



HALFLIFE

Hackers Beute

Eine winzige Lücke in Outlook hat ihm gereicht: Der Hacker Osama hat einem Software-Hersteller eine profitable und langjährige Spiele-Entwicklung geklaut. *von Thomas Papadhimas*

Ein einziger Hacker, vielleicht noch minderjährig, bringt eine Firma um ihren Lohn, an dem sie fünf Jahre lang gearbeitet hat. Der Kriminelle, der sich selbst „Osama bin Leaker“ nennt, richtet einen enormen Schaden an. Der beklaute Hersteller Valve wollte das Produkt

nicht nur verkaufen, sondern mit dem geistigen Wissen über weitere Firmen mit Lizenzgebühren und Marketingpartnerschaften Umsatz erzeugen. Das ist nun gelaufen. So schadet ein einziger Hacker einer ganzen Branche. Seine Beute: der Quellcode des Computerspiels Half Life 2.

In den Startlöchern krepirt

Half Life erschien 1998 und entwickelte sich schnell zum Dauerbrenner. Zahlreiche Erweiterungen und Online-Varianten wie Counterstrike hielten die Gemeinschaft bei Laune. Deshalb zählt Half Life und seine Erweiterungen noch heute zu den Top-Spielen. Fünf Jahre lang hatte Hersteller Valve nun an der Fortsetzung Half Life 2 gearbeitet. Auch die Grafikkartenhersteller rochen die Imagekraft. Ein Gerücht: Ati zahlte sechs Millionen Dollar für die Rechte, Half Life 2 zusammen mit ihren neuesten Grafikkarten vermarkten zu dürfen. Bereits im Vorfeld wurde die Werbetrommel kräftig gerührt. Unbestätigte Benchmark-Ergebnisse und Demofilme, welche die Karten von Ati ins rechte Licht rückten, kursierten im Netz – kein PC-Redakteur blieb verschont.

Der 30. September sollte der Tag werden. Auf einem großen Event in München wollte Ati die ersten Karten der europäischen Presse vorstellen. An diesem Tag sollten auch Bilder von Half Life 2 den Abend füllen, beide Produkte sollten ja zusammen den Markt erobern. Doch das Event blieb in den Startlöchern stecken. In einer Videobotschaft des Half-Life-Programmierers



Gabe Newell bekräftigte dieser die Zusammenarbeit von Valve und Ati. Danach wurde es stumm. Der Hersteller gab auf Nachfrage zu, dass er Half Life 2 an diesem Abend nicht mit den neuen Grafikkarten präsentieren durfte.

Einbruch in die Programmierer-Höhle

In einem offenen Brief an die Community gab Gabe Newell die Einzelheiten über das Desaster bekannt: Ein Hacker hatte sich in das Firmennetzwerk von Valve eingeklinkt und einen Teil des Quellcodes gestohlen. Wie das geschehen konnte, ist noch unklar. Immerhin arbeiten hochkarätige Programmierer in der Firma und keine Computeranfänger. Valve spekuliert, dass eine Sicherheitslücke in Outlook dies ermöglicht haben soll. Der Hacker konnte dadurch einen Keylogger, eine Software, die Benutzereingaben aufzeichnet, auf den Rechnern installieren, um Passwörter zu erspähen. Mit diesen konnte er in das System eindringen.

Hacker stehlen andauernd Software, denken viele. Doch diese Tat ist mehr als nur der Diebstahl von einigen Codezeilen: Da der Code durch Tauschbörsen in die Öffentlichkeit ge-

langte, ist er für Valve wertlos. Viele Spielehersteller leben nicht vom Spiel allein, sondern verkaufen Grafik- und Netzwerkcode an andere Firmen weiter. Die Partner bauen dann völlig neue Spieletitel aus den eingekauften Programmierkünsten. Da der Quellcode jetzt überall in diversen Tauschbörsen erhältlich ist, dürften diese Einnahmen für Valve verloren sein. Und große und lang ersehnte Projekte verschlingen gern mehrere Millionen Dollar, welche sich erst durch den Verkauf des Spiels und die Lizenzgebühren des Quelltextes wieder rechnen oder gar Gewinn erwirtschaften.

