Durch die Hintertür

Eine französische Firma zeigt dem US-Geheimdienst und anderen, wie man in fremde Computer eindringt VON PHILIPP ALVARES DE SOUZA SOARES

Der Suchmaschinenbetreiber Google schrieb im Frühjahr 2011 einen Preis aus. 60 000 US-Dollar sollten an den IT-Spezialisten gehen, der die Sicherungssysteme von Googles neuem Internetbrowser Chrome als Erster umgehen konnte. Bedingung: Der Gewinner musste Google erklären, wie er bei dem digitalen Einbruch vorging. Dem Franzosen Chaouki Bekrar und seinem Team gelang das Kunststück, doch sie verzichteten auf das Preisgeld. Bekrar sagte damals, er wolle seine Erkenntnisse lieber seinen Kunden anbieten – die würden mehr dafür zahlen.

Bekrar ist der Geschäftsführer des IT-Sicherheitsunternehmens Vupen aus Montpellier. Die Firma hat sich darauf spezialisiert, Sicherheitslücken in Computerprogrammen ausfindig zu machen. Dass es Schwachstellen in Software gibt, ist an sich nicht ungewöhnlich. Hersteller entdecken immer wieder welche. Sie sind nicht zuletzt der Grund dafür, dass man sich regelmäßig Updates herunterladen muss, um die Sicherheitslücken zu schließen. Doch Vupen geht anders vor: Die Firma sucht solche Schwachstellen und hält sie geheim. Dann bekommen die Schwachstellen einen besonderen Charakter, sie werden zu sogenannten Zero-Day-Exploits. Die Kenntnis solch exklusiver Geheimwege macht es möglich, unbemerkt die Kontrolle über einen fremden Computer zu übernehmen, Daten von ihm zu stehlen oder sie zu vernichten. Und Bekrars Team gehört zu den Besten, wenn es darum geht, solche Hintertüren in Programmcodes aufzuspüren.

Zero-Day-Exploits bedeuten für ihre Besitzer vor allem eines: Macht. Manchmal dauert es Jahre, bis eine Lücke entdeckt und geschlossen wird. So lange lässt sie sich etwa dazu nutzen, unbemerkt Menschen auszuspionieren oder Geschäftsgeheimnisse zu stehlen. Richtig eingesetzt, können sie sogar zur Waffe werden: Der Computerwurm Stuxnet, den die USA und Israel allem Anschein nach dazu nutzten, um iranische Atomanlagen zu beschädigen, wurde ebenfalls über eine solche Hintertür eingeschleust. Vupens Kunden sind diese digitalen Einbruchswerkzeuge viel Geld Wert. Branchenkenner gehen von Marktpreisen um die 100 000 US-Dollar pro Schwachstelle aus, wenn sie sich zur Attacke auf ein weitverbreitetes Programm wie beispielsweise einen Internetbrowser nutzen lässt. Der Umsatz von Vupen hat sich in den vergangenen Jahren jeweils verdoppelt. 2011 machte das junge Unternehmen bei knapp einer Million Euro Umsatz rund 415 000 Euro Gewinn.

Doch wer kauft die Sicherheitslücken überhaupt? Bekrar schweigt zu dieser Frage grundsätzlich. Vorletzte Woche wurde jedoch bekannt, dass der US-Geheimdienst NSA zu Vupens Kunden zählt. Die Anfrage einer Aktivistin nach dem Freedom of Information Act brachte einen entsprechenden Vertrag ans Licht. Die Amerikaner haben demnach im September 2012 ein Jahresabonnement für Exploits bei Vupen abgeschlossen. Angaben zu Preisen und weiteren Details wurden geschwärzt. Laut einem Bericht der *Washington Post* von Ende August gab die NSA in diesem Jahr insgesamt bereits 25 Millionen US-Dollar für Zero-Day-Exploits aus.

Weitere Vupen-Kunden sind nicht bekannt. Bekrar beteuert, dass er nur mit Strafverfolgungsbehörden und Geheimdiensten aus Nato-Mitgliedsstaaten oder deren Partnerländern zusammenarbeite. Selbst wenn das stimmt: Der Handel mit den exklusiven Software-Hintertüren ist legal und wird kaum reguliert. »Es gibt keine gesetzliche Grundlage, um den Handel mit Zero-Day-Exploits zu kontrollieren«, sagt Patrick Pailloux, Direktor der französischen Agentur für IT-Sicherheit ANSSI.

Ob Vupen mit französischen Geheimdiensten zusammenarbeitet, ist offen. Ein Sprecher der Regierung wollte dies auf Anfrage der *ZEIT* nicht kommentieren. Und deutsche Behörden? Das Verteidigungsministerium räumt zwar ein, dass die Bundeswehr Informationen über Bedrohungen durch Zero-Day-Exploits von Privatunternehmen beziehe, bestreitet aber eine Zusammenarbeit mit Vupen. Laut Bundesinnenministerium greift von den ihm unterstellten Behörden lediglich das Bundesamt für Sicherheit in der Informationstechnik auf solche Informationen von Privatunternehmen zu. Die Informationen würden zum Schutz der IT-Infrastruktur des Bundes eingesetzt. Zu weiteren Details, etwa den Firmennamen der Lieferanten, möchte man keine Auskunft geben. Der Bundesnachrichtendienst lehnte eine Stellungnahme ab.

