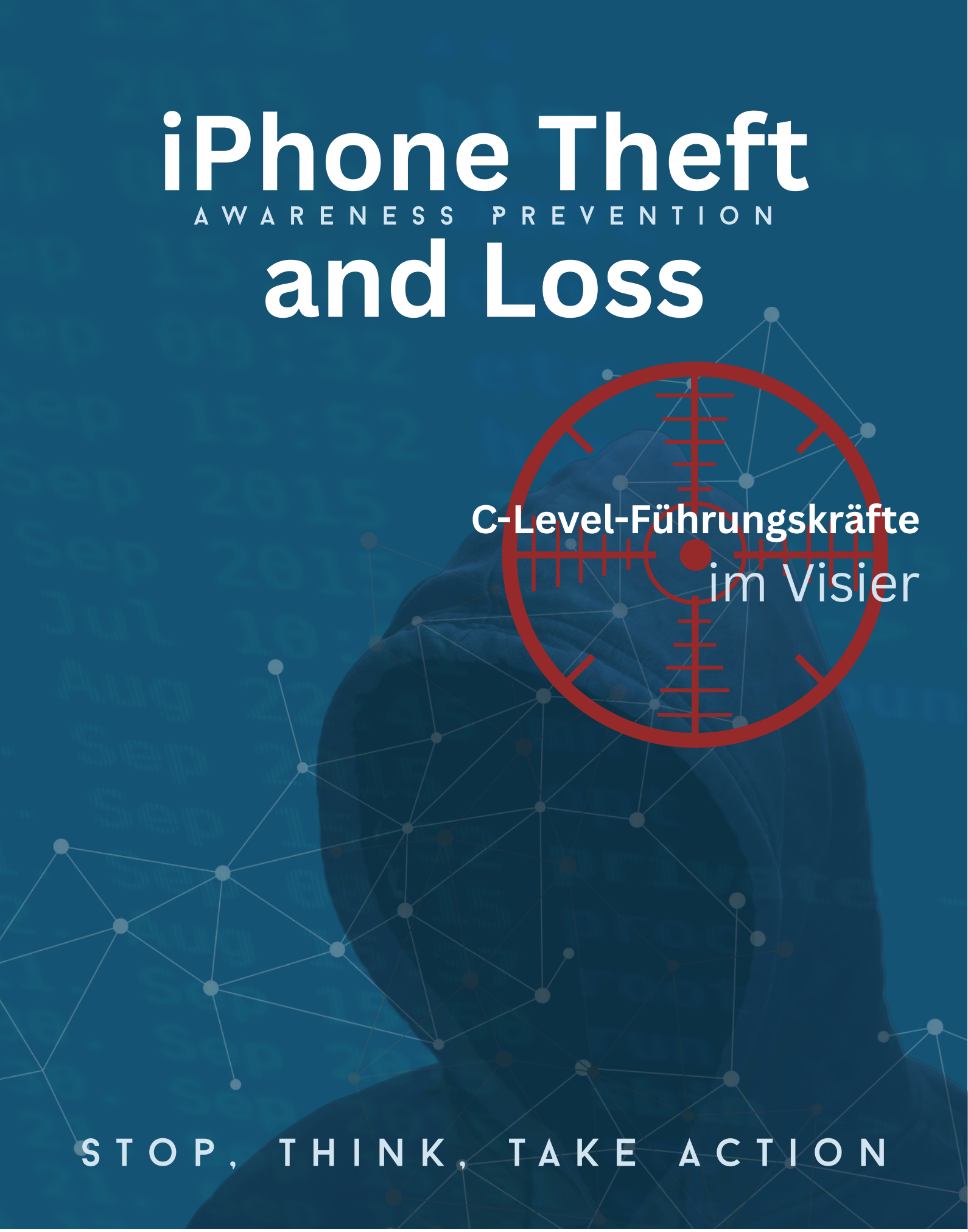
iPhone Theft and Loss

AWARENESS PREVENTION



C-Level-Führungskräfte im Visier

STOP, THINK, TAKE ACTION

MDS.LEGAL
Meißner Datenschutz GmbH
Markt 31 | 25821 Bredstedt
Tel. 04671 93 10 31
www.mds.legal

Zunahme mobiler Bedrohungen im Unternehmenskontext

Die mobile Bedrohungslandschaft hat sich in den Jahren 2024 und 2025 drastisch verändert, wobei Cyberkriminelle und staatlich unterstützte Akteure mobile Geräte zunehmend als Einstiegspunkt für Angriffe nutzen.

Besonders besorgniserregend ist, dass iOS-Geräte laut dem *Lookout Mobile Threat Landscape Report 2024* doppelt so häufig wie Android-Geräte durch Phishing-Angriffe kompromittiert wurden.

Diese Entwicklung ist besonders relevant für Unternehmen, da gestohlene oder kompromittierte iPhones ein erhebliches Sicherheitsrisiko darstellen können.