Mogeln leicht gemacht

Zudem können Programmierer mit dem Quelltext schnell und einfach Mogelprogramme entwickeln. Damit werden Spielfiguren sogar in Online-Partien unverwundbar, sie können durch Wände sehen oder auf Knopfdruck alle Waffen besitzen. Es wird Mitspieler geben, die solche Mogeleyen, Cheats genannt, verwenden (Mogler werden Cheater oder Lamer genannt). Welcher Online-Spieler verliert da nicht schnell den Spaß, gegen solche Gegner antreten zu müssen – und kauft sich ein anderes Spiel. Für Valve kritisch dabei: Vor allem die Online-Zocker oder deren finanzstarke Eltern gelten als besonders kaufkräftige Zielgruppe.

Lässt sich das Spiel noch retten?

Half Life 2 soll laut Valve nun erst im April 2004 erscheinen. Andere Quellen behaupten, dass es der Action-Knaller bis Weihnachten in die Läden schaffen soll. Sicher ist: Das Spiel hat sich verspätet, soll aber auf den Markt kommen. Laut Valve müssen viele der geklauten Codezeilen neu programmiert werden. Der Hacker hat inzwischen sogar schon eine lauffähige Version über Tauschbörsen im Internet veröffentlicht. Diese Version enthält noch keine Story, doch einen großen Teil des Spiels. Zwischen den zahlreichen Suchergebnissen für Half-Life-2-Downloads befinden sich hunderte Textdateien von anderen Benutzern, die das Problem erkannt haben und flehend bitten, Half Life 2 nicht herunterzuladen, um das Spiel zu retten.

Ein kleines Loch hat es ermöglicht, einer ganze Branche den Angstschweiß auf die Stirn zu treiben. Doch auch private Anwender sind von diesem Fehler betroffen: Wenn ein Hacker aus einem Büro, in dem erfahrene Programmierer arbeiten, sensible Daten stehlen kann – wie leicht wird es dann bei Privatanwendern gehen? PCgo hat die wichtigsten Sicherheitstipps gesammelt. Mit den Tipps in der rechten Spalte machen Sie Ihre Schotten dicht und schützen Ihre Daten. ■

RECHNER ABSCHOTTEN

Firewall von Windows XP aktivieren

Klicken Sie mit der rechten Maustaste auf die Netzwerkumgebung und wählen Sie „Eigenschaften“. Klicken Sie doppelt auf Ihre Internetverbindung und aktivieren Sie in der Kartei „Erweitert“ die Option „Diesen Computer und das Netzwerk schützen, indem das Zugreifen auf diesen Computer vom Internet eingeschränkt oder verhindert wird.“. Jetzt ist die Windows-Firewall aktiviert und wehrt Angriffe von außen ab.

Netzwerkaktivitäten überwachen

Aktivieren Sie in der Kartei „Allgemein“ der Einstellungen Ihrer Internetverbindung (siehe oben) die Option „Symbol bei Verbindung im Infobereich anzeigen“. Ein kleines Symbol neben der Windows-Uhr zeigt jetzt den Datenfluss ins Internet und von außen an. Dadurch bemerken Sie Sicherheitslecks leichter. Beachten Sie dabei: Sind Sie online, sendet Ihr Rechner in gewissen Intervallen einige Datenpakete, damit die Internetverbindung bestehen bleibt. Dieser Datenverkehr ist völlig normal. Leuchten die Statuslampen jedoch längere Zeit oder häufiger, obwohl kein Download oder Upload läuft, sollten Sie stutzig werden.

Outlook Express-Sicherheitseinstellungen

Die Sicherheitsoptionen von Outlook Express finden Sie unter „Extras/Optionen“ im Reiter „Sicherheit“. Achten Sie darauf, dass die Funktionen „Warnung anzeigen, wenn andere Anwendungen versuchen, E-Mail unter meinem Namen zu versenden“ und „Speichern oder Öffnen von Anlagen, die möglicherweise einen Virus enthalten könnten, nicht zulassen“ aktiviert sind.

Virensplanen

Viele Virens Scanner bieten einen Terminplaner an. Darin können Sie festlegen, wann der Scanner Ihr System nach Viren durchsuchen soll. Stellen Sie ihn so ein, dass er einmal in der Woche eine gründliche Suche startet. AntiViren-Schilder oder -Wächter sind ständig aktiv und überwachen jeden Dateizugriff oder Mail-Versand. Bietet Ihre Software diesen Schutz, sollten Sie ihn nutzen.

Links zum Thema

Hinweise über den Datenklau bei Valve nimmt der Hersteller unter helpvalve@valvesoftware.com entgegen.

■ www.windowsupdate.com

■ www.anti-trojan.net/de/

■ <http://passwortcheck.datenschutz.ch/check.php?lang=de>

■ www.it-sec.de/index/inhalt/vulchk.php/?sid=1f99038ad772a336f17e4b07a563d871