Newsletter 02/2023

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

Meldungen aus unserem internationalen Netzwerk deuten darauf hin, dass Ausspähen (a) massiv zunimmt und dass (b) dabei angesichts gesteigerter Wachsamkeit in der IT verstärkt "klassische" Spionagemethoden Anwendung finden.

Dabei geht es längst nicht immer um "Kronjuwelen". Sabotage wird zum immer öfter eingesetzten Mittel, um Lieferprozesse zu stören oder um gezielt die Reputation von, als verlässlich bekannten, Lieferanten zu beschädigen. Letzteres steht oft in Verbindung mit gleichzeitig auftretenden Desinformationen über Social-Media-Plattformen.

FM-nøspy hat bereits reagiert und realisiert aktuell zahlreiche strukturierte Workshops mit dem Ziel, potentielle Schwachstellen für Sabotage zu lokalisieren und Maßnahmen zu definieren, um sich gegen eventuelle Angriffe zu wappnen.
Mehr dazu am Ende dieses Newsletters.

Unabhängig davon wie immer Neues und Interessantes aus der Welt der Wirtschafts- und Industriespionage …

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

Misstrauen beim Einsatz von TikTok und WhatsApp …

Wegen massiv zunehmender Sicherheitsbedenken müssen ab sofort die Mitarbeitenden der EU-Kommission die Social-Media-App TikTok auf ihren Dienstgeräten löschen. Zudem müsse die, zum chinesischen Bytedance-Konzern gehörende, Software bis zum 15. März von privaten Geräten entfernt werden, auf denen Apps der EU-Kommission genutzt werden.
Damit folgt die EU zahlreichen Behörden in Mitgliederstatten und den USA.
TikTok wird schon lange unzureichende Datensicherheit und ein Mangel an Schutz junger Nutzerinnen und Nutzer vorgeworfen. Befürchtet wird, dass der Staat China Zugriff auf Tiktok-Daten haben könnte.
Uns bekannte israelische Quellen bezeichnen TikTok (aber auch WhatsApp und einige andere Apps) als moderne Trojanische Pferde.

FM-nøspy entdeckt weitere potentielle russische Ausspäher

Erneut führten individuelle Beratungen durch **FM-nøspy** bei Klienten zu "näherem Hinsehen" bei Neueinstellungen in schützenswerten Unternehmensbereichen. Mit dem Ergebnis, dass in einem Fall ein neu angestellter, angeblich ukrainischer Staatsbürger offensichtlich nicht aus der Ukraine stammte, obwohl er echte Papiere besaß. Im zweiten Fall stimmte offensichtlich die Vita eines russischen IT-Spezialisten nicht. Da man beiden juristisch nichts vorwerfen konnte, trennte man sich vorsichtshalber.

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

Chaos schafft ideale Rahmenbedingungen für Spionage

Verstärkt werden wir zu Fällen gerufen, in denen offensichtliches internes "Durcheinander" genutzt wurde, um gezielt auszuspähen. In vielen Fällen sind dies unklare Arbeitsprozesse oder organisatorisches Chaos im Unternehmen.

Immer öfter jedoch auch kurzzeitige Konfusion, welche von Angreifern gezielt hervorgerufen wird. Diese Form der Sabotage wird oft gar nicht als solche erkannt. So steckt zum Beispiel hinter längst nicht jedem Fehlalarm eines Feuermelders eine technische Fehlfunktion …

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 oft freien Zugang zum Unternehmen.

Diese Schwachstelle ist nicht selten eine regelrechte Einladung, um Wichtiges auszuspionieren, zu stehlen oder gezielt (Rache) zu sabotieren).
Eine entsprechende Anpassung von Freistellungs- und Kündigungsprozeduren ist deshalb dringend anzuraten.

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 wurde. Nicht selten als offensichtlicher "Auftragsjob" und gegen gutes Geld.
Ohne die Personen allerdings in Flagranti zu ertappen, ist ein juristisch verwendbarer Nachweis nur sehr selten zu erbringen …

"Kronjuwelen-Workshops" durch (und mit) FM-nøspy

Die Gefahren, durch klassische "Vorfeld-Spionage" gezielten Angriffen ausgesetzt zu sein, nehmen nachweislich deutlich zu! Oft mit dramatischen Auswirkungen)

Es ist deshalb sehr sinnvoll, sich umgehend 2-4 Stunden mit relevanten Fachleuten Ihrerseits, sowie erfahrenen Spezialisten unsererseits zusammen zu setzen und eine strukturierte Analyse potentieller Schwachstellen im Unternehmen durchzuführen!

Nur so können etwaig sinnvolle Maßnahmen zu Prävention und Abwehr hinsichtlich Aufwand und Kosten in vernünftigem Rahmen evaluiert und geplant werden.

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

Das perfekte 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 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