Newsletter 01/2024

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

in der Hoffnung, Sie gesund und munter vorzufinden, melden wir uns zum ersten Mal in diesem Jahr, wieder mit Wissenswertem und Interessantem aus der Welt der Wirtschafts- und Industriespionage.
Der Trend zu Sabotage setzt sich fort. Sei es durch direktes Beschädigen von produktionsrelevanten Komponenten als auch mittels gezielter Rufschädigung durch bezahlte “Internet-Trolle“, welche das Netz mit entsprechenden Fake News fluten.
Auch das gezielten Abwerben von Mitarbeitern mit seltenen Inselkompetenzen ist eine Form der Sabotage.
Dazu kommen völlig neue Gefahren durch eine, sich rasend schnell erweiternde und immer effektiver agierende Szene im Themenfeld “künstliche Intelligenz“ (A/ bzw. KI).

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

Angebohrte Leitungen

Offenbar gibt es Versuche, den Bau der Pipeline "ETL 180" in Schleswig-Holstein zu stören. So wurde die Gasleitung an mindestens acht Stellen angebohrt, verteilt über 1 KM Länge. Die dazu verwendete (nötige) Verwendung von Spezialbohrern deutet auf beauftragte Profis hin.
Nach vorläufigen Schätzungen entstand ein Schaden von mindestens 1,6 Mio. Euro. Wer dahinter steckt, ist bisher nicht bekannt.
Für von derartiger Sabotage bedrohte Unternehmen bedeutet dies, sensible Leitungen schon während des Baus permanent im Auge zu behalten, da (z.B. nach “Zubauen“ von Leitungsabschnitten) Reparaturen extrem aufwändig werden können.

Vermehrt Angriffe mit Venusfallen

Dass Russland versucht, mittels Lockvögeln über Internetkanäle und Plattformen Ukrainische Soldaten auszufragen, ist inzwischen gut bekannt und beobachtet.
Zahlreiche Hinweise zeigen jedoch, dass dies inzwischen auch bei Mitarbeitern europäischer Ziel-Unternehmen verstärkt der Fall ist.

Menschen mit von Russland gesuchtem Wissen, sowie unzufriedene Mitarbeiter werden gezielt über gängige Plattformen kontaktiert.
Letztere, indem man offen-sichtlich Kommentare zu veröffentlichten Posts mitliest, die extra dafür ins Netz gestellt werden.
Die “Damen“ agieren mit gefälschten Fotos und oft mit dem Argument, in den Westen flüchten zu wollen. Schon bald schließen sich Video-Chats an, bei denen inzwischen KI immer ausgefeilter eingesetzt wird. Gesichter werden hierbei ebenso (live!) gefälscht, wie Stimmen und Geräusche. Finales Ziel ist es meist, an firmeninterne Informationen heran zu kommen.

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

Die Optimierung von KI-Software immer schneller …

Obwohl KI-generierte Informationen meist immer noch an, relativ leicht erkennbaren Fehlern erkennbar sind, sind diese Desinformationen immer erfolgreicher. Mit ein Grund ist die kurze Aufmerksamkeitsspanne vieler Menschen. Ein Bild (ein Videoclip) wird oft nur 3-5 Sekunden betrachtet, bevor weitergeblättert wird – ohne das Gesehene auf Sinnhaftigkeit zu überprüfen. Für einen "Abdruck im Gehirn" reicht dies.

Die Lernfähigkeit der Programme wird dabei rasend schnell besser.
Nachfolgend ein Bild aus 2022 und (rechts daneben) eines aus 2023 – beide mit demselben "Prompt" (Befehl an das Programm) gestartet..

Gleichzeitig wird das zeitnahe Überprüfen der Informationen (Bilder/Videos/Texte) immer schwieriger. Inzwischen schießen "Fakt Checker"-Unternehmen wie Pilze aus dem Boden. Sie auch als Unternehmen zu beauftragen, ist oftmals sehr sinnvoll.

KI und die Zugangsdaten von Videokonferenzen …

Wir kennen erste geglückte(!) Fälle auf, bei denen sich unbekannte Externe mit Hilfe von KI-gesteuerten Kopien bekannter leitender, sich auf Reisen befindlicher Mitarbeiter in Videokonferenzen eingeloggt haben. Ausreichend Rohmaterial vorausgesetzt, ist es immer einfacher möglich, kopierte Köpfe mit Oberkörpern und täuschend ähnlichen Stimmen (einschließlich Betonung und Akzent) in Echtzeit(!) agieren zu lassen.
Eventuelles Ruckeln von Bild und Ton wurde in den bekannten Fällen mit "schlechter Internetverbindung im Hotel" begründet und von den Anderen akzeptiert.

Security Schulungen von FM-nøspy unter den meistgebuchten

Wir freuen uns, berichten zu können, dass nach Auskunft mehrerer Fachverbände unsere Schulungen zum Themenfeld “Erkennen und Abwehr von Social Engineering“ europaweit zu den meist gebuchten zählen.
Mit ein Grund dürfte sein, dass diese 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.

Dolmetscher und Übersetzungsbüros als Spionageziele

Nicht nur das US-Militär ist aktuell von Angriffen auf diese Zielgruppe betroffen. Mehrere Europäische Unternehmen erkennen, dass ihre vertraulichen Informationen wahrscheinlich auf Umwegen über “Sprachübersetzer“ unterschiedlicher Art ausspioniert wurden. Diese Dienstleister (nicht selten “One-Man-Shows“) sind oft im kurzzeitigen Besitz hoch vertraulicher Unterlagen, jedoch so gut wie nie auf die Gefahr vorbereitet, selbst Spionageziel zu sein.
FM-nøspy bietet seit langem die Möglichkeit an, für Sie Ihre externen Dienstleister hinsichtlich deren Sorgfalt im Umgang mit Vertraulichem zu prüfen und zu beraten. Erfahrungsgemäß wird diese Möglichkeiten von den meisten Dienstleistern begrüßt.

ChatGPT durch leichtsinnige Anwender eine Gefahr?

Der (inzwischen nicht mehr ganz so beliebte) Textroboter mit künstlicher Intelligenz könnte möglicherweise durch leichtsinnige Anwender schnell zum Lieferant vertraulicher Informationen werden.
Mehrfach haben Anwender für Auftragstexte hoch vertrauliche Informationen an die Software übermittelt. Dies obwohl noch nicht geklärt ist, ob und wo bei ChatGPT möglicherweise potentiell einfache Möglichkeiten eines Zugriffs bestehen.
Deshalb haben bereits mehrere Unternehmen die dienstliche Verwendung dieser Textsoftware strikt untersagt.
Ungeklärt ist bisher übrigens auch, wie man vertrauliche Texte generell gegen Abgreifen durch ChatGPT oder vergleichbare Software schützen könnte.

***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 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