

Seit es Internet-Schachserver gibt, muss niemand mehr auf den Vereinsabend warten, wenn er Lust auf ein paar Blitzpartien hat. Es gibt auch keine Probleme mehr mit Spielern, die vorher zehn Bier und zum Mittag Zwiebelringe im Knoblauchkranz hatten. Es gibt aber ein ganz neues Problem: Betrüger, die ausnutzen, dass die Partner sich nicht mehr von Angesicht zu Angesicht gegenüber sitzen. Sie versuchen, sich mehr Bedenkzeit zu erschleichen oder heimlich ein Schachprogramm um Rat zu fragen, um mit unfairen Mitteln ein paar Partien zu gewinnen. Und noch andere dunkle Gefahren lauern in der rasanten Welt des Internet-Schachs.

Wer kennt das nicht? Beim Blitzen auf einem Schachserver hat man den Gegner schon im Sack und dazu noch mehr Zeit auf der Uhr. Doch irgendwie scheint die Zeit des Gegners nicht weniger zu werden, obwohl es jedes Mal ein erkleckliches Weilchen dauert, bis er zieht. Die eigene Zeit dagegen läuft ab wie Wasser aus der Badewanne, und irgendwann gewinnt der Gegner trotz Dame weniger auf Zeit. Das ist ärgerlich, und natürlich liegt der Verdacht nahe, der Gegner habe das absichtlich so eingefädelt. Aber geht das überhaupt?

Ein anderes Szenario: Nach einer Reihe von Partien wird man müde, ohnehin ist Schlafenszeit, also runter vom Server und ins Bett. Ach halt, es fehlen nur noch fünf Server-Elo an der nächsten Hundertergrenze, die nehmen wir noch mit. Dafür reicht ein Aufbaugegner, der zwei-, dreihundert Punkte weniger hat. Man findet einen, doch der spielt wie ein Großmeister. Ausgangs der Eröffnung steht man schon platt, und die Mittelspiel-Hinrichtung erfolgt schnell und effektiv auf die allertaktischste Weise. Der Kerl muss doch ein Schachprogramm benutzt haben! So ein Schummler, wieso erwischt den keiner?



Thomas Morus (Quelle: wikipedia.de)

Die meisten derartigen Fälle dürften einfach auf unglückliche Umstände zurückzuführen sein. „Wenn uns etwas Böses angetan wird, pflegen wir es in Stein zu meißeln; wenn uns aber Gutes getan wird, schreiben wir es in den Sand“, sagte Thomas Morus. Falls der Gegner die Verbindung verliert, wenn wir gerade auf Sieg stehen, merken wir uns das einfach besser, als wenn wir auf Verlust stehen. Auch ist diese Verbindungsverzögerung, neudeutsch Lag genannt, durchaus gegenseitig. Wer weiß, ob der Gegner nicht genau dasselbe Gefühl hat, betrogen zu werden?

Und wenn ein schwacher Gegner mal spielt wie ein Großmeister, dann kann das auch Zufall sein – die meisten Spieler haben viele tausend Partien auf den Servern gespielt. Schon rein statistisch gesehen können sie ab und zu mal eine aus Versehen geniale Partie abliefern, versteckt unter tausend Stümper-Runden. Trotzdem bleibt natürlich ein Restrisiko. Überall, wo es um etwas geht, und seien es auch nur lumpige Phantasie-Elos, finden sich Betrüger ein, die versuchen, Schwächen der Technik auszunutzen. Diese teilen sich in mindestens zwei Gruppen:

Die Dummen tun es nur, um ein paar Server-Elo zu ergattern oder mal einem starken Spieler eine Niederlage beizubringen, sie wirken rein destruktiv und lassen sich meist leicht enttarnen, weil sie kein technisches Verständnis haben und sich einfach dämlich anstellen. Es gibt aber noch *die Cleveren*, die es als intellektuelle

Herausforderung ansehen, Schwachpunkte in den Programmen zu finden und so lange wie möglich unentdeckt zu betrügen. Diese können potenziell sogar gefährlich sein für die Sicherheit der Computer ihrer Gegner. Hier hilft nur Aufklärung, denn nur wer die Tricks der Cheater wenigstens prinzipiell kennt, kann sich gegen sie schützen.