Methoden der Kompromittierung

- Ausnutzung von Zero-Day-Schwachstellen
- **Physischer Diebstahl mit anschließendem Hacken**
- Phishing-Angriffe auf iOS-Geräte

Ausnutzung von Zero-Day-Schwachstellen

Im März 2025 wurden Fälle bekannt, bei denen Angreifer eine Sicherheitslücke namens "Nickname" in iMessage ausnutzten, um iPhones ohne jegliche Nutzerinteraktion zu kompromittieren. Diese Schwachstelle betraf iOS-Versionen bis 18.1.1 und wurde erst in iOS 18.3.1 behoben. Die Angriffe zielten auf hochrangige Personen in Unternehmen, Regierungen und Medienorganisationen ab.

MDS.LEGAL
Meißner Datenschutz GmbH
Markt 31 | 25821 Bredstedt
Tel. 04671 93 10 31
www.mds.legal

Physischer Diebstahl mit anschließendem Hacken

Eine besonders beunruhigende Entwicklung ist die Zunahme von iPhone-Diebstählen mit anschließendem Hacken. Im Jahr 2024 wurden allein in London etwa 78.000 Smartphones als gestohlen gemeldet, was einem Anstieg von 150 Prozent entspricht. In den USA wurden im selben Zeitraum etwa 1,4 Millionen Mobiltelefone gestohlen. Besorgniserregend ist, dass hochrangige Unternehmensvertreter und **C-Level-Führungskräfte** aufgrund der wertvollen Informationen auf ihren Geräten **bevorzugte Ziele** sind.

Phishing-Angriffe auf iOS-Geräte

Phishing-Angriffe auf iOS-Geräte haben 2024 deutlich zugenommen. Laut einer Studie waren 26 Prozent der iOS-Nutzer von mobilen Phishing-Angriffen betroffen, während es bei Android-Nutzern nur 12 Prozent waren. Diese Angriffe sind webbasiert und können über jede App auf jedes Gerät gelangen, was sie besonders gefährlich macht.

Schutzmaßnahmen für Unternehmen

- Aktivierung des Lockdown-Modus
- Mobile Sicherheitslösungen implementieren
- Schulung der Mitarbeiter durchführen

Der Verlust eines iPhones erfordert sowohl technische Sofortmaßnahmen als auch die Erfüllung rechtlicher Meldepflichten. Durch präventive Sicherheitseinstellungen und schnelles Handeln im Schadensfall können die Risiken minimiert werden.

MDS.LEGAL
Meißner Datenschutz GmbH
Markt 31 | 25821 Bredstedt
Tel. 04671 93 10 31
www.mds.legal

MDS.LEGAL

Allgemeine empfohlene technische Maßnahmen

System- und Datensicherheit

- Betriebssystem aktuell halten
- Schutz für gestohlene Geräte aktivieren
- Biometrische Authentifizierung nutzen (z. B. Face-ID)
- Starken Gerätecode verwenden
- Automatische Datenlöschung aktivieren
- USB-Beschränkungsmodus nutzen

Account- und Passwortsicherheit

- Zwei-Faktor-Authentifizierung aktivieren
- Passwort-Manager verwenden
- Sicherheitsempfehlungen beachten

Netzwerk- und App-Sicherheit

- Keine automatische Verbindung mit unbekannten WLAN-Netzwerken oder Hotspots
- Apps nur aus dem App Store installieren
- App-Berechtigungen prüfen
- App Tracking Transparency aktivieren

Zusätzliche Maßnahmen

- Anonym surfen mit iCloud Private Relay (Die Aktivierung von iCloud Private Relay, dient dem Schutz von IP-Adresse und DNS-Anfragen beim Surfen

MDS.LEGAL
Meißner Datenschutz GmbH
Markt 31 | 25821 Bredstedt
Tel. 04671 93 10 31
www.mds.legal

MDS.LEGAL

Von Apple Inc. empfohlene Sofortmaßnahmen

- Auf iCloud.com/find als verloren markieren
- Vorfall der örtlichen Polizei melden
- Mobilfunkanbieter kontaktieren (Account sperren)
- iPhone per Fernzugriff löschen
- Gerät aus dem Apple Account entfernen
- Apple Account-Informationen prüfen und aktualisieren

Detaillierte Informationen

https://support.apple.com/de-de/120837

Achtung: Meldepflicht an die Aufsichtsbehörde prüfen!

Der Verlust eines iPhones mit personenbezogenen Daten stellt grundsätzlich eine "Verletzung des Schutzes personenbezogener Daten" im Sinne der DSGVO dar. Eine solche Verletzung liegt vor, wenn es zur Vernichtung, zum Verlust oder zur unbefugten Offenlegung von personenbezogenen Daten kommt[2].

1) Autoren: Jonathan Vincent (Cyber Intel Lead) und Saba Sattar (Intelligence Analyst III, Cyber Intel Lead),
Quelle: https://www.crisis24.com/articles/increasing-rates-of-phone-thefts-worldwide-pose-significant-data-security-risks
2) Autor: Der Landesbeauftragte für den Datenschutz Niedersachsen,
Quelle: https://www.lfd.niedersachsen.de/faq/faq-meldung-von-datenschutzverstossen-167312.html

Zum Kontaktformular

Bis bald

Marcus Valentin-Herms
Senior Consultant

Wir unterstützen Sie gern.

iPhone Theft
AWARENESS PREVENTION
and Loss

MDS.LEGAL
Meißner Datenschutz GmbH
Markt 31 | 25821 Bredstedt
Tel. 04671 93 10 31
www.mds.legal

MDS.LEGAL