DIE KUNST DES EINBRUCHS

KEVIN MITNICK

& William Simon

mitp

RISIKOFAKTOR IT

Inhalt

Vorwort

Hacker spielen ein Spiel miteinander. Sie versuchen, sich gegenseitig auszutricksen, sich zu überrumpeln, sich eins auszuwischen. Eins der begehrtesten Ziele wäre eindeutig, damit angeben zu können, sich in die Website meiner Security Company oder in meinen eigenen Rechner gehackt zu haben.

Ein anderes wäre, einfach einen Hack zu erfinden und mir und meinem Koautor Bill Simon alles so plausibel zu verkaufen, dass wir ihn für bare Münze nehmen und in diesem Buch veröffentlichen.

Das ergab eine faszinierende Herausforderung, ein geistiges Wettspiel, das Bill und ich immer und immer wieder gespielt haben, als wir die Interviews für dieses Buch führten. Für die meisten Journalisten und Autoren ist die Klärung der Echtheit eine ziemliche Routineangelegenheit: Ist dies wirklich die Person, für die er oder sie sich ausgibt? Hat diese Person wirklich für die Organisation gearbeitet oder arbeitet sie immer noch dort, wie sie behauptet? Hatte diese Person die von ihr behauptete Stellung inne? Kann diese Person die eigene Story mit Dokumenten oder Beweisen belegen und kann ich überprüfen, ob diese Dokumente echt sind? Gibt es seriöse Leute, die für die Echtheit der Story oder von Teilen davon bürgen?

Bei Hackern ist die Quellenprüfung ziemlich vertrackt. Den meisten der Leute, deren Stories in diesem Buch erscheinen, droht ein Strafverfahren, wenn ihre wahre Identität herauskommt – andere sind deswegen bereits ins Gefängnis gewandert. Also ist es ein zweifelhaftes Unterfangen, nach den wahren Namen zu fragen, oder zu erwarten, dass sie als Beweis geliefert werden.

Diese Menschen sind mit ihren Geschichten nur an die Öffentlichkeit gegangen, weil sie mir vertrauen. Sie wissen, dass ich selbst hinter Gittern gesessen habe, und verlassen sich darauf, dass ich sie nicht hereinlegen und in eine solche Situation bringen werde. Und doch haben viele ungeachtet der Risiken handfeste Beweise für ihre Hacks angeführt.

Und trotzdem bleibt es möglich – und ist sogar wahrscheinlich –, dass einige ihre Stories durch Details aufbauschen, um sie überzeugender zu gestal-

ten, oder ein Lügengebäude errichten, aber drum herum genug funktionierende Exploits konstruiert haben, damit alles den Anschein der Wahrheit erhält.

Wegen dieses Risikos haben wir sorgfältig auf ein hohes Maß an Zuverlässigkeit geachtet. Bei allen Interviews habe ich jedes einzelne technische Detail abgeklopft, eingehend nach Erklärungen für alles gefragt, das sich irgendwie merkwürdig angehört hat, und bin so ab und zu wieder darauf zurück gekommen, um zu sehen, ob die Story immer noch die gleiche war oder ob er beim zweiten Mal etwas anderes erzählt. Oder ob sich diese Person auf einmal »nicht mehr genau erinnern konnte«, wenn sie nach einem schwer zu bewerkstelligen Schritt befragt wurde, der auf einmal bei der Story fehlte. Oder ob diese Person einfach nicht genug von dem zu wissen schien, was er oder sie getan zu haben behauptete, oder nicht erklären konnte, wie er oder sie von Punkt A zu Punkt B gekommen ist.

Jede der ausführlicheren Geschichten in diesem Buch hat, wenn nicht anders erwähnt, meinen »Riechtest« bestanden. Mein Koautor und ich sind uns über die Glaubwürdigkeit aller Personen einig, deren Stories wir hier aufgenommen haben. Allerdings sind oft die Details verändert worden, um den Hacker und das Opfer zu schützen. In mehreren Stories wurden die Identitäten der Firmen verschleiert. Ich habe die Namen, Branchen und Standorte der Zielorganisationen verändert. In einigen Fällen sollen irreführende Informationen die Identität des Opfers schützen oder eine Wiederholung des Delikts verhindern. Aber die grundlegenden Schwachstellen und die Beschaffenheit der Vorfälle sind korrekt geblieben.

Gleichzeitig funktionieren nur wenige der Exploits aus diesem Buch immer noch so wie beschrieben, weil Softwareprogrammierer und Hardwarehersteller fortlaufend die Schwachstellen der Sicherheit durch Patches und neue Versionen ihrer Produkte beheben. Das könnte den allzu selbstsicheren Leser zu der Meinung verführen, dass er oder sie sich keine Sorgen zu machen brauche, da die Schwachstellen bereits ausgebügelt und korrigiert worden sind, und weder die Leser noch ihre Firmen beunruhigt sein müssten. Aber wir können aus diesen Stories – egal ob sie sechs Monate oder sechs Jahre alt sind – die Lektion lernen, dass Hacker täglich neue Schwachstellen finden. Lesen Sie das Buch nicht, um etwas über spezielle Schwachstellen in bestimmten Produkten zu erfahren, sondern um Ihre Einstellungen zu ändern und zu einer neuen Entschlossenheit zu gelangen.

Und lesen Sie das Buch auch, damit Sie sich von all diesen immer wieder überraschenden Exploits jener heimtückischen und cleveren Hacker unterhalten, einschüchtern und erschrecken lassen können.

Einige sind schockierend, andere sind regelrechte Augenöffner, wieder andere Hacker machen Ihnen Spaß, da sie Nerven wie Drahtseile haben. Falls Sie ein IT- oder Sicherheitsprofi sind, bringt jede Story für Sie einige Lektionen mit sich, damit Sie Ihre Organisation sicherer machen können. Falls Sie keinen technischen Hintergrund haben und einfach gerne Thriller mögen, in denen es um Waghalsigkeit, Risikobereitschaft und echten Mumm geht, dann ist dies Buch für Sie genau das richtige.

Bei jedem einzelnen der hier vorgestellten Abenteuer bestand die Gefahr, dass draußen jemand an die Tür klopft und ein Trupp Polizisten, FBI-Agenten und Leute vom Geheimdienst bereits mit Handschellen wartet. Und in einigen Fällen ist auch genau das passiert.

Bei den anderen besteht diese Möglichkeit immer noch. Kein Wunder, dass die meisten dieser Hacker noch niemals vorher bereit waren, ihre Stories zu erzählen. Die meisten der Abenteuer, die Sie hier lesen können, werden zum allerersten Mal veröffentlicht.

Kapitel 1

Der Casino-Hack für eine Million Dollar

Jedes Mal, wenn irgendein [Programmierer] sagt: »Keiner wird sich je eine solche Mühe machen«, wird gerade irgendein Bengel in Finnland sich genau diese Mühe machen.

Alex Mayfield

Da kommt bei einem Zocker dieser magische Moment, wenn schlichter Nervenkitzel sich vervielfacht, um zu einer 3D-Fantasie zu werden – der Moment, in dem die Habgier die Moral frisst und das Casinosystem einfach zu einem weiteren Berg wird, der erobert werden will. In genau jenem Moment ist man nicht nur von einem idiotensicheren Weg überzeugt, um am Roulettetisch oder beim Einarmigen Banditen abzuräumen, sondern es verschlägt einem regelrecht den Atem.

Alex Mayfield und drei seiner Freunde haben mehr getan, als nur einem Tagtraum nachzuhängen. Wie viele andere Hacks begann auch dieser als intellektuelle Übung, um die bloße Machbarkeit zu prüfen. Am Ende haben die vier tatsächlich das System geschlagen und die Casinos um »etwa eine Million Dollar« gebracht, sagt Alex.

In den frühen 90ern arbeiteten die vier als Consultants im Hightech-Bereich und ließen das Leben locker angehen. »Wissen Sie, da arbeitet man und verdient Geld und dann setzt man aus, bis man wieder pleite ist.«

Las Vegas war weit weg und mehr eine Kulisse für Filme und TV-Shows. Als eine Technologiefirma ihnen einen Auftrag zur Softwareentwicklung gab und sie ihr Produkt dann im Rahmen einer Trade Show auf einer Hightech-Messe vorstellen sollten, packten sie die Gelegenheit beim Schopf. Sie waren alle das erste Mal in Las Vegas und hatten die Chance, bei voller Spesenübernahme

die Glitzerwelt selbst zu erleben – wer hätte das abgelehnt? Da sie in einem großen Hotel separate Zimmer hatten, bedeutete das, Alex konnte seine Frau und Mike seine Freundin zu diesem Spaß mitnehmen. Gemeinsam mit Larry und Marco brachen die beiden Paare auf, um es in *Sin City* so richtig krachen zu lassen.

Alex sagt, sie hatten vom Spielen keine Ahnung und wussten nicht, was sie erwartete. »Du steigst aus dem Flugzeug und siehst all die alten Ladys an den Einarmigen Banditen. Das wirkt komisch und ironisch und du saugst es wie ein Schwamm auf.«

Nach der Trade Show saßen die vier mit den beiden Damen im Casino ihres Hotels, spielten an den Automaten und genossen die freien Getränke, als Alex' Frau sie vor eine Herausforderung stellte:

> *»Diese Maschinen arbeiten doch mit Computern, oder? Ihr kennt euch doch mit den Dingern aus, könnt ihr da nicht was drehen, damit wir mehr gewinnen?«*

Sie gingen zurück auf Mikes Hotelzimmer, wo sie zusammensaßen und sich den Kopf zerbrachen, um sich Theorien über die Funktionsweise der Maschinen einfallen zu lassen.