Es gibt noch einen Aspekt: Die Betreiber der kommerziellen Server haben im Interesse ihrer Kunden natürlich etwas dagegen, wenn Cheater ihr finsternes Werk verrichten. Darum versuchen die Programmierer, den Betrügern so viele Steine wie möglich in den Weg zu legen. Das ist ein grundsätzlich positiver Ansatz, der sich aber schnell ins Gegenteil verkehren kann, genau dann nämlich, wenn ein Schachprogramm anfängt, auf dem Rechner des Benutzers herumzuspüffeln und nach anderen Schachprogrammen zu suchen. Derartige Gerüchte laufen über den Chessbase-Client um. Ob da was dran ist? Und falls ja, kann man dagegen etwas tun?

Letzten Endes drohen auch noch Gefahren durch die Direktverbindung – man liefert dem Gegner ja seine IP-Adresse auf dem Silbertablett. Das ist zum Glück bei angemessener Vorsorge gar kein Problem, CSS Online zeigt, was es zu unternehmen gilt.

Hilfe, mein Schachprogramm spioniert

Im Blitz pusten selbst mittelmäßige Schachprogramme jeden Großmeister aus den Schuhen. Was läge für einen Betrüger also näher, als während einer laufenden Partie ein Schachprogramm mitrechnen zu lassen? Damit solche Spaßbremsen nicht die Server überfluten und die vorderen Ränge nur unter sich ausmachen, ergreifen die Server-Betreiber Gegenmaßnahmen. Der freie Schachserver FICS setzt vor allem auf die Selbstheilungskräfte der Gemeinschaft: wer glaubt, betrogen worden zu sein, meldet das bei einem Administrator, und wenn solche Meldungen über einen Spieler öfter eintreffen, werden seine Partien überprüft und er gegebenenfalls ausgeschlossen. Mehr passiert nicht, und ein ernsthaftes Betrüger-Problem existiert auf FICS nicht – diese Methode scheint also recht wirkungsvoll zu sein.

Die Betreiber kommerzieller Server glauben sich verpflichtet, technische Maßnahmen zu ergreifen. So überwacht beispielsweise der Chessbase-Client den Rechner des Benutzers auf Taskwechsel: holt man während einer Partie mehrfach ein anderes Fenster in den Vordergrund, hält der Client den Betrug für hinreichend erwiesen, löscht die Elo des vermeintlichen Betrügers und gibt eine Meldung in den Chat – auch wenn es nur die Textverarbeitung oder der E-Mail-Client war, der ab und zu aktiviert wurde.



Schummel-Meldung des Playchess-Clients

Im Internet kursieren Gerüchte, der Chessbase-Client tue noch mehr, nämlich die Prozessliste sowie die Titelzeilen aller geöffneten Fenster überwachen und darin nach bestimmten, auf Schachprogramme hindeutenden Begriffen schnüffeln. Der

Geschäftsführer von Chessbase, Matthias Wüllenweber, dementierte diese Gerüchte gegenüber der Computerzeitschrift c't; der Client überwache wie andere ausschließlich, ob er den Windows-Fokus verliere. Man habe aber nichts dagegen, dass die Leute glauben, er schnüffele herum, das sei sogar nützlich, weil es dadurch weniger Cheater gebe.

