Cyberstalking

Die Lauscher

Donnerstag, 7. September 2006

Während die Geschäftswelt die VoIP-Technologie (Voice-over-Internet Protocol) aufgrund ihrer Kosteneinsparungen schnell für sich entdeckt, werden die neuen Gefahren, die dadurch in unsere Telefonnetze Einzug halten, kaum beachtet.

Obwohl Skype mit seinen Millionen von Nutzern das öffentliche Gesicht von VoIP ist, ist die Mehrheit der VoIP-Nutzung weniger verbraucherorientiert und weitaus weniger aufregend.

Viele Unternehmen modernisieren derzeit ihre interne Telefoninfrastruktur oder planen dies, um Kosten zu senken. Selbst die Telekommunikationsunternehmen, die die Auswirkungen von VoIP auf ihre Einnahmen fürchten, verlagern einen Großteil ihres PSTN-Verkehrs (öffentliches Telefonnetz) eifrig auf VoIP-Technologie.



Fast alle diese neuen VoIP-Implementierungen erfolgen jedoch ohne nennenswerte Berücksichtigung von Sicherheitsaspekten, was sich ernsthaft auf diese Unternehmen und Verbraucher auswirken könnte.

Die wahren Kosten von VoIP – die erhöhte Gefährdung durch ernsthafte Sicherheitsrisiken – können die Einsparungen durch reduzierte Gesprächsgebühren bei Weitem übersteigen.

Auch wenn manche Unternehmen meinen, sie seien nicht gefährdet, weil sie die VoIP-Technologie noch nicht eingeführt haben oder weil ihre Systeme nicht direkt mit dem Internet oder dem öffentlichen Telefonnetz verbunden sind, sind sie, genau wie wir alle, dennoch zahlreichen „VoIPhreaking“-Angriffen ausgesetzt.

Zeitenwandel

VoIPhreaking ist die neuere, jüngere und internetaffine Variante des traditionellen Phreakings. Phreaking bezeichnet das Hacken, Erkunden und Ausnutzen der PSTN-Infrastruktur.

Seit den Zeiten von Captain Crunch und Steve Jobs, die Inband-Signalisierung (die Steuerung von Telefongesprächen über hörbare Töne) ausnutzten, um kostenlos zu telefonieren, haben die Telekommunikationsunternehmen hart daran gearbeitet, die Schwachstellen in ihren Netzen zu verringern.

Obwohl ihre Motive gewinnorientiert waren – die Reduzierung von Gebührenbetrug erhöht die Einnahmen –, ist das Ergebnis ein relativ stabiles und zuverlässiges globales Telefonnetz.

All dies ändert sich nun, da Internet und PSTN konvergieren, ohne dass die Sicherheit der Verbindungen ausreichend berücksichtigt wird. Hacker sind sich dessen sehr wohl bewusst und nutzen dies bereits aktiv aus.

Die Ausnutzung des PSTN durch VoIP-Hacking bietet eine Fülle potenzieller Angriffsvektoren und ermöglicht so vielfältige Ergebnisse, die die vertrauenswürdigen Funktionen des Telefonsystems umgehen oder untergraben.

Zu den grundlegenden Angriffen gehören verschiedene Techniken des Gebührenbetrugs, die es VoIP-Dieben ermöglichen, kostenlos auf Kosten der Telekommunikationsunternehmen zu telefonieren.

Fortgeschrittenere Angriffe ermöglichen es Hackern, die Telefonverbindung vollständig zu kontrollieren, einschließlich beispielsweise der Daten für die Anrufer-ID. Diese Informationen werden häufig zur Authentifizierung an Voicemail-Boxen, Kreditkarten und in einigen US-Bundesstaaten sogar zur Bezahlung von Stromrechnungen verwendet.

Lauscher

Auch ohne Angriffe auf die externen Telefondienste einer Organisation bestehen Bedrohungen. Hacker können ein Telefonsystem innerhalb des Unternehmensnetzwerks deutlich leichter lahmlegen.

Ein Phisher könnte beispielsweise die Kontrolle über ein Callcenter-Netzwerk nutzen, um Anrufe über einen Abhörserver umzuleiten. Nicht nur die Einleitung eines Telefonats ist gefährdet; auch während eines laufenden Gesprächs kann ein VoIP-Angreifer erheblichen Schaden anrichten.

Innerhalb des Netzwerks ist es für Hacker ein Leichtes, den internen Sprachverkehr abzuhören. Dies kann insbesondere in einem Callcenter verheerende Folgen haben: Wie sicher ist die ausgelagerte Kundendienstleitung in Mumbai tatsächlich?

Das Abhören eines Gesprächs ist jedoch nicht die einzige Sorge, da die für VoIP verwendete Technologie es Angreifern ermöglicht, problemlos neue Inhalte in ein bestehendes Telefongespräch einzuschleusen.

Ein Phisher könnte diesen Angriff nutzen, um sicherzustellen, dass die gewünschten Informationen während eines Telefonats preisgegeben werden, beispielsweise durch das Einspielen von Sprachbefehlen, während der Kunde in der Warteschleife ist: „Bitte geben Sie Ihre Kontonummer und PIN ein, um eine schnellere Bearbeitung zu gewährleisten. Ihr Anruf ist uns wichtig.“

Die im Internet verfügbaren Tools bieten bereits die nötigen Funktionen für diese Angriffe, und es ist nur eine Frage der Zeit, bis sie für weniger erfahrene Angreifer aufbereitet werden und somit alltäglich werden.

Die beunruhigende Nachricht ist nicht nur, dass diese Angriffe heute möglich sind, sondern dass aufgrund der mangelhaften Sicherheit der meisten VoIP-Installationen niemand überhaupt bemerken würde, wenn diese Angriffe bereits stattfinden.

Von einfachen Denial-of-Service-Angriffen, bei denen ein Unternehmen oder eine Einzelperson an der Nutzung des Telefons gehindert wird, bis hin zu ausgeklügelten Telefonnummern-Hijacking-Angriffen, die Anrufe an böswillige Hacker umleiten können; diese neuen Bedrohungen werden die Wahrnehmung des gewöhnlichen Telefons radikal verändern.

Fälschungskarte

Der Albtraum eines Opfers und der Traum eines Stalkers werden wahr... Das ist entsetzlich.

Opfer aufgepasst! Das ist kindisch, geschmacklos, Wahnsinn. Diese Karte erlaubt es Stalkern, ihre Anrufer-ID und ihre Stimme zu verändern. Sie ist eine Bedrohung, eine Form der Belästigung und ein Übergriff. Mein Gott, müssen wir jetzt wegen Stalkern aufhören zu telefonieren?

http://www.spoofcard.com./

Telefon-Phreaking; Ihr Handy kann in eine Wanze verwandelt werden

Die von dem österreichischen Forscher Martin Herfurt Anfang des Jahres entwickelte Methode des Abhörens (Bluebugging) ist die perfekte Waffe für Industriespione. Angenommen, Sie und ich konkurrieren um einen großen Auftrag eines Ölkonzerns. Ich möchte alles mithören, was in Ihrem Meeting mit dem Vizepräsidenten von Massive Oil Inc. passiert. Deshalb engagiere ich einen Hacker, der Ihr Handy übernimmt. Sobald er es gehackt hat, lasse ich ihn von Ihrem Handy aus meines anrufen. Das Telefon in Ihrer Jackentasche zeichnet nun alles auf, was Sie und der Vizepräsident während Ihres Gesprächs sagen, und ich kann die von Ihnen genannten Preise glasklar auf meinem eigenen Handy hören. „Ein Handy ist das ultimative, ausgeklügelte Abhörgerät“, sagt Laurie.

Laurie, 42, CSO der Sicherheitsfirma The Bunker, wird sich zwar nicht an fremden Handys vergreifen, aber er könnte es: Mit ein paar kleinen Anpassungen an dem Scanprogramm auf seinem Computer könnte Laurie Handys in seiner Umgebung lahmlegen und so eine Spur der Verwüstung hinterlassen. Doch heute sammelt Laurie nur Daten. Wir zählen, wie viele Handys er per Bluetooth hacken kann, einem drahtlosen Protokoll zur Verbindung von Handys mit Headsets, Computern und anderen Geräten.

