Newsletter 03/2023

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

in der Hoffnung, Sie alle wohlauf vorzufinden, melden wir uns zum dritten Mal in diesem Jahr mit Wissenswertem und Interessantem aus der Welt der Wirtschafts- und Industriespionage.
Immer häufiger geht es dabei weniger um das direkte Stehlen von hoch vertraulichen "Kronjuwelen". Vieles deutet darauf hin, dass vermehrt Mitarbeiter mit Inselwissen gezielt abgeworben werden. Auch dies ist (indirekt) eine sehr erfolgreiche Form der Spionage.
Ungeachtet davon wird Sabotage zum immer häufiger eingesetzten Mittel, um Lieferprozesse zu stören oder gezielt die Reputation von, als verlässlich bekannten, Lieferanten zu beschädigen (wir warnen permanent davor). Letzteres steht nicht selten in Zusammenhang zu gleichzeitig auftretenden Desinformationen über Social-Media.

Viel Spaß beim Lesen!
Ihr Team von **FM-nøspy**

Dolmetscher und Übersetzungsbüros als Spionageziele

Nicht nur das US-Militär ist aktuell von Angriffen auf diese Zielgruppe betroffen. Mehrere Europäische Unternehmen erkennen, dass ihre vertraulichen Informationen wahrscheinlich auf Umwegen über "Sprachübersetzer" unterschiedlicher Art ausspioniert wurden. Diese Dienstleister (nicht selten "One-Man-Shows") sind oft im kurzzeitigen Besitz hoch vertraulicher Unterlagen, jedoch so gut wie nie auf die Gefahr vorbereitet, selbst Spionageziel zu sein.
FM-nøspy bietet seit langem die Möglichkeit an, für Sie Ihre externen Dienstleister hinsichtlich deren Sorgfalt im Umgang mit Vertraulichem zu prüfen und zu beraten. Erfahrungsgemäß wird diese Möglichkeiten von den meisten Dienstleistern begrüßt.

Die Ferien nahen – ideale Zeit für Ausspähung!

Jedes Jahr wieder sind die Ferienzeiten eine gute Gelegenheit zu spionieren. Schlecht eingearbeitete Urlaubsvertretungen und unklare Entscheidungsprozesse werden von angeblichen Kunden- oder Behördenvertretern per Telefon geschickt genutzt, um sich von Puzzlestein zu Puzzlestein dem eigentlichen Ziel zu nähern.

Das Wissen in den Köpfen …

… von Mitarbeitern, die (aus welchen Gründen auch immer) Unternehmen verlassen, stellt für Mitanbieter oft ein heiß begehrtes Spionageziel dar. Nicht nur im zivilen Bereich – auch im militärischen. So wirbt z.B. China in Europa Ex-Kampfpiloten als Trainer für eigene Piloten an, um taktische Vorgehensweisen zu schulen.

FM-nøspy ist als ein Unternehmen der FRED MARO Gruppe auf Prävention und Abwehr von Industriespionage spezialisiert
D-53703 Siegburg/Germany, Pf. 1303, www.fm-nospy.com / info@fm-nospy.com / +49-2241-1272-699

Und immer häufiger “Sabotage“

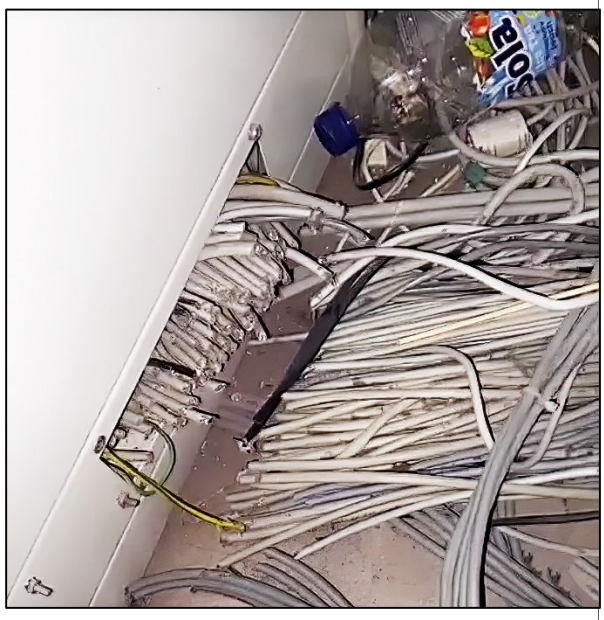
Dabei sind die Vorgehensweisen dieser beauftragten Spezialisten sehr unterschiedlich und werden als solche meist nicht erkannt. Nachfolgend einige Beispiele:

Chaos schafft ideale Rahmenbedingungen für Spionage
Offensichtliches internes “Durcheinander“ wird genutzt, um gezielt auszuspähen. Ob Büro-Umzüge, Wasserrohrbrüche, Fehlalarme, unklare Arbeitsprozesse oder organisatorisches Chaos im Unternehmen. All dies lässt sich hervorragend nutzen, um zu unerkannt stehlen und zu spionieren.

