SONDERLAGEBERICHT | 04. MÄRZ 2026

# Hybride Kriegsführung, Iran und was das für Ihr Unternehmen bedeutet

Drei Bedrohungsakteure. Reale Angriffstechniken. Konkrete Gegenmaßnahmen.

Zielgruppe
**Mittelständische regulierte Unternehmen (DACH)**

Regulatorik
**NIS2 · DORA · ISO 27001:2022 · KRITIS**

Klassifizierung
**TLP:WHITE — Weitergabe erlaubt**

Quellen
**Recorded Future Insikt Group, Unit 42, OSINT**

Stand
**04. März 2026**

## Management Summary

| Was ist passiert? | Was bedeutet das? | Was müssen wir tun? |
|---|---|---|
| Am 28.02.2026 starteten die USA und Israel eine koordinierte Militäroperation gegen den Iran. Der Oberste Führer Ali Khamenei wurde getötet. Iran reagierte mit Vergeltungsschlägen in neun Ländern und koordinierten Cyberoperationen über den neu gegründeten „Electronic Operations Room“. | Pro-iranische Hacktivistengruppen und staatlich gesteuerte APT-Gruppen eskalieren ihre Cyberoperationen. Ziele sind kritische Infrastruktur, Energie, Finanzen und Forschung, auch in Europa. Physische Bedrohungen in Westeuropa sind laut Recorded Future sehr wahrscheinlich. | **Sofort:** MFA prüfen (FIDO2), Exchange patchen, Offline-Backups testen, IR-Playbooks aktualisieren, Mitarbeitersensibilisierung für Social Engineering durchführen. |

**Warum dieses Briefing regulatorisch relevant ist**

NIS2 (Art. 21 Abs. 2), DORA (Art. 11) und ISO 27001:2022 (A-5.7) verlangen den systematischen Umgang mit Bedrohungsintelligenz. Dieser Bericht trägt zur Nachweisführung bei. Die beschriebenen Akteure greifen genau die Sektoren an, die diese Regelwerke schützen sollen: kritische Infrastruktur, Energie, Verteidigung, Finanzsektor und Forschungseinrichtungen.

## Die Lage

Am 28. Februar 2026 starteten die USA und Israel eine koordinierte Militäroperation gegen den Iran (US: Operation Epic Fury, Israel: Operation Lion’s Roar). Innerhalb weniger Stunden wurde der iranische Oberste Führer Ali Khamenei getötet, gemeinsam mit über 40 hochrangigen Kommandeuren der Iranischen Revolutionsgarde (Islamic Revolutionary Guard Corps, IRGC). Was folgte, war nicht nur kinetische Vergeltung — es war auch eine sofortige Eskalation im Cyberraum.

Iran gründete am selben Tag den „Electronic Operations Room“ — eine Koordinierungsstelle für staatlich ausgerichtete Hacktivistengruppen. Laut Unit 42 (Palo Alto Networks) und Recorded Future waren innerhalb von 48 Stunden rund 60 Gruppen aktiv, darunter pro-iranische und pro-russische Akteure. Gleichzeitig fiel die iranische Internetkonnektivität auf etwa 4% — ein Hinweis auf massive US-israelische Cyberoperationen parallel zu den Luftschlägen.

Der Iran reagierte unter „Operation Truthful Promise 4“ mit Raketen- und Drohnenangriffen auf US-Militäreinrichtungen in mindestens neun Ländern. Die Straße von Hormuz wurde per VHF-Warnung als geschlossen deklariert.

## Bedrohungsakteure

Die folgenden Akteure sind für Unternehmen unter NIS2, DORA oder KRITIS besonders relevant. Handala ist im aktuellen Konflikt durch Recorded Future als aktivster iranischer Akteur dokumentiert. APT33 und APT35 sind historisch dokumentierte iranische APT-Gruppen, deren Reaktivierung in der aktuellen Eskalation hochwahrscheinlich ist.

