



Newsletter 03/2025

Sehr geehrte Klientinnen und Klienten, liebe Freunde von **FM-nospy**,

Spionage hat inzwischen längst nicht nur den Zweck, vertrauliche Informationen von Geschäftsleitungen oder irgendwelchen Laboren auszuspähen.

Immer öfter dient Spionage zu, gezielte Sabotage(!) vorzubereiten! Dabei muss diese nicht unbedingt "haptisch" erfolgen – auch für Sabotage durch Ruf- und Reputations-schädigung wird im Vorfeld intensiv ausgespäht.

Nachfolgend wie immer Aktuelles und Interessantes aus der Welt der Industrie- und Wirtschaftsspionage. „Möge die Sicherheit mit Ihnen sein“ ...!

Ihr Team von **FM-nospy**

Stahlspäne im Zylinderkopf – Sabotage bei der Dt. Marine

Unbekannte Saboteure beschädigen Kriegsschiffe der Bundeswehr!

Zudem mehren sich Versuche, in Stützpunkte einzudringen. Security Insider erkennen eine wachsende Bedrohung durch Russland, die besonders seit Anfang 2025 stark zunimmt.

Informationen zufolge wurde im Januar bei einer Kontrolle entdeckt, dass mehrere Kilogramm Metallspäne in den Antrieb eines Kriegsschiffs gekippt worden waren. Unentdeckt hätte dies zu erheblichen Schäden geführt.

Neben Sabotageversuchen an Marine-Schiffen gebe es von Land und See Fälle von Eindringen in Marine-Stützpunkte und zahlreiche "Anbahnungsversuche" mit Hilfe von Social Engineering, besonders bei Soldaten in Uniform auf dem Weg nach Hause.

Marine Vizeadmiral Kaack: "Unsere Bewertung: Man testet uns. Man versucht, unsere Gesellschaft zu verunsichern, gesamtstaatlich und im Bündnis. Und man schafft womöglich die Grundlage für spätere aktive militärische Aktivitäten".

Und wieder einmal – ein Wächter spioniert

Immer wieder erlebt **FM-nospy**, dass Mitarbeiter von Sicherheits- und Wartungsdiensten angeworben werden, um sich als Amateurspione zu versuchen. Nachts auf Streife gehend oder Wartungsarbeiten vornehmend und oft mit allen wichtigen Schlüsseln versehen, wird fotografiert, gesucht und gestohlen.

Dabei sind die uns Amateurspione mehrfach auf videoüberwachte Honey-Pots hereingefallen, weshalb wir ihre Motivation auszuspionieren (Geld), kennen.

Unsere Erfolge ändern nichts daran, dass diese Schwachstelle im Sicherheitsgefüge vieler Unternehmen weiter bestehen bleibt.

Zumal inzwischen immer öfter vorab via Social Engineering ausgespähte Menschen mit finanziellen oder anderen Problemen durch (russische?) Spezialisten als eine Art "Wegwerfspione" gezielt angesprochen und angeworben werden.



Verstärkt Desinformation als Sabotage via Social Media

In den letzten Monaten nehmen in den gängigen Sozialen Medien professionell gestaltete Desinformationskampagnen massiv zu!

Fachleute sprechen von einem Fake-News-Anteil (z.B. bei Facebook, X oder Instagram, sowie TikTok) von über 70% aller Beiträge.

Abgesehen von "Posts", die mit Hilfe von Falschmeldungen "nur" auf eine Werbeseite locken oder von Wichtigtuern, die auf der Suche nach Klicks sind, tauchen vermehrt gute gemachte, nicht selten mit AI-gefälschten Originalstimmen versehene "Aussagen Betroffener" auf, die sich (z.B.) über angeblich erlebte Mängel beim Service oder den Produkten eines Unternehmens auslassen.

Diese meist in einem regelrechten Schwarm scheinbar unterschiedlicher Absender auftretenden "FakeNews-Varianten" haben offensichtlich den Zweck, die Reputation von Personen, Parteien, Unternehmen oder deren Produkten zu beschädigen.

Für Betroffene jedwelcher Art bedeutet dies, im Ernstfall sehr schnell reagieren zu müssen, was nur durch speziell dafür beauftragte Spezialisten (intern oder extern) möglich ist. Diese Experten sollten (zusammen mit dem PR-Bereich) direkt an die Geschäftsleitung berichten und gegebenenfalls augenblicklich gemeinsame Termine einberufen können. Für Gegenreaktionen sind nämlich oft nur Minuten Zeit ...

Eine Spielzeugdrohne reicht völlig!

Speziell an Wochenenden sind in vielen Gegenden Hobbypiloten kleiner, nicht kommerzieller Drohnen unterwegs. Obwohl mit professionellen Fluggeräten nicht vergleichbar, reichen die Kameras dieser Spielzeuge durchaus, um Lagerplätze, Lüftungsfenster, Feuertreppen, Zaunlücken und mehr zu fotografieren, die ansonsten von außerhalb des Firmengeländes her schlecht einsehbar sind.

Sowohl Spionage als auch Diebstahl wird auf diese Weise sehr effektiv vorbereitet.

Wie professionell man gegen diese Gefahren vorgehen kann, hängt vom Einzelfall (und im Extremfall leider auch vom verfügbaren Budget für Abwehrtechnik) ab.

FM-nospy ist eines der wenigen Unternehmen in Europa, die sich im Rahmen des Informationsschutzes explizit auf Abwehr von "Social-Engineering" als meist verwendetes Werkzeug bei Wirtschafts- und Industriespionage spezialisiert haben.

Das umfangreiche Know-How und die Erfahrung seiner Spezialisten bietet eine geschätzte Komponente im Bestreben von Management, Security und Compliance, präventiv zu handeln.

Verantwortlich für den Inhalt: Fred Oppl-Maró / FM-nospy.

Disclaimer: Wenn Sie diesen, etwa vierteljährlich erscheinenden Newsletter nicht mehr zugesandt haben möchten, so bitten wir um kurze Nachricht an info@fm-nospy.com