Das kann man Herrn Wüllenweber jetzt glauben oder es lassen – wer es gern mal ausprobieren möchte, kann von der Homepage des Autors das kleine Programm *Manni* herunterladen, das die Taskwechsel-Erkennung austrickst und auch erlaubt, die Titelzeilen der Fenster nach Belieben zu ändern. Damit könnte man also, während man auf irgendeinem Schachserver spielt, nebenher ein Schachprogramm bedienen, ohne dass der Client einen Fensterwechsel bemerkt und auf diese Weise mal testen, wie weit es wirklich her ist mit der Cheater-Erkennung der verschiedenen Server, ob sie also auf dem Rechner herumschnüffeln – was sich mit *Manni* effektiv verhindern lässt.



Manni kann andere Programme im Hintergrund bedienbar machen



Shredder schwebt dank Manni über der CB-GUI, ohne dass diese etwas merkt

Auch Versuche, ein Schachprogramm direkt anzubinden, gab es angeblich bereits auf dem Chessbase-Server. Unter Windows ist es überhaupt kein Problem, Informationen über fremde Fenster zu bekommen, ebenso über die Steuerelemente, die sie enthalten, also Buttons, Grafiken und so weiter. Es ist viel Arbeit, aber machbar, Fritzens grafisches Schachbrett auszulesen, regelmäßig auf Veränderungen zu untersuchen und daraus den gespielten Zug abzuleiten. Dann noch ein UCI-Interface drangebastelt, und schon kann man die Züge einem Schachprogramm übergeben. Dessen Antwort in Fritz einzugeben ist trivial und funktioniert über das Simulieren von Tastendrücken. Dieses Programm, falls es tatsächlich existierte, ist nirgends veröffentlicht worden, aber jeder, der die Arbeit nicht scheut und gern in der API-Dokumentation wühlt, kann sich selbst eins schreiben. Prinzipiell gibt es dagegen keinen funktionierenden technischen Schutz.

Die eleganteste und wirkungsvollste Möglichkeit, Schummler zu entlarven, besteht darin, Betrug direkt an den gespielten Partien zu erkennen. Die naive Methode, einfach alle Züge einer Partie mit einem Schachprogramm auf die Anzahl der Übereinstimmungen zu überprüfen, funktioniert nicht. Einmal, weil es sehr viele Schachprogramme gibt, die oft durchaus unterschiedliche Züge vorschlagen, vor allem aber, weil man damit, wenn überhaupt, nur die ganz dummen Cheater erwischen könnte, welche die komplette Partie von einem Programm spielen lassen.

Für die klugen Cheater hat sich Chessbase etwas Besseres einfallen lassen: eine statistische Analyse der Spielweise. Für Spieler jeder Stärke gibt es typische Fehlerhäufigkeiten. Auch, wie oft ein Spieler gegnerische Fehler bestraft, lässt sich statistisch erfassen, denn „manche Fehlzüge sind schwieriger zu widerlegen als andere – für Menschen. Für Programme ist alles leicht“, sagte Matthias Wüllenweber gegenüber der c't. Allerdings funktioniert diese Methode nur, wenn von dem betreffenden Spieler schon einige Partien vorliegen, je mehr, desto besser. Es soll laut Wüllenweber möglich sein, sogar Großmeister, die nur ab und zu in kritischen Stellungen Programmzüge ausführen, damit zu enttarnen. Als Beweis führt er die Deutsche Internet-Meisterschaft an, während deren Austragung auf dem Chessbase-Server ein Internationaler Meister überführt wurde. Bereits in der



Vorrunde unter Verdacht geraten, sei er für "vermutlich unschuldig" erklärt worden. Im Finale aber habe die Software in 15 der 22 Partien angeschlagen – normal soll ein Fehlalarm in etwa 30 Partien sein. Auch Großmeister Arkadi Naiditsch bekam schon die schwere Hand der Software zu spüren; er stritt immer ab, betrogen zu haben, was ihn aber nicht vor Repressalien bewahrte, unter anderem von Seiten des Deutschen Schachbundes.