NACHFORSCHUNGEN

Das war der Auslöser. Die vier wurden »echt neugierig auf die ganze Sache und wir haben uns das genauer angeschaut, als wir wieder zu Hause waren«, sagt Alex und ruft sich die lebhaften Erinnerungen dieser kreativen Phase wieder ins Gedächtnis. Sie brauchten nur ein paar Nachforschungen anstellen, um ihre Vermutungen bestätigen zu sehen. »Ja, im Prinzip sind das Computerprogramme. Also haben wir uns überlegt, ob es Möglichkeiten gibt, wie man diese Maschinen knacken könnte.«

Es hat Leute gegeben, die Spielautomaten besiegen konnten, indem sie »die Firmware ersetzt hatten« – indem sie also an den Computerchip im Gerät gekommen waren und das Programm gegen eine Version ersetzt hatten, bei der deutlich bessere Ausschüttungen als vom Casino beabsichtigt möglich wurden. Andere Teams hatten das geschafft, aber dazu mussten sie offenbar mit Angestellten des Casinos gemeinsame Sache machen, und auch nicht einfach mit irgendwem, sondern mit einem der Spielgerätetechniker. Für Alex und seine Kumpel war »ein ROM-Austausch in etwa so wie einer alten Dame eins überzuziehen und dann mit ihrer Handtasche abzuhauen«. Wenn sie sich schon einer solchen Herausforderung stellten, dann wollten sie es als Test für ihr Geschick als Programmierer und ihren Intellekt sehen. Und ihnen fehlten obendrein die speziellen Talente des Social Engineerings; sie kamen aus dem

Computerbereich und hatten keine Ahnung, wie man sich an einen Casinomitarbeiter heranmacht und ihm eine kleine Gaunerei vorschlägt, um an fremdes Geld kommen zu können.

Aber wie konnten sie das Problem nun angehen? Alex erklärte:

> *Wir haben uns gefragt, ob wir die Reihenfolge der Karten irgendwie voraussagen könnten. Oder ob es da vielleicht eine Backdoor [Softwarecode, der nachträglich einen unerlaubten Zugriff auf das Programm möglich macht] gibt, die ein Programmierer sich praktischerweise selbst eingebaut hat. Alle Programme werden von Programmierern geschrieben, und in jedem Programmierer steckt ein kleines Schlitzohr. Wir haben gehofft, dass wir vielleicht auf eine Backdoor stoßen, so wie das Drücken einer bestimmten Tastensequenz, um die Gewinnchancen zu erhöhen, oder einen einfachen Programmierfehler, den wir ausnutzen konnten.*

Alex las das Buch *The Eudaemonic Pie* von Thomas Bass (dt. *Der Las Vegas Coup*), die Geschichte einer Gruppe von Computerfreaks und Physikern, die in den 80er Jahren in Las Vegas beim Roulette gewannen, indem sie einen selbst erfundenen »wearable computer« (tragbarer Computer) in Zigarettenschachtelgröße benutzten, um die Ergebnisse beim Roulettespiel vorherzusagen. Ein Teammitglied hatte dabei am Tisch gestanden und über Tastenklicks die Geschwindigkeit des Rouletterades und die Art der Kugeldrehung eingegeben, und der Computer hat über Funk Töne an ein Hörgerät im Ohr eines anderen Teammitglieds gesendet. Diese Person hat dann die Signale interpretiert und beim Roulette entsprechend gesetzt. Sie hätten eigentlich Taschen voller Geld wegtragen müssen, aber das war nicht der Fall. Nach Meinung von Alex hatte »ihr Plan eindeutig Potenzial, krankte aber an schwerfälliger und unzuverlässiger Technologie. Und es gab eine Menge Beteiligte, also war das Zwischenmenschliche problematisch. Wir hatten uns fest vorgenommen, diese Fehler nicht zu wiederholen.«

Alex fand, ein computerbasiertes Spiel sei leichter zu besiegen, »denn der Computer ist absolut deterministisch« – das Ergebnis beruht auf vorher abgelaufenen Vorgängen oder nach einem alten Programmierspruch: »Gute Daten rein, gute Daten raus.« (Ursprünglich lautet dies negativ formuliert: »Müll rein, Müll raus« (*garbage in, garbage out*)).

Das war ganz nach seinem Geschmack. Als Jugendlicher war Alex Musiker in einer Kultband gewesen und hatte von einer Karriere als Rockstar geträumt. Als das nichts wurde, hat er auf ein Mathematikstudium umgesattelt. Mathematik lag ihm, und obwohl er sich nicht sonderlich um eine Aus-

bildung gekümmert (und das College abgebrochen) hatte, war er hier lange genug dran geblieben, um ein solides Kompetenzwissen zu haben.

Er beschloss, nähere Nachforschungen anzustellen, und machte sich auf die Reise nach Washington, DC, um dort im Patentbüro einige Akten einzusehen. »Mir ging durch den Kopf, vielleicht ist jemand dumm genug gewesen und hat den ganzen Code einem Patent beigelegt«, das für ein Videopokergerät gestellt wurde. Und tatsächlich behielt er Recht. »Damals konnte man die eigene Erfindung schützen, wenn man dem Patent den Maschinencode beilegt, weil der Code mit Sicherheit eine vollständige Beschreibung der Erfindung enthält, aber in einer nicht sonderlich benutzerfreundlichen Form. Ich bekam einen Mikrofilm mit dem Maschinencode und suchte in der Hex-Darstellung der Seiten nach interessanten Abschnitten, die in [verwendbare Form] disassembliert werden mussten.«

Bei der Analyse des Codes fanden sich einige Geheimnisse, die das Team faszinierend fand, aber sie beschlossen, der einzige Weg für echte Fortschritte bestünde darin, genau die Art von Maschine in die Finger zu kriegen, die sie zu hacken versuchten, um sich den Code dort selbst anschauen zu können.

Als Team ergänzten sie sich untereinander sehr gut. Mike war ein überdurchschnittlich kompetenter Programmierer, im Hardwaredesign bewanderter als die anderen drei. Marco, ebenfalls ein gewiefter Programmierer, war aus Osteuropa eingewandert und sah aus wie ein Teenager. Aber er war ein ziemlicher Draufgänger, ein Großmaul mit einer »Lass mich mal ran«-Haltung. Alex glänzte beim Programmieren und war derjenige, der die nötigen Kenntnisse der Kryptographie beisteuern konnte. Larry war nicht der große Programmierer und konnte wegen eines Motorradunfalls nicht viel reisen, war aber ein ausgezeichneter Organisator und hielt das Projekt auf Spur, damit alle darauf konzentriert blieben, was in der jeweiligen Phase gerade erledigt werden musste.

Nach den ersten Nachforschungen hatte Alex das Projekt »irgendwie vergessen«. Marco war dagegen voll auf die Idee eingestiegen. Er bestand darauf: »Das ist keine große Sache, es gibt dreizehn Staaten, in denen man diese Geräte legal kaufen kann.« Schließlich hatte er die anderen dazu überredet, wenigstens einen Versuch zu machen. »Wir dachten uns, ach, was soll's?« Jeder warf soviel Geld in den Topf, dass sie sich die Reise und die Kosten eines Gerätes leisten konnten. Wieder machten sie sich nach Vegas auf – dieses Mal auf eigene Kosten und mit einem anderen Ziel vor Augen.

Alex sagt: »Um eine Slotmaschine zu kaufen, muss man im Grunde einfach nur hingehen und einen Ausweis aus einem Staat vorlegen, in dem der Besitz legal ist. Mit einem Führerschein aus einem solchen Bundesstaat haben die wirklich kaum Fragen gestellt.« Einer aus der Gruppe kannte praktischerweise jemanden, der in Nevada lebte. »Der war so was wie der Onkel einer Freundin von einem Bekannten und hat in Vegas gewohnt.«

Sie entschieden sich dafür, dass Mike mit diesem Mann reden sollte, weil er »so etwas von einem Geschäftsmann an sich hat, er ist ein sehr präsentabler Typ. Es wird unterstellt, dass damit illegale Glücksspiele gemacht werden sollen. Das ist wie mit Waffen«, erklärte Alex. Viele der Geräte gehen über den *grauen Markt* weg, d.h. sie werden außerhalb akzeptierter Vertriebswege an Vereine oder Clubhäuser verkauft. Aber er war trotzdem doch überrascht, dass »wir genau die gleichen Geräte kaufen konnten, wie sie in den Casinos eingesetzt werden«.

Mike gab dem Mann für den Geldspielautomaten einer japanischen Marke 1.500 Dollar. »Dann packten zwei von uns dieses verdammte Dings ins Auto. Wir fuhren es nach Hause, als hätten wir ein Baby auf dem Rücksitz.«

DER HACK WIRD ENTWICKELT

Mike, Alex und Marco schleppten die Maschine in den ersten Stock eines Hauses, wo sie ein Zimmer nutzen konnten. Was für ein Nervenkitzel diese Erfahrung war, erinnert sich Alex heute noch, er zählt sie zu einer der aufregendsten seines Lebens.

