WHITEPAPER

# Deutsche Firmen verlieren 180 Milliarden Euro durch Cyberangriffe!

## Finde heraus, ob dein Unternehmen das nächste ist.

Cyberangriffe verursachen enormen Schaden. Eine der größten Ursachen sind Fehlkonfigurationen auf IT-Systemen.

Zahlreiche Regulatorik (NIS2, DORA, TISAX etc.) fordern zwingend die sichere Konfiguration und einen Umsetzungsnachweis.

**Die Lösung ist Systemhärtung**

**Doch was ist das eigentlich?**

TEAL
ALWAYS CHALLENGING IT

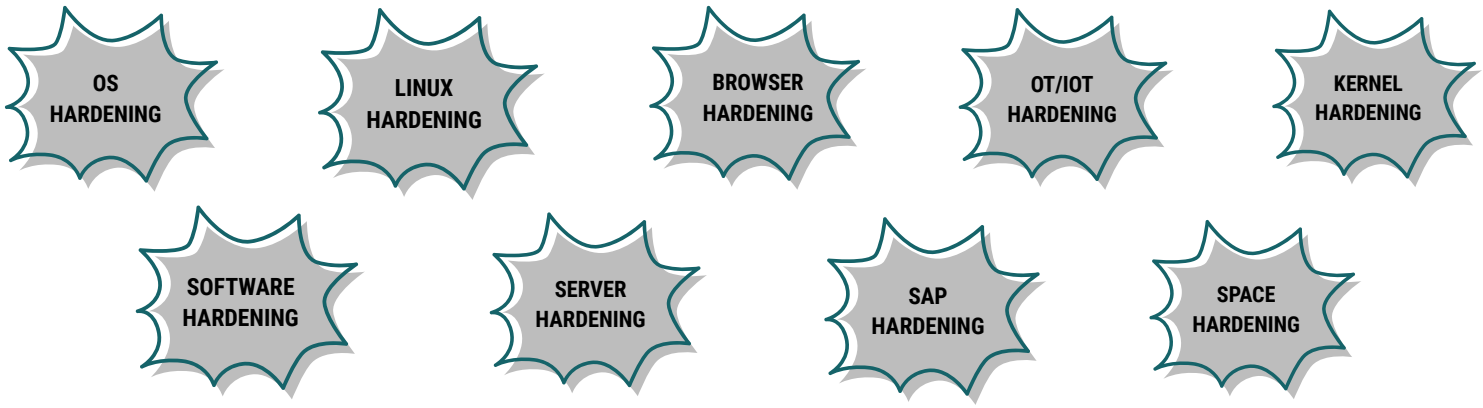
**Wie gut sind deine IT-Systeme wirklich gegen Angriffe geschützt?** Viele Unternehmen investieren in Firewalls, Antivirenprogramme und Monitoring-Tools, doch eine oft unterschätzte Schwachstelle bleibt bestehen: falsch oder unzureichend konfigurierte Systeme. Genau hier setzen gezielte Maßnahmen zur Systemhärtung an.

## Was ist Systemhärtung?

Als Systemhärtung oder Härtung bezeichnet man die sichere Konfiguration von IT-Systemen. Ziel ist es, durch verschiedene technische Maßnahmen Sicherheitslücken zu schließen und Angriffsflächen für Cyber-Angriffe zu reduzieren.

Systemhärtung bzw. das Härten von Systemen gilt somit per Definition als eine **präventive IT-Security-Maßnahme**. Es dient dazu, sowohl einzelne Computer als auch große Systemlandschaften resilienter zu machen.

## Welche Arten von Systemhärtung gibt es ?




## Was bringt Systemhärtung?

Da auf IT-Systemen unter anderem höchst sensible Informationen eines Unternehmens sowie personenbezogene Daten verarbeitet und gespeichert werden, müssen die verwendeten Systeme besonderen Schutzmaßnahmen unterzogen werden.

