

Wirecard: Im Rätsel um Spionage-Software führt die Spur in den Kreml

By Jan-Philipp Hein

Published: 2021-11-19 · Archived: 2026-04-05 17:25:48 UTC

Ein deutscher Geschäftsmann mit besten Kreml-Kontakten bewirbt eine Software, die angeblich jeden Menschen in eine Datenwolke verwandeln kann. Auch Ex-Wirecard-Chef Jan Marsalek kennt die Firma. Die ganze Geschichte aus dem FOCUS Magazin jetzt vorab auf FOCUS Online.

Die Mail von Ende August 2018 war aus mehreren Gründen bemerkenswert. Absender war einer der umtriebigen politischen Strippenzieher der Republik Österreich. Er heißt Florian Stermann und ist eine schillernde Figur, die in staatsanwaltschaftlichen Untersuchungen als „Vertrauensmann“ der damals mitregierenden FPÖ eingeschätzt wird.

In jener E-Mail im August wandte sich Stermann, Generalsekretär der Russisch-Österreichischen Freundschaftsgesellschaft, an einen Mann aus dem Olymp der globalen Finanzindustrie. „Wie besprochen“ erhielt der „liebe Jan“ eine Firmenpräsentation weitergeleitet.

Angehängt war das PDF einer aufwendig gestalteten 23-seitigen Unternehmensdarstellung. Eine Firma mit dem sperrigen Namen „DSR Decision Supporting Information Research Forensic GmbH“ (DSIRF) stellte darin ihre Dienste vor. Es ging um Cyberkrieg, von biometrischer Gesichtserkennung und „der Enttarnung fremder Informationskriegstaktiken“ war die Rede. Letztlich boten die vermeintlichen IT-Cracks ein spezielles Hacking-Tool namens „Subzero“ an. Es handelt sich um Dienstleistungen, die in der EU so gut wie nicht legal zu erbringen sind.

Alle Elemente eines dystopischen Krimis – und Ex-Wirecard-Chef Jan Marsalek mittendrin

Der „liebe Jan“ heißt mit vollem Namen Jan Marsalek. Die Angebotspalette von DSIRF passte genau in die Schattenwelt, die man ihm zuschreibt. Damals stand er dem gehypten Finanzdienstleister Wirecard vor. Heute, drei Jahre später, gilt er als einer der meistgesuchten Wirtschaftsverbrecher der Welt. Er soll Mastermind hinter den Milliardenbetrügereien des untergegangenen Dax-Konzerns sein. Fahnder vermuten den flüchtigen 41-Jährigen nahe Moskau – unter Obhut des russischen Inlandsdienstes FSB. Denn neben seinem Beruf als Finanzjongleur verstand sich Marsalek als alpenländischer 007-Verschnitt.

Jeden Samstag am Kiosk: Das neue FOCUS Magazin

Außerdem im neuen Heft:

+ **Ministerkarussell: Wer wird was in der Regierung Scholz**

+ **Mentale Gesundheit: So bleiben Sie fit im Job**

+ **Weise Worte: Paul McCartney erklärt den Jahrhundertssong „Let it be“**

[Hier geht es zum aktuellen Magazin](#)

Die Story um DSIRF hat alle Elemente eines dystopischen Krimis: Politisch vernetzte Protagonisten mit hervorragenden Kontakten nach Moskau interessieren sich für eine Software, die das perfekte Unterdrückungswerkzeug für autoritäre Herrscher wäre. Und, im kommerziellen Bereich eingesetzt, der Albtraum für Daten- und Konsumentenschützer.

Eine Welt der Totalüberwachung – und immer wieder Moskau

Wie so oft, wenn's um Marsalek geht, führen auch bei DSIRF viele Spuren nach Osten. Die Firma residiert in Wien. Laut österreichischem Finanzministerium gehört das Unternehmen Peter Dietenberger. Einem Deutschen mit Wohnsitzen in Österreich und der Schweiz. Der 54-Jährige legt viel Wert auf Diskretion. Eines aber ist sicher: Er ist Spezialist für West-Ost-Beziehungen. Für europäische Unternehmen, die in Russland Geschäfte machen wollten, galt er lange als besonders wertvoll, weil seine Freunde und Bekannten zur russischen Nomenklatura gehören. Sein Visum wies ihn sogar als Gast der Präsidentschaftsverwaltung aus.

Die Homepage der 2016 gegründeten DSIRF wirkt professionell zurückhaltend. Ausgewählte potenzielle Kunden erhalten dazu exklusive Präsentationen – wie die in der Mail an Marsalek. Mit einem „Computer-Überwachungswerkzeug“ auf dem „letzten Stand der Technik“ verspricht DSIRF darin die „volle Kontrolle über Zielcomputer“ und den „kompletten Zugang zu allen Passwörtern“. Regierungen würden damit alle Daten zur Verfügung stehen, die sie zu lückenloser Überwachung bräuchten. Dreißig hoch qualifizierte Mitarbeiter hätten zudem Kenntnisse im Bereich Datendiebstahl, Informationskriegstechniken sowie in beeinflussendem politischem Campaigning.