Die Statistik-Methode kann natürlich keinen handfesten Beweis liefern, wohl aber ein durch gnadenlose Statistik mathematisch kalkulierbares Indiz. Allerdings ist das Verfahren zu aufwendig, um jede der knapp 200.000 pro Tag auf Schach.de gespielten Partien zu analysieren, sie kommt daher nur bei speziellen Preisgeld-Turnieren zum Einsatz. Und bei bestimmten Verdachtsfällen, beispielsweise, wenn ein Spieler sich in kurzer Zeit sehr stark verbessert.



CB-Chef Mathias Wüllenweber

Gegen die statistische Analyse gibt es aus Datenschutz-Sicht nichts einzuwenden, wohl aber gegen technische Maßnahmen. Wenn ein Programm den Computer des Anwenders darauf überwacht, welche Fenster im Vordergrund sind und daraus Verstöße gegen die Nutzungsbedingungen von Schachservern ableitet, dann handelt es sich um Spionage-Software. Das gälte umso mehr, falls es tatsächlich in Fenstertiteln und Prozessliste herumschnüffeln würde. Der Erfolg solcher Spionage dürfte ohnehin zweifelhaft sein, denn damit kann man gar nichts tun gegen ein Schachprogramm, das auf einem anderen Rechner läuft, etwa dem neben dem Monitor stehenden Laptop, oder auch nur ein Schachprogramm, welches auf demselben Rechner, aber in einer Virtual Machine gestartet wurde. Auch ist es absolut kein Problem, diese technische Überwachung ins Leere laufen zu lassen – ein Programm im Hintergrund bedienen oder seine Titelzeile verändern geht mit dem Manni-Tool sehr leicht, und unter welchem Namen ein Programm im Taskmanager steht, hängt am Dateinamen, der sich im Explorer verändern lässt.

Und wenn der Gegner auch mal Lag hat

Als Lag bezeichnet man die Verbindungsverzögerung: wenn zwei Computer über das Internet miteinander kommunizieren, dauert es eine kleine Weile, bis die gesendeten Daten von einem zum anderen gelangen, weil sie über verschiedene Server im Internet laufen müssen. Wie viele das sind, hängt davon ab, über welchen Provider die Gegner ihre Internet-Verbindung aufbauen und auch davon, wie weit sie räumlich voneinander entfernt sind. Wer sich dafür interessiert, welchen Weg seine Daten nehmen, kann auf der Windows-Kommandozeile beispielsweise mal *tracert www.playchess.com* eintippen – das Programm *tracert* zeigt die Zwischenstationen der Kommunikation mit der Webseite in einer Liste an.

Für Verzögerungen kann es viele Gründe geben; als Anwender hat man keinen Einfluss darauf, welchen Weg die Daten nehmen und wie lange sie brauchen. Gerade beim Blitz und Bullet sollen Verbindungsverzögerungen aber nicht zu Lasten der Bedenkzeit gehen, darum rechnen alle Schachserver diese Verzögerung wieder heraus. Die Software synchronisiert beim Start einer Partie die Uhren der Computer beider Gegner und merkt sich, wann genau ein Zug eintraf und wann der Gegenzug abgeschickt wurde. Aus den Differenzen bestimmt sie die Laufzeit der Übertragung und schlägt sie auf die inzwischen natürlich weitergelaufenen Uhren wieder drauf.

Praktisch führt das zu folgendem Phänomen: Einer der Spieler führt einen Zug aus. Darauf beginnt auf seinem Rechner die Uhr des Gegners zu laufen. Während sich der Zug in Form von IP-Paketen durch den Rechnerdschungel des Internets kämpft, läuft auf dem Rechner des Gegners aber noch die Uhr des Spielers, der gerade gezogen und den Zug schon abgeschickt hat. Kommt der endlich an, rechnet der Client die Übertragungszeit heraus und korrigiert die Uhr. Normalerweise dauert es nur Sekundenbruchteile den Zug zu übertragen, und die Korrektur der Uhr fällt nicht auf. Wenn aus irgendwelchen Gründen der Zug aber länger unterwegs ist, kann es passieren, dass beim Gegner plötzlich mehr Bedenkzeit angezeigt wird, sobald sein Zug eintrifft.

Die sehr faire Idee, niemanden für Verbindungsverzögerung zu bestrafen, sondern wirklich nur die tatsächlich verbrauchte Zeit von der Gesamtbedenkzeit abzuziehen, hat aber einen kleinen Schwachpunkt, denn man kann die Uhrensynchronisation austricksen und der Software vorgaukeln, der Zug wäre lange unterwegs gewesen. Auf diese Weise kann man beispielsweise fünf Sekunden pro Zug nachdenken, während die Software fest glaubt, es vergeht nur eine halbe Sekunde. In einer Bullet-Partie mit einer Minute Bedenkzeit ist das so, als ob ein Gegner eine und der andere zehn Minuten Bedenkzeit hätte. So was ist natürlich absolut tödlich; Lag-Cheating gehört zu den unangenehmsten Formen des Betrugs. Gegen einen, der ein Schachprogramm benutzt, hat man die Sache wenigstens schnell hinter sich, während Lag-Cheater sich immer mehr Bedenkzeit erschleichen und die Partie sich ewig hinziehen kann. Man kann natürlich nie sicher sein, ob der Gegner vielleicht in einem bolivianischen Dschungeldorf per Akustikkoppler online geht oder ob er wirklich ein Cheater ist. Verdächtig wird es, wenn er am Anfang einer Partie keinen Lag hat, sondern erst, wenn er auf die Verliererstraße gerät.

Das Problem ist, dass ein Lag so einfach zu simulieren ist. Der simple Trick besteht darin, die Zeitsynchronisation zu veralbern, indem man *die Uhr des Rechners verlangsamt*, auf dem der Schach-Client läuft. Man bekommt einen Zug geschickt, die Client-Software führt ihn auf dem Schachbrett aus und startet die Schachuhr. Diese aber fragt die Rechner-Uhr nach der Zeit, und wenn die Rechneruhr langsamer läuft, tut es auch die Schachuhr. Man kann es so einrichten, dass man die Zehntelsekunden in Superzeitlupe verrinnen sieht. Führt man dann seinen Zug aus, sind vielleicht zehn Sekunden vergangen, die Rechneruhr glaubt aber, es hätte nur eine Sekunde gedauert, und teilt das auch dem Client des Gegners mit. Auf dessen Rechner sind natürlich zehn Sekunden vergangen, aber der Client, der an eine langsame Internet-Verbindung glaubt, korrigiert den Zeitverbrauch auf eine Sekunde.

Das Verfahren ist flexibel; je nachdem, wie viel Zeit jemand erschwindeln will, kann er die Uhr verschieden stark korrigieren. Die meisten Server, darunter auch FICS, setzen beispielsweise das Programm *Timeseal* ein, um die Uhren zu synchronisieren. Der Autor dieses Beitrags hat knapp fünf Minuten gebraucht, um ein Programm zu schreiben, welches die Rechneruhr jede halbe Sekunde um 450 Millisekunden zurückstellt. Das reicht völlig, um *Timeseal* nachhaltig zu verwirren und mal eben die zehnfache Bedenkzeit zu bekommen!

Der Chessbase-Client stellt sich ein bisschen cleverer an und lässt sich nicht so leicht austricksen; offenbar synchronisiert er sich nicht an der Systemuhr, sondern vielleicht an irgendeinem Prozessor-Counter. Es gibt aber ein anderes, sehr einfaches Verfahren, gegen welches auch der Chessbase-Client machtlos ist: die Uhr nicht zurückzustellen, sondern sie *von vornherein langsamer* laufen zu lassen.