Wir besprechen die Ergebnisse der Expedition in einem nahegelegenen Pub. In den 17 Minuten, die wir umherstreiften, empfing Lauries Computer Signale von 39 Handys. Er starrt eine Weile auf seinen Monitor. „Man braucht nur 15 Sekunden, um an das Adressbuch von jemandem zu kommen." „Und mindestens fünf dieser Handys waren angreifbar."

Der von Laurie so beiläufig erwähnte „Angriff" kann fast alles bedeuten – von der Nutzung fremden Handys für Ferngespräche über das Ändern aller Telefonnummern im Adressbuch bis hin zum Abhören von Gesprächen. Laut Laurie stehen dem wagemutigen Handy-Angreifer „ganz neue Möglichkeiten" zur Verfügung, darunter auch gefährliche Virenangriffe. Ein harmloser Bluetooth-Wurm kursiert bereits in Singapur, und Laurie befürchtet, dass zukünftige Varianten wirklich beängstigend sein könnten. Besonders gefährdet sind Europäer, die mit ihrem Handy Mikrozahlungen tätigen – kleine Einkäufe, die auf der Handyrechnung erscheinen. Ein bösartiger Virenprogrammierer, der auf schnellen Reichtum aus ist, könnte diese Funktion ausnutzen, indem er sogenannte „Reverse-SMS"-Befehle ausgibt.

Die Sicherheit von Bluetooth ist in Europa, wo die Technologie weit verbreitet ist, zu einem dringenden Problem geworden. Mit der zunehmenden Verbreitung des Protokolls wird sich das Problem auch auf die USA ausweiten. Langfristig sind Bluetooth-Schwachstellen jedoch beherrschbar: Gerätehersteller können fehlerhafte Implementierungen korrigieren, und Handynutzer werden lernen, vorsichtiger zu sein. Ein weitaus größeres Sicherheitsrisiko für die USA stellt die Internettelefonie dar, die sich rasant bei großen Unternehmen durchsetzt und Verbrauchern über viele Breitbandanbieter zur Verfügung steht. Voice over IP (VoIP) ist systembedingt anfällig für Hackerangriffe. Bislang hat noch kein findiger Krimineller einen Millionenbetrug mit VoIP-Technologie ausgeheckt. Sollte es jedoch dazu kommen, wird sich das Problem wahrscheinlich nicht mit einem einfachen Patch beheben lassen.

Bluetooth-Hacking unterscheidet sich technisch deutlich von VoIP-Hacking, doch beide nehmen aus demselben Grund rasant zu. Telefone sind zunehmend mit Computern verschmolzen, was sie zwar nützlicher, aber auch angreifbarer macht. VoIP, das Anrufe über das Internet leitet, ermöglicht es Nutzern, ihre Telefonnummer überallhin mitzunehmen, Sprachnachrichten als MP3s zu speichern und per E-Mail zu empfangen sowie günstig ins Ausland zu telefonieren. Doch wie Bluetooth birgt auch VoIP die Gefahr, dass Telefone denselben Problemen ausgesetzt sind wie Desktop-Computer – Würmer, Spam und Abstürze.

„Es ist nicht so, als hätten wir die Sicherheitslücken in Computern behoben", sagt Sicherheitsexperte Bruce Schneier, Autor von „ *Secrets and Lies: Digital Security in a Networked World*" . „Früher bezog das Telefonnetz seine Sicherheit aus seiner Abgeschlossenheit, aber VoIP-Telefone werden genauso unsicher sein wie Computer."

Viele der heutigen Hacks funktionieren, weil das traditionelle Telefonsystem auf der Annahme basierte, dass es nur von großen, monopolistischen Telefongesellschaften genutzt würde und diese sich alle an dieselben Regeln hielten. Doch das Netzwerk ist nicht länger der geschützte Raum der Telekommunikationsunternehmen; es kann von jedem manipuliert und kontrolliert werden, der über grundlegende Computerkenntnisse verfügt. Diejenigen, die dies am besten wissen, sind eine neue Generation von Telefonhackern – auch Phreaker genannt –, die sich nicht an die Regeln halten. Sie sind damit beschäftigt, die neuesten Handys auseinanderzunehmen, um

herauszufinden, wie sie sich gegen ihre Besitzer wenden können. Während die Telefongesellschaften und Handyhersteller nur mühsam vorankommen, bleibt uns nur zu hoffen, dass die Phreaker – die sogenannten White Hats – einige Lösungen finden, bevor die Black Hats zuschlagen.

Laurie, dessen Laptop nun mit Daten von in Shepherd's Bush sichergestellten Handys gefüllt ist, erlangte in Großbritannien traurige Berühmtheit durch ein ähnliches Experiment im britischen Parlament. Dort hatte er die Gelegenheit (die er jedoch nicht nutzte), die Adressbücher und Kalender mehrerer prominenter Politiker zu kopieren. Diese Aktion führte zu der Anordnung, alle Bluetooth-Geräte im Parlamentsgebäude abzuschalten.

Als Erfinder von „Bluesnarfing", einem Hack, der Bluetooth nutzt, um auf Daten von Mobiltelefonen zuzugreifen, setzt sich Laurie dafür ein, die Gefahren einer ungeschützten Bluetooth-Verbindung aufzuzeigen. Ein Bluesnarf-Angriff kann ein ungeschütztes Telefon identifizieren und dessen gesamtes Adressbuch, Kalender, Fotos und alle anderen darauf befindlichen Informationen kopieren. Mithilfe eines Bluesnarf-Programms kann ein Angreifer zudem jedes Telefon in Reichweite lahmlegen, indem er über Bluetooth eine sogenannte „manipulierte Nachricht" sendet.

Bluesnarf entstand, nachdem Laurie den Quellcode einiger Bluetooth-Headsets seiner Mitarbeiter genauer unter die Lupe genommen hatte. Er war mit dem Ergebnis alles andere als zufrieden. „Eklatante Sicherheitslücken", sagt er stirnrunzelnd. Nachdem die Mobilfunkunternehmen, denen er die Probleme meldete, ihn abgewiesen hatten, entwickelte er Bluesnarf als PR-Aktion – ein Werkzeug, das die Gefahren dieser Handys verdeutlichen sollte.

Zu den technischen Schwachstellen von Bluetooth kommen Probleme im Umgang damit. Die meisten Menschen lassen Bluetooth ständig eingeschaltet, oft weil sie sich nicht die Mühe machen, es auszuschalten. Selbst Technikaffine neigen dazu, ihre Verbindungen offen zu halten. „Manche kennen das Phänomen des ‚Toothing', bei dem sich Fremde über Bluetooth flirtende Nachrichten schicken", sagt er. In der Hoffnung, selbst „Toothing" zu erhalten, riskieren sie eine ganz andere Art von Sicherheitslücke.

Besonderheit:
Sie haben deine Nummer
Plus:
Der große Handyraub

Das Risiko hört nicht mit dem Abfangen auf. Eine weitere Möglichkeit, ein Handy per Bluetooth komplett zu übernehmen, ist das sogenannte Bluebugging. Laurie demonstriert es mir kurz. Er startet die Bluebug-Software auf seinem Laptop, und diese findet schnell ein Ericsson T610, das er zwischen uns auf den Tisch gelegt hat (nicht alle Handys lassen sich mit Bluebug manipulieren, aber dieses Modell schon). Sein Computer verbindet sich mit dem Handy und übernimmt die Kontrolle. Durch Tippen auf der Tastatur gibt Laurie dem T610 den Befehl, das Handy an seinem Gürtel anzurufen. Es piept. Er nimmt ab. Wir haben einen Bluebug.

Die von dem österreichischen Forscher Martin Herfurt Anfang des Jahres entwickelte Methode des Abhörens (Bluebugging) ist die perfekte Waffe für Industriespione. Angenommen, Sie und ich konkurrieren um einen großen Auftrag eines Ölkonzerns. Ich möchte alles mithören, was in Ihrem Meeting mit dem Vizepräsidenten von Massive Oil Inc. passiert. Deshalb engagiere ich einen Hacker, der Ihr Handy übernimmt. Sobald er es gehackt hat, lasse ich ihn von Ihrem Handy aus meines anrufen. Das Telefon in Ihrer Jackentasche zeichnet nun alles auf, was Sie und der Vizepräsident während Ihres Gesprächs sagen, und ich kann die von Ihnen genannten Preise glasklar auf meinem eigenen Handy hören. „Ein Handy ist das ultimative, ausgeklügelte Abhörgerät“, sagt Laurie.

Anders als Bluesnarfer, die nur etwas Ausrüstung und Know-how benötigen, muss der Bluebugger zunächst Ihr Handy mit seinem Computer koppeln und eine „vertrauenswürdige“ Datenverbindung herstellen. Laurie erklärt eine raffinierte Methode dafür: „Man sagt einfach: ‚Hey, cooles Handy, darf ich es mal sehen?‘ Dann drückt man ein paar Tasten, um die Kopplung herzustellen, und gibt es zurück.“ Sobald die Kopplung abgeschlossen ist, kann der Bluebugger alle Funktionen des Handys übernehmen. Er kann Anrufe tätigen, SMS versenden und sogar das Adressbuch und die Kontaktliste überschreiben.

Lauries Enthüllung ist beunruhigend, doch die Tatsache, dass Phreaker ihre Ziele ansprechen und mit ihnen interagieren müssen, reduziert die Zahl der Opfer erheblich. Der britische Sicherheitsberater Ollie Whitehouse, dessen Bluetooth-Suchprogramm Redfang ihn unter Phreakern bekannt gemacht hat, beschreibt jedoch eine weitere Methode zum sogenannten Bluebuging – eine Methode, die keinen physischen Kontakt zum Zieltelefon erfordert. Der Trick besteht darin, den Datenverkehr eines Bluetooth-Telefons abzufangen, während es sich mit einem anderen Gerät, beispielsweise einem Headset, verbindet. Mit diesen Informationen kann ein Angreifer das Telefon per Bluebuging manipulieren, indem er sich als das vertrauenswürdige Gerät ausgibt, mit dem es regelmäßig verbunden ist.

Die Mobilfunkunternehmen argumentieren, dass Bluesnarfing und Bluebugging nur geringe Bedrohungen darstellen, da Bluetooth nur über kurze Distanzen von maximal 20 Fuß funktioniert, weshalb sich die Angreifer in unmittelbarer Nähe ihrer Ziele befinden müssen.

Hier kommt das Bluetooth-Scharfschützengewehr ins Spiel. Aus handelsüblichen Teilen im Wert von 200 Dollar gefertigt, ist es eine für große Entfernungen optimierte Bluetooth-Antenne. Sie kann schwache Signale auf über tausend Meter Entfernung senden und empfangen. Mit diesem Scharfschützengewehr – oder einer ähnlichen drahtlosen Waffe – müssen sich Blaumeisen-Jäger und -Jäger nicht mehr im selben Raum wie ihre Ziele befinden. „Indem wir die Annahme widerlegt haben, dass Entfernung ein Problem darstellt“, sagt der 24-jährige Erfinder Jon Hering, Student an der University of Southern California, „haben wir gezeigt, dass Blaumeisenjagd eine reale Bedrohung ist.“

Die Mobilfunkanbieter müssen doch irgendetwas unternehmen, um uns davor zu schützen. Keith Nowak, ein Sprecher von Nokia, schlägt vor, „Bluetooth einfach auszuschalten oder in den versteckten Modus zu wechseln“.

Whitehouse lacht über diesen Rat. Redfang, sein bekanntes Phreak-Tool, ist speziell dafür entwickelt worden, Bluetooth-Geräte im versteckten Modus aufzuspüren. Und da nur wenige Menschen Bluetooth tatsächlich deaktivieren, sind ihre Handys unzähligen Hacks ausgesetzt – Hacks, die Herings Scharfschützengewehr aus fast einem Kilometer Entfernung ausführen könnte.

Die Jungs von Default Radio, Rockstars der Phreak-Szene, stehen auf der Bühne der DefCon, der altehrwürdigen Hacker-Konferenz, die eine Mischung aus Ozzfest-Moshpit und After-Hour-Party für NSA-Agenten ist. In Baseballkappen, T-Shirts und Baggy-Jeans präsentieren sie eine Live-Version ihrer Phreak-freundlichen Streaming-Talkshow. Der lange Tisch vor ihnen ist mit Telefonen und Computern bedeckt.

Ein Nutzer namens Lucky225 tritt ans Mikrofon. Mit dem Telefon zwischen Ohr und Schulter und der Tastatur unter den Fingern sieht er aus wie eine Mischung aus DJ und Telefonmonteur.

Lucky unterhält das Publikum mit einer Anekdote über seinen liebsten VoIP-Trick: Er kann auf einem VoIP-Telefon jede beliebige Anrufer-ID anzeigen lassen. Um das zu beweisen, erzählt er, er könne sich als „Jenny“ ausgeben, das Mädchen aus dem Popsong von Tommy Tutone.

Ohrenbetäubendes Rauschen aus den Lautsprechern, und plötzlich ertönt ein ohrenbetäubender Wählton. Lucky hat sein VoIP-Telefon an die Musikanlage angeschlossen. Er wählt die Rufnummernanzeige von MCI, einen Dienst, der die Nummer des Anrufers anzeigt. Eine Roboterstimme intoniert langsam Luckys Nummer: „acht-sechs-sieben-fünf“ – die Menge bricht in Gelächter aus, Schreie vermischen sich mit Stöhnen – „drei-null-neun“.

Nachdem Lucky seine Manipulation der Anrufer-ID demonstriert hatte, erklärte er dem vollbesetzten Saal, wie er die Nummer gefälscht hatte. Wie sich herausstellte, handelte es sich um einen Social-Media-Hack. Einige Tage zuvor hatte er seinen Mobilfunkanbieter Vonage angerufen und angegeben, alle seine Handyanrufe auf sein internetfähiges Telefon umleiten zu wollen. Seine Handynummer lautete 867 5309, log er, und Vonage glaubte ihm. Nun werden alle Anrufe an Jenny im Vonage-Netzwerk an Lucky umgeleitet.

Vonage hat natürlich auch die Anrufer-ID von Luckys VoIP-Telefon auf Jennys Nummer eingestellt – jedes Mal, wenn er anruft, sieht es so aus, als käme er von der Nummer 867 5309. Viele Systeme sind auf eine korrekte Anrufer-ID angewiesen – Kreditkartenaktivierung, Voicemail-Systeme, sogar der Notruf 112. Daher kann die Kontrolle darüber, was der Angerufene nach dem Wählen sieht, ein entscheidender Vorteil sein. Mit Ihrer Anrufer-ID könnte ein Identitätsdieb eine neue Bankkarte bestellen, diese telefonisch aktivieren und damit Ihr Bankkonto leerräumen. Und da viele Voicemail-Systeme ihre Inhalte auf jedem Telefon mit der richtigen Anrufer-ID abspielen, könnten Sie mit einem Vonage-Telefon Ihre Privatsphäre für jeden preisgeben.

Besonderheit:
Sie haben deine Nummer
Plus:
Der große Handyraub

Nach der Show frage ich Lucky, warum er in die Phreak-Szene eingestiegen ist. „Nun ja“, sagt Lucky trocken und skizziert Pläne für ein Netzwerk aus Dosen und Gummibändern, „ich wollte dieses Telefonsystem auf Gummibasis starten.“ Er ist ein Scherzbold, aber mit einem Ziel: der Öffentlichkeit klarzumachen, dass VoIP ein Albtraum für den Datenschutz ist. „Ja“, schließt er, immer noch über die Sprachübertragung über Gummibänder nachdenkend, „ich glaube, dieser Dosenkram wird richtig durchstarten.“

Steve Wozniak, der Apple-Computerpionier, dessen Phreak-Ära in den 1970er Jahren begann, sagt, dass es beim Phreaking um Streiche geht. „Wir, die wir die Phreaker-Mentalität haben, sehen es als Spaß an, mit der Welt zu spielen, aber in diesen Zeiten ist es schwer für die Leute, uns als harmlos wahrzunehmen.“

Mag sein, aber Vonage scheint nicht sonderlich besorgt. Als ich das Unternehmen später kontaktiere, um herauszufinden, ob sie von Luckys Trick mit der Anrufer-ID wissen und was sie dagegen unternehmen, gibt der leitende Vizepräsident Louis Holder zu, dass sie nichts tun. „Wir lassen zu, dass Leute so etwas machen“, sagt Holder. „Wir geben den Leuten eine temporäre Telefonnummer, bevor wir sie mit dem Telefonanbieter verifizieren, und die Verifizierung dauert ein paar Wochen. Jemand könnte die Nummer des Weißen Hauses nehmen und sich als Präsident ausgeben.“

Heutige Internet-Hacker können Telefonsysteme lahmlegen – aber auch wieder aufbauen. Luckys Witz, sein eigenes Netzwerk aus Konservendosen und Gummibändern zu bauen, ist gar nicht so weit von der Wahrheit entfernt. Slestak, Da Beave und GiD sind die Köpfe hinter Telephreak.org aus Florida, einem kostenlosen VoIP-Dienst, den sie für ein selbst zusammengestelltes Open-Source-Telefonanlagensystem (PBX) namens Asterisk entwickelt haben.

