Cyberkriminelle nutzen eine Vielzahl von Methoden, um sich Zugriff auf Unternehmenssysteme zu verschaffen. Hier ist ein **Ranking der häufigsten und effektivsten Angriffsmechanismen**, basierend auf Bedrohungsberichten führender Sicherheitsfirmen:

Top 10 Methoden, mit denen Cyberkriminelle Unternehmenssysteme kompromittieren

1 Phishing & Spear-Phishing (E-Mail & Social Engineering)

- **Wie funktioniert es?**
    - Mitarbeiter erhalten gefälschte E-Mails, die sie zum Klicken auf schädliche Links oder zum Öffnen infizierter Anhänge verleiten.
    - Oft als „Dringend!“ oder „Ihr Passwort läuft ab“ getarnt.
    - Spear-Phishing ist gezielter (z. B. auf CEOs oder IT-Administratoren).
- **Warum gefährlich?**
    - 90 % aller Cyberangriffe beginnen mit Phishing.
    - Kann Login-Daten, Finanzinformationen oder Malware verbreiten.

---

2 Kompromittierte Zugangsdaten & Passwort-Hacks

- **Wie funktioniert es?**
    - Cyberkriminelle nutzen gestohlene oder geleakte Passwörter aus Datenlecks.
    - **Credential Stuffing**: Angreifer probieren bekannte Passwörter auf anderen Plattformen.
    - **Brute-Force-Angriffe**: Automatische Programme testen Millionen von Passwort-Kombinationen.
- **Warum gefährlich?**
    - Viele Nutzer verwenden dasselbe Passwort auf mehreren Plattformen.
    - Fehlende Multi-Faktor-Authentifizierung (MFA) macht Unternehmen verwundbar.

---

3 Ransomware-Angriffe (Erpressung durch Verschlüsselung)

- **Wie funktioniert es?**
    - Angreifer verschlüsseln Unternehmensdaten und verlangen Lösegeld für die Entschlüsselung.

- Wird oft durch Phishing, unsichere RDP-Zugänge oder Exploits eingeschleust.

- **Warum gefährlich?**
  - Unternehmen werden lahmgelegt (Bsp.: **Colonial Pipeline, 2021**).
  - Wiederherstellungskosten sind oft höher als das Lösegeld.

---

4 Schwachstellen in Software & ungepatchte Systeme

- **Wie funktioniert es?**
  - Angreifer suchen nach ungepatchten Sicherheitslücken (Zero-Day-Exploits).
  - Besonders beliebt: VPN-Software, Webserver, ERP-Systeme, alte Windows-Versionen.
- **Warum gefährlich?**
  - Unternehmen zögern oft mit Updates (Downtime, Kompatibilitätsprobleme).
  - Angriffe können **automatisiert** mit Exploit-Kits erfolgen.

---

5 Unzureichend gesicherte Remote-Zugänge (RDP, VPN, Cloud)

- **Wie funktioniert es?**
  - Hacker scannen das Internet nach offenen **Remote Desktop Protocol (RDP)**-Ports oder ungesicherten VPN-Zugängen.
  - Fehlende Zwei-Faktor-Authentifizierung (2FA) macht es leicht, sich Zugang zu verschaffen.
- **Warum gefährlich?**
  - Seit der Pandemie ist Remote-Arbeit weit verbreitet.
  - Cyberkriminelle verkaufen RDP-Zugänge im Darknet.

---

6 Insider-Bedrohungen (böswillige oder nachlässige Mitarbeiter)

- **Wie funktioniert es?**
  - Unzufriedene oder bestochene Mitarbeiter verkaufen Daten oder installieren Malware.
  - Nachlässigkeit (USB-Sticks mit Malware, schwache Passwörter, öffentliche WLAN-Nutzung).

- **Warum gefährlich?**
    - Interne Mitarbeiter haben oft **direkten Zugriff auf sensible Systeme**.
    - Lässt sich schwer technisch verhindern.

---

7 Business Email Compromise (BEC) & CEO-Fraud

- **Wie funktioniert es?**
    - Kriminelle kapern oder fälschen E-Mail-Adressen von Führungskräften.
    - Ziel: Geldüberweisungen an Fake-Konten veranlassen oder interne Informationen stehlen.
- **Warum gefährlich?**
    - Hohe Erfolgsquote, da Mitarbeiter oft Anweisungen von „Vorgesetzten“ nicht hinterfragen.
    - Verluste können in die Millionen gehen.

---

8 Supply-Chain-Angriffe (Drittanbieter kompromittieren)

- **Wie funktioniert es?**
    - Hacker greifen IT-Dienstleister, Software-Anbieter oder Logistikunternehmen an, um große Unternehmen zu infizieren.
    - Oft über kompromittierte Updates oder gekaperte Zugänge.
- **Warum gefährlich?**
    - Große Unternehmen verlassen sich auf viele Dienstleister.
    - Bsp.: **SolarWinds-Hack 2020** – russische Hacker infizierten Tausende Unternehmen und Behörden.

---

9 Malvertising & Drive-by-Downloads (bösartige Werbung & Webseiten)

- **Wie funktioniert es?**
    - Nutzer klicken auf infizierte Werbung oder besuchen kompromittierte Websites.
    - Malware wird automatisch heruntergeladen (z. B. Keylogger, Remote-Access-Trojaner).

- **Warum gefährlich?**
    - **Zero-Click-Exploits** können Geräte infizieren, ohne dass der Nutzer etwas tut.
    - Sicherheitslücken in Browsern oder Plugins (Adobe Flash, Java, veraltetes Chrome) werden ausgenutzt.

---

10 Cloud-Sicherheitslücken & Fehlkonfigurationen

- **Wie funktioniert es?**
    - Unternehmen speichern sensible Daten in der Cloud, aber **vergessen Sicherheitseinstellungen**.
    - Öffentliche S3-Buckets, fehlende Zugriffskontrollen oder schlecht konfigurierte APIs.
- **Warum gefährlich?**
    - Datenlecks durch **falsch konfigurierte Amazon S3, Google Cloud oder Azure-Konten** sind häufig.
    - Angreifer können **Admin-Zugänge übernehmen** und Unternehmen erpressen.

Fazit: Welche Angriffe sind am häufigsten?

Basierend auf **aktuellen Cybersecurity-Berichten (z. B. Verizon DBIR, Mandiant, IBM X-Force)** sind die **Top-3 Methoden**:

1 Phishing & Social Engineering (meistverbreitet)
2 Gestohlene Zugangsdaten & schwache Passwörter
3 Ransomware (am teuersten für Unternehmen)

Was hilft dagegen?
Mitarbeiterschulungen gegen Phishing
Multi-Faktor-Authentifizierung (MFA) aktivieren
Regelmäßige Updates & Patch-Management
Zero-Trust-Strategie umsetzen (Minimale Rechtevergabe)
Security Monitoring & SIEM-Systeme nutzen