

Lagebericht Ausspähen

Ausspähen heisst, Daten mithilfe oder über IT zu erlangen, ohne dass das Ziel etwas davon erfährt. Ausspähen ist ein aktuelles Thema und wird im grossen Umfang durchgeführt. Durch die Möglichkeiten, grosse Datenmengen zu analysieren (Stichwort BigData), ist es umso wertvoller, möglichst viel Daten zu erlangen. Der Lagebericht ausspähen befasst sich mit der Definition von Ausspähen und stellt eine Übersicht über die aktuellen Arten der Spionage Bereit, welche in der Grafik am ende dieses Handouts ersichtlich sind. Folgendermassen werden in dem Lagebericht die Arten von Ausspähen kategorisiert:

Aggressivität: Man unterscheidet zwischen Footprinting, Vulnerability Scanning und Penetration Testing. Während Footprinting generelle Daten eines Ziels sammelt, und diese korreliert, sucht der Vulnerability Scan spezifisch nach Schwachstellen bei dem Ziel. Der Penetration Test versucht, diese Schwachstellen zu missbrauchen, Zugang auf das System zu erlangen und möglichst viel "Schaden" anzurichten.

Ziel: Ziele von Ausspähen können natürliche Personen sein, oder die IT Infrastruktur selber. Letztere ist wichtig, für zusätzliche Angriffe auf eine natürliche Person.

Aktiv/Passiv: Eine wichtige Unterscheidung bei Ausspähen, ist der Kontakt mit dem Ziel. Bei aktivem Ausspähen wird auf irgendeinem Weg mit dem Ziel interagiert, während bei passivem Ausspähen kein Kontakt mit dem Ziel herrscht, sondern nur Informationen auf "neutralen" Plattformen gesammelt werden.

Bei anschliessender Grafik sieht man eine Übersicht verschiedener Arten von Ausspähen, kategorisiert in obenstehende Definitionen:

