Newsletter 03/2022

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

im Themenfeld der Ausspähung nutzen Angreifer bevorzugt Situationen aus, in denen plötzlich Chaos herrscht. War dies lange Zeit die Pandemie, so sind es jetzt volatile Zeiten, verursacht durch den Russischen Angriff auf die Ukraine.
Was selten bedacht wird ist, dass besonders in Kriegszeiten beauftragte Teams versuchen, im Chaos unterschiedlichste Vorteile zu erringen. Nicht zuletzt auch im Bereich der Wirtschaftsspionage.

Nachfolgend zum dritten Mal in diesem Jahr Aktuelles aus dieser Schattenwelt.

Viel “Spass“ beim Lesen

Ihr Team von FM-nospy

Warnungen vor gezielten IT-Angriffen auf Energieversorger

Waren derartige Attacken wegen ihrer Komplexität bisher eher “Superspezialisten“ vorbehalten, so gibt es seit Neuem einen Malware-Baukasten im Netz, dessen Handhabung es auch weniger IT-kompetenten Akteuren ermöglicht, gezielt Versorger anzugreifen. Der Baukasten erhielt den Namen “Pipedream“. *Quelle: Dragos/USA*

Da hierbei auch Komponenten angegriffen werden, die in vielen Produktionsanlagen verwendet werden, sind deutlich mehr Unternehmen gefährdet als nur Energie-versorger.

Entwicklung bei Dronen macht Sorgen

Der Trend zu Miniaturisierung in der Technologie weist auf neue Spionagegefahren hin. So wurden auf einem US-Kongress Dronen in Streichholzschachtelgröße vorgestellt, die ferngesteuert großen Dronen in nichts nachstehen. In Top-Qualität filmen, fotografieren und lauschen, lange ruhig schweben, Aufgenommenes an beliebige Orte senden und allein zum Startort zurück kehren..
Auf derselben Veranstaltung wurden Einmal-Dronen vorgestellt, die Sprengstoff enthalten! Sie können ferngesteuert sechs Meilen weit fliegen, anschließend 20 Minuten (zentimetergenau) hoch (und kaum erkennbar) über einem Ziel schweben und danach, auf Knopfdruck abstürzend, präzise treffen. Mit der Sprenggewalt mehrerer üblicher Handgranaten. Da diese Dronen miteinander kommunizieren, können ganze Schwärme auf einmal starten …
Abgesehen vom militärischen “Wert“ entsteht damit auch eine zivile Sabotagegefahr, sobald die Geräte preiswert im Handel sind … was wohl nicht all zu lange dauern wird.

Warnungen vor Flüchtlings-Mitläufern

Es ist erschütternd – jedoch leider anscheinend Realität. Bekannt gut informierte Intel-Insider warnen vor russischen Akteuren, die im Feld der Ukrainischen Flüchtlingswelle mitschwimmen und anschließend in Europa gezielt Jobs bei vorher definierten Unternehmen suchen.

Als Beispiel hier ein Fall, in dem seltene Fachkompetenzen einer “Ukrainerin mit verloren gegangenen Papieren“ zu einer schnellen Vermittlung in einem technisch innovativ agierenden Unternehmen führten. Aufgefallen ist sie einem Mitarbeiter der Personalabteilung (selbst gebürtiger Ukrainer) im Unternehmen, dem der russische Akzent der Bewerberin verdächtig vorkam.
Ein teurer Background-Check legte die vorhergehende Tätigkeit der Frau als Mitarbeiterin eines der russischen Geheimdienste offen.

Verstärkte Gefahren für Smartphones

Die Software “Pegasus“ soll eigentlich helfen, Terroristen und Schwerkriminelle zu überwachen. Zugang zum Programm haben offiziell nur Geheimdienste und staatliche Behörden. Die Crux dabei: Nicht alle Staaten halten sich an die Spielregeln.
Mit dem Ergebnis, dass Pegasus inzwischen auch über bestimmte Kanäle für “zivile Nutzung“ erhältlich ist.
Das von der israelischen NSO-Group entwickelte Programm namens gilt Berichten zufolge unter Experten als das derzeit leistungsfähigste Spähprogramm für Handys und ist als Cyberwaffe eingestuft worden. Es ist demnach in der Lage, infiltrierte Mobiltelefone in Echtzeit auszuspähen und die Verschlüsselung von Messenger-Diensten wie Whatsapp oder Signal zu umgehen. *Quelle: mba/AFP/CIA*

