Ökonomie des Angriffs

Kosten

- Zeit
- Internetanbindung
- Nur ein Minimum an Soft- und Hardware nötig
- Kein bis wenig Fachwissen

Nutzen

- Einnahmen auf Basis von Erpressung, Verkauf von gestohlenen Informationen und geistigem Eigentum sowie illegale Nutzung von Gütern & Ressourcen

Angriff Ohne Konsequenz Für den Angreifer! ~~Risiko?~~

Politische Kontextualisierung

Anonymität

Attribution ist schwer!

Staatsgrenzen als Schutz vor Strafverfolgung

Virtualisierung des Verbrechens

Mögliche Auswirkungen

Datendiebstahl

- Verlust von geistiges Eigentum an die Konkurrenz
- Verlust von Mitarbeiterdaten
- Entwendete Zahlungsinformationen

Erpressung

- Reputationsverlust
- Produktionsunterbrechung
- Konventionalstrafen

Sabotage

- Wettbewerb
- Politische Agenda

Was muss der Mittelstand tun?

- **Akzeptanz der Realität**
- Einhaltung von Mindeststandards
- Einführung von Prozessen
- Mitarbeiterschulung - Umsetzung von Konzepten wie "Lebenslanges Lernen"
- **Anwendung von KI-unterstützter Technologie zur Prevention**
- **Anwendung von Zero-Trust Strategien**

Schlussfolgerung

Firmen die sich nicht vorbereiten, werden mit ungeahnten Herausforderungen konfrontiert werden

- Angriffe werden weiter zunehmen
- Jede Firma wird irgendwann betroffen sein
- Der Mittelstand wird weiter in den Fokus rücken
- Wir müssen jetzt agieren um in Zukunft sicher zu sein

Cybersichere Firmen gleich welcher Größe, werden den Wettbewerb anführen