Akt. 28.10.09; 10:47 Pub. 28.10.09; 10:47

HACKERANGRIFF AUF EDA

IT-Experte: «Hacker kann man nicht finden»

von Lukas Mäder

Tagelang zwingt ein Hackerangriff das Aussendepartement in die Knie. Für Hacker-Experte Stefan Frei keine Überraschung. Die Chancen, die Urheber der Attacke zu finden, sind für ihn gleich Null.

Professionelle Hacker haben die Computer des Departements für auswärtige Angelegenheiten angegriffen. Die Spezialisten sind tagelang damit beschäftigt, die schädliche Software, genannt Malware, zu finden (20 Minuten Online berichtete). Das überrascht den Cybercrime-Experten Stefan Frei von der ETH Zürich nicht. «Solche Angriffe wird es in Zukunft vermutlich vermehrt geben», sagt er. In den letzten Jahren habe sich Cybercrime professionalisiert und kommerzialisiert, die Grenzen zu Cyberwarfare (dem Krieg im Internet zwischen politischen Akteuren) ist fliessend. Inzwischen würden auch bei Cyber-Angriffen industriemässig Arbeitsteilung und Spezialisierung betrieben, schreibt Frei als Autor in einem Aufsatz. Das benötigte Spezialwissen werde eingekauft.

Hacker-Angriffe auf Computer-Netzwerke des Bundes werde es in Zukunft vermutlich vermehrt geben, sagt Stefan Frei, Cybercrime-Experte von der ETH Zürich. (Bild: pd)

Malware mit Geld-zurück-Garantie kaufen

Bei Angriffen auf spezifische Ziele wie Regierungen oder Firmen, sogenannte High value targets, haben laut Frei Virenschutzprogramme kaum eine Chance. Massgeschneiderte Schadsoftware (customized malware) wird solange angepasst, bis sie Virenscanner nicht mehr erkennen. «Im Untergrund gibt es Online-Dienste, die Malware automatisch gegen alle bekannten Virenscanner prüfen», sagt Frei. Oder man kauft die ganze Lösung gleich extern ein: «Malware wird auf dem Netz mit einer Geld-zurück-Garantie angeboten.

Link-Box

Die Website von Hacker-Experte Stefan Frei

Info-Box

Internetzugriff des EDA weitgehend wiederhergestellt

Die Mitarbeiter des Departement für auswärtige Angelegenheiten (EDA) können nach mehreren Tagen wieder normal

Erkennt sie ein Virenprogramm sechs Monate nach dem Kauf, bekommt der Käufer sein Geld zurück oder die neuste und verbesserte Version der Malware.» Die Qualität der Schadprogramme hängt unter anderem von der Höhe der Investitionen ab. Je höher der Wert des Ziels, desto mehr darf die Malware-Entwicklung kosten, und die Schadsoftware ist dementsprechend schwieriger zu identifizieren.

Das Einschleusen einer solchen Malware kann auf verschiedene Wege erfolgen. Das Ziel wird dabei direkt anvisiert, beispielsweise mit einer personalisierten E-Mail. Dank Informationen über die Zielperson — zu finden unter anderem auf Facebook — kann ein Angebot kreiert werden, das der Empfänger anklicken wird. Am Ende des Links wartet eine infizierte Webseite, erstellt nur für das Ziel des Hackers. Beim grossen Angriff auf das EDA und das Staatssekretariat für Wirtschaft Ende 2007 haben die Hacker beispielsweise E-Mails mit einem Fotowettbewerb verschickt, dessen Webseite im Look des Bundes daherkam.

Befehle empfängt der Trojaner per Bild

Ist die Malware einmal im gewünschten Netzwerk, kann es lange dauern, bis sie entdeckt wird. «Eine der wenigen Konstanten solcher schädlicher Programme ist, dass sie früher oder später eine Verbindung nach draussen aufnehmen müssen», sagt Frei. Dort setzen Programme an, die Malware entdecken können. Einfach ist aber auch das nicht: Denn die Kommunikation findet verschleiert statt. So gibt es Trojaner, die ihre Befehle als Bilder empfangen. Die Malware holt sich mit einem normalen Webrequest, wie ihn jeder Webbrowser ständig abschickt, ein Bild von einem Server, sagt Frei. Im Bild eingebaut sind Befehle zur Steuerung des Programms.

Die Sperrung der Internet-Verbindung nach der Entdeckung der Malware, wie sie auch beim EDA durchgeführt wurde, ist ein sinnvoller Schritt: «Solange man nicht weiss, wie das Programm nach aussen kommuniziert, kann so ein weiterer Schaden verhindert werden», sagt Frei. Haben die Spezialisten die Kommunikationsart entdeckt, können sie sich dadurch auch auf die Suche der Hacker machen. Doch Frei räumt den Strafverfolgungsbehörden wenig Chancen ein: «Einen professionellen Hacker kann man nicht finden, wenn er nicht gefunden werden will.» Die einzige Chance sei ein Fehler aus Dummheit oder Nachlässigkeit, sagt Frei. Oder wenn der Hacker mit seiner Tat angibt.

arbeiten. Der Internetzugriff ist wieder uneingeschränkt möglich, nachdem bereits am Montagabend der E-Mail-Verkehr wieder funktionierte. Das sagte EDA-Sprecher Georg Farago gegenüber 20 Minuten Online. Der Internetzugriff war am letzten Donnerstag gesperrt worden, nachdem Spezialisten einen Hackerangriff auf das EDA festgestellt hatten. Einige Spezialdienste sind jedoch weiterhin abgeschaltet. So können EDA-Mitarbeiter weiterhin nicht von aussen auf ihre E-Mails und die EDA-Laufwerke zugreifen, wie Farago sagt. Damit sei es noch nicht wieder möglich, von zu Hause aus zu arbeiten. Über den Stand der Untersuchung gibt das EDA keine Neuigkeiten bekannt. *(mdr)*