Newsletter 01/2023

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

wir hoffen, dass Sie alle sind gut in das neue Jahr gestartet sind und drücken Ihnen alle verfügbaren Daumen für viel Erfolg und sichere Zeiten!

In unserem letzten Newsletter 2022 warnten wir, dass Angreifer angesichts gesteigerter IT-Wachsamkeit verstärkt auf "klassische" Spionagemethoden zurückgreifen. Weiterhin wiesen wir darauf hin, dass das Thema "Sabotage" merklich öfter im Fokus vorauslaufender Spionageaktivitäten steht, wie unser Sicherheitsnetzwerk berichtet.

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**

China wirbt frühere britische Kampfpiloten ab

Ehemalige britische Militärpiloten werden, Geheimdienstberichten zufolge, mit hohen Geldsummen nach China gelockt, um ihr Fachwissen an das chinesische Militär weiter zu geben. Insidern zufolge sollen bereits etwa 30 Briten dem Ruf Pekings gefolgt sein und das Angebot von umgerechnet bis zu € 275.000 Euro angenommen haben.

Die pensionierten Piloten sollen zeigen, wie westliche Militärflugzeuge und Piloten strategisch operieren. Informationen, die im Konfliktfall, beispielsweise bei einer Eskalation des Taiwan-Problems, von Bedeutung sein könnten.

Zahlreiche Verfassungsschutz Ämter in Europa warnen

Sie alle sehen klare Anzeichen für gesteigerte Aufklärungsversuche, übrigens nicht nur aus Russland.
Seit dessen Angriff auf die Ukraine ist deren Geheimdienst in Europa aktiver denn je! Die zunehmenden Aufklärungsversuche werden unter anderem durch die Festnahme einer ganzen Reihe mutmaßlicher Spione deutlich.
Weitere Länder mit registrierbarer Intensivierung ihrer Spionagetätigkeiten sind China und der Iran. Alle drei Staaten scheinen (neben militärischen Interessen) besonders an innovativen Unternehmen in den Bereichen Chemie, Pharma und Elektronik interessiert zu sein. Hierbei werden fast ausschließlich klassische Social-Engineering-Methoden eingesetzt.

Einbruch + Diebstahl im Winterurlaub

Zurück von der Schipiste bemerkte die Projektleiterin eines Pharma Unternehmens, dass während ihres Schitages jemand ihrem Quartier einen Besuch abgestattet hatte. Gestohlen waren Schmuck, sowie ihr Laptop und Papiere mit Projektdetails.
Letztere hatte sie mitgenommen, um auch in den Urlaubstagen daran arbeiten zu können. Der (echte) Schmuck wurde übrigens vor der Pension auf der Terrasse wiedergefunden …

Geschulte Mitarbeiter verhindern Spionageangriff

So böse Spionageaktivitäten auch sind, uns freut es jedes Mal, wenn von uns geschulte Mitarbeiter anschließend irgendwann Ausspähungsversuche erfolgreich verhindern. So geschehen in Bayern, als eine Schulungsteilnehmerin zwei, in Produktionsanlagen herum spazierende, gut gekleidete Unbekannte ansprach und sich nicht von deren Ausreden täuschen ließ. Bevor sie Alarm schlagen konnte, verließen beide im Laufschritt fluchtartig das Haus. Später wurde klar, das zwei Büros offensichtlich bereits “besucht“ worden waren.

Kennen Sie Ihre Chatpartner wirklich?

Zum wiederholten Mal stellt sich (fast immer leider zu spät) heraus, dass (angeblich hoch qualifizierte und bekannte) Chatpartner-Innen gar nicht existieren. In allen Fällen tauschten sich Wissenschaftler in Internet-Fachforen mit angeblichen “Kollegen“ über sensible Themen aus, deren Details unternehmensintern oft hoch vertraulich waren.

Das Tückische bei derartigem Austausch: Während in einem direktem Gespräch Auge in Auge mangelnde Fachkenntnis eines Spions schnell auffallen würde, ist dies über den Internet-Chat kaum zu bemerken.
Der Ausspäher selbst ist da nur schreibend aktiv. Fehlendes Fachwissen und Fachterminologie kommen meist Kundigen, die unmittelbar neben ihm sitzten …

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

Gefahren, durch klassische “Vorfeld-Spionage“ gezielten Angriffen (oft mit dramatischen Auswirkungen) ausgesetzt zu sein, nehmen nachweislich deutlich zu!

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