DIE 5 GEFÄHRLICHSTEN FORTINET-FEHLKONFIGURATIONEN

KOSTENLOSER REPORT – PFLICHTLEKTÜRE FÜR JEDEN IT-LEITER.

FORTINET

100+ FORTINET-PROJEKTE

In 10 Minuten wissen Sie, ob Ihre Umgebung verwundbar ist.

Erstellt vom einzigen Fortinet Partner Deutschlands mit 4 NSE8-Experten in einem Team.

2F·IT
IT SOLUTIONS

WIE SICHER IST IHRE FORTINET-UMGEBUNG WIRKLICH?

SCHÜTZEN SIE IHR FORTINET INVESTMENT!

Viele Unternehmen investieren in Fortinet – aber nutzen das volle Potenzial nicht.

Unsere Erfahrung aus über 100 Fortinet-Reviews:
8 von 10 Umgebungen weisen Fehlkonfigurationen auf, die Angreifern das Leben unnötig leicht machen.

TYPISCHE URSACHEN

- **Hohe Auslastung der internen IT**
- **Kein dediziertes Fortinet-Know-how**
- **Historisch gewachsene Konfigurationen**
- **Kein konsequentes Policy- und Change-Management**

ZIEL DIESES REPORTS

Sie erhalten einen kompakten Überblick über die 5 häufigsten Fehlkonfigurationen – inklusive konkreter Self-Checks, mit denen Sie Ihre eigene Umgebung kritisch hinterfragen können.

Erstellt vom einzigen Fortinet Partner Deutschlands mit 4 NSE8-Experten in einem Team.

4 NSE8-zertifizierte Experten — Deutschlands höchste Dichte pro Team

ERSTELLT VOM 2F-IT FORTINET-KOMPETENZZENTRUM MIT 3× NSE8 / FCX-EXPERTEN

(EINES DER ERFAHRENSTEN FORTINET-TEAMS IN DEUTSCHLAND)

DIE 5 HÄUFIGSTEN FORTINET-FEHLKONFIGURATIONEN

FEHLER #1

FEHLENDE SEGMENTIERUNG & ZU PERMISSIVE POLICIES

TYPISCH:

- Wenige oder keine echten Sicherheitszonen
- Interne Any–Any-Policies
- Kritische Systeme (Server, DMZ, OT) nicht getrennt

RISIKEN:

- Lateral Movement nach einem einzigen Einstieg
- Komplette Kompromittierung von Produktions- oder Finanzsystemen
- Keine klare Trennung von IT- und OT-Netzen

BEST PRACTICE:

- Mikrosegmentierung nach Geschäftsbereichen
- Strenges Least-Privilege-Prinzip
- Nutzung von Internal Segmentation Firewalls (ISFW)
- Regelmäßige Policy-Reviews (mindestens 1–2× pro Jahr)

SELF-CHECK:

- ☐ Gibt es klar definierte Zonen (z. B. Office, Server, DMZ, OT)?
- ☐ Sind besonders kritische Systeme in eigenen Segmenten isoliert?
- ☐ Haben Sie interne Any–Any-Regeln konsequent eliminiert?
- ☐ Werden Policies regelmäßig bereinigt und rezertifiziert?

UNSER GARANTIEVERSPRECHEN

Mit 2F-IT erhalten Sie mehr als IT-Sicherheit – Sie erhalten ein belastbares Sicherheitsfundament, auf das Sie sich verlassen können.

