Newsletter 01/2022

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

eine nicht zu enden scheinende Pandemie, verbunden mit immer wieder neuen Regelungen, sowie massiven Ausfällen von Mitarbeitern durch Omikron, schaffen für Industriespionage fast perfekte Rahmenbedingungen.
Ein Lichtblick ist in diesem Zusammenhang jedoch, dass das Interesse an aktivem Schutz sensibler Informationen inzwischen deutlich zunimmt.
FM-nøspy berät inzwischen europaweit und in unterschiedlichsten Varianten.

Nachfolgend (wie immer) Interessantes aus der Welt der Industriespionage.
Viel Spaß beim Lesen.

Ihr Fred Maro + Team

Massive Zunahme von Social Engineering am Jahresende

FM-nøspy erhielt Anfang Januar 2022 mehrere Berichte über massive Versuche, Hotlines und HomeOffices mit Hilfe von Social Engineering Techniken zu überlisten.
Spionierende nützen gerne Zeiten von Urlaubs- oder Krankheitsvertretungen, sowie mangelhafte Jobübergaben. All dies war zwischen Weihnachten und den ersten Januartagen reichlich vorzufinden.
In allen, die für die Spionierenden erfolgreichen Fällen, waren die Ansprechpartner nicht(!) auf diese Form des Ausspähens vorbereitet und wurden ausgetrickst…

Olympiade in China steigert den Verkauf von Smartphones …

Zumindest bei immer mehr Nationalmannschaften und deren Funktionären.
Eine erhebliche Zahl der teilnehmenden Länder bittet die Mitglieder ihrer Olympiamannschaften, private Smartphones, Tabletts und Laptops zu Hause zu lassen. Gleichzeitig werden den Sportlern alternativ neu gekaufte Geräte als Ersatz gratis angeboten, die nach der Olympiade vernichtet werden sollen.
Grund dieser ungewöhnlichen Aktivitäten sind deutliche Indikatoren dafür, dass die Gefahren, über Smartphones, Tabletts und Laptops von staatlicher Seite her ausgelesen zu werden, während des Aufenthaltes in China zunehmen werden.

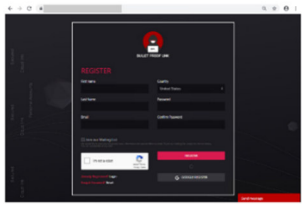
Versuche von Bestechung im Themenfeld Spionage nehmen zu

Versuche, Geheimnisträger durch Angebote relativ hoher Geldbeträge zu verleiten, Vertrauliches einzusammeln und weiter zu reichen, scheinen zuzunehmen.
In uns bekannten Fällen geschah dies zum Beispiel in Unternehmen, welche (pandemiebedingt) Projekte temporär stoppten und dabei involvierte Berater in Wartepositionen versetzten.

Der “Cyber War“ im zivilen Bereich nimmt zu …

Nicht nur der Staat Ukraine wurde vor Kurzem Opfer eines massiven, gezielten Internet Angriffs auf seine Webseiten und seine staatliche IT-Infrastruktur. Dabei wurden umfangreiche Daten gezielt zerstört.
Ähnliches erfahren wir auch aus anderen Ländern. Betroffen sind fast immer Unternehmen aller Größen, in denen entweder innovativ Produkte entwickelt werden oder die sich in wichtigen Verhandlungen befinden. Jedes Mal wurden Daten und IT-Systeme offensichtlich mit dem Zweck zerstört, die angegriffenen Unternehmen möglichst lange zu lähmen oder auszuschalten.
Hier ging es also nicht um Erpressung, sondern um gezielte Cyber-Sabotage, zu der es auf dem Markt inzwischen sogar erste konkrete Offerten von Anbietern gibt …

Phishing Anbieter mit hidden Agenda …



Die tagtägliche E-Mail-Spam Flut ist nicht nur unglaublich lästig, sie ist bekannterweise auch gefährlich.
Nun hat Microsoft ein kriminelles Netzwerk entdeckt, das unter dem Deckmantel eines “beliebten“ Anbieters von Phishing-Dienstleistungen steckt.
“BulletProofLink“ vertreibt nicht nur Phishing-Kits für Jedermann und bietet Phishing als Dienstleistungs-Komplettpaket an. Die Kriminellen hinter dem Unternehmen verkaufen erbeuteten Daten an Dritte und nutzen sie zusätzlich für die Erpressung der Phishing Opfer.
Auch wenn die Gangster ihren Phishing-Dienst ganz offen vermarkten, konnten sie bisher nicht gestoppt werden. Sie sind in der Lage, beliebig viele Subdomains mit eindeutigen Adressen zu erzeugen und fallen so durch übliche Erkennungsmethoden, die auf der exakten Übereinstimmung von Domains und URLs beruhen.

FM-nøspy berät und schult auch in Pandemiezeiten!

Ähnlich wie es Viren immer wieder schaffen, selbst gut gesicherte menschliche Körper auszutricksen, suchen beauftragte Spionierende Schwachstellen zu nutzen, die es ohne diese konfusen Zeiten so wahrscheinlich nicht geben würde. Hierbei mangelt es den Angreifern nicht an Ideen.
Gefragt ist somit Erfahrung und Wissen um aktuelle Trends und Methoden der Angreifer. Aus diesem Grund beraten und schulen wir auch in Zeiten der HomeOffices, verschlossenen Büros und konfusen Kommunikationswegen.
Ob bei Ihnen vor Ort oder online … wir sind für Sie da!
Auf der Folgeseite erfahren Sie Details zu unserem, auch in diesen “spannenden Zeiten“ viel gefragten Unterstützungspaket.

Das ideale Schutzpaket für kleine + mittelständische Unternehmen sowie Institutionen und Behörden

Das Thema:
Für viele mittelständische Unternehmen und Behörden stellt die Einrichtung eines erschwinglichen und zugleich professionellen Informationsschutzes eine 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 Paket 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 / Einkauf / Reise / Evakuierung / BCM / Dienstleister) 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 (durch erfahrene Partner) Prüfung der unternehmensinternen IT in Bezug zu zeitaktuell modernem Schutz gegen Eindringen und Phishing *)

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. **) zuzüglich der Reisekosten, sowie der ges. USt.

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.

D-53703 Siegburg/Germany, Pf. 1303, www.fm-nospy.com / info@fm-nospy.com / +49-2241-1272-699