtuell angreifen (= 10 Km). Solche Hacker-Module befinden sich auch in einigen Firmen- und Staatscomputern.

2. Der Virtuelle Kampf

Der Virtuelle Kampf orientiert sich am Personenkampf.

1) Der Hacker scannt die Geräte in der Umgebung oder erfasst direkt das entsprechende Gerät.
   - Störsender verhindern ein Scannen und somit auch ein freies Hacken.

2) Der Hacker greift an
   - Für einen erfolgreichen Angriff muss der TW auf INF (oder WS) gelingen, sonst ist der Angriff misslungen. Ein neuer Versuch wäre in der nächsten Aktion möglich, jedoch dann – 2 WM. Bei einem Patzer kann dieses System von der Person in der nächsten ¼ Std. nicht mehr angegriffen werden.

3) Das System verteidigt sich automatisch
   - Die Firewall wird aktiv und macht einen einfachen TW auf WS.
   - Sollte ein Androide angegriffen werden, handelt es sich auch um eine automatische Parade, mit einem TW auf WS.
   - Misslingt die Parade, hat der Hacker in seiner nächsten Aktion den freien Zugang zum System.
   - Gelingt die Parade, wurde der Angriff bemerkt. Das System kann daraufhin eine Warnung ertönen lassen, evtl. auch den Angreifer lokalisieren und evtl. sogar automatisch einen Gegenangriff durchführen.

4) Das System unternimmt einen Gegenangriff
   - Einige Systeme mit einem WS-Wert von mind. 17 unternehmen automatisch einen Gegenangriff. Das System wird dann ans Ende der Kampfliste gesetzt und wenn es an der Reihe ist startet es seinen Angriff auf den bereits lokalisierten Angreifer. Wenn der Angriff erfolgreich war und die Parade misslungen ist, hat das System gewonnen und zerstört das feindliche Hacker-System.
   - War der Hacker ein Androide und wurde durch das betroffene System durch einen Gegenangriff erfolgreich bekämpft, ist das Hacker-Modul des Androiden zerstört, jedoch nicht der Androide selbst.

5) Das System wurde erfolgreich gehackt
   - Der Hacker kann nun Daten abrufen, lesen, übertragen, ändern, er kann das System zwingen, seine Befehle auszuführen und er kann in das System ein Virus einspeisen, um dem System langfristig zu schaden. Wer einmal erfolgreich in das System eindringen konnte, kann auch Zugriffscodes lesen, um immer wieder kampflos in das System einzudringen. Das geht so lange, bis der Zugriffscode geändert wird.
   - Jede Ausführung, die der Hacker im System vornimmt, benötigt eine Aktion.
   - Nach einer ¼ Std. greift das besetzte System erneut an, sofern die Firewall nicht deaktiviert wurde.
   - Wurde ein Androide erfolgreich gehackt, hat der Hacker die Kontrolle über den Androiden.

- Wenn ein Androide einen Hacker-Angriff durchführt, kostet es ihm gelungen oder misslungen – 1 WS.

<u>Beispiele eines erfolgreichen Hackerangriffs</u>:

- *Eine elektronische Granate wird zur Explosion gebracht.*
- *Die Übersetzungen eines Kom-Links werden manipuliert.*
- *Der Kom-Link gibt einen Hochfrequenzton frei, wodurch der Hörer – 1 LE und einen Schock erleidet.*
- *Eine elektronische Waffe wird funktionsunfähig gemacht oder löst absichtlich einen Schuss aus.*
- *Informationen werden aus einem Pulsator heraus gelesen.*
- *Die Daten eines implantierten Registrierchips werden gelesen.*
- *Das Interkom einer Tür öffnet oder verschließt diese.*
- *Die Stromzufuhr eines Hauses wird unterbrochen.*
- *Ein kybernetisches Bein wird funktionsunfähig.*
- *Die Steuerung eines Sphärikers wird übernommen.*
- *Ein Androide wird eine ¼ Std. lang unter Kontrolle genommen.*
- *Ein Toaster wird aktiviert*
- *Von diesem System aus hackt man sich in das nächste System.*
- *...*

3. Grenzen

- **Virtuelle Spuren**: Informatiker mit einem Wert von mind. 17 können bei einem späteren Datenabgleich erkennen, wenn in ein System ein Angriff vorgenommen wurde und woher er ungefähr kam.

- **Militärabwehr**: Staatliche Militärabwehrsysteme besitzen mehrere Computersysteme, mit denen sie ihre Verteidigung steuern, um bei einem Hackerangriff noch weitere Systeme nutzen zu können. Man kann sich also nicht in die Militärabwehr gesamt einhacken. Solche Computer besitzen meistens auch eine Firewall mit dem Wert 20. Auch Banken nutzen solche Systeme.