> *Wir machen das Teil auf, wir nehmen das ROM raus und versuchen herauszukriegen, um was für einen Prozessor es sich handelt. Ich hatte die Entscheidung für dieses japanische Gerät getroffen, das wie der Nachbau einer der großen Marken aussah. Ich dachte so bei mir, vielleicht haben die Ingenieure unter größerem Druck gearbeitet und waren ein wenig faul oder nachlässig gewesen.*
> *Es stellte sich heraus, dass ich Recht hatte. Sie hatten einen 6809 [Chip] genommen, ähnlich wie ein 6502, den man in einem Apple II oder einem Atari findet. Es war ein 8-Bit-Chip mit einem 64K Speicherplatz. Ich war ein Assembler-Programmierer, also war mir das vertraut.*

Die von Alex ausgewählte Maschine war eine, die schon seit zehn Jahren benutzt wurde. Immer wenn ein Casino einen Geldspielautomaten mit einem neuen Design kaufen will, muss die *Las Vegas Gaming Commission* die Programmierung genau untersuchen und gewährleisten, dass das Design faire Auszahlungen an die Spieler ermöglicht. Die Zulassung neuer Gerätevarianten kann ein langwieriger Prozess sein, also neigen die Casinos dazu, alte Geräte länger zu nutzen, als man erwarten dürfte. Bei einem älteren Gerät hoffte das Team, eher auf eine überholte Technologie zu treffen, die dann wohl weniger anspruchsvoll und leichter anzugreifen war.

Der Computercode, den sie aus dem Chip downgeloadet haben, war in binärer Form, also eine Folge von Einsen und Nullen – die grundlegendste

Ebene von Computeranweisungen. Um das in eine verarbeitbare Form zu übersetzen, mussten sie zuerst etwas *Reverse Engineering* machen – bei diesem Prozess versucht ein Ingenieur oder Programmierer herauszubekommen, wie ein vorhandenes Produkt designt ist. In diesem Falle hieß das, alles von der Maschinensprache in eine Form zu konvertieren, die sie verstehen und mit der sie arbeiten konnten.

Alex brauchte einen *Disassembler*, um den Code zu übersetzen. Die Vier wollten ihr Vorhaben nicht durch den Kauf der Software verraten – ein Akt, der für sie wie der Gang zur örtlichen Bibliothek gewesen wäre, um dort Bücher über Bombenbau zu finden. Sie haben sich ihren eigenen Disassembler geschrieben, und diese Arbeit beschreibt Alex als »kein Kinderspiel, aber es hat Spaß gemacht und war relativ leicht«.

Als der Code des Videopokergeräts erst einmal durch den neuen Disassembler geschickt worden war, setzten sich die drei Programmierer zusammen, um alles durchzusehen. Normalerweise ist es für einen fähigen Softwareingenieur leicht, schnell die Programmabschnitte zu lokalisieren, auf die er oder sie sich konzentrieren will. Das liegt daran, dass jemand, der Code schreibt, überall »Straßenschilder« einbaut – Notizen, Kommentare und Erläuterungen, die die Funktion eines jeden Abschnitts erklären, so wie es in einem Buch Überschriften für die verschiedenen Abschnitte, Kapitel und Unterteilungen eines Kapitels gibt.

Wenn ein Programm in die Form kompiliert wird, die die Maschine lesen kann, werden diese Hinweisschilder ignoriert – der Computer oder Mikroprozessor hat für sie keine Verwendung. Somit fehlen dem Code nach dem Reverse Engineering all diese hilfreichen Erklärungen; um in der Straßenschildmetapher zu bleiben, ist dieser hergestellte Code wie eine Straßenkarte ohne Ortsnamen oder Kennzeichen für Autobahnen und Straßen.

Sie gingen auf dem Monitor die Seiten mit dem Code durch und suchten nach Hinweisen auf die grundlegenden Fragen: »Worin besteht die Logik? Wie werden die Karten gemischt? Wie werden die Ersatzkarten ausgewählt?« Aber das Hauptaugenmerk der Gruppe in diesem Augenblick war, den Code für den Zufallszahlengenerator (*Random Number Generator* – RNG) zu lokalisieren. Alex' Vermutung, dass die japanischen Programmierer beim Schreiben des Codes für diese Maschine Shortcuts (Abkürzungen) eingebaut haben könnten, die zu Fehlern in der Gestaltung des Zufallszahlengenerators führen, stellte sich als korrekt heraus.

UMSCHREIBEN DES CODES

Alex klingt stolz, als er diese Arbeit beschreibt. »Wir waren Programmierer, wir waren in unserer Arbeit echt gut. Wir haben herausbekommen, wie sich die Zahlen im Code in Spielkarten auf der Maschine verwandelten, und

haben dann ein bisschen was in C geschrieben, der das Gleiche macht«, sagt er, wobei er sich auf die Programmiersprache »C« bezieht.

> *Wir waren motiviert und haben rund um die Uhr eine Menge Arbeit reingesteckt. Ich würde sagen, es hat etwa zwei oder drei Wochen gedauert, bis wir an den Punkt kamen, wo wir die Funktionsweise des Codes ziemlich gut durchschaut haben.*
>
> *Du untersuchst alles, stellst Vermutungen an, schreibst neuen Code, brennst ihn in das ROM [den Computerchip], steckst alles wieder in das Gerät und schaust, was passiert. Wir haben beispielsweise Routinen geschrieben, durch die auf dem Bildschirm oben auf den Karten Hex-Zahlen [hexadezimale] ausgegeben wurden. Also wir haben uns erstmal um die Grundprinzipien gekümmert, wie der Code die Karten ausgibt.*
>
> *Es war eine Kombination aus Versuch und Irrtum und einer immer feiner werdenden Analyse; wir sind dem Code ziemlich schnell auf die Schliche gekommen. So haben wir schließlich genau kapiert, wie die Zahlen im Rechner zu den Karten auf dem Bildschirm wurden.*
>
> *Unsere Hoffnung war, dass der Zufallszahlengenerator sich als relativ simpel herausstellen würde. Und in diesem Fall in den frühen 90ern war das auch so. Ich habe da noch ein paar Nachforschungen angestellt und herausgefunden, dass er auf Arbeiten von Donald Knuth aus den 60ern basierte. Diese Typen haben von dem ganzen Kram nichts neu erfunden, sie haben einfach schon vorhandene Forschungsergebnisse über Monte-Carlo-Methoden und so etwas genommen und das in ihren Code gepackt.*
>
> *Wir haben ganz genau herausbekommen, welchen Algorithmus sie benutzt haben, um die Karten zu generieren; das nennt man einen linear feedback shift register[1], und es war ein ziemlich guter Zufallszahlengenerator.*

Aber bald entdeckten sie, dass der Zufallszahlengenerator einen schweren Fehler aufwies, der ihre Aufgabe deutlich erleichtert hat. Mike erklärte, dass es »ein relativ simpler 32-Bit-RNG war, also lag für das Knacken die Berechnungskomplexität in Reichweite und wurde mit ein paar guten Optimierungen fast trivial«.

Die produzierten Zahlen waren also nicht wirklich zufällig. Aber Alex denkt, dass das auch seinen guten Grund hat:

1. Linear rückgekoppeltes Schieberegister

Wenn es wirklich zufällig wäre, könnten sie die Gewinnchancen nicht einstellen. Sie könnten nicht verifizieren, wie die Chancen wirklich sind. Auf manchen Maschinen wurden mehrere Royal Flushes nacheinander ausgegeben. Das hätte überhaupt nicht passieren dürfen. Also wollen die Designer prüfen können, ob sie die richtigen Statistiken haben, sonst meinen sie, dass sie keine Kontrolle über das Spiel haben.
Was die Designer beim Entwurf dieser Maschine ebenfalls nicht erkannt haben, war, dass sie im Grunde genommen nicht nur einen Zufallszahlengenerator brauchen. Statistisch gesehen gibt es in jeder Geberunde zehn Karten – die fünf, die zuerst gezeigt werden, und eine alternative Karte für jede dieser fünf, die aufgedeckt wird, falls der Spieler Karten ablegt. Bei diesen frühen Versionen der Maschine stellte sich heraus, dass diese zehn Karten im Grunde zehn aufeinander folgende Zufallszahlen vom Zufallszahlengenerator waren.

Alex und seine Partner begriffen, dass die Programmanweisungen bei dieser frühen Produktversion einfach schlecht durchdacht waren. Und aufgrund dieser Fehler erkannten sie, dass sie einen relativ simplen, aber eleganten und cleveren Algorithmus schreiben konnten, um die Maschine zu besiegen.

Alex erkannte, dass der Trick darin bestehen konnte, nach Spielbeginn zu schauen, welche Karten vom Gerät angezeigt werden, und dann die Daten in ihren Computer zu Hause einzugeben, um diese Karten zu identifizieren. Ihr Algorithmus könnte den Punkt berechnen, an dem sich der Zufallsgenerator befand und durch wie viele Zahlen er noch gehen musste, bevor er das gesuchte Blatt anzeigt – den Royal Flush.

Wir gehen also an unsere Testmaschine und lassen unser kleines Programm laufen und es gibt uns korrekt die jeweils nächste Kartensequenz aus. Wir waren ganz schön aus dem Häuschen.

Alex führt diese Aufregung darauf zurück, »dass du weißt, du bist schlauer als ein anderer und kannst ihn besiegen. Und dass wir in unserem Fall damit ganz schön Geld machen konnten.«

Sie gingen shoppen und fanden eine Casio-Armbanduhr, die einen auf Zehntelsekunden einstellbaren Countdown hatte. Davon haben sie drei gekauft, eine für jeden, der ins Casino ging. Larry hat derweil hinter dem Computer die Stellung gehalten.