Uhren-Trickserei mit einer Zeitmaschine

Das geht ganz einfach und sogar völlig ohne Programmierkenntnisse: mit VMWare. Dabei handelt es sich um ein (für Privatanwender kostenloses) Programm, das so tut, als wäre es ein ganzer Computer. Man kann in VMWare beliebig viele virtuelle Computer erzeugen und ein Betriebssystem auf ihnen installieren, irgendeine Windows-Version, DOS oder ein beliebiges Linux. Genügend Speicher vorausgesetzt, kann man beliebig viele gleichzeitig in verschiedenen Fenstern laufen lassen. Zum Lag-Cheaten reichen zwei dieser Virtual Machines. In einer läuft der Schach-Client, in der anderen irgendein rechenzeitintensives Programm. VMWare teilt die verfügbare Rechenzeit unter beiden Virtual Machines



auf, aber ein Schachclient braucht kaum Rechenzeit. Nun passiert auf Rechnern mit dynamischer Taktung (das sind die meisten modernen Systeme) etwas Merkwürdiges: Die Uhr der Virtual Machine, welche die meiste Rechenzeit verbraucht, läuft normal weiter, die der anderen aber, in der das Schachprogramm läuft, geht plötzlich viel langsamer. Der Trick ist dosierbar, die Ablauf-Geschwindigkeit der virtuellen Zeit in der Schach-VM folgt brav der Belastung der anderen; je mehr es dort zu rechnen gibt, desto langsamer läuft hier die Uhr. Dabei wird die Bedienung keineswegs zäher, denn wenn Rechenzeit gebraucht wird, bekommt jede der VMs die Hälfte, der Schach-Client lässt sich also trotz in Zeitlupe verrinnender Zehntelsekunden flüssig bedienen.

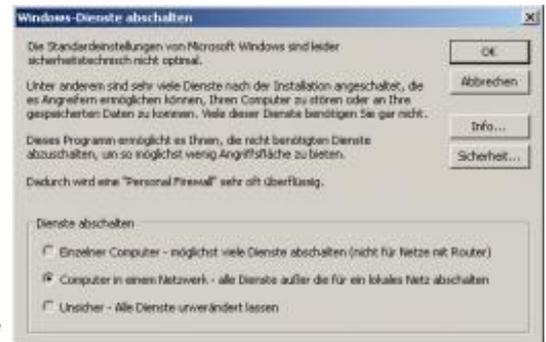
Lag-Cheater werden noch eine Menge anderer Tricks auf Lager haben, um die Clients zu beschummeln. Es ist aber nicht nötig, hier noch mehr aufzuführen, weil nur gezeigt werden sollte, wie einfach es ist, die Schach-Server auszutricksen. Das ist freilich nicht das, was man erwartet, wenn man 30 Euro für Chessbase oder 50 US-Dollar für ICC pro Jahr ausgibt, um im Netz Schach zu spielen – die Betreiber kommerzieller Server sollten hier etwas unternehmen, denn das kann man für sein sauer verdientes und in Online-Schach investiertes Geld doch wohl erwarten, oder? Zum Beispiel die Methode des kostenlosen FICS anwenden und ein paar gute Admins anstellen, welche die Selbstheilungskräfte der Community steuern.

IPs auf dem Silbertablett

Der Chessbase-Client bietet an, zwei Spieler direkt miteinander zu verbinden, statt die Züge über den Server auszutauschen. Es reduziert sowohl die Arbeit für den Server als auch den Lag, wenn die Spieler direkt miteinander verbunden werden, weil die Kommunikation der Spielpartner nicht den Umweg über den Server gehen muss. Das Problem an der Geschichte: Man serviert einem völlig Fremden seine IP-Adresse auf dem Silbertablett. Damit Schindluder zu treiben und an einem fremden Rechner herumzuhacken bewegt sich zwar schon an der Grenze zur Illegalität, ist aber schwer nachzuweisen.