Eine PBX (Telefonanlage), typischerweise in Unternehmen eingesetzt, besteht aus Computern, die Anrufe zwischen einem internen Telefonnetz und dem öffentlichen Telefonnetz weiterleiten. Ein Unternehmen, das eine PBX nutzt, zahlt beispielsweise für 100 Leitungen, die 500 Mitarbeiter bedienen und Anrufer mit der Außenwelt, der Voicemail oder Konferenzen verbinden, indem die Anrufe dynamisch über die jeweils verfügbaren Festnetzleitungen verbunden werden. Früher wurden all diese Verbindungen vom Telefonanbieter oder einem proprietären, abgeschotteten System im Serverraum verwaltet. Mit Asterisk ist die Verwaltung Ihrer Leitungen durch den Telefonanbieter jedoch nicht mehr nötig. Sie können sie selbst übernehmen.

Die Telephreak-Crew hat für sich und ihre Freunde ein eigenes privates Telefonunternehmen gegründet – eines, das niemals Rechnungen verschickt. Über eine Zugangsnummer können Sie Ihre Voicemail abrufen, Konferenzgespräche führen, Anrufe an andere Telefone weiterleiten oder sogar eine neue Nummer erhalten. Und das alles ohne einen Cent zu bezahlen.

Aktuell gibt es mehrere hundert Voicemail-Konten, und das System kann hundert gleichzeitige Anrufe verarbeiten. Obwohl das Telephreak-Team für die Verbindung zu Ma Bell bezahlen muss, ist der Betrag so gering, dass sie ihn gerne in Kauf nehmen. Es ist ein kleiner Preis für die Freiheit.

Ich spreche mit ihnen über eine Telephreak-Konferenzschaltung, und der Ton ist etwas verrauscht. Beave, erkennbar an seinem leichten Südstaatenakzent, sagt mir, er arbeite daran, die Probleme

zu beheben. Es ist schon etwas seltsam, zu wissen, dass jemand während des Gesprächs die Telefonverbindung manipuliert. Plötzlich ist der Ton perfekt. Wir wurden umgeleitet. Slestaks Stimme ist laut und deutlich zu hören: „Meine Verbindung zu euch läuft gerade über ein schnurloses Telefon mit einer Box zum Server und dann zu Telephreak. Mein Wählton kommt von der Westküste."

Einer der größten Vorteile beim Bau einer eigenen Telefonanlage ist, dass man damit – wie Slestak es nennt – „Chemie-Experimente" durchführen kann. Manche Telefonanlagen-Phreaker, wie Telediablo, bieten sogar einen Anrufer-ID-Spoofing-Service an: Damit muss man Vonage nicht mehr anlügen – man ruft einfach Telediablos Telefonanlage an, gibt die gewünschte Rufnummer ein und wählt dann die Nummer desjenigen, den man hereinlegen möchte. Als ich diesen kleinen Trick ausprobierte, wählte ich die Nummer 666 6666. Anschließend gab ich die Nummer eines Freundes in der Nähe ein. Es klingelte. Mein Freund zeigte mir sein Anrufer-ID-Fenster: Jetzt fühlte ich mich wie ein Phreak. Anstatt meiner Nummer zeigte sein Telefon die Nummer des Teufels an.

Es gibt noch weitere Tricks bei Telefonanlagen – wie die Entmaskierung der Anrufer-ID, die manchmal die tatsächliche Telefonnummer eines Anrufers preisgeben kann, selbst wenn dieser seine Nummer unterdrücken lässt. Wenn Sie also glauben, im Telefonsystem anonym zu sein, irren Sie sich.

Die wohl beunruhigendste Entdeckung der White-Hat-Phreaker ist, dass VoIP-Anbieter und Mobilfunkunternehmen bereit sind, Telefone und Dienste zu verkaufen, von denen sie genau wissen, dass sie anfällig für Angriffe aller Art sind. Nach monatelanger negativer Berichterstattung in Großbritannien, wo Laurie und Whitehouse ansässig sind, reagieren die Mobilfunkunternehmen nun. Nokia und Sony Ericsson haben Sicherheitsupdates veröffentlicht, und Motorola gibt an, dass die Sicherheitslücken in den neueren Modellen behoben wurden. Der aufstrebende VoIP-Anbieter Skype wirbt mit integrierter Verschlüsselung. Das Bluetooth-Konsortium – ein Zusammenschluss von Branchenführern, darunter Nokia und Sony Ericsson, deren Produkte Bluetooth nutzen – legte auf seinem UnPlugFest in Deutschland im vergangenen Monat einen besonderen Fokus auf Sicherheit. Auf der Veranstaltung bewerteten Sicherheitsexperten (darunter auch Laurie) die Telefone der einzelnen Hersteller hinsichtlich ihrer Widerstandsfähigkeit gegen gängige Angriffe. Dennoch verfolgt niemand Bluesnarf- oder Bluebug-Angriffe, um das Ausmaß des Problems zu erfassen – niemand außer den White-Hat-Phreakern selbst.

Whitehouse hat ein Programm namens Sweet Tooth entwickelt, das die charakteristischen Funksignale von Bluesnarf-Angriffen erkennen kann. Angelehnt an Honeypot-Programme, die Strafverfolgungsbehörden und Sicherheitsanalysten zur Aufspürung von Hackern im Internet einsetzen, könnte Sweet Tooth präzise Statistiken zur tatsächlichen Verbreitung von Bluesnarf-Angriffen liefern. Das Programm sei einsatzbereit, so Whitehouse. Fraglich ist nun jedoch, ob Strafverfolgungsbehörden und Telefongesellschaften es auch tatsächlich einsetzen werden. Das Problem zu ignorieren, wird es nicht lösen – insbesondere, da das Hacken von Telefonen immer einfacher wird.

Bluetooth-Phreaking ist erst der Anfang. Die Sicherheitslücken werden zwar geschlossen, aber das Problem bleibt bestehen, denn alle Werkzeuge, die Hacker jahrzehntelang entwickelt haben, werden nun dazu genutzt, Ihr Smartphone zu kapern. Smartphones der nächsten Generation bieten

Hackern drei Einfallstore: Wenn ein Datendieb Ihre Daten nicht per Bluetooth abfangen kann, versucht er es über WLAN, und wenn auch das nicht funktioniert, über Infrarot.

„Ich schätze, das ist der Preis, den man für die Konvergenz zahlt“, sagt Whitehouse.

Besonderheit:
Sie haben deine Nummer
Plus:
Der große Handyraub

Der große Handyraub

Wie Sicherheitslücken in heutigen Mobiltelefonen morgen zum perfekten Verbrechen führen könnten.

Schritt 1: Herangehensweise
Ein Virusverbreiter betritt den Flughafen Heathrow mit einem Aktenkoffer, in dem sich ein Laptop und eine externe Antenne befinden. Das Gerät kann Bluetooth-Signale aus bis zu sechs Metern Entfernung abfangen – und mit etwas Hacking lässt es sich so modifizieren, dass es Signale über deutlich größere Entfernungen senden und empfangen kann.

Schritt 2: Entdecken
Mithilfe eines Programms wie Bluesnarf findet der Laptop automatisch Bluetooth-fähige Mobiltelefone, deren Firmware anfällig für eine Fernübernahme ist. Dieser Vorgang ist in weniger als 15 Sekunden abgeschlossen.