Sie waren bereit, ihre Methode auszuprobieren. Einer aus dem Team sollte mit dem Spielen anfangen und das Blatt ansagen, das er bekommen hatte – den Wert und die Farbe jeder der fünf Karten. Larry sollte dann die Daten in

ihren eigenen Computer eingeben. Zwar war das keine bekannte Marke, aber doch ein Gerät, das bei Nerds und Computerfreaks beliebt und für diesen Zweck ganz großartig war, denn sein Chip war viel schneller als der aus dem japanischen Videopokergerät. Es dauerte nur ein paar Momente, die genaue Zeit zu berechnen, die bei den Countdowntimern eingestellt werden musste.

Wenn der Alarm losging, sollte ihr Mann an der Slotmaschine auf den Play-Knopf drücken. Aber das musste auf den Bruchteil einer Sekunde exakt passieren. Das war nicht so problematisch, wie es erscheint, erklärt Alex:

> *Zwei von uns haben eine Zeitlang als Musiker gearbeitet. Wenn du ein Musiker bist und einigermaßen Rhythmusgefühl hast, kannst du einen Knopf auf plus oder minus fünf Millisekunden genau drücken.*

Wenn alles so klappte wie gewünscht, sollte die Maschine den heiß ersehnten Royal Flush anzeigen. Sie testeten das auf ihrem eigenen Gerät und übten so lange, bis alle bei ihren Versuchen mit einer anständigen Prozentzahl den Royal Flush treffen konnten.

In den vergangenen Monaten hatten sie – in Mikes Worten – »über Reverse Engineering die Arbeitsweise der Maschine herausgefunden, genau erfahren, wie die Zufallszahlen zu Karten auf dem Bildschirm verwandelt werden, wo und wann ganz genau der RNG iteriert hat, sowie alle relevanten Eigenheiten der Maschine, und ein Programm entwickelt, das diese Variablen berücksichtigt, damit wir, wenn wir den Status einer bestimmten Maschine an einem exakten Zeitpunkt kennen, mit hoher Genauigkeit die exakte Iteration des RNG zu jedem beliebigen Zeitpunkt innerhalb der nächsten Stunden oder gar Tage vorhersagen können«.

Sie hatten die Maschine geschlagen und zu ihrem Sklaven gemacht. Sie hatten sich der intellektuellen Herausforderung eines Hackers gestellt und waren erfolgreich gewesen. Mit diesem Wissen konnten sie reich werden.

Es machte Spaß, solchen Tagträumen nachzuhängen. Konnten sie das aber auch im Tohuwabohu eines Casinos bewerkstelligen?

ZURÜCK INS CASINO UND AN DIE SPIELAUTOMATEN

Es ist eine Sache, an einem privaten, sicheren Standort an der eigenen Maschine herumzufummeln. Etwas völlig anderes ist es dagegen, in der Mitte eines hektischen Casinos zu sitzen und dessen Geld zu stehlen. Dafür braucht man Nerven wie Drahtseile.

Ihre Frauen freuten sich schon mächtig auf die Reise. Die Männer ermunterten sie zu engen Kleidern und auffälligem Verhalten, also Zocken, Plaudern, Kichern, Drinks bestellen, in der Hoffnung, dass sich die Leute im

Überwachungsraum, die die »Eye in the Sky«-Kameras bedienten, von hübschen Gesichtern und einer Menge Haut ablenken ließen. »Also haben wir das so stark wie möglich forciert«, erinnert sich Alex.

Die Hoffnung war, dass sie einfach hineinpassen und in der Menge aufgehen würden. »Mike konnte das am besten. Er bekam schon langsam eine Glatze. Mit seiner Frau zusammen sahen sie wie die typischen Spieler aus.«

Alex beschreibt die Szene, als wäre das alles gestern erst passiert. Marco und Mike sind wohl etwas anders vorgegangen, aber für Alex ist es wie folgt gelaufen: Mit seiner Frau Annie hat er sich zuerst für ein Casino entschieden und dann ein Videopokergerät ausgesucht. Er musste ganz genau den exakten Zyklus der Maschine kennen. Eine ihrer Methoden war, eine Videokamera in einer Schultertasche zu verstecken. Im Casino hat der Spieler die Tasche dann so hingestellt, dass die Kameralinse auf den Bildschirm des Videopokergeräts zeigte, und die Kamera dann eine Weile laufen lassen. »Es konnte ganz schön verzwickt sein«, erinnert er sich, »die Tasche so hinzustellen, dass sie genau in der richtigen Position ist, ohne dass es aussieht, als wäre die Position wirklich wichtig. Wir haben einfach alles vermieden, das irgendwie verdächtig wirkt und Aufmerksamkeit auf sich zieht.« Mike bevorzugte eine andere, nicht so anspruchsvolle Methode: »Um das Timing für den Zyklus von unbekannten Geräten berechnen zu können, haben wir am Bildschirm die Karten zu zwei verschiedenen Zeitpunkten abgelesen, die viele Stunden auseinander lagen.« Er musste darauf achten, dass an der Maschine in der Zwischenzeit nicht gespielt wurde, weil das die Iterationsrate verändert hätte, aber das war leicht: Er brauchte nur nachzusehen, ob immer noch die gleichen Karten wie bei seinem letzten Besuch im Display angezeigt wurden, und das war meist der Fall, denn »an Geräten mit hohen Wetteinsätzen wird normalerweise nicht so häufig gespielt.«

Beim zweiten Ablesen der angezeigten Karten hat er auch seinen Casio-Timer synchronisiert und dann per Telefon die Zeitdaten und Kartenfolgen der Maschine an Larry übermittelt, der diese Daten dann in ihren Computer zu Hause in ihr Programm eingab. Auf diesen Daten basierend konnte der Computer nun den Zeitpunkt des nächsten Royal Flush vorhersagen. »Wir haben gehofft, das in nur ein paar Stunden schaffen zu können, aber manchmal dauerte es Tage«, und in diesem Fall mussten sie bei einem anderen Gerät alles von vorne beginnen, vielleicht auch sogar in einem anderen Hotel. In dieser Phase konnte die Zeiteinstellung der Casio-Uhr schon um etwa eine Minute verschoben sein, das war aber noch nah genug dran.

Für den Fall, dass jemand bereits an der Zielmaschine spielte, kehrten Alex und Annie extra früh ins Casino zurück, um in der Zwischenzeit an anderen Geräten zu spielen, bis der Zocker weggegangen war. Dann setzte sich Alex an die Zielmaschine und Annie an das Gerät daneben. Beim Spielen achteten sie betont darauf zu wirken, als ob sie viel Spaß hätten. Alex erinnert sich:

Ich hab dann ein Spiel angefangen und es sorgfältig mit meinem Casio-Timer synchronisiert. Wenn das Blatt angezeigt wurde, habe ich es mir gemerkt – den Wert und die Farben der fünf verschiedenen Karten, und dann weitergespielt, bis ich acht aufeinander folgende Karten im Gedächtnis hatte. Ich hab dann meiner Frau zugenickt, dass ich mich auf den Weg mache, und bin zu einer unverdächtigen Telefonzelle direkt im Casinobereich gegangen. Mir blieben etwa acht Minuten, in denen ich zum Telefon kommen, dort das Nötige erledigen und es wieder an das Gerät schaffen musste. Meine Frau hat mit dem Spielen weitergemacht. Jedem, der an meinem Gerät spielen wollte, hat sie gesagt, dass ihr Mann da sitzt.

Wir hatten uns eine Möglichkeit ausgedacht, wie wir einen Anruf bei Larrys Pieper machen und die Zahlen auf der Telefontastatur eingeben können, um ihm die Karten durchzugeben. So brauchten wir die Kartenwerte nicht laut aussprechen – die Casinoleute achten immer auf solche Sachen. Larry hat dann die Karten wieder in den Computer eingegeben und unser Programm gestartet.

Dann hab ich ihn angerufen. Larry hat den Hörer an den Computer gehalten, der zwei kurze Hinweistöne von sich gab. Beim ersten hab ich die Pausentaste auf der Stoppuhr gedrückt, um den Countdown anzuhalten. Beim zweiten hab ich die Pause wieder losgelassen, um die Stoppuhr neu zu starten.

Die von Alex übermittelten Karten haben dem Computer einen exakten Anhaltspunkt gegeben, an welcher Stelle sich der Zufallszahlengenerator der Maschine befand. Indem er die vom Computer berechnete Verzögerung eingab, hat Alex eine wesentliche Korrektur für die Stoppuhr der Casio-Uhr vorgenommen, damit sie in genau dem richtigen Moment losging, wenn der Royal Flush erscheinen sollte.

Nach dem Neustart der Stoppuhr ging ich zu dem Gerät zurück. Als sie dann »biep, biep, nööt« machte, hab ich genau beim »nööt« auf der Maschine wieder die Play-Taste gedrückt.

Bei diesem ersten Mal haben wir $ 35.000 gewonnen, glaube ich.

Wir kamen an den Punkt, an dem wir ungefähr 30 bis 40 Prozent Treffer hatten, weil es wirklich gut ausgearbeitet war. Es hat nur dann nicht richtig geklappt, wenn wir das Timing nicht richtig hinbekommen haben.

