Newsletter 02/2022

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

der Schutz sensibler Informationen wird deutlich wichtiger – und schwieriger zugleich. Einerseits nutzen professionelle Angreifer immer noch vielfach bestehende Nachlässigkeiten im HomeOffice-Betrieb aus.
Andererseits explodieren geradezu Spionageaktivitäten, die im weitesten Sinne mit dem Ukraine-Krieg zu tun haben. Bitte bedenken Sie in diesem Zusammenhang, dass Sie oder Ihr Unternehmen nicht zwingend Endziel von Ausspähung sein müssen, sondern dass Sie einfach benutzt wird, um Angriffe auf Ihre Kunden oder Geschäftspartner zu realisieren.

Nachfolgend zum zweiten Mal in diesem Jahr Aktuelles aus dieser Schattenwelt.
Viel “Spass“ beim Lesen
Ihr Team von FM-nospy

BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten

Angesichts des aktuellen Russischen Angriffs auf die Ukraine sprechen das BSI und mehrere Geheimdienste weltweit deutliche Warnungen aus, Produkte des russischen Sicherheitsunternehmens Kaspersky einzusetzen.
Hintergrund sind Drohungen seitens der Russischen Regierung gegen den Westen, Cyberangriffe massiv einzusetzen. Verbunden mit der Sorge dass Kaspersky genutzt (gezwungen?) werden könnte, seine Produkte für staatliche Angriffe zu öffnen.
Mehr dazu im Anhang zu diesem Newsletter.

Die Wiederauferstehung der Toten Briefkästen

Astlöcher, hohle Mauerziegel und ähnliches sind seit Jahrzehnten die geheimen Übergabestellen für Informationen. Im Digitalen Zeitalter übernahm dies teilweise die Steganographie, mit deren Hilfe man Informationen z.B. in Fotos etc. verstecken kann. Moderne IT Prüfmethoden kommen dem allerdings immer öfter auf die Schliche.

Vor einigen Jahren versuchten Britische Spione in Russland, klassische “haptische Briefkästen“ mit IT zu kombinieren, indem sie Steine auslegten, deren Inhalt über Bluetooth Botschaften verbreitete. Jeder der Bescheid wusste, konnte (scheinbar zufällig vorbei laufend) diese Daten abgreifen und sogar eigene Daten zurück laden.
Russland entdeckte diese Kommunikationsstellen allerdings …

Nun scheint die ausgefallene Briefkastenmethode nach Jahren des Vergessens ihre Wiederauferstehung zu feiern.
Vor kurzem wurde ein “Briefkasten“ mit neuester Technologie auf einem Firmengelände entdeckt, der nur auffiel, weil er im Rahmen von Bauarbeiten zufällig auseinanderbrach.

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

Schutz von Whistleblowern weiter auf tönernen Füßen

Allen mit Informationsschutz und Compliance befassten sind dankbar, wenn sie Hinweise auf Nichtkonformes oder Schwachstellen erhalten.
Auf dem regelmäßig in Köln stattfindenden Symposium “Suspektrum“ wurde wieder einmal deutlich, dass “Whistleblower“ in Deutschland kaum ernsthaft zu schützen sind. Entsprechend groß ist die Sorge von potentiellen Hinweisgebern, persönliche Nachteile zu erleiden, wenn sie helfen, Kriminelles oder Gefährliches zu bekämpfen.

Bemerkenswert dabei: Alle entsprechenden Initiativen für einen soliden Schutz von Whistleblowern wurden (und werden) von der Politik regelmäßig ausgebremst. Wir verkneifen uns jetzt einmal die Frage, warum dies so ist …

Abhören von Gesprächen wird beinahe Alltag

Wir wiederholen uns ungern. Jedoch zeigt sich, dass der Einsatz von Abhörtechnik massiv zunimmt.
Mit ein Grund ist, dass viele dieser “Wanzen“ heutzutage nicht mehr Aufgenommenes nur speichern (und danach aus dem Versteck geholt werden müssen). Moderne Geräte lassen sich mit einem einfachen Prepaid Telefonchip bestücken, den man nach Platzieren der Wanze beliebig durch Anrufe ein und ausschalten kann.
Eingeschaltet lauschen die “Tierchen“ in HD-Qualität und senden Belauschtes (mittels Rufumleitung) an beliebige Orte weltweit.

Erhältlich im freien Internet (kein Darknet Besuch nötig). Verblüffend niedrige Preise führen dazu, dass auch Nicht-Profis inzwischen Gespräche aufzeichnen.
Vom Personalgespräch, über Strategiesitzungen bis zu heimlich gefilmten sexuellen Abenteuern. Letztere werden dann gerne für große und kleine Erpressungen verwendet …

Vorbeugen ist in allen Aspekten günstiger als Reparieren

Einerlei, ob Daten kopiert oder verschwunden, Anlagen ausgefallen oder die Reputation auf Monate hinaus beschädigt sind …

Aus diesem Grund haben wir unser viel gebuchtes Mittelstandspaket hinsichtlich der zeitaktuellen Herausforderungen aktualisiert. Mehr dazu im Anhang.