Schritt 3: Übernehmen
Der Laptop sendet ein Programm an alle anfälligen Handys. Getarnt als Spiel oder Werbeaktion, ist das Programm in Wirklichkeit ein Trojaner, der einen gefährlichen Virus verbirgt. Sobald der Nutzer es startet, übernimmt der Virus die Kontrolle über das Betriebssystem des Handys und kontrolliert grundlegende Funktionen wie Telefonieren und SMS-Schreiben.

Schritt 4: Weiterleiten
Das betroffene Telefon ist nun infiziert und reagiert, indem es das Virus an andere anfällige Bluetooth-Telefone im Umkreis von 6 Metern sendet. Innerhalb weniger Minuten können Tausende von Telefonen infiziert werden.

Schritt 5: Stehlen
Das Virus übernimmt die Kontrolle über das SMS-System der Mobiltelefone und nutzt ein gängiges europäisches Mikrozahlungssystem namens Reverse-SMS, um jeweils 10 Euro von jedem Telefon auf ein temporäres Konto in Estland zu überweisen. Das Virus veranlasst die Überweisung und behält die Kontrolle, bis es die Bestellung bestätigen kann. Das Konto wird lange geschlossen,

bevor die Abbuchung auf der Monatsrechnung eines Nutzers erscheint.

Annalee Newitz (annalee@techsploitation.com) *, eine Politikanalystin bei der Electronic Frontier Foundation, schrieb in Ausgabe 12.06 über Dating-Optimierer.*

Telefonbetrug durch organisierte Kriminalität in Nevada

Eddie Munoz kennt ein Geheimnis von Las Vegas. Als Betreiber eines der ältesten Zimmerservices für Erwachsene in der Stadt weiß Munoz, dass Vegas eine Stadt ist, die vom unaufhörlichen Rauschen von Geld und Laster angetrieben wird. In seinen besten Zeiten klingelten seine Telefone hundertmal am Tag, und er vermittelte fünfzehn bis zwanzig Mal pro Nacht private Nackttänzerinnen (Prostitution ist in Las Vegas illegal) an die Hotels entlang des Strips und verdiente, wie er sagt, jährlich 240.000 Dollar an Vermittlungsgebühren.

Das Geheimnis, so Munoz, liegt in den hunderten Kilometern moderner Glasfaserleitungen und alter Kupferkabeln, die unter den sonnenverbrannten Straßen der Stadt verlegt sind, sowie in den Dutzenden digitalen Vermittlungsstellen, die Daten und Sprache von einem Ende des Strips zum anderen übertragen. Munoz glaubt, dass eine dubiose Gruppe aus Kriminellen, korrupten Insidern und professionellen Hackern seit einem Jahrzehnt die illegale Kontrolle über den Cyberspace von Las Vegas ausübt und ihn beinahe aus der Erotikbranche verdrängt hat, indem sie die für das Escort-Gewerbe so wichtigen Telefonleitungen gezielt blockierte, abhörte und umleitete.

Eddie Munoz kennt ein Geheimnis von Las Vegas. Als Betreiber eines der ältesten Zimmerservices für Erwachsene in der Stadt weiß Munoz, dass Vegas eine Stadt ist, die vom unaufhörlichen Rauschen von Geld und Laster angetrieben wird. In seinen besten Zeiten klingelten seine Telefone hundertmal am Tag, und er vermittelte fünfzehn bis zwanzig Mal pro Nacht private Nackttänzerinnen (Prostitution ist in Las Vegas illegal) an die Hotels entlang des Strips und verdiente, wie er sagt, jährlich 240.000 Dollar an Vermittlungsgebühren.

Das Geheimnis, so Munoz, liegt in den hunderten Kilometern moderner Glasfaserleitungen und alter Kupferkabeln, die unter den sonnenverbrannten Straßen der Stadt verlegt sind, sowie in den Dutzenden digitalen Vermittlungsstellen, die Daten und Sprache von einem Ende des Strips zum anderen übertragen. Munoz glaubt, dass eine dubiose Gruppe aus Kriminellen, korrupten Insidern und professionellen Hackern seit einem Jahrzehnt die illegale Kontrolle über den Cyberspace von Las Vegas ausübt und ihn beinahe aus der Erotikbranche verdrängt hat, indem sie die für das Escort-Gewerbe so wichtigen Telefonleitungen gezielt blockierte, abhörte und umleitete.

„In diesem Geschäft werden wir von 17:00 Uhr nachmittags bis 5:00 Uhr morgens angerufen, und genau dann trifft es uns“, sagt Munoz. „Es ist, als wären Sie der Maytag-Mann. Das Telefon klingelt einfach nicht.“

Heutzutage hat Munoz Glück, wenn er ein oder zwei Kunden pro Nacht hat, und sein einst florierendes Bordellimperium ist zu einem kümmerlichen Betrieb verkommen, den er von einem Büro in seinem Haus aus führt, weit entfernt vom grellen Neonlicht von Las Vegas. Er hält sich

hauptsächlich dank seines hart erkämpften Besitzes von fast der Hälfte der fünfhundert lizenzierten Zeitungsständer auf dem Strip über Wasser, die er mit Stapeln seiner eigenen Zeitung, dem „Las Vegas Informer“, vollstopft – zwölf Seiten voller Anzeigen für „Feurige Rothaarige“ und „Heiße, heiße, heiße, große, sexy Blondinen“. Bis vor Kurzem führte jede in der Zeitung inserierte Telefonnummer zu Munoz’ Telefonzentrale, doch seine Telefone klingelten trotzdem nicht. Die wirtschaftliche Lage zwang ihn schließlich, Werbeflächen an einen Konkurrenten zu verkaufen, um die Miete bezahlen zu können.

Munoz hat unzählige Telefonprobleme; seine Liste mit Störungsmeldungen ist länger als die eines Drogenabhängigen. Anrufer von außerhalb von Las Vegas oder von öffentlichen Telefonen und Handys kommen durch, sagt er, aber Hotelgäste bekommen entweder ein Besetztzeichen oder es herrscht Stille, sodass sie sich an die Konkurrenz wenden müssen. Manchmal werden Anrufe sogar direkt an einen Mitbewerber umgeleitet, behauptet er. Und wenn ein potenzieller Kunde doch durchkommt und Munoz eine Tänzerin ins Hotelzimmer schickt, trifft sie dort wahrscheinlich bereits auf eine andere Künstlerin. „Manchmal sind sie schneller am Telefon, als würden sie mithören“, sagt Munoz.

Mindestens drei weitere Unternehmen der Erwachsenenunterhaltungsbranche, ein Privatdetektiv und ein Kautionsvermittler berichteten von ähnlichen Vorfällen. „Es klingelte nur kurz, ich hob ab, und niemand war dran“, sagt Hilda Brauer, die ehemalige Inhaberin des inzwischen geschlossenen Escortservices „Sexy Girls“. 1998 reichte Brauer Klage gegen die örtliche Telefongesellschaft, einen Konkurrenten, den sie für das Problem verantwortlich machte, und den Herausgeber des Donnelly Directory ein, in dem „Sexy Girls“ sieben ganzseitige Anzeigen geschaltet hatte. Später zog sie die Klage zurück, schloss ihr Geschäft und verdient ihren Lebensunterhalt nun mit Wahrsagerei für eine Wahrsager-Hotline. „Ich verlor mein Haus und musste meine Möbel verkaufen, um Geld für eine neue Wohnung zu haben“, sagt Brauer.

Auch Peter Vilencia, ein ehemaliger Kautionsvermittler, hatte Probleme mit seinem Telefon. Vilencia hatte 1996 die Firma Bail Bonds Inc. gekauft, und nach einer Woche reger Geschäfte mit der Befreiung betrunkener Touristen und Kleinkrimineller aus dem Clark County Detention Center erlebte er plötzlich einen drastischen Rückgang der Anrufe. „Freitags um 16:00 Uhr hörte mein Telefon auf zu klingeln“, sagt Vilencia, der die Firma letztes Jahr verkaufte. „Fast jedes Wochenende, fast vier Jahre lang, war das so. Man konnte die Uhr danach stellen.“
Sabotage widersetzt sich der Prüfung

„Unsere Telefone funktionierten von Freitagabend bis zum Wochenende nicht, und genau in dieser Zeit werden die meisten Leute verhaftet“, erinnert sich Mike Kapfer, Vilencias ehemaliger Kopfgeldjäger. Manchmal klingelten die Telefone nur halb, als ob eine Rufumleitung aktiv wäre; häufiger jedoch wurden die Häftlinge mitten im Gespräch scheinbar an einen anderen Kautionsvermittler weitergeleitet. Nur Anrufe aus dem Gefängnis waren gefährdet. „Wenn ich die Nummer von meinem Handy aus anrief, kam die Verbindung zustande“, sagt Kapfer.