| Akteur | Profil | Bedrohungsstufe |
|---|---|---|
| **Handala Hack Team**<br>Iranisches Ministerium für Geheimdienst und Sicherheit (MOIS) | Prominenteste iranische Hacktivist-Persona im aktuellen Konflikt (Quelle: Recorded Future). Staatlich gesteuerte Psychological-Warfare-Operation des MOIS (Ministry of Intelligence and Security). Dokumentierte Angriffe auf israelische Energieunternehmen, jordanische Treibstoffsysteme und israelische Gesundheitsinfrastruktur. Bekannt für den Übergang von opportunistischen zu strategischen Angriffen, einschließlich Supply-Chain-Targeting. | **HOCH** |
| **APT33 / Peach Sandstorm**<br>Iranische Revolutionsgarde (IRGC) | Seit 2013 aktiv. Systematische Angriffe auf Energie-, Verteidigungs- und Technologieunternehmen. Seit 2023 großangelegte Password-Spraying-Kampagnen. 2024: betrügerische Azure-Subscriptions als Command-and-Control-Infrastruktur (C2), Tickler-Backdoor gegen Verteidigungs- und Raumfahrtunternehmen. Europäische Zielgruppe dokumentiert. | **KRITISCH** |
| **APT35 / Charming Kitten**<br>IRGC Cyber-Electronic Command | Social-Engineering-Einheit des IRGC. Baut über Wochen Vertrauen auf als Journalist, Forscher oder NGO-Mitarbeiter. Phishing über legitime Google-Dienste (Google Sites, Google Meet). Laut nicht unabhängig verifiziertem Datenleck (Okt. 2025): Deutsche Exchange-Server auf der Zielliste. | **KRITISCH** |

## TTP-Mapping und Gegenmaßnahmen

| Akteur | Relevante TTPs | Warum relevant | Prioritäre Gegenmaßnahme |
|---|---|---|---|
| Handala | T1485 (Data Destruction / Wiper)<br>T1498 (DDoS)<br>T1539 (Session Hijacking) | *Zielt auf unwiderrufliche Zerstörung von Geschäftsdaten, um den Betrieb kritischer Infrastruktur lahmzulegen.* | CIS Control 11 — Getestete **Offline-Backups** mit dokumentierten Restore-Prozeduren |
| APT33 | T1110.003 (Password Spraying)<br>T1583.006 (Fraudulent Cloud Infra)<br>T1547 (Registry Persistence) | *Automatisiertes Durchprobieren von Passwörtern gegen Cloud-Zugänge. Nutzt kompromittierte Azure-Subscriptions als verdeckte Angriffsinfrastruktur.* | CIS Control 6 — **Phishing-resistente MFA** für alle Cloud-/Remote-Zugänge, Conditional Access Policies |
| APT35 | T1598 (Phishing for Information)<br>T1556 (Credential Harvesting)<br>T1114 (Email Collection) | *Langfristig aufgebaute Fake-Identitäten (Journalist, Forscher) führen zu Credential Theft über täuschend echte Login-Seiten auf Google-Infrastruktur.* | CIS Control 6 — **FIDO2-MFA**, CIS Control 14 — Security Awareness Training |

## Was das für Ihr Unternehmen bedeutet

| Thema | Bewertung |
|---|---|
| **Kinetischer Konflikt hat einen unmittelbaren Cyber-Schatten** | Mehrere pro-iranische Hacktivistengruppen haben koordinierte Cyberoperationen angekündigt. Die Fachdiskussion warnt: Auch wenn großangelegte Intrusions noch nicht unabhängig bestätigt sind, sollte das Risiko nicht unterschätzt werden. Handala hat eine dokumentierte Geschichte des Übergangs von opportunistischen zu strategischen Angriffen. |
| **Irans Internet-Blackout schneidet in beide Richtungen** | Iranische Konnektivität fiel auf ca. 4%. Das limitiert kurzfristig inländische Gruppen. Aber: Mehrere pro-iranische Akteure operieren von außerhalb Irans auf verteilter Infrastruktur — sie bleiben voll operationsfähig. |
| **Eskalationspfade im Cyberraum** | Bei fortgesetzter Eskalation steigt die Wahrscheinlichkeit destruktiver staatlicher Cyberoperationen gegen kritische Infrastruktur erheblich. Zielprofile: Medien, Telekommunikation, KMU. Europäische Unternehmen mit US-/Israel-Verbindungen sind indirekte Ziele. |
| **Straße von Hormuz** | Über 100 Containerschiffe, 200 Massengutfrachter und 450 Tanker zum Zeitpunkt der Schließungswarnung. Direkte Auswirkungen auf Energiemärkte, Versicherungskosten und Lieferketten. Energie-, Maritime- und Finanzunternehmen sollten Monitoring erhöhen. |
| **Physische Bedrohungen in Westeuropa** | Recorded Future bewertet es als sehr wahrscheinlich, dass Iran westliche Länder über gewaltbereite nicht-staatliche Akteure asymmetrisch trifft. Wahrscheinliche Ziele: US/israelische Offizielle, iranische Dissidenten, israelisch-jüdische Einrichtungen, Unternehmen mit US/Israel-Verbindung (Rüstung, Versicherungen, Banken, KRITIS). |

