Newsletter 01/2025

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

in diesen mehr als „unruhigen“ Zeiten warnen so gut wie alle relevanten Behörden vor einem massiven Anstieg von Spionage und Sabotage.

FM-nøspy warnt in seinen Newslettern seit etwa 3 Jahren immer wieder vor dieser, von uns schon lange als kritisch eingeschätzten, inzwischen als sehr hoch einzustufenden Gefahr für Unternehmen aller Größen und Branchen.

Die (wohl in der Mehrzahl aus dem russischen Umfeld) kommenden Angriffsversuche laufen längst nicht mehr nur über die, immer zuerst verdächtigten Wege der IT.
Seit Längerem bemerken wir international eine verstärkte Rückkehr zu klassischen “guten alten“ Wegen des Ausspähens.
Vom Ausnützen von Flüchtlingsströmen, um Menschen mit gesuchten Kompetenzen in Unternehmen einzuschleusen, über das verdeckte Eindringen in Gebäude, bis hin zum Anwerben frustrierter oder von Kündigung bedrohter Mitarbeiter.

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

Ihr Team von **FM-nøspy**

Praktisch jede Sabotage erfordert vorab ein Ausspähen!

Symbolisch gesagt: Wenn Sie planen, ein Kabel durchzuschneiden, so müssen Sie zuerst herausfinden, wo es liegt, wie Sie herankommen und (nicht zuletzt) wie Sie unentdeckt wieder verschwinden können …
Vor Allem wenn nicht die IT selbst das Ziel ist, so ist dieses Ausforschen beinahe immer nur mit Techniken des “Social Engineerings“ erfolgreich.
Für die Angreifer sind diese Spionageergebnisse extrem wichtig, da es oft nur eine einzige, zeitlich begrenzte Chance zum Erfolg gibt.
Die Auswirkungen von gezielter Sabotage sind für die Betroffenen meist dramatisch, sehr teuer und nicht selten existenzgefährdend!

~~Sehr hohes Risiko für sensible Projektgruppen!~~

~~Erstaunlicherweise sind die meisten Unternehmen genau hier sehr nachlässig und fahrlässig. Ob Gespräche innerhalb Projektgruppen, die hoch vertrauliche Entwicklungen betreffen oder im militärischen Bereich; jedes Mal belegen erfolgreiche Angriffe fahrlässiges Ignorieren grundlegender Sicherheitsregeln durch “Türöffner“.~~
~~Nachfolgend ein, vielen bereits bekanntes Beispiel.~~

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

Reputationsschädigung als nachhaltig wirkende Sabotage:

Nur wenige Unternehmen sind sich bewusst, dass es ein Leichtes ist, ihre Reputation und Ihre Produkte mit Hilfe gekonnter Desinformation nachhaltig zu schädigen.
Im Gegensatz zu "normaler Sabotage" ist hierbei nicht einmal vorausgehendes umfangreiches Spionieren nötig.

Ein aktuelles Beispiel: Russland hebt aktuell in den USA strategische Desinformation auf ein neues Level: "Narrative" nennen Forscher diese durchgeplanten Kampagnen des Kreml. Dieser überschwemmt soziale Netzwerke mithilfe von KI(AI), durch Schauspieler und bezahlte Influencer mit engeblichen Stories und Erlebnissen scheinbar Betroffener..
Zwei Tage nach der US-Wahl beobachten Social-Engineering-Profis, wie ein sehr prominenter "Fan" Trumps ein Video mit seinen 1,1 Millionen Followern auf X teilt. Es zeigt ukrainische Uniformierte, die auf einen Dummy mit roter "Make America Great Again"-Kappe schießen und ihn anzünden. "Wir finanzieren keine Kriege in Ländern mehr, die Amerikaner hassen", steht dabei.
Das Video ist belegbar eine Fälschung, wie das Zentrums für Medienforensik an der Clemson University darstellt. Trotzdem wurde es bis Anfang November mehr als 30 Millionen Mal angesehen.
Seit zwei Jahren ist zu beobachten, wie Moskau mit solchen, "Narrative" bildenden Inhalten die Unterstützung für den Verteidigungskrieg der Ukraine gegen Russland zu untergraben versucht. Nachdem Grundsatz "steter Tropfen höhlt den Stein" …
Es ist ein konstanter Strom durch hunderte beauftragte (auch amerikanische, vom FBI beobachtete!) bezahlte Trolls und Influencer.
Hier aus dem Feld der Politik, jedoch jederzeit auf die Wirtschaft transferierbar.
Es ist eine Kleinigkeit, dieses Prinzip auf Unternehmen oder Produktgruppen umzumünzen. Zuletzt erlebbar bei zahlreichen Initiativen, Impfstoffe zu diskreditieren.

- 3 -

~~Erste AI-DeepFakes tauchen in Videokonferenzen auf!~~

- ~~Aus dem Urlaub klinkt sich ein leitender Mitarbeiter in einen Video-RoundTable seiner wichtigsten Projektgruppe ein. Unscharfes Bild und Sprachstörungen begründet er mit schwachem Internet im Hotel, weshalb er in der Hauptsache "nur zuhörte" und sich nach 20 Minuten verabschiedete …~~
  ~~Anmerkung: Realtime-Fake von Gesicht und Stimme machten es möglich. Die echte Führungskraft saß zu dieser Zeit irgendwo in einer Sauna.~~

- ~~Ein auf Reisen befindlicher Vorstand kündigt an einem Samstag Nachmittag(!) per Telefon seiner Assistentin für Montag den Anruf eines wichtigen Kunden an, der ein bestimmtes vertrauliches Dokument benötigen würde.~~
  ~~Sowohl die Stimme des Vorstandes als auch die des "Kunden", sowie die Telefonnummern beider waren sehr gut gefälscht … Angriff erfolgreich!~~

- 3 –

Security Schulungen von FM-nøspy unter den meistgebuchten

Wir freuen uns, berichten zu können, dass nach Auskunft mehrerer Fachverbände unsere Beratungen und Schulungen zum Themenfeld "Erkennen und Abwehr von Social Engineering" europaweit zu den meist gebuchten zählen.

Mit ein Grund dafür dürfte sein, dass diese Beratungen extrem realitätsgerecht und die Schulungen zielgruppen-spezifisch ungewöhnlich gestaltet sind (und damit hohen Aufmerksamkeits- und Erinnerungswert besitzen).
Spezielle Aktivitäten zur Generierung von Nachhaltigkeit der "Awareness" ergänzen die erlebnisreichen Stunden.

FM-nøspy *ist eines der wenigen Unternehmen in Europa, die sich im Rahmen des Informationsschutzes explizit auf Abwehr von "Social-Engineering" 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-Maro / FM-nøspy.

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