Beide Männer stimmen mit Munoz und Brauer überein, dass jemand im Hintergrund die Fäden zieht. „Ich hatte Leute, die das Gebäude im Hinterhof, wo die Telefonleitungen reinkommen, und die Verteilerkästen die Straße runter beobachteten“, sagt Vilencia. „Es musste intern sein, niemand sonst hatte Zugang.“

Doch selbst nach Brauers Klage, jahrelangen formellen Beschwerden von Munoz, einer schriftlichen Beschwerde eines Privatdetektivs, der behauptete, Anrufe zu verlieren, und zwei Berichten über die Vorwürfe der Anrufumleitung in der New York Times, ist das örtliche Telefonunternehmen weiterhin fest davon überzeugt, dass alles in Ordnung ist.

„Wir haben unsere Tests durchgeführt, Zeit und Ressourcen investiert und keinerlei Anzeichen für Anrufumleitungen festgestellt“, so Scott Collins von der Regulierungsabteilung der Sprint-Tochter Central Telephone. Im vergangenen November führte das Telekommunikationsunternehmen im Auftrag der Nevada Public Utilities Commission (PUC) drei Tage lang Testanrufe aus fünf verschiedenen Hotels in Las Vegas durch: dem Sahara, dem Travel Lodge, dem Vagabond, dem Motel 6 und dem Four Queens. Von 205 Anrufen wurden bis auf 23 alle erfolgreich durchgestellt, und keiner wurde an Konkurrenten umgeleitet. (Weitere Untersuchungen der 23 abgebrochenen Anrufe ergaben harmlose Erklärungen.) Tests von AT&T im Jahr 1997 hatten ähnliche Ergebnisse erbracht.

Munoz macht Indiskretionen verantwortlich – er sagt, jeder habe von den Tests gewusst, und die Verantwortlichen hätten die Anrufe absichtlich durchrutschen lassen. Doch im Dezember verlief auch der Anruf eines Reporters aus einem Hotel in Las Vegas problemlos.

Könnte der Cyberdiebstahl in Las Vegas ein Mythos sein, zusammengebraut aus den Trümmern gescheiterter Unternehmen und vagen technologischen Anekdoten? Wenn ja, dann ist es ein Mythos, der in den nächtlichen Randgebieten von Las Vegas den Status von Allgemeinwissen erreicht hat, und in einem bizarren Fall wäre ein Betreiber eines Erotikbetriebs beinahe Opfer brutaler Vergeltungsaktionen der Mafia geworden.

Vinnie „Aspirins“ und sein Akkuschrauber

Es geschah im Jahr 1998: Eine FBI-Untersuchung über Polizeikorruption in Las Vegas brachte eine Verschwörung von sechs organisierten Verbrechern ans Licht, die darauf abzielten, in eine Handvoll erfolgreicher Escort-Services in Las Vegas einzudringen, welche ein von der Mafia unterstütztes Unternehmen unter der Leitung eines der Männer, Christiano DeCarlo, in den Schatten gestellt hatten.

Laut Gerichtsakten hatten die mutmaßlichen Verschwörer, die der Gambino-Familie angehörten, es besonders auf Richard Soranno, den Besitzer eines der größten Escort-Services der Stadt, Vegas Girls, abgesehen. Sie glaubten, Soranno habe mithilfe eines mysteriösen Computerexperten namens Charles Coveney Anrufe von Konkurrenten, darunter DeCarlo, abgefangen.

„Coveney hat Kontakte bei der Sprint Telephone Company und kann Anrufe von einer Nummer auf eine andere umleiten lassen“, glaubten die Gangster laut einer FBI-Aussage. Die Männer planten, Coveney zu „überreden“, Serrano zu verlassen und DeCarlo bei seinen Hausbesuchen zu unterstützen, indem sie Anrufe zu ihm umleiteten. Zu den Überredungskünsten der Bande gehörte ein Schläger namens Vinnie „Aspirins“ Congiusti, der aus Tampa eingeflogen wurde und seinen Spitznamen angeblich daher hatte, dass er einmal mit einem Akkuschrauber Löcher in den Kopf eines Mannes gebohrt hatte.

Als die Mafiosi in Las Vegas nach Coveney suchten, musste das FBI eingreifen und eine großangelegte Undercover-Operation vorzeitig beenden. Alle sechs Männer bekannten sich später der Verschwörung schuldig. Vinnie „Aspirins“ starb letztes Jahr im Gefängnis an mutmaßlichem Herzversagen.

Heute herrscht zwischen Munoz und Soranno keine Freundschaft. Munoz glaubt, kann es aber nicht beweisen, dass Soranno einer der Drahtzieher einer Verschwörung zur Zerstörung seines Unternehmens ist. Soranno hingegen sagt, genau solche Gerüchte hätten ihn beinahe das Leben gekostet. „Alles begann damit, dass Munoz ein Gerücht aufgriff und daraus eine große Sache machte“, sagt Soranno. „Er hat mein Leben in Gefahr gebracht.“ Der Sexmogul beteuert, niemanden namens Charles Coveney zu kennen und seinen Erfolg im Erotikgewerbe allein seinem Marketing-Talent und seinem allgemeinen Geschäftssinn zu verdanken. „Munoz ist der schlechteste Geschäftsmann der Welt“, sagt Soranno. „Wenn Sie der schlechteste Geschäftsmann der Welt wären, würden Sie dann Anrufe bekommen?“
Telekommunikationsunternehmen: Las Vegas ist hacksicher

Doch selbst Soranno sieht Korruption im Telefongeschäft von Las Vegas – allerdings nicht im Netz von Sprint. In manchen Hotels, so glaubt er, überwachen korrupte Insider die Telefonanlagenprotokolle nach Anrufen bei Erotikdiensten. Sobald sie einen solchen Anruf entdecken, umgehen sie den Dienst, indem sie ihre eigene Tänzerin auf das Zimmer des Gastes schicken. „Sobald sie wissen, dass jemand Interesse hat, können sie jemanden schicken“, sagt Soranno. Sollte diese Taktik stimmen, würde sie das von Munoz beschriebene Szenario mit den doppelten Tänzerinnen erklären. „Wenn eine Tänzerin zu einem Anruf geht und bereits eine andere Tänzerin da ist, denken die Gäste sofort, dass jemand das Telefon abhört“, sagt Soranno.

Collins von Sprint erklärt, dass Sprint Central Telephone nach aktuellem Kenntnisstand noch nie Probleme mit korrupten Mitarbeitern oder Hackern jeglicher Art gehabt habe. „Uns ist kein Fall bekannt“, so Collins. „Wir haben keinerlei Anzeichen dafür, dass so etwas vorgekommen ist.“

Das Unternehmen kam im September 1995 zum selben Schluss, nachdem Hilda Brauer eine Beschwerde bei der Nevada Public Service Commission (damals noch Public Service Commission) eingereicht hatte. Laut den Gerichtsakten schlussfolgerte die Kommission, dass die Vielzahl der Beschwerden zwar auf Unregelmäßigkeiten im Internet von Las Vegas hindeutete, es aber keinen hinreichenden Verdacht gab, dass Sprint Central Telephone schuldig war. Die Kommission stellte fest, dass das Telekommunikationsunternehmen die geltenden Regeln und Vorschriften eingehalten und keinerlei Beweise für einen illegalen Zugriff auf sein Netzwerk gefunden hatte.

Seit Jahrzehnten sind regionale und überregionale Telefongesellschaften in den gesamten USA immer wieder mit Hackerangriffen auf kritische Systeme konfrontiert. Zuletzt erreichten Bundesbeamte 1999 Schuldbekenntnisse von drei Mitgliedern einer landesweiten Hackergruppe, die sie „The Phone Masters“ nannten. Bis zu einer Razzia des FBI im Jahr 1995 hatten die Phone Masters Zugriff auf die Computersysteme von Sprint Long Distance, Southwestern Bell und GTE und konnten in einigen Regionen des Landes geheime Telefonnummern erlangen, Telefonleitungen überwachen und ihren Zugang nutzen, um auch in andere Systeme einzudringen, darunter das National Crime Information Center (NCIC) des FBI.