Putin macht Industriespionage zur Priorität

Der Kreml setzt angesichts der westlichen Sanktionen verstärkt auf Industriespionage. "Wie auch schon früher, liegt eine der Prioritäten bei der Arbeit des SWR *(Anm.: Russ. Auslandsgeheimdienst)* darin, die Entwicklung des Industriepotenzials zu unterstützen", sagt Russlands Präsident Wladimir Putin. Dies sei angesichts der westlichen Sanktionen besonders wichtig. Die Agenten müssten nicht nur Informationen aus der Industrie beschaffen, sondern auch die Basis für die strategische Planung und Analyse internationaler Prozesse liefern, so der Kremlchef. *Quelle(n): Russisches Staats-TV*

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 Fachleute 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

---

- Anhang -

Newsletter 03/2022

Das perfekte Informationsschutz Paket für kleine und mittelständische Unternehmen sowie Institutionen und Behörden

Das Thema:
Für viele mittelständische Unternehmen und Behörden stellt die Einrichtung eines erschwinglichen und zugleich professionellen Informationsschutzes eine ungewohnte 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 Analyse-, Schulungs- und Beratungspaket 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 / Reise / BCM / Evakuierung / Dienstleister / HomeOffice) 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.

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

Whistleblower als Chance!

NEU! FM-nøspy als hoch vertraulicher Anlaufpunkt für Hinweisgeber

FM-nøspy ist international im Themenfeld der Prävention und Abwehr von Industrie- und Wirtschaftsspionage erfolgreich. Dies vor Allem aus drei Gründen:

- Wir sind Fachleute für zwischenmenschliche Kommunikation
- Wir agieren erwiesenermaßen besonders lösungsorientiert und praxisgerecht
- Wir haben das volle Vertrauen aller, an unseren Seminaren teilnehmenden Mitarbeiter. Nicht zuletzt deshalb erfahren wir dadurch z.B. zahlreiche Sicherheitsschwachpunkte, die den eigentlich Zuständigen kaum oder gar nicht bekannt sind

Das europäische **"Hinweisgeberschutzgesetz"** nimmt in diesem Tagen auch in Deutschland konkrete Formen an. Bisher galten nur schwammige EU-Richtlinien.

Nun sind allerdings in Kürze alle Unternehmen mit mehr als 50 Mitarbeitern verpflichtet, eine neutrale, hoch vertrauensvoll agierende Anlaufstelle für Hinweisgeber einzurichten.

Kluge Unternehmen erkennen hier zugleich eine Chance, aktuelle oder potentielle Missstände im Unternehmen früher zu erfahren und somit eventuell drohenden schwerwiegenderen Folgen frühzeitig entgegen wirken zu können.

FM-nøspy besitzt naturgemäß nicht nur hohe Kompetenz im Umgang mit Hinweisgebern; als Kommunikationsexperten sind seine Mitarbeiter auch in vertraulichen, sensiblen Situationen äußerst erfahren. Verbunden mit einem, in Security-Schulungen meist entstandenen, hohen Vertrauen der Schulungsteilnehmer in uns, sind wir die perfekte externe(!), hoch sichere Anlaufstelle für vertrauliche Hinweise.

Vorteile dieser externen Anlaufstelle für Unternehmen und deren Mitarbeiter:

- Sie spart enorm Kosten, bei gleichzeitiger Wahrung aller gesetzlichen Vorschriften
- Sie informiert und berichtet ausschließlich an den Auftraggeber (Geschäftsleitung)
- Sie sichert absolute Vertraulichkeit (24/360) trotz Einhaltung festgelegter Reportwege
- Sie gestattet Mitarbeitern und Dienstleistern vielfältige anonyme Kontaktwege zu uns
- Sie stellt für Mitarbeiter einen angst- und sorgenfreier Zugang dar.
  (weil keine interne Abteilung, kein Anwaltsbüro, keine "Auditoren")

Ab August 2022 stellt **FM-nøspy** die dazu nötige technische und personelle Infrastruktur bereit. Diese wird dann zusammen mit Ihnen den individuellen Anforderungen und Bedürfnissen Ihrer Geschäftsleitung, des BR und denen Ihrer Mitarbeiter angepasst.

Nähere Informationen gerne und kurzfristig unter info@fm-nospy.com