DIE 5 HÄUFIGSTEN FORTINET-FEHLKONFIGURATIONEN

FEHLER #2

VERALTETE FIRMWARE & FEHLENDER PATCH-PROZESS

TYPISCH:

- FortiGate-Firmware mehrere Major Releases zurück
- FortiGate-Firmware auf neusten unstabilen Major Release
- Patches werden nur bei Problemen eingespielt, nicht proaktiv

RISIKEN:

- Ausnutzbare, bekannte Schwachstellen
- Fehlende Security-Funktionen aus neuen Releases
- Instabilitäten und unerwartetes Verhalten

BEST PRACTICE:

- Klar definierte Update-Strategie (Wer? Wann? Wie?)
- Testsystem oder Wartungsfenster für kritische Änderungen
- Monitoring neuer Fortinet-Releases und Security-Advisories

SELF-CHECK:

- [ ] Sind alle Firmwarestände zentral dokumentiert?
- [ ] Gibt es einen standardisierten Ablauf für Firmware-Updates?
- [ ] Werden sicherheitskritische Patches priorisiert umgesetzt?
- [ ] Werden Änderungen und mögliche Rollbacks dokumentiert?

Wir können 2F-IT vor allem aufgrund der Expertise und Erfahrung im Bereich Fortinet nur empfehlen!

TIM RIEKERT, Head of it + bpm

DIE 5 HÄUFIGSTEN FORTINET-FEHLKONFIGURATIONEN

FEHLER #3

NICHT GENUTZTE SECURITY-FABRIC-FUNKTIONEN

TYPISCH:

- FortiAnalyzer nur als „Log-Ablage“
- Security Fabric nur rudimentär verbunden
- Kaum Automation Stitches oder Security Rating im Einsatz

RISIKEN:

- Fehlende Übersicht über Bedrohungen & Events
- Kein automatisiertes Reagieren auf sicherheitsrelevante Ereignisse
- Potenzial der kompletten Fortinet-Landschaft bleibt ungenutzt

BEST PRACTICE:

- Vollständige Aktivierung der Fortinet Security Fabric
- FortiAnalyzer als zentrales Monitoring- und Reporting-System
- Nutzung von Automation Stitches zur Reaktion auf definierte Events
- Security Rating als Steuerungs-KPI für Security-Reife

SELF-CHECK:

- [ ] Ist die Security Fabric mit allen Fortinet-Komponenten verbunden?
- [ ] Nutzen Sie FortiAnalyzer aktiv für Dashboards, Alarme und Reports?
- [ ] Haben Sie Automatisierungen für typische Security-Events definiert?
- [ ] Wird das Security Rating regelmäßig geprüft?

„Ich empfehle 2F-IT als optimalen Partner für die Fortinet Integration."
Martin Schlipp, VEGA Grieshaber KG

VEGA

DIE 5 HÄUFIGSTEN FORTINET-FEHLKONFIGURATIONEN

FEHLER #4

UNVOLLSTÄNDIGES LOGGING & FEHLENDES SECURITY-MONITORING

TYPISCH:

- Nur Traffic-Logs aktiv
- Keine oder unzureichende Logs zu Admin-, System- oder Security-Events
- Logs werden zwar geschrieben, aber nicht systematisch ausgewertet

RISIKEN:

- Vorfälle bleiben unentdeckt oder werden zu spät erkannt
- Keine Audit-Trails für interne oder externe Audits
- Compliance-Risiken (z. B. ISO 27001, KRITIS)

BEST PRACTICE:

- Vollständige Log-Abdeckung (Traffic, System, Security, Admin)
- Zentrale Sammlung im FortiAnalyzer
- Relevante Alarme (z. B. Policy-Changes, fehlgeschlagene Logins, IPS-Treffer)
- Regelmäßige Auswertung und Incident-Response-Prozesse

SELF-CHECK:

- ☐ Sind alle wichtigen Log-Typen aktiviert?
- ☐ Werden Logs zentral gespeichert und ausreichend lange vorgehalten?
- ☐ Gibt es definierte Alarme für sicherheitskritische Events?
- ☐ Findet eine regelmäßige, dokumentierte Log-Analyse statt?

Wenn es um echte Fortinet Exzellenz geht, sind wir der Fortinet Partner mit der höchsten technischen Fortinet-Expertise in Deutschland.

