Wie funktioniert IT-Sicherheit / Hacking?

Sicherheitslücke

- Schwachstelle in Soft- oder Hardware
- Kann durch Fehler im Code oder fehlerhafte Konfiguration entstehen

Exploit

- Ausnutzen einer Sicherheitslücke
- Kann Zugriff oder Manipulation von Daten erlauben

Responsible Disclosure

- Verantwortungsbewusste Offenlegung von Sicherheitslücken
- Hacker informiert den betroffenen Anbieter zuerst
- Gibt dem Anbieter Zeit zur Behebung der Lücke
- Veröffentlichung der Lücke erst nach einer festgelegten Frist oder nach Behebung

Zero-Day vulnerability

- Sicherheitslücke, die dem Entwickler meist nicht bekannt ist und für die kein Fix verfügbar ist
- Kann von Konzernen, Strafverfolgungsbehörden und Geheimdiensten auf dem Schwarzmarkt eingekauft werden.

Cellebrite

- Firma für digitale Forensik
- Kauft Zero-Day Vulnerabilities
- Bietet Tools zur Datenextraktion von Mobilgeräten
- Wird von einigen Strafvervolgungsbehörden eingekauft