

Interview zum Stuxnet-Sabotagevirus

## "Die Büchse der Pandora ist geöffnet"

01.10.2010, 17:35

Interview: Johannes Kuhn

**Der IT-Sicherheitsspezialist Ralph Langner brachte als erster das gefährliche Stuxnet-Virus mit den iranischen Atomanlagen in Verbindung. Die Attacke ist seiner Ansicht nach nur der Anfang - und Deutschland besonders gefährdet.**

*Mit den Worten "Welcome to cyberwar" schließt [die Analyse, die den Stein ins Rollen brachte](#): Der deutsche IT-Sicherheitsspezialist Ralph Langner hatte darin das Stuxnet-Virus unter die Lupe genommen, ein Schadprogramm, das rund um die Welt Rechner in Industrieanlagen mit Siemens-Steuerung infiziert hat.*



Ralph Langner ist IT-Sicherheitsexperte im Bereich von Industriekontrollsystemen und Chef von Langner Communications, einer Software- und IT-Beratungsfirma. Er hat den Code der Stuxnet-Schadsoftware untersucht und stellte als erster die Theorie auf, dass das Programm iranische Atomanlagen attackieren sollte. (© Langner Communications, oH)

*Seit der digitale Eindringling im Juli entdeckt worden war, hatte die IT-Fachwelt über seinen Zweck gerätselt. Das Programm war nicht nur äußerst komplex, sondern auch ziemlich hinterhältig: Es nutzte gleich mehrere unbekannte Sicherheitslücken im Windows-Betriebssystem und verwendete zur Tarnung gestohlene Sicherheitszertifikate.*

*Die These, dass es sich um Industriespionage handeln könnte, ist seit Langners Analyse vom 16. September hinfällig. Die von Langner geäußerte Vermutung, die Sabotage iranische Atomanlagen seien das Ziel des Schädling gewesen, kann zwar nicht bewiesen werden, wird aber von vielen IT-Sicherheitsanalysten geteilt. [Der Leiter des](#)*

[iranischen Atomkraftwerks](#) in Buschir hat inzwischen zugegeben, dass Rechner in der Anlage befallen seien. Iran bestreitet, dass es einen erfolgreichen Angriff gegeben habe, musste aber die Anschaltung der Anlage um einige Monate verschieben.

*Im Interview spricht Langner über Stuxnet und die Bedrohung deutscher Unternehmen durch Cyber-Sabotage.*

**sueddeutsche.de:** Herr Langner, wie ist der Kenntnisstand zum Stuxnet-Virus?

**Ralph Langner:** Unsere technische Analyse ist beendet und zeigt: Erstmals in unserer Geschichte hat ein Schadprogramm die Steuerungstechnik in einer Industrieanlage angegriffen, um sie zu sabotieren. Die genaue Untersuchung beweist zudem, dass eine ganz bestimmte Art von Maschine angegriffen wurde. Durch den injizierten Schadcode sollte ein Aggregat, also zum Beispiel ein Antrieb, eine Pumpe oder ein Ventil gestört werden.

**sueddeutsche.de:** Sie hegen wie viele andere Experten die Vermutung, ein Staat stecke hinter der Attacke. Warum?

**Langner:** Alleine schon der Windows-Hack benötigt Fähigkeiten, wie wir sie nur bei den weltbesten Hackern vermuten. Es wurden dort vier vorher nicht bekannte Sicherheitslücken ausgenutzt, dafür müssten Sie auf dem Schwarzmarkt eine Summe von einer halben Million Euro zahlen. Zwei digitale Signaturen wurden gestohlen, das System des russischen Zulieferers für die Atomanlage war offensichtlich genau bekannt und wurde mit einem USB-Stick infiziert. Die Steuertechnik für eine solche Anlage selbst ist ebenfalls hochkomplex, da kennen sich vielleicht zehn Menschen auf der ganzen Welt gut genug damit aus, um einen Angriff zu planen. Hinzu kommt, dass ich eine solche Attacke natürlich in einem Labor testen muss. All das zusammen lässt nur einen Schluss zu: Hier steckt ein Staat dahinter, keine Hackerbude, kein Terrorist.

**sueddeutsche.de:** Wie kommen Sie darauf, dass eine bestimmte Anlage angegriffen wurde? Immerhin ist Stuxnet auf zigtausenden Industrierechnern zu finden.

**Langner:** Sie müssen sich das Programm wie eine Rakete vorstellen: Ein Teil hat sich auf Windows-Rechnern eingenistet, das ist die Trägerrakete. Wenn Sie eine Nuklearanlage angreifen möchten, können Sie nicht einfach eine Webseite aufrufen und sind plötzlich in den iranischen Atomanlagen in Buschehr oder Natans drin. Deshalb haben die Angreifer

wohl den Umweg über die russische Firma AtomStroyExport gewählt, die das Kraftwerk in Buschir gebaut hat, und haben dort im System mit Hilfe der Lücken im Windows-Betriebssystem die "Trägerrakete" platziert. Das erklärt auch, weshalb so viele Rechner in Indonesien und Indien infiziert sind - auch dort ist AtomStroyExport tätig.