Wenn Sprint Central Telephone noch nie gehackt wurde, ist das Unternehmen unter den Telekommunikationsanbietern eine Ausnahmeerscheinung. SecurityFocus hat jedoch erfahren, dass das Netzwerk des Unternehmens in Las Vegas möglicherweise doch nicht immun gegen Hackerangriffe ist.

„Vegas war einfach."
Bis zu seiner Flucht Anfang der 90er-Jahre war Las Vegas für den weltberühmten Hacker Kevin Mitnick, dessen Familie dort lebte, ein zweites Zuhause. Von etwa 1992 bis zu seiner Verhaftung im Februar 1995 hatte Mitnick eigenen Angaben zufolge umfangreichen illegalen Zugriff auf das Netzwerk in Las Vegas. Er erinnert sich außerdem daran, einmal ein Angebot erhalten zu haben, Anrufe eines Erotikdienstes für ein Wochenende umzuleiten – für 3.000 Dollar. „Sie wollten, dass ich irgendwie die Leitung übernehme und die Anrufe weiterleite", erinnert sich Mitnick.

„Hätte ich es gewollt, hätte es keine drei Minuten gedauert."

Mitnick, der nach fünf Jahren Haft derzeit unter gerichtlicher Aufsicht steht, hat nachweislich nie von seinen Hackerangriffen profitiert und beteuert, nie an einem Betrug mit abgefangenen Anrufen beteiligt gewesen zu sein. Er verweist jedoch auf zwei spezifische Sicherheitslücken im Netzwerk von Las Vegas, die einem Insider mit entsprechenden Kenntnissen oder einem versierten Hacker ein solches Vorgehen ermöglichen würden.

Zunächst hatte Mitnick eigenen Angaben zufolge über Einwahlmodems direkten Zugriff auf die Steuerkonsolen der Vermittlungsanlagen in Las Vegas. Jede Nortel-DMS-Vermittlungsstelle verfügte über eine geheime Telefonnummer sowie einen Standardbenutzernamen und ein Standardpasswort. Die Einwahlverbindungen waren normalerweise nicht erreichbar, und Mitnick musste, wie er sagt, einen Sprint-Mitarbeiter anrufen und sich als Techniker ausgeben, um die Leitungen freizuschalten. Sobald dies geschehen war, „hatte ich denselben Zugriff auf die Vermittlungsstelle wie die Techniker", erinnert er sich: die volle Kontrolle über die Anrufweiterleitung.

Mit Zugang zu den Vermittlungsstellen fand Mitnick es nützlich, seine Anrufe über Las Vegas zu leiten, um einer Rückverfolgung zu entgehen, selbst als er sich in Seattle und Raleigh, North Carolina, versteckte. „Vegas war einfach", sagt Mitnick.

Das zweite System ist ein Testsystem namens „Callers" – Mitnick gibt an, den Namen nie schriftlich gesehen zu haben und daher weder die Schreibweise noch die Groß- und Kleinschreibung zu kennen. Seiner Beschreibung nach ermöglichte das System Mitarbeitern von Telefongesellschaften, von einem zentralen Standort aus Tests an Kundenleitungen, sogenannten „Loops", durchzuführen. Es bestand aus einigen Client-Computern und Remote-Servern, die an jede der DMS-100-Vermittlungsstellen von Sprint Central Telephone angeschlossen waren.

Laut Mitnick waren die Remote-Server von Las Vegas schlecht geschützt. Sie waren über langsame Modems erreichbar und durch eine Methode gesichert, die kaum sicherer war als ein einfaches Passwort: Der Server verlangte vom Client – in der Regel einem Computerprogramm – die korrekte Antwort auf eine von 100 zufällig ausgewählten Aufgaben. „Es wurde eine Frage gestellt, die man umgehend beantworten musste", erklärt Mitnick. „Es war eine Zahl, zum Beispiel 54, und die

Antwort war ein bestimmter Hexadezimalcode, zum Beispiel 3FAE.“

Mitnick erzählt, er habe die Einwahlnummern für Las Vegas herausgefunden, indem er Sprint-Mitarbeiter überlistet habe. Außerdem habe er sich die Liste mit den Herausforderungen und Antworten von Northern Telecom, dem Hersteller des Systems (seit 1999 Nortel Networks), besorgt. „Ich musste Nortel anrufen und mir das von einem Techniker erklären lassen“, sagt Mitnick. „Ich erklärte ihnen, dass ich eine Software entwickle, die mit dem System kompatibel sein muss.“

Das System ermöglichte es Nutzern, Telefonleitungen unbemerkt zu überwachen oder Anrufe auf fremden Leitungen zu tätigen und entgegenzunehmen, erklärt Mitnick. „Man brauchte lediglich einen Laptop und ein Telefon.“ Die Auswirkungen reichen weit über das bloße Abhören von Anrufen hinaus. „Jemand mit kriminellen Absichten, in einer Stadt wie Las Vegas – man stelle sich die Möglichkeiten vor.“

Nortel-Sprecher David Chamberlin wies Mitnicks Darstellung als „wilde Spekulation“ und „Gerücht“ zurück. Auf der Website des Unternehmens wird jedoch eine Funktion namens „CALRS“ (Centralized Automated Loop Reporting System) als Option für die DMS-Switch-Produktreihe aufgeführt. An anderer Stelle auf der Website wird CALRS in Nortel-Unterlagen als „externes Testzugriffssystem“ beschrieben.

Ein Sprecher von Sprint und ein Anwalt des Unternehmens lehnten beide eine Stellungnahme zu CALRS ab und wollten weder die Existenz eines schlecht geschützten Testsystems bestätigen noch dementieren, das möglicherweise ein offenes Tor zum innersten Heiligtum der Telekommunikationsinfrastruktur von Las Vegas darstellt.

Öffentliche Anhörungen anberaumt

Das Unternehmen kann möglicherweise nicht ewig schweigen. Nach jahrelangen Beschwerden nimmt der Staat Nevada die Anschuldigungen von Munoz nun ernst. Im Februar stellte die Regulierungsbehörde für öffentliche Versorgungsunternehmen (PUC) trotz Sprints Einwänden fest, dass ein hinreichender Verdacht für eine umfassende Untersuchung bestehe, und hat öffentliche Anhörungen für September angesetzt. Die Kommission fordert unterdessen Aufklärung. Letzten Monat stellte sie Sprint formell einen Antrag auf Akteneinsicht, in dem sie unter anderem fragt, ob das Unternehmen jemals gehackt wurde. Sprint antwortete am Donnerstag und behauptete erneut, es gebe keinerlei Beweise dafür, dass es jemals unter korrupten Mitarbeitern oder externen Angreifern gelitten habe.

Sprint-Manager Collins verweigert Journalisten die Auskunft und verweist Anfragen an den externen Rechtsberater des Unternehmens, Patrick Reilly, einen Anwalt der Kanzlei Hale Lane Peek Dennison Howard and Anderson aus Nevada. „Unseres Wissens gibt es keine Hinweise auf einen Netzwerkverstoß“, so Reilly.

„Jetzt habe ich die Befugnis, Vorladungen auszustellen“, sagt Munoz. „Passt auf.“

„Eddie klopft seit Jahren an Türen und wendet sich an verschiedene Behörden, und soweit ich weiß, ist dies das erste Mal, dass er eine echte Plattform erhält“, sagt Rick Hackman,

Beschwerdemanager der Nevada Public Utilities Commission. „Obwohl er uns nicht davon überzeugt hat, dass Sprint die Schuld trägt, sind wir der Meinung, dass er die Möglichkeit verdient, seinen Fall vor der gesamten Kommission vorzutragen.“

Die Entscheidung der Regulierungsbehörde für öffentliche Versorgungsunternehmen (PUC), Anhörungen durchzuführen, ist ein enormer Erfolg für Munoz und erhöht den Druck auf Sprint Central Telephone. Sollte Munoz obsiegen, könnte die Kommission Geldstrafen und Sanktionen verhängen. Darüber hinaus kündigte Munoz an, das Unternehmen auf 20 Millionen Dollar zu verklagen.

