Newsletter 03/2024

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

Russische Profis und Deutsche Generäle …

Noch ist nicht komplett aufgeklärt, was wer und wie falsch gemacht hat. Tatsache ist, dass Russland genüsslich eine halbstündige Diskussion von mehreren Deutschen Generälen im russischen TV präsentiert, in der mehr als kritische, hoch vertrauliche Details zum Ukraine Krieg ausgetauscht werden.
Experten bezeichnen den Mitschnitt als zu 99% authentisch. Was die Frage aufwirft, wie ignorant und unglaublich fahrlässig die Diskussionsteilnehmer gegenüber grundlegenden Sicherheitsregeln gewesen sein mussten.
Wissend(?), dass sie allein von ihrer beruflichen Position her mit Sicherheit im Visier hoch professioneller Spione stehen. Anstatt sich VOR entsprechenden Gesprächen mit, sicher vorhandenen internen Abwehrprofis in Verbindung zu setzen, sind sie naiv in eine, wahrscheinlich relativ einfach gestaltete, Abhörfalle gelaufen.

Ein gutes Abendessen reicht

Während der CFO eines Unternehmens mit Kunden gemütlich zu Abend isst, wurde der, in seinem Hotelzimmer verbleibende Laptop offensichtlich ausgelesen. Weitere Erkenntnisse deuten darauf hin, dass Telefonate abgehört wurden, die der CFO von seinem Hotelzimmer aus geführt hatte.
Auch dies sind häufig anzutreffende Beispiele von Ignoranz gegenüber, leider inzwischen allgegenwärtigen, Gefahren. Für Profis gibt es ein Dutzend Wege, in praktisch jedes Hotelzimmer zu gelangen. Genauso wie es für sie kein Problem, ist, einen Laptop auszulesen, auf dem wahrscheinlich Vertrauliches gelagert ist. Und wenn es "nur" Telefonnummern, Besprechungstermine und Konferenz-Einwahldaten sind.
Die (wahrscheinlich 2) Spione hatten es einfach! Während der Eine mit im Restaurant am Nebentisch saß und dem Kollegen meldete, wenn das Opfer seine Rechnung beglich, hatte der Gewarnte jede Menge Zeit, in aller Ruhe zu agieren.
Derartige oder ähnlich gelagerte Fälle werden meist erst (wenn überhaupt) Tage oder Wochen nach den Angriffen aufgedeckt. Weil der Laptop versagt oder Andere offensichtlich Details wissen, die sie nur so in Erfahrung gebracht haben können.
Was rein rechtlich meist nicht zu belegen ist …

"Perfektes" Ausspähen führt zu dramatischer Sabotage

Welch böse Auswirkungen erfolgreiches Spionieren, verbunden mit einem, erst dadurch möglichen, perfiden Sabotageplan haben kann, zeigt der erfolgreiche Angriff Israels auf Hamas.
Ein 2-Jahrsprojekt, das ähnlich durchaus auch in ziviler Wirtschaftssabotage erfolgreich sein könnte. Es wäre naiv zu glauben, dass hier nicht schon erste Blaupausen irgendwo in Arbeit sind …

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

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