Eine sehr wirkungsvolle Maßnahme zur Absicherung stellt die Systemhärtung dar. Sie sichert das Betriebssystem ab, unabhängig davon, ob es sich um ein physisches, virtuelles oder Cloud-basiertes System handelt. Zudem werden Applikationen wie Office-Programme und Browser sicherer gemacht - beispielsweise gegen Datendiebstahl.

Durch eine nachhaltige Systemhärtung kann das Risiko eines erfolgreichen Cyber-Angriffs deutlich reduziert werden. Darüber hinaus kannst du Hardening-Audits zur Anomalieerkennung nutzen, das SOC-Team entlasten und auch Forensiker arbeiten dank Systemhärtung effizienter.

**Unterm Strich schützt du mit einer Härtung wichtige Unternehmensdaten und -systeme! Kommt es hier zu Kompromittierungen, sind meist extrem hohe Schäden die Folge. Im schlimmsten Fall muss dein Unternehmen den Betrieb einstellen und Insolvenz anmelden.**

## Welche Bedrohungen bestehen ohne Systemhärtung?

Die wesentlichen Bedrohungen bei nicht gehärteten Betriebssystemen & Anwendungen sind u.A.:

- Identitätsdiebstahl bei Angriffen auf die zentrale Identitäts-Management-Struktur
- Daten-Manipulation von personenbezogenen Daten und sensiblen Unternehmensdaten
- Datenabfluss wie das Kopieren gesamter Datenbanken
- Manipulation von Anwendungen oder damit verbundener Systeme
- Sabotage oder Spionage bei Betriebs- und Produktionsabläufen
- Einschleusen und Verbreitung von Malware
- “Datenkraken” sammeln detaillierte Nutzerdaten, um Werbeprofile zu erstellen.
- Immense Kosten, um die Folgen der Cyber-Angriffe zu beseitigen

Wie verschiedene Zahlen zeigen, ist ein Großteil aller Unternehmen von Hacker-Angriffen, Datendiebstahl & Spionage betroffen. Deswegen sind die Informationssicherheit und Härtung von Systemen so wichtig!

## Welche Unternehmen müssen sich mit Systemhärtung beschäftigen?

**Alle!** Gleichgültig, ob **Solo-Unternehmer, Startup, mittelständisches Unternehmen** oder **Konzern**: Überall sollten die IT-Systeme bestmöglich gehärtet sein. Denn bei jeder Unternehmensgröße haben Schwachstellen unter Umständen schwerwiegende Folgen.

Dass die Größe eines Unternehmens kaum eine Rolle bei der Absicherung von IT-Infrastrukturen spielt, zeigen auch diverse neue IT-Gesetze, -Regularien und -Normen (ISO27001:20222, NSA, CISA, ...).

## Wie gut sind deine Systeme gehärtet?

# Die nächsten Schritte

Als erfahrenes IT-Security-Consulting-Unternehmen unterstützt **Teal Technology Consulting GmbH** dich dabei, deine Systeme nachhaltig zu härten und Sicherheitslücken zu schließen. Unsere Lösungen basieren auf bewährten Best Practices und aktuellen Sicherheitsstandards wie BSI und CIS.

**Vereinbare jetzt ein kostenloses 30-minütiges Beratungsgespräch**, um gemeinsam zu analysieren, wie wir deine IT-Sicherheitsstrategie optimieren können. In diesem Gespräch erhältst du:

- ✓ Eine individuelle Einschätzung deiner aktuellen Sicherheitslage
- ✓ Konkrete Handlungsempfehlungen zu Systemhärtung
- ✓ Einblick in bewährte Methoden und Tools

Nutze jetzt die Gelegenheit, um deine IT-Infrastruktur proaktiv zu schützen und dich gegen zukünftige Bedrohungen zu wappnen.

**BERATUNGSGESPRÄCH VEREINBAREN**

TEAL
ALWAYS CHALLENGING IT