Was kann passieren? Windows ist im Auslieferungszustand ein unsicher konfiguriertes Betriebssystem, das weiß jeder, der mal ein Windows 2000 oder XP ohne Servicepacks installiert hat und dann damit ins Internet gegangen ist – es dauert im Mittel anderthalb Minuten, bis über eine Sicherheitslücke der Rechner von böser Software infiziert wird. Auch wenn alle bekannten Updates eingespielt wurden, kann man einen Windows-Rechner relativ problemlos aus dem Internet außer Gefecht setzen. Es gibt ein ganzes Rudel Programme, die es ermöglichen, den Rechner eines zu betrogenden Schachgegners so lange ärgern, bis der die Zeit überschritten hat.

Woran liegt das? Der Grund ist, dass Windows verschiedene Programme startet, die auf Verbindungen aus dem Internet warten. Man spricht in diesem Zusammenhang von offenen Ports – ein offener Port ist nichts anderes als ein Programm, welches an der Internet-Verbindung lauscht und auf bestimmte ankommende Verbindungs-Anfragen reagiert. Das ist meist unerwünscht, darum sollte man sein Windows sauber konfigurieren, indem man derartige Programme nicht startet. Das geht per Hand in der System-Verwaltung, einfacher aber mit dem kostenlosen Programm „Windows-Dienste abschalten“, das von Sicherheits-Experten des Chaos Computer Clubs entwickelt wurde.



Dienste abschalten ist sicherer als Personal Firewall laufen lassen

Statt die Ursachen für offene Ports zu beseitigen, kann man natürlich auch an den Symptomen herumdoktern und dafür sorgen, dass die Programme, die ihre Lauscher gen Internet aufstellen, einfach keinen Internet-Zugang mehr haben. Dafür gibt es „Personal Firewalls“, vergleichbar mit einem Stück Pappe, das jemand vor eine Taschenlampe hält, wenn er kein Licht mehr wünscht, statt sie einfach auszuknippen. Personal Firewalls sind nicht immer komplett nutzlos, meist überwiegt der potenzielle Schaden jedoch den erhofften Nutzen: jede Woche geistern Meldungen u.a. durch den Heise-Newsticker, die wieder Sicherheitslücken in vermeintlichen Sicherheits-Programmen anzeigen, beispielsweise hier. Wer sich auf dem Laufenden halten möchte, sollte gelegentlich bei Heise Security reinschauen.