## Konkrete Gegenmaßnahmen — Sofort umsetzbar

Die beschriebenen Akteure nutzen keine Zero-Days. Sie nutzen schwache MFA-Konfigurationen, ungepatchte Exchange-Server und Mitarbeiter, die einer überzeugend wirkenden Nachricht vertrauen. Das sind lösbare Probleme — wenn man weiß, wo man anfangen muss.

| Maßnahme | CIS Control | Umsetzung | Relevant für |
|---|---|---|---|
| **MFA für alle Cloud- und Remote-Zugänge** | Control 6 | Phishing-resistente MFA (**FIDO2/WebAuthn**). Conditional Access Policies. Password-Spraying-Erkennung aktivieren. | APT33, APT35 |
| **Offline-Backup-Strategie testen** | Control 11 | Getestete **Offline-Backups**. Dokumentierte Restore-Prozeduren. Wiper-Szenarien in Backup-Tests einbeziehen. | Handala |
| **Exchange-Server patchen und härten** | Control 7 | Alle Exchange-Server auf aktuellen Patchstand. **Extern exponierte Instanzen eliminieren** oder isolieren. | APT35 |
| **Security Awareness Training** | Control 14 | Sensibilisierung für Social Engineering. Fokus: **LinkedIn-basierte Kontaktanbahnung**, gefälschte Forscher/Journalisten. | APT35 |
| **Incident Response Readiness** | Control 17 | IR-Playbooks aktualisieren. Eskalationswege dokumentieren. **Tabletop Exercise mit Wiper-Szenario**. | Alle Akteure |

## Wie wir Sie bei der Umsetzung unterstützen können

Dieser Bericht zeigt, welche Bedrohungsakteure für Ihre Branche relevant sind und welche Maßnahmen Priorität haben. Die Umsetzung erfordert jedoch eine individuelle Bewertung Ihrer spezifischen Infrastruktur, Ihrer bestehenden Sicherheitsmaßnahmen und Ihrer regulatorischen Anforderungen.

### TIRAS — Threat-Informed Resilience & Advisory System

TIRAS übersetzt aktuelle Bedrohungsintelligenz in priorisierte, umsetzbare Maßnahmen — zugeschnitten auf Ihr Unternehmensprofil. Kein generisches Framework-Mapping. Keine Compliance-Checklisten. Threat Intelligence, die zeigt, welche TTPs für Ihre Branche und Ihre Infrastruktur heute relevant sind — und welche CIS-Controls Sie priorisieren sollten.

Bevor Sie in kostenintensive Penetrationstests investieren, hilft TIRAS Ihnen dabei, Ihre Ressourcen gezielt dort einzusetzen, wo die reale Bedrohungslage es erfordert.

**Interesse? Kontaktieren Sie uns für ein erstes Gespräch.**

kontakt@threat-informed.de | www.threat-informed.de

*Quellen: Recorded Future Insikt Group (02.03.2026), Unit 42 / Palo Alto Networks (02.03.2026), CrowdStrike, Halcyon RRC, OSINT. Alle Informationen basieren auf öffentlich verfügbaren Quellen.*

*Dieser Bericht ist Teil unserer regelmäßigen Threat Briefings für Unternehmen unter NIS2, DORA und KRITIS in der DACH-Region. TLP:WHITE — Weitergabe erlaubt.*

## Glossar

| Abkürzung | Bedeutung |
|---|---|
| APT | Advanced Persistent Threat — staatlich gesteuerte, langfristig operierende Angreifergruppe |
| C2 | Command and Control — Infrastruktur zur Fernsteuerung kompromittierter Systeme |
| CIS Controls | Center for Internet Security Controls — priorisierter Maßnahmenkatalog für IT-Sicherheit |
| DDoS | Distributed Denial of Service — Überlastungsangriff auf Netzwerkdienste |
| FIDO2 | Fast Identity Online 2 — Phishing-resistenter Authentifizierungsstandard |
| IRGC | Islamic Revolutionary Guard Corps — Iranische Revolutionsgarde |
| MOIS | Ministry of Intelligence and Security — Iranisches Ministerium für Geheimdienst und Sicherheit |
| MFA | Multi-Faktor-Authentifizierung |
| TTP | Tactics, Techniques & Procedures — Vorgehensweisen von Angreifern (MITRE ATT&CK) |