

04. Oktober 2009  
17:54 MESZ

## Ein Virus unter der Goldhaube

Bundesheer setzt sich mit Bedrohungen für Staat und Wirtschaft, die aus dem Internet kommen, auseinander

---

Wien - Ein Virus hat man sich schnell eingefangen - bei aller Vorsicht. Diese ist bei sensiblen militärischen Anlagen zwar besonders hoch, aber offenbar nicht hoch genug: Im Frühsommer wurde bei einer der ortsfesten Radaranlagen, die den passiven Teil des Luftraumüberwachungssystems Goldhaube darstellen, ein [Computervirus](#) eingeschleust. Der italienische Hersteller des Software-Updates hatte den Schädling in der Testphase übersehen, die Radarstation fiel aus.

"Wir haben das rechtzeitig bemerkt und bekämpft. Und weil das System entsprechende Redundanzen hat, ist die Luftraumüberwachung immer gewährleistet gewesen", sagt Oberst Walter J. Unger, der für elektronische Abwehr zuständige Geheimdienstoffizier des Bundesheeres im Gespräch mit dem Standard.

"Wir wollen nicht Panik schüren", versichert auch Edwin Potocnik, der neue Chef des Abwehramts. Aber er will sensibilisieren, im militärischen Bereich sowieso, aber auch im zivilen. Denn elektronische Kriegsführung mit Viren und Trojanern, mit professionellen Botnetzen zur gezielten Überlastung gewisser Bereiche des Internets und mit verschleierte Identitäten zum Datenklau werden heute vor allem Unternehmen angegriffen, die die Infrastruktur eines Landes betreiben.

Unter Militärexperten gilt als sicher, dass in China etwa 30.000 Spezialisten damit befasst sind, gezielte Internet-Attacken vorzubereiten. Damit waren im Vorjahr etwa Sympathisanten konfrontiert, die sich für die Unruhen in Tibet interessiert haben: Wer eine (angeblich von der Uno stammende) pdf-Datei mit Infos über Tibet auf seinem Rechner öffnete, bekam gleichzeitig einen Keylogger eingeschleust, mit dem sich der chinesische Geheimdienst über sämtliche Aktivitäten der angegriffenen User auf dem Laufenden halten konnte.

Dies berichtete Joe Pichlmayr von Ikarus Security Software bei der IKT-Sicherheitskonferenz, die das Abwehramt in der Vorwoche gemeinsam mit der Fachhochschule Hagenberg ausgerichtet hat. Pichlmayr beobachtete auch, dass bei den Uiguren-Aufständen im August dieses Jahres ein ähnliches Angriffsmuster verfolgt wurde - nur haben sich die Angreifer gleich einen Remote-Zugang zu den infizierten Systemen verschafft.

Sicherheitssoftware ist übrigens nur bedingt hilfreich: "Nur weil Sie Sicherheitssoftware einsetzen, heißt das nicht, dass Sie selber sich sicher verhalten", bläute Pichlmayr den Konferenzteilnehmern ein. So würden bedenkenlos fremde USB-Sticks eingesetzt, die inzwischen als Überträger von Malware fast so gängig sind wie Mails und manipulierte Websites. Die größte Sicherheitslücke der Computersysteme ist der Mensch. (Conrad Seidl, DER STANDARD, Printausgabe, 5.10.2009)

Diesen Artikel auf <http://derstandard.at> lesen.

---