Für Alex war das erste Mal, als er gewonnen hatte, »ganz schön aufregend, aber auch Furcht einflößend. Der Pit-Boss[2] war so ein miesepetriger Italiener. Ich war sicher, dass er mich komisch anschaute; vielleicht hatte er diesen verwunderten Gesichtsausdruck, weil ich dauernd zum Telefonieren ging. Ich glaube, er ist vielleicht hochgegangen und hat sich die Aufzeichnungen angeschaut.« Trotz der Anspannungen brachte das »doch einen Nervenkitzel mit sich«. Mike erinnert sich, er sei »natürlich nervös gewesen, dass jemandem bei mir ein komisches Verhalten aufgefallen sein könnte, aber eigentlich hat mich niemand irgendwie seltsam angesehen. Meine Frau und ich wurden einfach wie Gewinner bei hohen Einsätzen behandelt – man gratulierte uns und machte uns Komplimente.«

Sie waren so erfolgreich, dass sie sich bei der Höhe der Gewinne Sorgen machen mussten, dass man auf sie aufmerksam wurde. Ihnen dämmerte die Erkenntnis, dass sie das merkwürdige Problem von zuviel Erfolg bekamen. »Das war eine ganz hohe Liga. Wir haben große Jackpots mit mehreren Zehntausend Dollar gewonnen. Für einen Royal Flush wurden 4.000 zu 1 gezahlt – bei einem Spielautomaten mit 5 Dollar Einsatz sind das zwanzig Riesen.«

Das war noch steigerungsfähig. Einige Spielvarianten nennen sich progressiv, das heißt, der Jackpot steigert sich, bis jemand ihn knackt, und die Gruppe konnte diese Spiele genau so leicht gewinnen.

> *Ich hatte einen mit 45 Riesen gewonnen. So ein Techniker in voller Montur kam dazu – wahrscheinlich der gleiche Typ, der auch rumgeht und die Maschinen repariert. Er hat einen Spezialschlüssel, den die Aufsichtsleute nicht haben. Er macht den Kasten auf, zieht das [elektronische] Board heraus und nimmt direkt vor meiner Nase den ROM-Chip heraus. Er hat ein ROM-Lesegerät bei sich, mit dem er den Chip aus dem Spielautomaten mit einem goldenen Master-Chip vergleicht, der unter Verschluss gehalten wird.*

Der ROM-Test ist schon seit Jahren eine Standardprozedur, erfuhr Alex. Er nimmt an, dass sie »auf diese Weise schon mal reingelegt wurden«, aber schließlich auf diese Masche gestoßen sind und dann den ROM-Check als Gegenmaßnahme eingeführt haben.

Durch die Aussage von Alex kam ich auf den Gedanken, ob die Casinos diesen Test wegen eines Kerls durchführen, den ich im Gefängnis getroffen habe und der tatsächlich die Firmware ausgetauscht hat. Ich fragte mich, wie das so schnell gemacht werden kann, ohne dass man erwischt wird. Alex meinte, das sei sicher über Social Engineering gelaufen, die Sicherheit sei kompromittiert und jemanden im Casino selbst bestochen worden. Er spekuliert, dass viel-

2. Führen in einem Casino die Aufsicht über mehrere Spieltische (A.d.Ü.)

leicht sogar der goldene Master-Chip ausgetauscht wurde, mit dem der Automatenchip verglichen wird.

Das Schöne bei diesem Hack des Teams war, beharrte Alex, dass sie die Firmware nicht auszutauschen brauchten. Und sie fanden, dass ihre eigene Vorgehensweise eine viel größere Herausforderung darstellte.

Das Team konnte mit den Gewinnen nicht in dem Maße weitermachen wie bisher; sie mussten befürchten, dass »irgendwann einer eins und eins zusammenzählt und sagt, den Kerl hab ich doch schon mal gesehen. Wir bekamen es mit der Angst zu tun, geschnappt zu werden.«

Neben der stets gegenwärtigen Sorge, erwischt zu werden, machten sie sich auch über das Problem mit der Steuer Gedanken: Bei jedem Gewinn über $ 1.200 fordert das Casino den Ausweis und meldet die Auszahlung an den IRS[3]. Mike sagt, dass »wenn der Spieler keinen Ausweis vorlegt, dann gingen wir davon aus, dass die Steuern von der Auszahlung abgezogen werden, aber wir wollten keine Aufmerksamkeit auf uns ziehen, um das herausfinden.« Das Bezahlen der Steuer war »kein großes Problem«, aber »dann gibt es Belege, dass man wahnsinnig viel Geld gewinnt. Also ging es bei der Logistik viel darum, wie wir unter dem Radar bleiben konnten.«

Sie mussten sich eine andere Vorgehensweise ausdenken. Nach dieser kurzen Zeit von »ET nach Hause telefonieren« begannen sie, sich etwas Neues einfallen zu lassen.

NEUER ANSATZ

Zu jener Zeit hatten unsere Leute zwei Ziele: Sie wollten eine Methode entwickeln, bei der sie mit Blättern wie einem Full House, einem Straight oder Flush gewinnen, damit die Ausschüttung nicht so immens sind, dass sie auffallen. Und sie wollten es weniger offensichtlich und weniger nervig gestalten, als immer vor jedem Spiel zum Telefon laufen zu müssen.

Weil die Casinos nur eine begrenzte Anzahl dieser japanischen Geräte besaßen, entschied sich die Gruppe dieses Mal für einen von einer amerikanischen Firma hergestellten Spielautomaten, der weiter verbreitet war. Sie haben diesen Apparat auf die gleiche Art und Weise auseinander genommen und entdeckt, dass der Vorgang der Zufallszahlengenerierung deutlich komplexer war. Diese Maschine benutzte anstatt einen gleich zwei Generatoren, die kombiniert operierten. »Die Programmierer waren sich sehr viel besser im Klaren darüber, daß hier die Möglichkeit bestand, gehackt zu werden«, folgerte Alex.

Aber wieder entdeckten die vier, dass die Konstrukteure einen fatalen Fehler gemacht hatten. »Sie haben offensichtlich in einem Artikel gelesen, dass man die Qualität der Zufälligkeit verbessert, wenn man einen zweiten Wert hinzu-

3. Internal Revenue Service = Finanzamt

fügt, aber sie haben das falsch angestellt.« Um jeweils eine Karte zu bestimmen, wurde zu einer Zahl aus dem ersten Zufallszahlengenerator eine Zahl aus dem zweiten addiert.

Der korrekte Weg dazu erfordert, dass der zweite Generator nach dem Austeilen jeder Karte *iteriert* – das heißt, seinen Wert ändert. Das hatten die Konstrukteure nicht gemacht; sie hatten den zweiten Zufallszahlengenerator so programmiert, dass nur zu Beginn einer Spielrunde iteriert wurde, so dass für jede ausgeteilte Karte zu dem Ergebnis aus dem ersten Register immer die gleiche Zahl addiert wurde.

Für Alex machte die Verwendung der beiden Zufallszahlengeneratoren die Herausforderung zu »einer kryptologischen Sache«; er erkannte, dass es ähnlich war wie ein Schritt, der manchmal in der Verschlüsselung von Nachrichten vorgenommen wird. Obwohl er sich bei diesem Thema kundig gemacht hatte, war es nicht genug, um einen Lösungsweg zu erkennen, also machte er zu einer nahe gelegenen Unibibliothek auf, um dort nachzulesen.

> *Wenn die Konstrukteure einige der Bücher über Kryptosysteme sorgfältiger gelesen hätten, wäre ihnen dieser Fehler nicht unterlaufen. Und sie hätten auch bei den Tests der Systeme auf Möglichkeiten zum Cracken, wie wir sie genutzt haben, methodischer vorgehen sollen.*
>
> *Wenn er erst einmal begriffen hat, was erforderlich ist, könnte wohl jeder gute Student mit Informatik als Hauptfach solchen Code schreiben, wie wir ihn gebraucht haben. Die echte Herausforderung dabei ist, Algorithmen herauszufinden, mit denen die Suche in ein paar Sekunden erledigt ist – das schafft nur ein Freak. Packt man das naiv an, dann braucht der Algorithmus Stunden.*
>
> *Wir sind ziemlich gute Programmierer, wir leben alle davon, das zu machen, also haben wir uns ein paar sehr clevere Optimierungen einfallen lassen. Aber ich würde nicht sagen, dass das trivial war.*

Ich erinnere mich an einen ähnlichen Fehler, den ein Programmierer bei Norton gemacht hat (bevor sie von Symantec gekauft wurden). Er hat an deren Diskreet-Produkt gearbeitet, einer Applikation, mit der ein Benutzer verschlüsselte virtuelle Laufwerke erstellen konnte. Der Programmierer implementierte den Algorithmus fälschlicherweise – oder vielleicht auch absichtlicherweise – so, dass der Speicherplatz für den Verschlüsselungsschlüssel von 56 Bits auf 30 reduziert wurde. Der behördliche Datenverschlüsselungsstandard verwendet einen 56-Bit-Schlüssel, der als nicht knackbar angesehen wurde, und Norton erweckte bei seinen Kunden den Eindruck, dass ihre Daten nach diesem Standard geschützt werden. Wegen dieses Programmier-

fehlers wurden die Benutzerdaten tatsächlich aber nur mit 30 Bit statt mit 56 verschlüsselt. Sogar damals schon konnte man mit Brute Force einen 30-Bit-Schlüssel knacken. Jeder, der dieses Produkt benutzte, arbeitete unter einem falschen Gefühl der Sicherheit. Ein Angreifer konnte in einer vertretbaren Zeitspanne an den Schlüssel kommen und auf die Daten des Benutzers zugreifen. Das Team hatte die gleiche Art Fehler in der Programmierung der Maschine gefunden.