In einem sechsminütigen Video mit dem Titel „Biometric Recognition“ präsentiert DSIRF eine Welt der Totalüberwachung. Bahnhöfe, Flughäfen, Kaufhäuser und Einkaufszentren werden darin als Einsatzgebiete von Überwachungskameras gezeigt – mit der Besonderheit, dass alle an ein „DSIRF-Datencenter“ angeschlossen sind, in dem biometrische Informationen mit Daten aus sozialen Netzwerken, Vorstrafen, Konsumgewohnheiten und Bezahlinformationen kombiniert und laufend angereichert werden. Diese „Biometric Recognition“-Software könne laut Firmenvideo das Gesicht einer jeden Zielperson auf über 2000 unterschiedliche Datenpunkte scannen: Es wird die Distanz zwischen den Augen gemessen. Die Hautbeschaffenheit von der Farbschattierung bis zur Struktur der Poren analysiert. Jede Person wird eindeutig identifizierbar.

Dazu könne das „DSIRF-Data-Center“ in Echtzeit alle ID-Daten liefern: Name, Geburtstag, Anschrift. Das System arbeitet so intelligent, dass es in Gebäuden zwischen verschiedenen Gruppen selektieren könne: Der Mann im Anzug arbeitet hier, die Dame im Rolli ist Kundin.

Klingt nach Hollywood-Science-Fiction – könnte aber Wirklichkeit werden

Ab Minute drei des Werbevideos geht es dann längst nicht mehr um den Schutz vor Anschlägen oder die legitime Entlarvung von Ladendieben. Da dreht sich alles ums Geschäft. Eine Kundin schlendert durch die

Kosmetikabteilung. Mit dem prüfenden Griff zur Wimperntusche beginnt es. Unaufhaltsam.

Die Konsumentin wird röntgenähnlich durchleuchtet: von Name, Adresse, Größe, Geburtsdatum, Social-Media-Aktivitäten, WhatsApp-Konversationen bis hin zu einem Kauf- und Bewegungsprofil der letzten Shoppingtouren. So erfährt der Verkäufer schnell, dass die Dame auf bunte Stiletto steht, und kann sie ihr direkt anbieten.

Klingt nach Hollywood-Science-Fiction. Könnte aber Wirklichkeit werden. Natürlich nur im Einklang mit der „nationalen Gesetzgebung“, die im Video beiläufig erwähnt wird.

Digitalexperten haben sich für FOCUS mit DSIRF beschäftigt und halten die Angebote der Firma für realistisch. Und im politischen Kontext der Moskau-Connection beängstigend.

Matthias Marx, Sprecher des Chaos Computer Clubs (CCC), meint: „Solche Angebote richten sich häufig an staatliche Akteure. Vergleichbare Programme wie die von DSIRF werden genutzt, um Journalisten, Menschenrechtsaktivistinnen und Oppositionelle zu überwachen.“

Damit spielt er auf Pegasus an. Die Spyware einer israelischen Firma dient nach Überzeugung der US-Regierung Diktaturen zur böswilligen Überwachung politischer Widersacher. Als sicher gilt, dass damit schon Tausende Politiker weltweit ausgespäht wurden, unter anderem Frankreichs Präsident Emmanuel Macron. Auch bei der Ermordung des arabischen Journalisten Jamal Khashoggi im saudischen Konsulat in Istanbul durch Geheimdienstmitarbeiter spielte Pegasus als Überwachungstool eine Rolle.

DSIRF: Dienstleister für Strafverfolger oder gar Geheimdienste?

DSIRF bemüht sich nicht um Transparenz. Dietenberger selbst beantwortet überhaupt keine Fragen, und sein Firmengeschäftsführer Drazen Mokic geht nur auf das ein, was eh schon bekannt ist. Die Präsentation, so Mokic, sei „vertraulich“ und „diente ausschließlich zur Vorlage bei Behörden und potenziellen Investoren“. DSIRF als Dienstleister für Strafverfolger oder gar Geheimdienste? Auf Nachfrage kann Mokic keine einzige Behörde nennen, die eine Zusammenarbeit mit DSIRF bestätigt. Das österreichische Innen- und das Justizministerium schließen jedenfalls aus, dass man selbst oder Geheimdienst, Polizei und die Justiz je mit DSIRF zusammengearbeitet hätten.

