Ressort: Technik

Siemens unter Peter Löscher, das iranische Atomprogramm & Stuxnet

Spur führte zu Mossad & CIA

München, 16.07.2019, 20:19 Uhr

GDN - Der aktuelle Fall einer Bedrohung des Siemens-CEO Joe Kaeser ruft einen Urheberrechtsfall bei der Generalstaatsanwaltschaft Frankfurt am Main ins Gedächtnis: Beschuldiger war ein iranischer Beschaffungsagent - in Bezug zu Siemens-Software.

In den Jahren 2010 und 2011 war der Österreicher Peter Löscher der amtierende Vorstandsvorsitzende der deutschen Siemens AG. Hierzu zunächst einmal eine Fundstelle zum Nachweis:

https://en.wikipedia.org/wiki/Peter_Löscher

Und in diesen Jahren hat es bei der Generalstaatsanwaltschaft Frankfurt am Main ein sehr brisantes Strafverfahren nach § 108 UrheberG gegeben, das in unmittelbaren Zusammenhang mit dem Atomprogramm des Iran und spezieller Software aus dem Hause Siemens gestanden ist. Hierzu weiß der Verfasser das Folgende aus persönlicher Kenntnis zu berichten:

In Wien war damals ein Beschaffungsagent des Iran aktiv, welcher zur Siemens AG enge Kontakte aufgebaut hatte. Über diese hat derselbe eine Betriebs-Software für Atomkraftwerke und sonstige Atomanlagen für Iran organisiert, wobei damals die Entwicklung einer Atombombe durch Iran virulent war. Gleichwohl hat die Siemens AG die betreffende Spezial-Software an diesen Besteller verkauft und auch ausgeliefert. Aber mit einem Compliance-Trick: In den Verträgen zum Erwerb dieser sehr speziellen Individual-Software war eine urheberrechtliche Klausel verankert, wonach eine Nutzung derselben in Iran bzw. auf iranischen Atomanlagen nicht gestattet ist.

Gleichwohl ist genau diese Betriebs-Software unmittelbar nach deren Auslieferung an den iranischen Beschaffungsagenten in Wien auf iranischen Atomanlagen, die Teil des Atombombenprogramms waren, installiert worden. Und das war dann de iure als vorsätzliche gewerbliche Urheberverletzung strafbar - wegen dem vorgenannten klauselmäßigen Ausschluss. Wegen diesem Tatvorwurf wurde sodann durch die (General-)Staatsanwaltschaft Frankfurt am Main ermittelt: Nämlich gegen den iranischen Beschaffungsagenten mit Aufenthalt in Wien. Alles das war eigentlich schon bei Vertragsschluss als de-facto-Entwicklung absehbar. Die betreffende Placebo-Klausel diente ausschließlich einer de-iure-mäßigen Haftungsfreizeichnung.

Zeitgleich ist es zu einer Virus-Attacke auf die mit der betreffenden Siemens-Software ausgersteten iranischen Atomanlagen gekommen, wie auch zu einem tötlichen Bombenanschlag auf einen iranischen Atomexperten in Teheran. Der zum besagten Angriff verwendete Computer-Virus wurde als “Stuxnet“ betitelt - wobei dieser Vorgang weltweit für Schlagzeilen sorgte. Die Rede war von einer Mossad-CIA-Operation zur Verhinderung einer iranischen Atombombe. Hierzu die folgenden Fundstellen zur Eigenlektüre:

https://de.wikipedia.org/wiki/Stuxnet

Hieraus zitiert wie folgt:

“Vermutungen über die Urheber und Ziele

Experten und Ingenieure

IT-Sicherheitsspezialisten, darunter als erster Ralph Langner, gehen davon aus, dass Stuxnetgezielt zur Sabotage iranischer Atomanlagen programmiert wurde. Der Aufwand für den Wurm sei gewaltig und teuer gewesen, zudem richte er nur in bestimmten Anlagen Schaden an, andere würden offenbar ohne Schaden lediglich infiziert. Als Verteiler käme vor allem die russische Atomstroiexport infrage.

Laut Wieland Simon (Siemens) müssen an der Entwicklung des Wurms Experten und Ingenieure aus ganz unterschiedlichen Bereichen beteiligt gewesen sein - neben Windows-Programmierern auch Fachleute für Automatisierungstechnik und große

Industrieanlagen. (...)

Nur ein solches Team wäre in der Lage, einen Schädling zu programmieren, der nacheinander mehrere technisch sehr unterschiedliche Hürden überwindet.

Wegen des großen Programmieraufwandes wird von Jewgeni Kasperski, Liam O Murchu (Symantec) und anderen Fachleuten angenommen, dass der Wurm nicht von Privatpersonen, sondern vermutlich von einer staatlichen Organisation stammt. Auch die hohen Entwicklungskosten für den Wurm, die auf einen 7-stelligen Dollar-Betrag geschätzt werden, sprächen dafür.