Während die Jungs an einem Computerprogramm arbeiteten, um an ihrer neuen Zielmaschine gewinnen zu können, nötigten sie Alex, sich etwas Neues auszudenken, um das Gelaufe zum Telefon überflüssig zu machen. Als Lösung ergab sich eine Idee, die auf dem Buch *Der Las Vegas Coup* basierte: ein »wearable« Computer. Alex entwickelte ein System, das aus einem Mini-Computer bestand, der um ein kleines Mikroprozessorboard herum gebaut war, das Mike und Marco in einem Katalog gefunden hatten – und zusätzlich einem Steuerungsknopf, der in einen Schuh passte, plus ein stummer Vibrator aus einem Handy. Sie nannten ihr System »den Taschencomputer«.

»Wir mussten uns ordentlich was einfallen lassen, um es auf einen kleinen Chip mit wenig Speicher zu kriegen«, sagte Alex. »Wir haben uns da was Schönes zusammengebaut, damit alles in den Schuh passt und ergonomisch ist.« (Mit »ergonomisch« ist in diesem Kontext meiner Ansicht nach gemeint, dass alles klein genug ist, damit man ohne Hinken gehen kann!)

DER NEUE ANGRIFF

Die Tests dieses neuen Plans strapazierten die Nerven des Teams ordentlich. Sicherlich konnten sie sich nun das verdächtige Verhalten ersparen, vor jedem Gewinn zu einer Telefonzelle zu laufen. Aber auch mit all den Probeläufen in ihrem »Büro« hieß es, dass sie es zur Premiere vor einem ziemlich großen Publikum aus stets argwöhnischen Sicherheitsleuten durchführen mussten.

Dieses Mal war das Programm so gestaltet, dass sie länger an einer Maschine sitzen und eine Serie von kleineren, weniger auffälligen Beträgen gewinnen konnten. Alex und Mike durchleben einiges von der Spannung noch einmal, als sie beschreiben, wie es funktionierte:

> *Alex: Ich habe den Computer normalerweise so eingepackt, das er wie ein kleines Taschentransistorradio aussah. Vom Computer haben wir einen Draht nach unten innerhalb des Strumpfs zu diesem Schalter im Schuh geführt.*
>
> *Mike: Meinen habe ich am Knöchel befestigt. Die Schalter haben wir aus kleinen Stücken Breadboard gemacht [Material, mit dem in einem Hardwarelabor Modelle von elektronischen Schaltkreisen gebaut werden]. Die Stücke waren etwa 2,5 Quadratzentimeter*

groß und hatten einen Minischalter. Und wir haben ein Gummiband draufgenäht, das um den großen Zeh gelegt wurde. Dann haben wir in eine Einlegesohle von Dr. Scholl ein Loch geschnitten, damit alles im Schuh an Ort und Stelle bleibt. Es war nur unbequem, wenn man es den ganzen Tag benutzt hat, dann war es echt eine Quälerei.

Alex: Also ich geh ins Casino, versuche ruhig zu wirken, verhalte mich ganz normal, als hätte ich keine Drähte in der Hose. Ich geh los und fang mit dem Spielen an. Wir hatten einen Code vereinbart, so was wie einen Morsecode. Ich steck also Geld rein, damit ich Kredit habe, um nicht immer Geld nachwerfen zu müssen, und fange an zu spielen. Wenn Karten erscheinen, klicke ich auf den Schalter im Schuh, um einzugeben, welche Karten angezeigt werden.

Das Signal aus dem Schuhschalter geht in den Computer, der in meiner Hosentasche steckt. Normalerweise brauchte es bei den frühen Maschinen sieben oder achten Karten, um die Synchronisierung hinzukriegen. Man bekommt fünf Karten, und üblicherweise werden bis zu drei weitere gezogen. Man hält also beispielsweise das Paar und zieht drei neue, das sind acht Karten.

Mike: Der Code für das Tippen auf dem Schalter im Schuh war binär, und es wurde auch eine Kompressionstechnik verwendet, den so genannten Huffman-Code. Also lang-kurz wäre dann eins-null, eine binäre Zwei. Lang-lang wäre eins-eins, eine binäre Drei und so weiter. Für keine Karte brauchte man mehr als drei Mal antippen.

Alex: Den Schalter länger als drei Sekunden gedrückt zu halten, sollte als Abbruch gelten. Und [der Computer] hat einem kleine Bedienerhinweise gegeben – so hieß dap-dap-dap »Okay, bin zur Eingabe bereit.« Wir haben das geübt und mussten uns konzentrieren, um das zu lernen. Nach einiger Zeit hatten wir es raus und konnten beim Tippen noch mit der Casino-Aufsicht reden.

Nachdem ich den Code getippt habe, um etwa acht Karten zu identifizieren, war das bei mir genug für eine Synchronisierung mit etwa 99 Prozent Genauigkeit. Dann dauerte es irgendwas von ein paar Sekunden bis zur einer Minute, und der Computer hat dann drei Mal gesummt.

Dann war ich startklar.

An diesem Punkt hatte der Taschencomputer die Stelle im Algorithmus gefunden, die die gerade ausgeteilten Karten repräsentierten. Weil der Algo-

rithmus der gleiche war wie in dem Videopokergerät, »wusste« der Computer bei jedem neu ausgegebenen Blatt, welche fünf zusätzlichen Karten warteten, nachdem der Spieler die abzulegenden Karten gewählt hatte, und konnte signalisieren, welche Karten für ein Gewinnerblatt gehalten werden mussten. Alex fuhr fort:

> *Der Computer sagt dir, was zu tun ist, indem er Signale an einen Vibrator in deiner Tasche schickt; die Vibratoren haben wir für lau bekommen, denn wir haben sie aus alten Pagern ausgebaut. Wenn der Computer dir sagen will, du sollst die dritte und fünfte Karte behalten, dann macht er biep, biep, biiiiep, biep, biiiiep, und das fühlst du als Vibration in deiner Tasche.*

Wir haben berechnet, dass wenn wir vorsichtig spielen, dann haben wir zwischen 20 und 40 Prozent Vigorish[4], das heißt einen 40prozentigen Vorteil bei jedem Blatt. Das ist gigantisch – die weltbesten Blackjack-Spieler kommen bestenfalls auf zweieinhalb Prozent.

> *Wenn du an einer $ 5-Maschine sitzt und fünf Münzen auf einmal einwirfst und das zwei Mal die Minute, kannst du $ 25 in der Minute machen. In einer halben Stunde sind das leicht $ 1.000. Jeden Tag setzt sich jemand da so hin und hat so viel Glück. Vielleicht kriegen fünf Prozent der Leute, die sich für eine halbe Stunde Spielen hinsetzen, das so gut hin. Aber eben nicht jedes Mal. Wir haben diese fünf Prozent jedes einzelne Mal gemacht.*

Immer wenn einer von ihnen in einem Casino ordentlich abgeräumt hatte, wechselte er in ein anderes. Jeder hat normalerweise vier oder fünf nacheinander geschafft. Wenn sie auf einer anderen Reise einen Monat später in das gleiche Casino gingen, haben sie darauf geachtet, zu einer anderen Uhrzeit dort zu sein, um auf Personal einer anderen Schicht zu treffen, damit es unwahrscheinlicher wurde, dass jemand sie erkennt. Sie haben auch die Casinos anderer Städte besucht, z.B. Reno oder Atlantic City.

Reisen, Spielen, Gewinnen – alles wurde nach und nach zur Routine. Aber bei einer Gelegenheit dachte Mike, der Moment, den sie alle befürchtet hatten, sei gekommen. Er hatte gerade »einen Gang höher geschaltet« und spielte zum ersten Mal an den Geräten für $ 25, was die Spannung noch erhöhte,

4. Kommission, die vor Auszahlung des Gewinns vom Einsatz abgezogen wird (A.d.Ü.)

denn die Maschinen werden desto stärker überwacht, je höher der Einsatz dabei ist.

> *Ich hatte etwas Muffensausen, aber die Sache lief besser als ich erwartete. Ich gewann etwa $ 5.000 in einer relativ kurzen Zeit. Dann hat mir dieser große, imposante Angestellte auf die Schulter getippt. Ich schaute zu ihm hoch und fühlte mich etwas mulmig im Bauch. Ich dachte: »Das war's jetzt.«*
> *»Ich hab gesehen, dass Sie schon eine ganze Zeit spielen«, sagte er. »Wollen Sie lieber rosa oder grün?«*

Wäre ich an seiner Stelle gewesen, hätte ich mich gefragt: »Was soll das jetzt – kann ich mir aussuchen, welche Farbe ich haben soll, nachdem sie mich zusammengeschlagen haben?« Ich glaube, ich hätte alles Geld zurück gelassen und versucht, so schnell wie möglich abzuhauen. Mike sagt, dass er mittlerweile erfahren genug war, um ruhig zu bleiben.

> *Der Mann sagte: »Wir möchten Ihnen gerne als Dankeschön einen Kaffeebecher überreichen.«*

Mike hat den grünen genommen.

Marco hatte auch seinen eigenen spannenden Moment. Er wartete auf ein Kartenblatt, mit dem er gewinnen konnte, als einer der Pit-Bosse unbemerkt an seine Seite trat. »Sie haben ja auf fünftausend Dollar verdoppelt – da haben Sie aber mächtig Glück!«, sagte er überrascht. Eine alte Dame am Spielautomaten nebenan meldete sich mit der heiseren Sandpapierstimme einer Raucherin zu Wort: »Das … war … kein … Glück.« Der Pit-Boss wurde angespannter, sein Argwohn war geweckt. »Das war *Mumm*«, krächzte sie. Der Pit-Boss lächelte und ging weiter.