Jeden Samstag am Kiosk: Das neue FOCUS Magazin

Außerdem im neuen Heft:

- + **Ministerkarussell: Wer wird was in der Regierung Scholz**
- + **Mentale Gesundheit: So bleiben Sie fit im Job**
- + **Weise Worte: Paul McCartney erklärt den Jahrhundertssong „Let it be“**

[Hier geht es zum aktuellen Magazin](#)

Mokic hat noch ein Problem: Angeblich kennt er weder den Russlandlobbyisten Stermann noch den flüchtigen Wirecard-Vorstand Marsalek, was bedeutet, dass seine diskrete Sicherheitsfirma undicht ist. Denn die PDF-Datei

brauchte nur knapp zwei Tage von ihrer Fertigstellung bis in Marsaleks Mailfach. Ein Anwalt der DSIRF erweckt den Eindruck, sie sei gestohlen worden, man werde „mit aller gebotenen Schärfe die notwendigen juristischen Konsequenzen ziehen“. Nun wüsste man gern von Stermann, ob er bereits Ärger mit Dietenberger und Mokic hat. Aber auch er beantwortet keine Fragen.

Türöffner westlicher Firmen in Putins Reich

Sollte Dietenberger, der Mann mit besten Verbindungen im Kreml, tatsächlich gezielt Hackerangriffe im Westen orchestrieren und Zugriff auf umfangreiche Datensätze über Millionen Passanten von Videokameras nehmen können, wäre dies ein enormes Sicherheitsrisiko. Deshalb sieht Russlandexperte Gustav Gressel vom European Council on Foreign Relations dringenden Handlungsbedarf. „Es muss geklärt werden, was diese Firma genau macht. Fälle von IT-Unternehmen, die im Interesse fremder Mächte Spionagesoftware einsetzen, sind immer wieder bekannt geworden.“

Internet von o2: DSL, Kabel, LTE oder 5G (Anzeige)

Die geheime Präsentation beinhaltet eine Art Kunden- bzw. Referenzliste. Auch dabei führen alle Spuren nach Moskau. Der Geschäftsführer des Ost-Ausschusses der Deutschen Wirtschaft gehört dazu. Ebenso das Unternehmen eines russischen Oligarchen, gegen den die USA Sanktionen verhängt haben und gegen den das FBI ermittelt. Eine ziemlich illustre Gesellschaft versammelt die DSIRF. Dietenbergers Vorleben als Türöffner westlicher Firmen in Putins Reich dürfte dabei der Schlüssel sein. So taucht in dem Präsentationsvideo auf der Firmenwebsite auch Rewe auf. Als Konzernrepräsentant unterstützte Dietenberger den Lebensmittelhändler vor rund 15 Jahren in Moskau mit seinem Adressbuch.

Der damalige Rewe-Manager, mit dem Dietenberger an der Expansion arbeitete, wird auch als DSIRF-Referenz erwähnt und war bis vor gut einem Jahr Manager der Unternehmensgruppe Signa des Tiroler Immobilienmoguls René Benko. Zu Signa gehören unter anderem die Reste von Karstadt, Kaufhof und das KaDeWe in Berlin. Die Holding bestätigt ein Auftragsverhältnis mit DSIRF. Angeblich sei die Firma vom eigenen Wirtschaftsprüfer vor rund fünf Jahren bei einem „Cyber-Security-Check bei Karstadt“ als Subauftragnehmerin mitgebracht worden. Anschließend habe man eine weitere Zusammenarbeit vereinbart.

Was für ein Zufall: Das Signa-Management und Dietenberger kannten sich lange, und dann bringt der Wirtschaftsprüfer – nach FOCUS-Informationen KPMG – ausgerechnet dessen zu dem Zeitpunkt wenige Monate alte Firma mit? Das klingt nicht sehr plausibel, aber auch KPMG äußert sich dazu nicht.

„Weiterer Mosaikstein“ im diffusen Bild von Marsalek

Die Politik sieht die DSIRF mit Sorge. Viola von Cramon, grüne Osteuropa-Expertin im Europaparlament: „Es ist eine ernste Bedrohung, wenn ein Unternehmen mit diesem Hintergrund und solchen Verbindungen zur russischen Staatsspitze in der EU derartige Dienste anbietet. Das muss gestoppt werden.“ Auch die Verbindung zu Jan Marsalek bedürfe einer genauen Untersuchung. Für Stephanie Krisper, die für die liberale Partei Neos im österreichischen Nationalrat sitzt, fügt der Fall dem diffusen Bild von Marsalek einen „weiteren Mosaikstein“ hinzu. Sie kündigt parlamentarische Anfragen an die Regierung an. Denn: „Auch der Schutz des einzelnen Bürgers muss garantiert werden.“

Unterdessen sorgt sich die Firma DSIRF um ihren eigenen Schutz. Sollte eine rechtswidrige Berichterstattung erfolgen, drohen Anwälte die Prüfung presserechtlicher Ansprüche an.

Privates gibt es nicht mehr. Staat und Unternehmen wissen alles.

Source: https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html