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 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

BSI-Warnung gemäß BSIG § 7

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht die vorliegende Warnung im Rahmen seines gesetzlichen Auftrags [1].

Virenschutzsoftware des Herstellers Kaspersky

Risikostufe [2]: 4 - hoch

1 Sachverhalt

Virenschutzsoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, ist essentiell zum Schutz von IT-Systemen. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt aber gerade Virenschutzsoftware ein besonderes Risiko für eine zu schützende IT-Infrastruktur. Um einen aktuellen und wirksamen Schutz vor Schadsoftware zu gewährleisten, verfügt sie über weitreichende Systemberechtigungen und muss systembedingt (zumindest für Aktualisierungen) eine dauerhafte, verschlüsselte und nicht prüfbare Verbindung zu Servern des Herstellers unterhalten. Daher ist Vertrauen in die Zuverlässigkeit und den Eigenschutz eines Herstellers sowie seiner authentischen Handlungsfähigkeit entscheidend für den sicheren Einsatz solcher Systeme. Virenschutzsoftware ist ein exponiertes Ziel von offensiven Operationen im Cyberraum, um potentielle Gegner auszuspionieren, die Integrität ihrer Systeme zu beeinträchtigen oder sogar die Verfügbarkeit der darauf gespeicherten Daten vollständig einzuschränken.

Das Vorgehen militärischer und/oder nachrichtendienstlicher Kräfte in Russland sowie die im Zuge des aktuellen kriegerischen Konflikts jüngst von russischer Seite ausgesprochenen Drohungen gegen die EU, die NATO und die Bundesrepublik Deutschland sind mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs mit weitreichenden Konsequenzen verbunden.

Ein russischer IT-Hersteller kann selbst offensive Operationen durchführen, gegen seinen eigenen Willen gezwungen werden, Zielsysteme anzugreifen, oder selbst als Opfer einer Cyber-Operation ohne seine Kenntnis ausspioniert oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht werden.

2 Auswirkung

Durch Manipulationen an der Software oder den Zugriff auf bei Kaspersky gespeicherte Daten können Aufklärungs- oder Sabotageaktionen gegen Deutschland, einzelne Personen oder bestimmte Unternehmen oder Organisationen durchgeführt oder zumindest unterstützt werden.

Alle Anwender und Nutzerinnen der Virenschutzsoftware können je nach Ihrer strategischen Bedeutung von einer schädigenden Operation betroffen sein. Abgestuft ist damit zu rechnen, dass Einrichtungen des Staates, der Kritischen Infrastrukturen, der Unternehmen im besonderen öffentlichen Interesse, des produzierenden Gewerbes sowie wichtiger gesellschaftlicher Bereiche betroffen sein können. Privatanwender ohne wichtige Funktion in Staat, Wirtschaft und Gesellschaft stehen möglicherweise am Wenigsten im Fokus, können aber in einem erfolgreichen Angriffsfall auch Opfer von Kollateralauswirkungen werden.

3 Betroffene Produkte

Betroffen ist das Portfolio von Virenschutzsoftware des Unternehmens Kaspersky.

4 Handlungsempfehlung

Virenschutzsoftware des Unternehmens Kaspersky sollte durch alternative Produkte ersetzt werden.

Unternehmen und Behörden mit besonderen Sicherheitsinteressen/Rahmenbedingungen und Einrichtungen Kritischer Infrastrukturen sind in besonderem Maß gefährdet. Sie haben die Möglichkeit, sich von den zuständigen Verfassungsschutzbehörden bzw. vom BSI beraten zu lassen.

Allgemeiner Hinweis: Der Wechsel wesentlicher Bestandteile einer IT-Sicherheits-infrastruktur muss im Enterprise-Bereich immer sorgfältig geplant und durchgeführt werden. Würden IT-Sicherheitsprodukte (also insbesondere Virenschutzsoftware) ohne Vorbereitung abgeschaltet, wäre man Angriffen aus dem Internet möglicherweise schutzlos ausgeliefert. Der notfallmäßige Umstieg auf andere Produkte ist auf jeden Fall mit vorübergehenden Komfort-, Funktions- und Sicherheitseinbußen verbunden.
Das BSI empfiehlt daher in jedem Fall eine individuelle Bewertung und Abwägung der aktuellen Situation sowie in einem erforderlichen Migrationsfall, Experten zur Umsetzungsplanung und -durchführung hinzuzuziehen.

5 Referenzen

[1] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)
https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Gesetz/bsi-gesetz_node.html
[2] BSI-Warnungen gemäß §7 und §7a BSIG
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/warnungen-nach-par-7_node.html
[3] Darstellung Risikostufen
https://www.cert-bund.de/risk