Zum Auftraggeber Israel

Mehrere Expertenteams fanden im Wurmcode Textbausteine, die nahelegen, dass die Angreifer ihr Projekt “Myrtus“ nannten. (...)

Der deutsche IT-Sicherheitsspezialist Langner wies als erster auf die mögliche Anspielung auf den ursprünglich hebräischen Namen der Bibelfigur Esther hin. Carol Newsom, Professorin für Altes Testament an der Emory University, bestätigte den linguistischen Zusammenhang der hebräischen Wörter für “Myrtus“ und “Esther“ (hebr. Hadassah). Das Buch Esther im Alten Testament erzählt die Geschichte eines geplanten Völkermords der Perser an den Juden, den letztere auf Initiative Esthers verhindern können, indem sie ihrerseits die Feinde vernichten.

In den Medien wurde diese Spekulation als Hinweis auf eine mögliche Urheberschaft Israels gewertet. (...)

Laut Süddeutsche Zeitung halten die meisten Fachleute diese These allerdings für eine Verschwörungstheorie. Es könnte auch eine falsch ausgelegte Fährte sein.
Shai Blitzblau, technischer Direktor und Chef von Maglan, eines israelischen IT-Sicherheitsunternehmens im Militärbereich, ist überzeugt, dass Israel nichts mit Stuxnet zu tun hat. Er vermutet Wirtschaftsspionage gegen Siemens oder eine Art “akademisches Experiment“.

Yossi Melman, Journalist der israelischen Tageszeitung Haaretz, hielt Israel 2010 für den wahrscheinlichen Urheber. Er führte an, dass der Vertrag des Direktors des israelischen Auslandsgeheimdienstes Mossad, Meir Dagan, 2009 verlängert wurde, da er in wichtige Projekte involviert sei.

Zudem hätte Israel den geschätzten Zeitpunkt, bis zu welchem Iran eine Atombombe besitzen soll, überraschend auf das Jahr 2014 nach hinten verschoben.
Laut einem Artikel der New York Times vom 30. September 2010 behauptet ein ehemaliges Mitglied der United States Intelligence Community, dass der israelische Nachrichtendienst Unit 8200, der mit der NSA vergleichbar ist, den Angriff mit Stuxnet ausgeführt habe. Laut einem späteren Artikel vom 15. Januar 2011 untersuchten das Ministerium für Innere Sicherheit der Vereinigten Staaten und das Idaho National Laboratory 2008 das betroffene PCS-7-Steuerungssystem von Siemens auf Schwachstellen. (...)

Anschließend soll der auf Grundlage dieser Erkenntnisse entwickelte Wurm im israelischen Negev-Nuklear-Forschungszentrum getestet worden sein; dort waren Gaszentrifugen pakistanischer Herkunft errichtet worden, die auch im Iran verwendet werden.

Weiter stehen laut Bericht der New York Times vom 15. Januar 2011 in Israels Atomwaffenzentrum “Dimona“ Zentrifugen, die mit den iranischen baugleich sind und daher als Test für den Wurm verwendet worden sein könnten.

Die israelische Tageszeitung Haaretz berichtete am 14. Februar 2011 von einem Video, in dem sich der seinerzeitige israelische Generalstabschef der IDF Gabi Ashkenazi brüstet, neben den israelischen Angriffen auf einen syrischen Atomreaktor auch für die erfolgreiche Stuxnet-Attacke verantwortlich gewesen zu sein.

Der ehemalige Geheimdienstmitarbeiter und Whistleblower Edward Snowden erhärtete im Juli 2013 den Verdacht, Stuxnet sei eine Entwicklung der NSA in Zusammenarbeit mit Israel."

In Bezug zu dem aktuellen Bedrohungsfall des gegenwärtigen Siemens-CEO Joe Kaeser wäre insoweit interessant zu wissen, welche Geschäfte im Verhältnis zu Iran die letzte Zeit so in der Pipeline waren.

Bericht online:
https://www.germandailynews.com/bericht-122836/siemens-unter-peter-loescher-das-iranische-atomprogramm-und-stuxnet.html

Redaktion und Veranwortlichkeit:
V.i.S.d.P. und gem. § 6 MDStV: Andreas Wisuschil

Haftungsausschluss:
Der Herausgeber übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der veröffentlichten Meldung, sondern stellt lediglich den Speicherplatz für die Bereitstellung und den Zugriff auf Inhalte Dritter zur Verfügung. Für den Inhalt der Meldung ist der allein jeweilige Autor verantwortlich. Andreas Wisuschil

Editorial program service of General News Agency:
United Press Association, Inc.
3651 Lindell Road, Suite D168
Las Vegas, NV 89103, USA
(702) 943.0321 Local
(702) 943.0233 Facsimile
info@unitedpressassociation.org
info@gna24.com
www.gna24.com