Über einen Zeitraum von etwa drei Jahren sind die Freunde immer wieder in seriöse Consulting-Jobs gewechselt, um ihre Kompetenzen und Kontakte zu erweitern, und haben gelegentlich an den Videopokergeräte gespielt, um ihr Konto aufzubessern. Sie haben zwei weitere Maschinen gekauft, darunter das am häufigsten eingesetzte Modell für Videopoker, und aktualisierten fortlaufend ihre Software.

Auf ihren Reisen suchten die drei vom Team, die verreisen konnten, verschiedene Casinos auf, »damit wir nicht alle im Pulk auflaufen«, sagte Alex. »Ein oder zwei Mal haben wir das gemacht, aber das war dumm.« Obwohl sie sich darauf verständigt hatten, einander zu informieren, was sie jeweils vorhatten, ist ab und zu mal einer von ihnen in eins der Spielerparadiese gefahren,

ohne den anderen Bescheid zu sagen. Aber sie haben ihr Spiel auf Casinos beschränkt und waren nie an Orten wie Supermärkten oder 7-Elevens[5], weil »es da meist nur ziemliche miese Auszahlungen gibt«.

ERWISCHT!

Alex und Mike achteten beide diszipliniert auf die Einhaltung »gewisser Regeln, von denen wir wussten, dass wir damit die Wahrscheinlichkeit aufzufallen reduzieren konnten. Eine davon war, niemals zu viel Geld an einem Ort zu machen, niemals irgendwo zu lange zu bleiben und niemals an zu vielen Tagen nacheinander dort zu erscheinen.«

Aber Mike hat diese Disziplin noch ernster genommen und war der Meinung, die anderen beiden seien nicht vorsichtig genug. Er wollte lieber in einer Stunde etwas weniger gewinnen und mehr wie ein typischer Spieler wirken. Wenn er zwei Asse auf der Hand hatte und der Computer ihm sagte, er sollte eins oder beide ablegen, um ein noch besseres Blatt zu kriegen, beispielsweise drei Buben, dann hat er das nicht gemacht. In allen Casinos wird aus einem Sicherheitszentrum über dem Casino der gesamte Spielbereich mit Kameras überwacht. Diese Kameras können gedreht und gezoomt werden, um Betrüger, unehrliche Angestellte und andere, die der Versuchung dieses vielen Geldes erlegen sind, auf die Finger zu schauen. Wenn einer der Beobachter zufällig gerade auf seinen Spielautomaten geschaut hat, hätte er sofort gewusst, dass da etwas faul ist, weil kein vernünftiger Spieler zwei Asse aufgegeben hätte. Niemand, der nicht irgendwie betrügt, hätte wissen können, dass ein besseres Blatt kommen würde.

Alex war nicht ganz so penibel. Und Marco noch weniger. »Marco war ein wenig großspurig«, schätzt Alex das ein:

> *Er ist ein sehr cleverer Typ, Autodidakt, hat nie die Highschool beendet, ist aber einer dieser brillanten Osteuropäer. Und großspurig.*
>
> *Er wusste alles über Computer, aber er war nicht davon abzubringen, dass die Casinos doof sind. Das konnte man ziemlich leicht denken, weil die uns mit so viel Geld abhauen ließen. Aber trotzdem glaube ich, dass er zu selbstsicher wurde.*
>
> *Er war mehr der Draufgängertyp und passte auch nicht in das Profil, weil er einfach aussah wie ein ausländischer Teenager. Also glaube ich, dass er dazu neigte, Verdacht zu erregen. Und er hat*

5. Internationale Kette von Einzelhandelsgeschäften (A.d.Ü.)

keine Freundin oder Frau mitgenommen, womit er auch besser reingepasst hätte.

Ich glaube, er hat schließlich einfach Sachen gemacht, durch die man auf ihn aufmerksam wurde. Und als wir nach einiger Zeit immer dreister wurden, haben wir uns auch weiter entwickelt und nahmen uns die teureren Spielautomaten vor, die größere Gewinne ausschütteten, und damit war die Operation auch größeren Risiken ausgesetzt.

Obwohl Mike da anderer Meinung ist, gibt Alex zu erkennen, dass sie alle drei bereit waren, Risiken einzugehen und den Bogen zu überspannen, um zu sehen, wie weit sie gehen konnten. In seinen Worten: »Ich glaube, im Grunde haben wir alle das Risiko immer höher geschraubt.«

Der Tag kam, an dem Marco eben noch an einem Spielautomaten in einem Casino saß und in der nächsten Minute von stämmigen Sicherheitsleuten umringt war, die ihn hochzogen und zum Verhör in ein Hinterzimmer brachten. Alex erzählte, wie sich das abspielte:

Es war ziemlich schrecklich, weil man ja so Stories hört von diesen Kerlen, die einen total zusammenschlagen. Diese Kerle sind berüchtigt dafür zu sagen, Scheiß auf die Polizei, das regeln wir selbst.

Marco stand unter Druck, aber er war ein ziemlich zäher Kerl. Ehrlich gesagt war ich beinahe glücklich, dass er derjenige war, den sie erwischt haben, wenn es denn einen von uns erwischen sollte, weil ich glaube, dass er derjenige von uns ist, der am besten mit einer solchen Situation umgehen kann. Nach allem, was ich weiß, hat er solche Sachen auch damals schon in Osteuropa durchgestanden.

Er legte eine gewisse Loyalität an den Tag und hat uns nicht verpfiffen. Er hat nicht über irgendwelche Partner oder so was gesprochen. Er war nervös und aufgeregt, aber unter Beschuss eben auch taff und sagte im Grunde, dass er alleine arbeite.

Er meinte: »Hören Sie, bin ich jetzt verhaftet, gehören Sie zur Polizei oder was?«

Es ist wie eine Art polizeilicher Vernehmung, außer dass die gar nicht zur Polizei gehören und keine echte Befugnis haben, und das ist schon merkwürdig. Sie fuhren fort, ihn zu befragen, aber sie haben ihn nicht wirklich grob behandelt.

Sie haben von ihm ein »Verbrecherfoto« gemacht, sagt Alex, und den Computer und sein ganzes Bargeld konfisziert, etwa $ 7.000. Nachdem sie ihn ungefähr eine Stunde verhört hatten oder vielleicht auch länger – er war zu aufgeregt, um sich da sicher zu sein –, haben sie ihn schließlich gehen lassen.

Auf dem Weg nach Haus rief Marco seine Partner an. Er klang völlig außer sich. Er meinte: »Ich muss euch sofort erzählen, was passiert ist. Ich hab Mist gebaut.«

Mike fuhr sofort zu ihrem Hauptquartier. »Alex und ich waren total panisch, als wir hörten, was passiert war. Ich fing sofort damit an, die Maschinen auseinander zu reißen, und verteilte die Teile überall in der Stadt in Mülltonnen.«

Alex und Mike waren beide ziemlich wütend auf Marco, dass er solch unnötige Risiken eingegangen war. Er wollte sich den Schalter nicht in seinen Schuh stecken wie die anderen beiden, sondern beharrte eigensinnig darauf, das Gerät in der Jackentasche zu tragen und es mit der Hand zu bedienen. Alex beschrieb Marco als einen Typ, der »dachte, die Sicherheitsleute wären so blöde, dass er es mit dem, was er direkt vor ihrer Nase macht, auf die Spitze treiben konnte«.

Alex ist überzeugt davon zu wissen, wie das abgelaufen ist, auch wenn er nicht dabei war. (Tatsächlich wussten die drei anderen gar nicht, dass Marco entgegen ihrer Abmachung, sich gegenseitig über ihre Pläne zu informieren, auf einen Casino-Trip gegangen war.) Nach Einschätzung von Alex »haben sie einfach gesehen, dass er unglaubliche Gewinne abzog und dass da irgendwas mit seiner Hand läuft«. Marco hatte einfach keinen Gedanken daran verschwendet, wodurch er den Angestellten im Casino auffallen könnte.

Das war für Alex der Schlusspunkt, obwohl er sich bei den anderen nicht völlig sicher ist. »Wir hatten von Anfang an beschlossen, dass wenn einer von uns erwischt wird, dann würden wir alle aufhören.« Er sagte: »Daran haben wir uns alle gehalten, soviel ich weiß.« Und einen Moment später fügte er mit weniger Gewissheit hinzu: »Zumindest ich hab das.« Mike stimmt zu, aber keiner von beiden hat Marco diese Frage direkt gestellt.

Die Casinos erstatten bei Angriffen wie denen, die von den vieren abgezogen wurden, im Allgemeinen keine Anzeige. »Das liegt daran, dass sie nicht öffentlich machen wollen, dass sie diese Schwachstellen haben«, erklärt Alex. Also kriegt man dann gesagt: »Verschwinde vor Sonnenuntergang aus der Stadt. Und wenn du dich daran hältst, niemals wieder einen Fuß in ein Casino zu setzen, kommst du noch mal davon.«

NACHSPIEL

Etwa ein halbes Jahr später bekam Marco einen Brief, dass es keine weitere Strafverfolgung gegen ihn geben werde.

Die vier sind immer noch befreundet, aber heute nicht mehr so eng wie damals. Alex schätzt, er habe aus diesem Abenteuer etwa $ 300.000 mitgenommen, und davon hat er wie vereinbart einen Teil an Larry abgedrückt. Die drei Partner, die in den Casinos gearbeitet und das ganze Risiko getragen haben, hatten anfangs gesagt, sie werden alles gleichmäßig aufteilen, aber Alex denkt, dass Mike und Marco wahrscheinlich jeder zwischen $ 400.000 und einer halben Million gekriegt haben. Mike wollte nicht bestätigen, dass er mehr als $ 300.000 eingesteckt habe, gibt aber zu, dass Alex wohl weniger als er selbst bekommen habe.

Die ganze Geschichte lief über etwa drei Jahre. Trotz des Geldes war Alex froh, dass es nun vorbei war. »In gewisser Weise war ich erleichtert. Der Spaß hat nachgelassen. Es war irgendwie zu einem reinen Job verkommen. Einem riskanten Job.« Mike war auch nicht böse drum, dass es vorbei war, und beklagte sich ein wenig, es sei »immer aufreibender geworden«.

Beide waren anfangs mit ihrer Geschichte sehr zurückhaltend, tauten aber immer mehr auf. Und warum auch nicht – in den etwa zehn Jahren, seitdem es passiert ist, hat keiner der vier nicht einmal andeutungsweise mit jemandem über diese Ereignisse gesprochen außer mit den daran beteiligten Ehefrauen und der Freundin. Es zum ersten Mal unter dem Schutz einer Vereinbarung absoluter Anonymität zu erzählen, schien wie eine Erleichterung zu sein. Sie haben es offensichtlich genossen, die Details noch einmal zu erleben, und Mike gab zu, dass es »eine der aufregendsten Sachen war, die ich jemals gemacht habe«.

Alex spricht wahrscheinlich für alle, wenn er seine Haltung bezüglich ihrer Eskapaden ausdrückt:

> *Ich habe kein sonderlich schlechtes Gewissen wegen des Geldes, das wir gewonnen haben. Für diese Branche ist das ein Tropfen auf dem heißen Stein. Ich muss ehrlich sagen: Wir haben uns moralisch nie schlecht gefühlt, weil es eben Casinos waren.*
>
> *Das konnten wir leicht rationalisieren. Wir haben von den Casinos geklaut, die von alten Damen geklaut haben, indem sie ihnen Spiele anbieten, die sie nicht gewinnen können. Vegas hat sich so angefühlt, als wären die Leute an Geld saugende Maschinen angeschlossen, und ihr Leben tröpfelt Münze für Münze weg. Also fühlten wir*

uns, als ob wir uns an Big Brother rächen, und nicht, als ob wir eine arme alte Dame um ihren Jackpot bringen.

Sie haben da ein Spiel angeboten, das hieß: »Wenn du die richtigen Karten wählst, gewinnst du.« Wir haben die richtigen Karten ausgewählt. Sie haben einfach nicht damit gerechnet, dass das jemand fertig bringt.

Heutzutage würde er so was nicht noch einmal probieren, sagt Alex. Aber seine Begründung dafür ist nicht die, die man erwartet hätte: »Ich kann über andere Wege an Geld kommen. Wenn ich finanziell wieder mal in eine solche Situation wie damals käme, würde ich es noch einmal machen.« Er hält das, was sie gemacht haben, für gerechtfertigt.

In diesem Katz-und-Maus-Spiel lernt die Katze dauernd die neuen Tricks der Maus und ergreift angemessene Maßnahmen. Heutzutage wird bei den Slotmaschinen eine deutlich besser entwickelte Software eingesetzt; die Jungs sind sich gar nicht so sicher, ob sie heute wieder so erfolgreich wären.

Aber nichtsdestotrotz wird es niemals eine perfekte Lösung für Probleme aus dem Bereich der technischen Sicherheit geben. Alex bringt das Problem auf den Punkt: »Jedes Mal, wenn irgendein [Programmierer] sagt: 'Keiner wird sich je eine solche Mühe machen', wird gerade irgendein Bengel in Finnland sich genau diese Mühe machen.«

Und nicht nur in Finnland, sondern auch in Amerika.

HINTERGRUND

In den 90ern hatten die Casinos und die Konstrukteure von Geldspielautomaten einige Sachen, die später offensichtlich wurden, noch nicht so verstanden. Ein Pseudo-Zufallszahlengenerator gibt nicht wirklich zufällige Zahlen heraus. Er speichert stattdessen eine Liste mit Zahlen in zufälliger Reihenfolge. In diesem Fall eine sehr lange Liste: 2^{32} oder über vier Milliarden Zahlen. Beim Start des Durchlaufs wählt die Software einen Punkt in der Liste zufällig. Aber danach verwendet sie die darauf folgenden Zahlen aus der Liste eine nach der anderen, bis ein neuer Spieldurchlauf gestartet wird.

Durch das Reverse Engineering der Software waren die vier an die Liste gekommen. Von jedem gegebenen Punkt in der »zufälligen« Liste konnten sie bestimmen, welche Zahlen in der Liste anschließend folgen, und mit der zusätzlichen Kenntnis über die Iterationsrate einer bestimmten Maschine konnten sie berechnen, wie lange es in Minuten und Sekunden dauert, bis die Maschine einen Royal Flush anzeigt.

GEGENMASSNAHMEN

Die Hersteller aller Produkte, die ROM-Chips und Software verwenden, sollten mögliche Sicherheitsprobleme im Vorfeld angehen. Und für jede Firma, die Software und auf Computern basierende Produkte benutzt – was heutzutage praktisch alle Firmen bis hinunter zu Ein-Personen-Unternehmen umfasst – ist die Annahme gefährlich, dass die Leute, die ihre Systeme gebaut haben, sich schon über alle Schwachstellen Gedanken gemacht haben. Die Programmierer der Software in der japanischen Slotmaschine haben insofern einen Fehler gemacht, dass sie sich nicht im Voraus auf mögliche Angriffsarten eingestellt haben. Sie haben keine Sicherheitsvorkehrungen getroffen, um die Firmware vor unbefugtem Zugriff zu schützen. Sie hätten vorher bedenken sollen, dass jemand einen solchen Spielautomaten kaufen, den ROM-Chip ausbauen, die Firmware auslesen und die Programminstruktionen entdecken könnte, die der Maschine ihre Funktionsweise vorschreibt. Auch wenn sie diese Möglichkeit in Erwägung gezogen haben, nahmen sie wahrscheinlich an, dass die Kenntnis der Arbeitsweise der Maschine nicht ausreichte, weil sie der Meinung waren, dass die Berechnungskomplexität für das Knacken des Zufallszahlengenerators jeden Versuch zum Scheitern verurteilt. Das mag heute vielleicht gelten, aber nicht damals.

Was sollten Sie also machen, wenn Ihre Firma technische Produkte mit eingebauten Computerchips verkauft, um sich einen adäquaten Schutz gegenüber einem Wettbewerber zu schaffen, der sich Ihre Software anschauen will, oder gegen die ausländische Organisation, die eine billiges Plagiat nachbauen will, oder den Hacker, der Sie betrügen will?

Der erste Schritt: Machen Sie es schwer, an die Firmware zu kommen. Dafür gibt es mehrere Vorgehensweisen:

- Verwenden Sie Chips einer Marke oder Art, die so gestaltet ist, dass sie gegen Angriffe geschützt ist. Die Chips bestimmter Firmen sind speziell für Einsatzbereiche konstruiert, in denen die Wahrscheinlichkeit eines Angriffs sehr hoch ist.
- Verwenden Sie *Chip on-Board Packaging* – bei diesem Design wird der Chip in das Mainboard eingebettet und kann nicht als separates Element entfernt werden.
- Verkleben Sie den Chip auf dem Motherboard mit Epoxydharz, so dass der Chip bei einem Ausbauversuch zerbrechen wird. Bei einer Verbesserung dieser Technik wird dem Epoxydharz Aluminiumpulver beigemischt; wenn ein Angreifer dann versucht, den Chip durch Erwärmen des Harzes zu entfernen, wird das Aluminium den Chip zerstören.

- Verwenden Sie ein BGA-Design (*ball grid array*). Bei dieser Anordnung kommen die Kontakte nicht mehr als Pins aus den Seiten des Chips, sondern befinden sich stattdessen als auflötbare Kügelchen unterhalb des Chips, und dadurch wird es schwer, wenn nicht gar unmöglich, den Signalfluss vom Chip abzufangen, solange er auf dem Board sitzt.

Bei einer anderen Gegenmaßnahme werden alle Identifizierungsinformationen vom Chip abgekratzt, damit kein Angreifer Informationen über den Hersteller und die Chipart bekommen kann.

Eine sehr übliche Praxis, die auch vom Hersteller des Spielautomaten in dieser Story verwendet wird, ist die Verwendung einer Prüfsumme (*Hashing*) einschließlich einer Prüfsummenroutine in der Software. Wenn das Programm verändert wurde, ist die Prüfsumme nicht korrekt und die Software wird nicht mit dem Gerät arbeiten. Allerdings werden findige Hacker, die dieses Vorgehen kennen, einfach die Software checken, ob eine Prüfsummenroutine vorhanden ist, und sie deaktivieren, falls sie eine finden. Also ist es ein deutlicher besserer Plan, über eine oder mehrere der obigen Methoden den Chip physisch zu schützen.

UNTERM STRICH

Wenn Ihre Firmware proprietär und wertvoll ist, sollten Sie die besten Sicherheitsquellen konsultieren, um herauszufinden, welche Techniken Hacker gegenwärtig einsetzen. Halten Sie Ihre Konstrukteure und Programmierer bei den neuesten Informationen *up to date*. Und achten Sie darauf, dass von ihnen alle erforderlichen Schritte eingehalten werden, um unter Berücksichtigung der Kosten das höchste Sicherheitslevel zu erreichen.