Vupen nimmt es gern mit den Großen auf. Bekrar zeigt Softwareherstellern wie Microsoft, Apple oder Google regelmäßig, dass sein Team auch die ausgefeiltesten Sicherungsmechanismen knacken kann. Als Microsoft im Herbst des vergangenen Jahres sein neues Betriebssystem Windows 8 vorstellte, prahlte Vupen bereits zum Verkaufsstart mit einer Hintertür. Nur ein, zwei seiner Leute hätten daran gearbeitet, sagte Bekrar im März am Rande eines Hackerkongresses, nach etwa drei Monaten hätten sie die Sicherung bereits durchbrochen.

Die Hersteller sind gegen den Handel mit Sicherheitslücken. »Das Geschäftsmodell von Vupen kann uns natürlich nicht recht sein«, sagt Thomas Baumgärtner von Microsoft. Microsoft setzt auf den Idealismus der Hacker und zahlt keine Prämien, wenn sie Schwachstellen in den eigenen Produkten aufdecken. »Wir wollen diesen Bieterwettbewerb nicht unterstützen«, sagt Baumgärtner.

»Wir müssen den Handel mit diesen digitalen Waffen eindämmen«

Bis vor drei Jahren hat auch Vupen Sicherheitslücken noch kostenlos an die Hersteller gemeldet. Doch Bekrar wollte mit seiner Expertise Geld verdienen, das Aufdecken von Zero-Day-Exploits sei schließlich teuer. »Die Softwarefirmen hatten ihre Chance. Jetzt ist es zu spät«, sagt er.

»Der Markt wächst und ist völlig intransparent«, sagt Candid Wüest von Symantec, einem bekannten Hersteller von Anti-Viren-Software. Das Problem sei, dass man nicht genau wisse, was mit den Exploits eigentlich nach dem Verkauf geschehe. Anders als konventionelle Waffen, sind sie beispielsweise mit keiner Seriennummer versehen, die eine Rückverfolgung möglich machen würde. Wenn Symantec-Mitarbeiter selbst auf eine Sicherheitslücke stoßen, melden sie diese kostenlos an die Hersteller und erst danach an ihre Kunden. So bleibt genug Zeit, um die Lücke vorher zu schließen.

Die Europaabgeordnete Marietje Schaake setzt sich als eine von wenigen Politikerinnen für eine härtere Regulierung des Handels mit Software-Schwachstellen ein. Sie will Firmen wie Vupen zwingen, eine Lizenz zu erwerben, die etwa an Exportbeschränkungen oder Offenlegungspflichten gebunden wäre. »Wenn wir mehr Sicherheit wollen, müssen wir den Handel mit diesen digitalen Waffen endlich eindämmen«, sagt sie. Candid Wüest glaubt indes nicht, dass strengere Regeln helfen. Schon heute würden sich sogar Privatleute heimlich mit Exploits eindecken. »Wahrscheinlich würde der Zero-Day-Handel dann noch intransparenter werden.«

QUENGEL-ZONE

»Nach Gutsherrenart«

MARCUS ROHWETTERS
unentbehrliche Einkaufshilfe

Im Supermarkt wurde mir bewusst, dass ich womöglich ein ambivalentes Verhältnis zur Leibeigenschaft habe. Am Wurstregal stehend, fiel mir nämlich auf, dass ich den Ausdruck »nach Gutsherrenart« im Zusammenhang mit Leberwurst als Auszeichnung, bezogen auf Regierungshandeln jedoch als Missbilligung betrachte.

Was nun?, fragte ich mich. Wie sollte ich mich im Angesicht der Gutsherrenleberwurst verhalten? Einerseits war die Zeit ja recht angenehm, als die Gutsherren auf ihren Landgütern noch das Sagen hatten. Sie konnten ihre Knechte herumkommandieren und sie die schwere Arbeit verrichten lassen. In der Küche ließen sie die Wurst so kräftig würzen, wie es ihnen beliebte. Eine feine Sache, vorausgesetzt natürlich, man war der Gutsherr und nicht etwa einer der Knechte. Letztere hatten gewiss einen anderen Blick auf die Thematik, und noch heute wirft man Politikern und Unternehmern gerne vor, »nach Gutsherrenart« zu regieren. Also nach eigenem Gutdünken. Ich begann zu grübeln, denn ich stand ja noch am Wurstregal.

Da erinnerte ich mich plötzlich, warum Führungsverhalten und Fleischverarbeitung doch kein Widerspruch sein müssen. Wie schon oft in der Zeitung zu lesen war, handeln Wurstproduzenten bisweilen ja auch nach eigenem Gutdünken, und zwar sowohl bei der Rezeptur (nicht deklariertes Pferdefleisch!) als auch beim Umgang mit den Mitarbeitern der in ihren Fabriken tätigen Subunternehmen, denen es ähnlich ergeht wie früher den Knechten. Wie hatte ich das übersehen können? Lag in dieser Wurst eine tiefere Wahrheit?

Ich habe sie übrigens nicht gekauft. Wegen meiner politischen Einstellung. Und weil man wissen muss, dass Kalbsleberwurst zwar Leber vom Kalb enthält, Gutsherrenleberwurst aber ausschließlich solche vom Schwein.

Von Verkäufern genötigt? Genervt von Werbe-Hohlsprech und Pseudo-Innovationen? Melden Sie sich: quengelzone@zeit.de