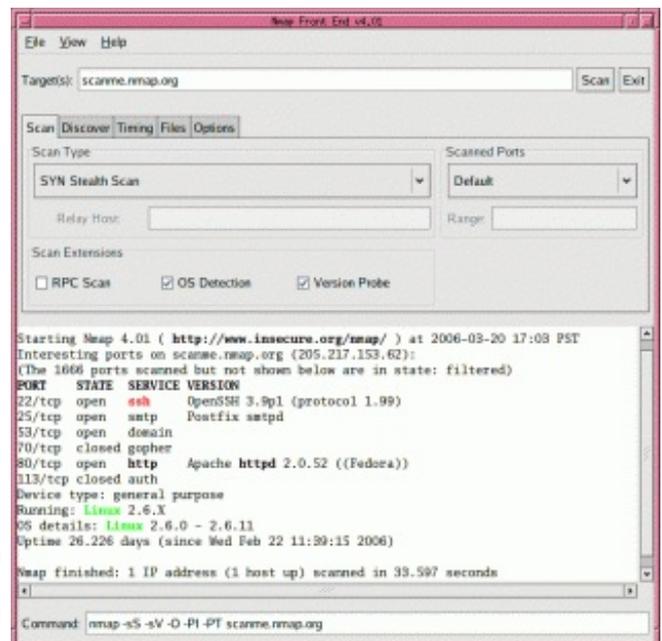


Für Online-Schachspieler halten Personal Firewalls neben der Sicherheitslücken-Problematik noch eine Hürde bereit: die Block-Funktion. Fast jede Personal Firewall bietet eine Funktion, bestimmte IP-Adressen eine Zeit lang zu sperren, sobald ein Angriff von ihnen ausging – wobei meist schon ein harmloser Portscan als Angriff interpretiert wird. Das bietet raffinierten Schummlern eine interessante Möglichkeit: sie können einen Portscan mit gefälschter Absender-IP auf den Rechner des Gegners loslassen. Das ist sehr leicht mit dem Standard-Portscanner NMAP. Die Personal Firewall wird dann brav diese IP-Adresse für eine halbe Stunde blockieren. Wenn die gefälschte Absender-IP aber „zufällig“ die des Schachservers war, wird das „Sicherheits“-Programm jede Kommunikation mit dem üblen Server unterbinden. Für den Server, der sich verzweifelt müht, Kontakt herzustellen, sieht das so aus, als habe ein Spieler die Verbindung verloren ...

Diese Block-Funktion war vor einigen Jahren nach der Installation einer PFW meist eingeschaltet, heute haben viele (aber nicht alle) Hersteller eingesehen, dass der Schaden doch überwiegen könnte und lassen sie deaktiviert. Wer diese oberflächlich betrachtet sinnvoll scheinende Funktion dennoch aktiviert, macht seinen Rechner damit aber nicht sicherer, sondern angreifbarer.

Weder eine Personal Firewall noch das Abschalten aller Dienste kann jedoch verhindern, dass zumindest ein Port offen ist: der, den das Schachprogramm benutzt, um mit seinem Server zu kommunizieren. Wenn irgendwelche Sicherheitslücken in den Clients, ob Blitzin oder Fritz, entdeckt werden, ist alle Hoffnung verloren.

Die Kommunikation zwischen Client und Server, zwischen Fritz und Schach.de oder Blitzin und ICC, läuft verschlüsselt über die Internet-Leitung. Wenn diese Verschlüsselung geknackt wird, ist ebenfalls Holland in Not. Wer das für



Den Portscanner NMAP gibt es für fast alle Betriebssysteme

unwahrscheinlich hält, kann hier eine nette Beschreibung finden, wie das ICC-Protokoll gehackt wurde. Der Chessbase-Server blieb bisher von erfolgreichen Hack-Attacken anscheinend verschont – oder auch nicht: Chessbase würde das ja kaum an die große Glocke hängen.

Fazit

Schummler haben es ziemlich leicht – wer betrügen will, wird locker einen Weg finden. Kommerzielle Schachserver tun so, als würden sie technische Vorsorge treffen, um die Nutzung eines Schachprogramms zu verhindern, aber die Taskwechsel- und Titelzeilen-Erkennung lässt sich viel zu leicht austricksen, und eine statistische Analyse ist bei der Vielzahl der gespielten Partien einfach zu aufwendig. Gegen Lag-Schummler tun die Server-Betreiber gar nichts und geben auch nicht vor, etwas zu tun. Die beste Lösung hat der Free Internet Chess Server (FICS) gefunden, er vertraut auf die Selbstheilungskräfte der Gemeinschaft. Freilich haben es die ehrenamtlichen FICS-Admins auch leichter als die Admins von Schach.de und ICC, denn wer wegen Schummelns bei FICS rausfliegt, kann nicht sagen, er wolle sein Geld zurück – er hat ja gar nichts bezahlt. Den Programmierern der kommerziellen Server kann man nur empfehlen, ihre Zeit nicht damit zu verschwenden, weitgehend nutzlose Schutzmechanismen zu programmieren.

Die Gefahren durch die Weitergabe der IP-Adresse bei Direktverbindung kann man glücklicherweise leicht abwehren. Wer sich hier nicht ganz sicher ist, sollte die Direktverbindung abschalten. Eine Personal Firewall von Drittanbietern ist grundsätzlich überflüssig, öffnet nur neue Einfallstore und schafft, wenn sie schlecht konfiguriert ist, sogar ganz neue Möglichkeiten für Schummelei beim Online-Schach. Nutzer von Windows XP sollten Servicepack 2 installieren, das bereits ein Programm enthält, welches unerwünschte Verbindungen aus dem Internet verhindert.

(Lars Bremer)
