

Schadsoftware überall

Auf seiner Geschäftskarte steht Hacker. Kleiner darunter vermerkt Gunnar Porada seine wahre Profession: Senior IT-Security Consultant. Über die Professionalisierung der Online-Mafia ist er sehr beunruhigt.

Von Jan-Bernd Meyer*

CW: Was hat sich in puncto Gefahrlage im Internet getan?

PORADA: Es zeigen sich einige Veränderungen, die mir große Sorgen machen. Zum einen fällt auf, dass es immer mehr gute Leute gibt, die sich in der Thematik und mit der Technik sehr gut auskennen, die aber legal keine Arbeit finden. Das scheint eigentlich unlogisch, denn Bedarf an kompetenten Sicherheitsleuten besteht ja.

CW: Sicherheitsexperten finden keine Arbeit und gleiten dann ab ins kriminelle Milieu?

PORADA: Wenn die Experten keine Beschäftigung finden, bekommen sie wirtschaftliche Probleme. Dann kommt der Punkt, an dem sie sich fragen, ob sie nicht bei der Gegenseite anheuern sollen. Die zahlt nämlich Geld für solche Kompetenz, und sie weiß Security-Know-how zu schätzen.

CW: Wie haben wir uns das vorzustellen: Heuern diese Leute als Hacker an?

PORADA: Nein, so nicht. Aber nehmen Sie etwa Zero-Day-Exploits, das Erkennen von Systemschwachstellen also. Die werden immer öfter gar nicht mehr an die betroffenen Firmen und die Öffentlichkeit gemeldet. Dieses Wissen wird vielmehr direkt an Internet-Kriminelle verkauft. Das ist oftmals nicht einmal illegal. In diesem Zusammenhang sollte man auch darauf hinweisen, dass der Ankauf von CDs mit Daten von Steuersündern durch die deutsche Regierung ein ganz schlechtes Signal ist. Das heißt nämlich ganz einfach, dass es offensichtlich ein Geschäftsmodell für geklaute Daten gibt.

CW: Welche Bedrohungen im Web sind momentan besonders aktuell?

PORADA: Web Application Security ist eines der größten Probleme, die wir momentan haben. Kaum ein Unternehmen lässt hierzu

Sicherheitstests betreiben, keiner macht Sicherheits-Scans. Das scheint niemanden zu interessieren. Normale Penetrationstests für Betriebssysteme und Server – daran besteht schon ein Interesse. Aber vermutlich auch nur, weil wir von denen schon seit zehn bis 15 Jahren reden.

CW: Damit wird gefahrloses Surfen immer schwieriger.

PORADA: Richtig, egal welche Website ich ansurfe, ich hole mir permanent Schadsoft-



Sicherheitsexperte Gunnar Porada misstraut herkömmlichen Web-Browsern. Deshalb hat er den Browser „FireCastor“ entwickelt.

ware auf den Rechner. Und das auch bei seriösen Websites. Ich hatte selbst bei „Spiegel Online“ mehrere Banner, die von meinem Virusprotektor geblockt wurden, weil dort Schadsoftware durch fremde Werbebanner eingebunden wurde.

CW: Dann liegt das Problem aber auch bei den Web-Servern und deren Betreibern?

PORADA: In der Tat kann man hier einen weiteren Trend sehen: Web-Server sind unsicher und werden als Virenschleudern missbraucht. Das Einfallstor der Schädlinge ist dabei der Web-Browser. Von denen ist einer wie der andere durchlöchert und voller Schwachstellen. Das ist eine Tendenz, die mich wirklich sehr erschreckt.

CW: Bei der „New York Times“ haben Hacker einen Banner komplett nachgestellt, sich als Anzeigenkunde ausgegeben und ihre Werbung ganz offiziell platziert.

PORADA: Hier wurde dem User beim Anklicken des Banners vorgegaukelt, er habe einen Virus. Gleichzeitig wurde ihm angeboten, einen kostenlosen Anti-Virus-Protektor herunterzuladen. Das war relativ plump. Da weiß der intelligente Surfer, was gespielt wird. Das kann man aber auch besser machen. Da merkt der User nicht mehr, was Sache ist. Allein beim Öffnen einer Seite kann man sich einen Virus einfangen durch unzählige Schwachstellen in den Web-Browsern und Plug-ins.

CW: Was sind denn besonders apart Methoden?

PORADA: Es gibt Fälle, da wird der Computer zuerst durch einen Virus verschlüsselt. Dann wird der PC-Nutzer aufgefordert, seine Kreditkartennummer einzugeben, damit er ihn entschlüsseln kann. Jetzt hat man die Wahl: Entweder man gibt den Kriminellen die Kreditkartennummer oder

eben nicht. In letzterem Fall kommen Sie nicht mehr an Ihre Daten ran.

CW: *Hört sich schon viel ausgebuffter an als früher bei den pickligen Teenagern, die mal einen Virus in die Welt setzten.*

PORADA: Das ist das Problem. Die Professionalität, mit der Internet-Kriminelle heutzutage zu Werke gehen, ist sehr hoch. Die Leute, mit denen wir es auf der kriminellen Seite zu tun haben, wollen nur noch eines: Geld ver-

„Einer platziert Viren, ein Zweiter kassiert, ein Dritter verwischt Spuren.“ —

dienen und ihre Spuren verschleiern oder auf Unschuldige übertragen. Nach einhelliger Meinung gehen diese Kriminellen dabei professionell arbeitsteilig vor: Die einen platzieren die Schadsoftware, die Zweiten kassieren ab, die Dritten verschleiern die Spuren.

CW: *Lassen sich die Wege verfolgen, die das gestohlene Geld nimmt?*

PORADA: Das ist viel schwieriger geworden. Innerhalb eines Bankenverbands kann man Geldwege noch verfolgen und rückbuchen.

CW: *Aber nicht, wenn die Gelder in Ländern verschwinden, in denen die juristische Verfolgung schwieriger ist?*

PORADA: Die Welt wächst zusammen. Bei diesen Geschäften spielen Länder mit, die sagen: „Uns interessiert es nicht, wenn eine deutsche Bank nach dem Weg von Geldern fragt.“ Da gibt es dann keine Antworten mehr.

CW: *Wie geschäftsmäßig wird Internet-Kriminalität betrieben?*

PORADA: Das Business ist sehr mächtig geworden, und es wächst immer weiter. Beim Bewusstsein in Sachen Gefährdung hat es aber kaum Veränderungen gegeben. Im Gegenteil: Es herrscht eine gefährliche Scheinsicherheit.

Oft haben Unternehmen Schwierigkeiten, die Ursache für Sicherheitsvorfälle herauszufinden, ja überhaupt als Sicherheitsproblem zu erkennen. Mir hat eine Firma erzählt, dass sie bei Ausschreibungen ständig unterboten wurde. Das Konkurrenzangebot lag immer knapp unter ihrem eigenen. Folglich verlor sie ständig Aufträge. Der neue Firmenverantwortliche kam dann auf die Idee, ein Angebot einmal nach alter Schule auf Papier zu formulieren und abzugeben. Folge: Er wurde nicht unterboten wie sonst immer und bekam den Auftrag. Meinem Kunden wurde schlagartig klar, dass sein Problem in der IT zu suchen war.

Auf die Idee, dass ihre Unternehmensdurchlöcher sein könnte, kommen jedoch die wenigsten. Solange da nicht endlich Bewusstsein geschaffen und vorgebeugt wird, solange es auch keine bessere Kommunikation zwischen Technik und Unternehmensleitung gibt, so lange begeben sich Firmen auf einen Blindflug. Da müssen wir erst noch mehr Unternehmen über die Konsequenzen sprechen.

CW: *Wie sieht es mit der Strafverfolgung von Internet-Kriminellen aus?*

PORADA: Computer und auch Kommunikationswege können zwar erkannt werden. Aber die Zuordnung zu Personen ist immer noch extrem schwierig und technisch oftmals gar nicht eindeutig möglich. Ein Alibi ist ein Traum für die Strafverfolgung.

„Botnets für Hacker-Angriffe kann man spottbillig mieten.“ —

CW: *Gerade erst gab es spektakuläre Erfolge bei der Aushebelung von Botnets. Warum sind sie so gefährlich?*

PORADA: Botnets sind deshalb so gefährlich, weil man über sie und mittels DDOS-Attacken Server lahmlegen und Unternehmen praktisch vom Internet abschneiden kann. Damit kann man sie erpressen. In der organisierten Verbrechen ist solch eine Geldbeschaffungsmaßnahme fast ideal. Sie ist mit wenig Arbeit verbunden, und so ein Botnet kann man spottbillig mieten.

CW: *Gibt es Beispiele?*

PORADA: Web-Seiten wie „Ghostmarket“, die jetzt vom Netz genommen wurden, haben allen boten alles an: Kreditkarten, Bank-Logins, auch gehackte Online-Banking-Zugänge, Trojaner-Baukästen. Für einen Zugang zu einem Bankkonto zahlte man einen Bruchteil des darauf vorhandenen Guthabens. Da bekam man Screenshots mit allen Informationen zu einem Konto und dessen Zugangsdaten. Da bekamen Sie sogar eine gewisse Garantie mitgeliefert.

CW: *Garantien von der Mafia?*

PORADA: Wenn ein Konto schon leer war, bekamen Sie Ihr Geld wieder.

Risikofaktor Botnet



*Jan-Bernd Meyer

jbmeyer@computerwoche.de