4. Die Firewall-Systeme

- **WS-Wert 9**
    - Die Firewall wehrt den Angreifer ab und löst einen Alarm aus.
    - Beispiele: Haushaltsgeräte, Kom-Links, elektronische Waffen, Visualik, Kybernetiken, Kraftfelder, Interkom-Geräte, Registrierchips, einfache Computer, einfache Pulsatoren
- **WS-Wert 13**
    - Die Firewall wehrt den Angreifer ab, löst einen Alarm aus und lokalisiert den Angreifer.
    - Beispiele: gute Pulsatoren, Fahrzeuge, Flugzeuge, Sphäriker, Robale, Roboter, Firmencomputer
- **WS-Wert 17**
    - Die Firewall wehrt den Angreifer ab, löst einen Alarm aus, lokalisiert den Angreifer und startet danach einen Gegenangriff.
    - Beispiele: Staatliche oder wirtschaftliche High-Tech-Computer, das Cockpit eines Raumschiffs
- **WS-Wert 20**
    - Die Firewall wehrt den Angreifer ab, löst einen Alarm aus, lokalisiert den Angreifer und startet danach einen Gegenangriff und kann das System mit einem Virus infiltrieren. Das Virus muss vorher jedoch hergestellt und auf die entsprechenden Bedürfnisse entworfen worden sein.
    - Beispiele: Militärische High-Tech-Computer, die Brücke eines Raumschiffs

5. Das Computervirus

Ein Computervirus ist ein selbst verbreitendes Programm, das in Systeme eingeschleust werden kann, um dort eine bestimmte Funktion auszuüben, von dem das betroffene System nichts bemerkt. Informatiker können Computerviren herstellen, aufspüren und eliminieren.

- Das Computervirus erhält den Wert, den auch der Informatiker besitzt, der es hergestellt hat.
- Der Informatiker kann dem Computervirus eine Aufgabe geben, die es dann in dem System erfüllt.

  Beispiel: Durch einen bestimmten Auslöser, z. B. ein gesprochenes Wort oder eine besondere Uhrzeit, soll das Virus aktiv werden. Es könnte ab dem Zeitpunkt eine dauerhafte falsche Information übermitteln, Scann-Vorgänge anders darstellen, die Firewall deaktivieren, das System herunterfahren, von diesem System aus ein anderes System angreifen, eine Waffe deaktivieren. Was das Virus alles kann, ist der Erfindungsgabe des Spielers überlassen.

- Nach dem erfolgreichen Angriff auf ein System, kann das Virus dort platziert werden.
- Um ein Virus zu finden, muss man sich bewusst auf die Suche nach einem Virus machen. Dies kann auch das System selbst übernehmen, wenn es dazu beauftragt wurde.
- Um ein Virus zu finden, benötigt man unterschiedlich lange Zeit, je nach Wert des Virus.
- Wurde das Virus gefunden, muss man es nach den üblichen Regeln angreifen und dadurch zerstören.

Die Zeit, um ein Virus aufzuspüren:

- Virus-Wert 9: W6 Min.
- Virus-Wert 13: W20 Min.
- Virus-Wert 17: W20 x eine ¼ Std.
- Virus-Wert 20: W20 Std.

Der Wurf wird vom SM geheim getätigt.

Die Zeit, um ein Virus herzustellen:

- Virus-Wert 9: W20 Min.
- Virus-Wert 13: W20 x eine ¼ Std.
- Virus-Wert 17: W20 Std.
- Virus-Wert 20: W100 Std.

Das Virus kann max. den Wert haben,
den auch der Informatiker besitzt.
Ein Spieler muss das während eines Abenteuers machen.
Er kann seine Tätigkeit auch unterbrechen.

6. Künstliche Intelligenz

Computersysteme mit einem Wert von mind. 17, sind eigenständig denkende KI-Systeme. Sie handeln nach den Vorgaben ihrer Entwickler. Sie sind allerdings auch in der Lage, eigenständig Angriffe oder Verteidigungen vorzunehmen, wenn es ihren Vorgaben entspricht. Sie können sich auch in verschiedene Computersysteme und Hyper-Net-Verbindungen vernetzen. Irgendwo hat die KI allerdings ihren Hauptsitz. Der lebensfeindliche Cluster ist beispielsweise eine weitreichend vernetzte KI, die mit ihren Androiden und Geräten, auch mit Raumschiffen und Waffensystemen vernetzt ist.