DIE 5 HÄUFIGSTEN FORTINET-FEHLKONFIGURATIONEN

FEHLER #5

FEHLENDE BACKUPS & NOTFALLKONZEPTE

TYPISCH:

- Konfigurationen werden nur sporadisch oder manuell gesichert
- Keine regelmäßig getesteten Wiederherstellungsprozesse
- Keine klaren Rollen und Abläufe im Fehler- oder Ausfallfall

RISIKEN:

- Lange Ausfallzeiten bei Hardwaredefekt oder Konfigurationsfehler
- Verlust von komplexen Setups und feinjustierten Policies
- Erhebliche wirtschaftliche Schäden durch Unterbrechungen

BEST PRACTICE:

- Tägliche automatische Konfigurationsbackups
- Versionierung der Konfigurationen
- Dokumentierte und getestete Restore-Prozesse
- HA-Design für kritische Standorte und Komponenten

SELF-CHECK:

- ☐ Werden Konfigurationen automatisiert und versioniert gesichert?
- ☐ Wurde ein Restore aus Backup in der Praxis getestet?
- ☐ Existiert ein dokumentierter Notfallplan (inkl. Verantwortlichkeiten)?
- ☐ Sind zentrale Systeme im HA-Verbund aufgebaut?

Wir sind der am höchsten zertifizierter Fortinet-Expertenteam in Deutschland

BONUS

SCHNELL-CHECK „10 TYPISCHE FORTIGATE-FEHLER“

IDEAL ALS CHECKLISTE IM TEAM-MEETING

- [ ] SECURITY FABRIC NICHT AKTIVIERT
- [ ] FIRMWARE ÄLTER ALS ZWEI MAJOR-RELEASES ODER „NEUSTE“ IM EINSATZ
- [ ] INTERNE ANY-ANY-POLICIES AKTIV
- [ ] LOGGING NUR TEILWEISE ODER OHNE ZENTRALE SAMMLUNG
- [ ] KEINE AUTOMATISIERTEN KONFIGURATIONSBACKUPS
- [ ] WEBFILTER MIT DEFAULT-PROFIL OHNE ANPASSUNG
- [ ] APPLICATION CONTROL NUR TEILWEISE ODER GAR NICHT GENUTZT
- [ ] IPS-SIGNATUREN NICHT AKTUELL / NICHT KONSEQUENT AKTIV
- [ ] SD-WAN NUR ALS „FAILOVER“, NICHT OPTIMIERT UND ÜBERWACHT
- [ ] ADMIN-INTERFACES ÖFFENTLICH ERREICHBAR (WAN-ACCESS AKTIV)

UNSER GARANTIEVERSPRECHEN

Mit 2F-IT erhalten Sie mehr als IT-Sicherheit – Sie erhalten ein belastbares Sicherheitsfundament, auf das Sie sich verlassen können.

SO GEHT ES WEITER: VOM SELF-CHECK ZUM PROFESSIONELLEN FORTINET REVIEW

Unser professioneller Fortinet Review findet die echten Ursachen in 3 Schritten
Unklarheit kostet Zeit Und Anfragen

SCHRITT 01

KICK-OFF & BESTANDSAUFNAHME

- Verständnis Ihrer Geschäfts- und Security-Anforderungen o
- Sichtung von Konzepten, Netzwerkdiagrammen und Dokumentation o
- Klärung der technischen Zugänge (read-only) für die relevanten Fortinet-Systeme

SCHRITT 02

TECHNISCHES FORTINET REVIEW

- Detaillierte Analyse von Design, Konfiguration und Policies o
- Abgleich mit Best Practices und Hersteller-Empfehlungen o
- Erstellung eines Prüfberichts mit klarer Priorisierung aller kritischen Findings.