Kündigungsfristen laden zu Spionage ein!
Frustrierte oder mangelhaft arbeitende Mitarbeiter stellen ein bekanntes Spionage-Risiko dar. Letztere werden oft unter Einhaltung gesetzlicher Fristen gekündigt, wobei sie meist bis zu ihrem letzten Tag weiter arbeiten. Werden sie von der Arbeit freigestellt, so haben sie oft trotzdem noch länger freien Zugang zum Unternehmen.
Diese Schwachstelle ist eine regelrechte Einladung, um vorsorglich an Vertrauliches zu gelangen oder gezielt (Rache) zu sabotieren).

Der Besuch beim ehemaligen Arbeitgeber …
Wer freut sich nicht, wenn ehemalige langjährige, in Rente gegangene Kollegen wieder einmal am früheren Arbeitsplatz vorbei schauen? **FM-nøspy** stellte mehrfach bei Recherchen fest, dass es genau diese Besuche waren, während denen (z.T. hoch vertrauliches) Material entwendet oder Produktionsprozesse gestört wurden. Nicht selten als offensichtlicher “Auftragsjob“ und wahrscheinlich gegen gutes Geld.

Sabotage um Projekte zu verzögern …
Manchmal geben sich Angreifer gar nicht erst die Mühe, komplex zu sabotieren.
Brachiale Gewalt ist nicht selten einfacher und schneller anzuwenden.
Zum Beispiel auf ungesicherten Baustellen, bei Renovierungen (an Wochenenden in häufig nur fahrlässig gesicherten Räumen) oder während Firmenumzügen, wenn entweder herumstehende Umzugskisten gestohlen oder neue Räume einfach unter Wasser gesetzt werden. Die danach häufig nötigen Trocknungsarbeiten generieren genau das Chaos, das engagierte Spione so lieben …
Manchmal werden auch “nur“ einfach viele Kabel durchgeschnitten …



Das Informationsschutz Paket für kleine und mittelständische Unternehmen sowie Institutionen und Behörden

Das Thema:
Für viele mittelständische Unternehmen und Behörden stellt die Einrichtung eines erschwinglichen und zugleich professionellen Informationsschutzes eine ungewohnte Herausforderung dar. Während IT-Schutz noch planbar erscheint, ist nachhaltig wirkende Prävention bezüglich der Ausspähung über den Mitarbeiter (Social-Engineering) ein scheinbar zu komplexes und schwierig zu gestaltendes Projekt.
Dem ist jedoch NICHT so!

Die Lösung:
Vermehrten Anfragen mittelständischer Unternehmen und Behörden folgend, hat das Team von **FM-nøspy** ein erfolgreiches "Präventionspaket" zusammengestellt, das alle nötigen Kriterien - mit zeitlich und finanziell gut überschaubarem Aufwand - erfüllt.
Dieses Analyse-, Schulungs- und Beratungspaket umfasst folgende Komponenten:

- Eine intensive und umfassende erste Einschätzung des Schutzbedarfes
- Ein Workshop zur Definition, Evaluierung und Lokalisierung von "Kronjuwelen"
- Eine gemeinsame Ortsbegehung, um räumliche Gegebenheiten in Bezug auf eine Gefährdung durch unerwünschtes Eindringen beurteilen zu können
- Die Prüfung von Standardprozessen (z.B. Personal / Besucher / Reise / BCM / Evakuierung / Dienstleister / HomeOffice) hinsichtlich potentieller Schwachstellen
- Die Erstellung von maßgeschneiderten "Spielregeln" gegen Spionageangriffe
- Vier (4) Intensivschulungen für gefährdete Mitarbeitergruppen (max. 10 Teilnehmer pro Schulung, um optimale Nachhaltigkeit zu gewährleisten)
- Die Durchführung eines Wettbewerbes für Mitarbeiter, um die Suche nach weiteren Schwachstellen zu erleichtern und Sicherheitsbewusstsein zu stärken
- Auf Wunsch gerne Prüfung der unternehmensinternen IT in Bezug zu zeitaktuell modernem Schutz gegen Eindringen und Phishing (durch erfahrene Partner) *)

All dies zu vernünftigen Paketkosten*), die nicht höher liegen, als die einer Managementtagung oder kleinen Betriebsfeier.
Bitte nehmen Sie zu weiteren Details Kontakt mit uns auf.

*) IT-Prüfung nicht im Paketpreis enthalten.

FM-nøspy *ist eines der wenigen Unternehmen, die sich im Rahmen des Informationsschutzes explizit auf Abwehr von "Social-Engineering" spezialisiert haben. Das umfangreiche Know-How seiner Spezialisten bietet eine geschätzte Komponente im Bestreben von Management, Security und Compliance, präventiv zu handeln.*
Verantwortlich für den Inhalt: Fred Oppl-Maro / 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