**sueddeutsche.de:** Aber für diese Rechner ist Stuxnet ungefährlich?

**Langner:** Genau, denn - und das ist ebenfalls neu - der eigentliche "Sprengkopf" war absolut spezifisch auf eine bestimmte Industrieanlage gerichtet. Man muss sich das so vorstellen, dass das Programm erst einmal prüft, ob es am richtigen Ort ist, bevor es attackiert.

**sueddeutsche.de:** Die Schnittstelle zwischen Windows und den Steuerungsanlagen ist die Siemens-Software WinCC bzw. Simatic Manager. Kritiker haben darauf hingewiesen, dass das System Schwächen hat, zum Beispiel nicht änderbare und öffentlich einsehbare Passwörter. Teilen Sie diese Kritik?

**Langner:** Diese Kritik geht am Kern der Sache vorbei. Ich sehe die Verantwortlichen eher bei den Betreibern. Sowohl Mittelstand, als auch die Industriekonzerne haben ihre Anlagen in den vergangenen Jahren stark vernetzt und automatisiert. Sicherheitslücken und die Bedrohungen durch Cyberangriffe wurden kaum ernst genommen, weil noch nichts passiert war. Bei Beratungsgesprächen hieß es beispielsweise oft: "Wenn ich jetzt von meinen Zulieferern höhere Standards verlange, bekomme ich Probleme mit unserem Einkauf, weil die Produkte teurer werden." Deshalb hat man darauf verzichtet, mit gefährlichen Konsequenzen.

**sueddeutsche.de:** Haben Sie mit einer solch großen Attacke gerechnet?

**Langner:** Natürlich war klar, dass die glückselige Zeit ohne nennenswerte Vorfälle mal zu Ende sein würde. Dass der erste echte Vorfall dieser Art allerdings gleich solche Dimension haben würde, hat uns überrascht. Wir hatten mit eher trivialen Hackerangriffen gerechnet, zum Beispiel einem Insider, der einmal absichtlich eine Produktionslinie bei einem Automobilzulieferer lahm legt.

**sueddeutsche.de:** Wurde in der Vergangenheit vielleicht zu viel über Spionage und zu wenig über Sabotage gesprochen?

**Langner:** Im Bereich der industriellen Automatisierungstechnik, über den wir hier reden, ist das Spionagerisiko eher gering. Tatsächlich wurde Sabotage bislang eher verdrängt. Eines ist klar: Mit Stuxnet beginnt eine völlig neue Zeitrechnung, die Büchse der Pandora wurde geöffnet. Wir

müssen davon ausgehen, dass es Nachahmungstaten geben wird, dass diese Art von Sabotageangriffen auf Kontrollsysteme auch für die organisierte Kriminalität, für Terroristen und ganz banal auch für gelangweilte Freizeit-Hacker interessant wird. Hier in Deutschland reden wir nicht von Angriffen auf Nuklearanlagen, sondern auf die Industrie - solche Steuerungssysteme finden sich praktisch in jeder deutschen Fabrik.

**sueddeutsche.de:** Wie gut ist Deutschland im internationalen Vergleich aufgestellt?

**Langner:** Wir sind hierzulande vergleichsweise schlecht auf so etwas vorbereitet, da sind die USA deutlich weiter. Nicht unbedingt technologisch, aber organisatorisch: Dort gibt es Standards, Überprüfungen und die Vernetzung geht bis ins Heimatschutzministerium. In Deutschland müssen die Verantwortlichen in der Industrie jetzt personell und organisatorisch Voraussetzungen schaffen, das Problem anzugehen. Bislang ist es doch oft so: In einem typischen Chemiewerk arbeiten beispielsweise 100 Mitarbeiter in der IT-Abteilung, aber wenn sie fragen, wer sich denn bei Produktion und Automatisierungstechnik mit der Cybersicherheit beschäftigt, gucken sie in fragende Gesichter. Oft haben ja Technik, mittleres Management oder Instandhalter das Problem erkannt, doch sobald es um zusätzliche Ressourcen geht, konnten sie sich bislang nicht durchsetzen. Das muss sich nun ändern.

**sueddeutsche.de:** Wie stehen die Chancen, dass sich etwas ändert?

**Langner:** Eigentlich nicht schlecht. Schließlich haben wir hierfür in Deutschland sehr gute juristische Grundlagen geschaffen. Die Gesetze sagen klipp und klar, dass die Einrichtung eines Risikomanagementsystems, explizit auch zu IT-Risiken, zu den Hauptpflichten der Geschäftsführung eines Unternehmens gehört. Der Gesetzgeber hat diesen Punkt so ernst genommen, dass er sogar die Beweislastumkehr und persönliche Haftung des Vorstands festgeschrieben hat. Nach Stuxnet kann nun kein Vorstand mehr sagen, von solchen Angriffen nichts mehr gewusst zu haben. Ich denke, da wird jetzt einiges in deutschen Vorstandsetagen in Bewegung kommen.

**URL:** <http://sueddeutsche.de/digital/interview-zum-stuxnet-sabotagevirus-die-buechse-der-pandora-ist-geoeffnet-1.1005985>

**Copyright:** sueddeutsche.de GmbH / Süddeutsche Zeitung GmbH

**Quelle:** (sueddeutsche.de/joku)