SCHRITT 03

ERGEBNIS-WORKSHOP & MASSNAHMENPLAN

- Präsentation des Prüfberichts (inkl. Priorisierung) o
- Diskussion technischer und organisatorischer Empfehlungen o
- Roadmap zur Umsetzung inkl. möglicher Unterstützung durch unser Team

2F-IT GARANTIE
Zufriedenheit + Kompetenz

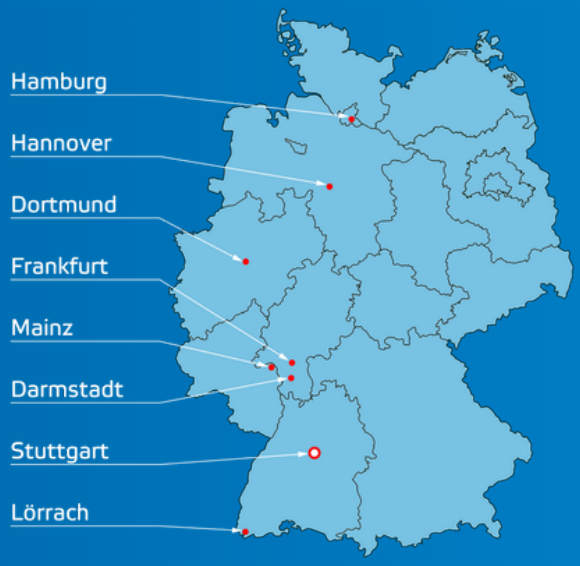
UNSER GARANTIEVERSPRECHEN

Wir begleiten Unternehmen bei der ganzheitlichen Nutzung des Fortinet-Portfolios – von Core-Produkten bis zu Securtiy Fabric-Integrationen.

WARUM 2F-IT (FORTINET KOMPETENZZENTRUM)?

Wenn es um echte **Fortinet** Exzellenz geht, sind wir der **Fortinet Partner** mit der höchsten technischen Fortinet-Expertise in **Deutschland**.

- **Fortinet Professional Services**
  Architektur, Design und Einführung moderner Sicherheitslösungen – On-Prem, Cloud oder Hybrid
- **Fortinet Managed Security Services**
  Vollständig betreuter Betrieb Ihrer Fortinet-Infrastruktur (24/7 optional) – auch co-managed mit Ihrem Team
- **Fortinet Solution Check-up & Review**
  Professionelle Analyse und Bewertung Ihrer aktuellen Fortinet-Umgebung inkl. Priorisierung und Best Practice Empfehlungen – mit optionaler Umsetzung durch unser Expertenteam



- **Einzigartig in Deutschland: 3 NSE8-/FCX-Experten in einem Team**
- **Fokus auf Fortinet & Security Fabric – kein Bauchladen, sondern Spezialist**
- **100 erfolgreich umgesetzte Fortinet-Projekte – vom Mittelstand bis Enterprise**
- **Consulting-, Tiger- und MSSP-Teams für Architektur, Implementierung und 24/7-Betrieb**

ENGAGE FORTINET ADVANCED PARTNER Integrator, MSSP, Cloud

FORTINET ENGAGE Account Specialization SASE

FORTINET ENGAGE Account Specialization SD-WAN

FORTINET ENGAGE Partner Specialization SECURE NETWORKING FIREWALL

FORTINET ENGAGE Account Specialization OPERATIONAL TECHNOLOGY

NÄCHSTER SCHRITT

Mit **2F-IT** erhalten Sie mehr als IT-Sicherheit – Sie erhalten ein belastbares Sicherheitsfundament, auf das Sie sich verlassen können.
Wir stehen für:

- Verlässlichkeit in der Betreuung
- Transparenz in der Kommunikation
- Zukunftssicherheit in der Architektur

Prüfen Sie Ihre Umgebung mit den Self-Checks aus diesem Report – und wenn Sie bei mehreren Punkten Zweifel haben, ist der Professioneller Fortinet Review der logische nächste Schritt.

+49 711 914 29 880
info@2f-it.de
Senefelderstr. 19 73760 Ostfildern

2F·IT IT SOLUTIONS

JETZT MIT UNS SPRECHEN
https://2f-it.de/fortinet/