Newsletter 02/2025

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 leider als sehr hoch einzustufenden Gefahr für Unternehmen aller Größen und Branchen.

Die (wohl im Moment 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.
Auch das Anwerben von "heimatfreundlichen" Menschen mit doppelten Staatsbürgerschaften nimmt zu.

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 …
Ebenso symbolisch gemeint: Wenn Sie eine Person bestechen oder erpressen möchten, damit sie Geheimnisse preis gibt oder an einem Betrug teilnimmt, so müssen Sie zu allererst herausfinden, ob diese Person überhaupt "mitspielen" würde.

Vor Allem wenn nicht die IT selbst das Ziel ist, so ist dieses "Herausfinden" (Ausforschen) beinahe immer nur mit Hilfe von “Social-Engineering-Techniken“ erfolgversprechend.
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!

Webseiten für Cybercrime-Dienstleistungen abgeschaltet

Deutsche Ermittler schalten mit "nulled.to" und "cracked.io" zwei Webseiten für Cybercrime-Dienstleistungen ab und nehmen im Rahmen einer internationalen Razzia mehrere Personen fest.
Auf den beiden Webseiten wurden weltweit Cybercrime-Dienstleistungen wie etwa Programme und Aufträge für Hackerangriffe gehandelt. Beide Seiten hatten demnach etwa zehn Millionen Nutzer.
An dem Schlag gegen die mutmaßlichen Betreiber waren Strafverfolger aus den USA, Australien, Spanien, Griechenland, Rumänien, Italien und Frankreich beteiligt.
Insgesamt wurden bei sieben Durchsuchungen 67 Geräte beschlagnahmt, darunter 17 Server.

Bauschaum im Auspuffrohr

Deutsche Sicherheitsbehörden machen Russland für eine Sabotageserie verantwortlich, bei der bundesweit Hunderte Autos beschädigt wurden. Dabei wurden mehr als 270 Fahrzeuge in Baden-Württemberg, Berlin, Brandenburg und Bayern Ziel der Attacken. An den Tatorten hinterließen die Saboteure Aufkleber mit dem Slogan "Sei grüner!" und einem Foto von Bundeswirtschaftsminister Robert Habeck.
Der Verdacht fiel zunächst auf radikale Klimaaktivisten. Inzwischen gehen die Behörden jedoch von einem anderen Hintergrund aus: Bei einer Polizeikontrolle im brandenburgischen Schönefeld waren im Dezember in der Nähe eines Tatorts drei Verdächtige aus Süddeutschland festgestellt worden, ein Serbe, ein Bosnier und ein Deutscher. Bei Wohnungsdurchsuchungen stellten die Ermittler später mehrere Dosen mit Bauschaum sowie Handys und Laptops sicher.
Erste Geständnisse, für diesen Versuch von Wahlmanipulation "angeworben worden zu sein", folgten … die Spur führt nach Russland.

Vermehrt Social Engineering Angriffe auf sensible Projektgruppen!

Ob Gespräche innerhalb vertraulicher Projektgruppen oder im militärischen Bereich; jedes Mal belegen erfolgreiche Angriffe fahrlässiges Ignorieren grundlegender Sicherheitsregeln durch “Türöffner“. Nachfolgend ein aktuelles Beispiel.

Während einer hoch vertraulichen Videokonferenz einer Projektgruppe schaltet sich der CEO von seinem Urlaubsort aus ein, um zu sehen "was seine Lieblingsprojektgruppe so treibt". Schlechte Bild- und Tonqualität entschuldigt er mit schwachem Internet im Urlaubsort. Später stellt sich heraus, dass die Teilnehmer einem AI-generierten "Avartar" aufgesessen sind, der nicht nur das Gesicht, sondern auch den seltenen Akzent des Originals perfekt imitierte – und der 30 Minuten lang Geheimnisse erfuhr. Nachforschungen deuten auch hier auf einen russischen Angriff hin …

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 Niveau:
"Narrative" nennen Forscher diese durchgeplanten Kampagnen des Kreml. Dieser überschwemmt soziale Netzwerke mithilfe von KI(AI), sowie durch Schauspieler und bezahlte Influencer mit angeblichen 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 eine Puppe mit roter "Make America Great Again"-Kappe schießen und sie 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 Desinformationsprinzip auf Unternehmen oder Produktgruppen umzumünzen. Zuletzt z.B. bei zahlreichen Initiativen erlebbar, die Impfstoffe diskreditierten oder Personen des öffentlichen Lebens mit Bergen von "FakeNews" zahlreicher "User" zu kompromittieren versuchten.

Unser Tipps:

- Organisieren Sie umgehend ein Workshop mit Fachleuten, welche mögliche Angriffsszenarien analysieren und Gegenstrategien erarbeiten.
- Intensivieren Sie Ihre Präsenz im Internet, um im Ernstfall nicht Zeit zu verlieren, sich erst bekannt machen zu müssen.

***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