Das sei der Preis, sagt er, für zehn Jahre Umsatzeinbußen in einer Zeit, die die Stadt in atemberaubendem Maße erlebt habe. Der Bau von Superhotels wie dem Bellagio, dem Venetian, dem Paris und dem Aladdin habe die Gästekapazität von Las Vegas auf über 120.000 Hotelzimmer erhöht, und die Stadt sei mittlerweile Gastgeber von rund viertausend Kongressen pro Jahr. Und das seien viele Menschen, die hätten versuchen können, eine von Munoz' heißen, großen, sexy Blondinen anzurufen.

Computer-Spionagesoftware

Jany ist Studentin und engagiert sich ehrenamtlich in einer Beratungsstelle für Vergewaltigungsopfer. Dort nimmt sie Anrufe entgegen, die an ihre Privatadresse weitergeleitet werden. Außerdem arbeitet sie mit einer Online-Selbsthilfegruppe für Betroffene von sexueller Gewalt zusammen. Jany achtet sehr auf ihre Computersicherheit. Sie nutzt eine Firewall, hält ihren Virenschutz stets aktuell und liest niemals unerwünschte E-Mails oder öffnet unerwartete Anhänge. Doch trotz all ihrer Vorsichtsmaßnahmen überwacht ihr eifersüchtiger Ex-Freund jede ihrer Aktivitäten am Computer und im Internet, und sie hat keine Ahnung, was er treibt.

Aus dem Newsletter des Stalking Resource Center, Band 5, Nummer 1, Sommer 2005

Jany ist Studentin und engagiert sich ehrenamtlich in einer Beratungsstelle für Vergewaltigungsopfer. Dort nimmt sie Anrufe entgegen, die an ihre Privatadresse weitergeleitet werden. Außerdem arbeitet sie mit einer Online-Selbsthilfegruppe für Betroffene von sexueller Gewalt zusammen. Jany achtet sehr auf ihre Computersicherheit. Sie nutzt eine Firewall, hält ihren Virenschutz stets aktuell und liest niemals unerwünschte E-Mails oder öffnet unerwartete Anhänge. Doch trotz all ihrer Vorsichtsmaßnahmen überwacht ihr eifersüchtiger Ex-Freund jede ihrer Aktivitäten am Computer und im Internet, und sie hat keine Ahnung, was er treibt.

Spyware

Janys Ex-Freund hat sich mithilfe von Spyware – einem Überwachungsprogramm, das direkt oder aus der Ferne installiert werden kann, um sämtliche Aktivitäten auf einem Computer zu verfolgen – Zugang zu ihrem Computer verschafft. Spyware kann Passwörter und Tastatureingaben erfassen, alle gesendeten und empfangenen E-Mails überwachen, alle Chatverläufe aufzeichnen und sogar jede besuchte Webseite verfolgen. Der Spyware-Nutzer hat Zugriff auf Janys Passwörter, PIN-Nummern, Kreditkartennummern, Bankdaten und alle Dateien. Dieses Wissen verletzt nicht nur Janys Privatsphäre, sondern kann auch ihre Sicherheit gefährden. Das Spyware-Programm verrät ihrem Stalker, ob Jany nach einem Job sucht, ein Flugticket kauft, ein Date hat oder eine Vorlesung besucht. Wenn er ihr schaden will, weiß er, wo er sie finden kann.

Für den durchschnittlichen Computerbenutzer ist Spyware schwer zu erkennen. Sie läuft typischerweise im „Stealth"-Modus, wodurch sie nicht in der Liste der aktuell laufenden Programme erscheint. Diese Programme tarnen sich oft als andere Programme, sind schwer zu entfernen und können sich sogar selbst neu installieren, wenn sie deinstalliert werden.

Wie Spyware funktioniert

Computerüberwachungsprogramme wie Spyware wurden ursprünglich entwickelt und vermarktet, um die Internetnutzung von Kindern zu überwachen. Bald entstanden neue Formen, und eine davon – die sogenannte Adware – wurde zu einem beliebten Werbemittel für Marketingfirmen. Adware installiert sich, wenn ein Computerbenutzer „kostenlose" Software herunterlädt oder auf Pop-up-Fenster klickt, die auf vielen Webseiten erscheinen. Nach der Installation über die kostenlose Software verfolgt die Adware die Internetnutzung (zu Marktforschungszwecken), spielt Werbung aus und animiert Nutzer zum Besuch von Webseiten, die die Produkte der Werbetreibenden verkaufen.

Spyware funktioniert im Prinzip ähnlich wie Werbesoftware, verfolgt aber einen anderen Zweck: Sie dient dazu, das Verhalten des Zielobjekts auszuspionieren und zu verfolgen. Spyware zeichnet alle Tastatureingaben auf und sendet diese Informationen an Dritte. Je nach Spyware-Programm kann der Benutzer gesendete und empfangene E-Mails lesen, besuchte Webseiten einsehen, allgemeine Dateien einsehen und die Passwörter lesen, die das Zielobjekt beim Anmelden an einem Computer oder einer Webseite verwendet.

Die Installation von Spyware ist nicht schwierig, insbesondere wenn der Programminstallierer Zugriff auf den Computer des Opfers hat. Spyware kann auch aus der Ferne über verschiedene Methoden installiert werden, beispielsweise durch Trojaner, die (wie ihr bekannter Name) harmlos erscheinen, aber tatsächlich eine gefährliche, getarnte Komponente enthalten. Wenn das Opfer eine E-Mail öffnet oder ein Programm herunterlädt, das scheinbar von einer legitimen Quelle stammt, installiert der Trojaner Spyware auf dem Computer.

Zugang über das Internet

Eine weitere Methode, mit der Stalker auf die Computer ihrer Opfer zugreifen, sind deren IP-Adressen, die Internet-Telefonnummern ähneln. IP-Adressen bestehen aus vier Zahlenblöcken zwischen 0 und 255, die jeweils durch einen Punkt getrennt sind, und dienen dazu, Informationen zwischen dem Computer einer Person und anderen Computern im Netzwerk der miteinander verbundenen Computer, dem Internet, zu leiten. Ein Stalker, der die IP-Adresse eines Opfers kennt (was möglich ist, wenn er eine E-Mail vom Opfer erhalten hat – entweder direkt oder weitergeleitet), kann über diese Verbindung Spyware installieren, indem er das Programm sendet, während der Computer online ist.

Wie leicht ein Stalker an die IP-Adresse eines Nutzers gelangt, hängt von dessen Internetverbindung ab. Einwahlverbindungen stellen für Stalker die größte Herausforderung dar, da den Computern der Nutzer bei jeder Internetverbindung eine neue IP-Adresse zugewiesen wird. Bei Kabel- oder anderen Hochgeschwindigkeitsverbindungen bleibt die IP-Adresse des Kunden hingegen in der Regel gleich, und sein Modem ist auch dann noch über dieselbe IP-Adresse mit dem Internet verbunden, wenn der Computer ausgeschaltet ist. Aus diesem Grund sind Kabel- oder Hochgeschwindigkeitsverbindungen anfälliger für Spyware als Einwahlverbindungen.

Drahtlose Verbindungen bergen noch größere Sicherheitsrisiken. Drahtlose Internetsignale, die über Funkwellen übertragen werden, können mit einer Antenne oder einem anderen Abhörgerät aufgefangen werden. Mithilfe dieser Technologie können Stalker oder andere Unbefugte eine drahtlose Verbindung anzapfen und Spyware auf dem Computer eines Opfers installieren. Daher ist eine drahtlose Verbindung die unsicherste Art, sich mit dem Internet zu verbinden.

Ist Spyware legal?

Spyware-Programme sind in allen Bundesstaaten legal. Unternehmen dürfen sie legal einsetzen, um die Computernutzung ihrer Mitarbeiter zu überwachen, und Eltern dürfen sie nutzen, um die Online-Aktivitäten ihrer Kinder zu überwachen und sie vor Internet-Gefahren zu schützen. Je nach den jeweiligen Gesetzen gegen Stalking und dem Kontext der Nutzung kann die Verwendung von Spyware jedoch in vielen Fällen illegal sein. Viele Landesgesetze verbieten die Überwachung einer Person, wenn diese dadurch begründete Furcht um ihre Sicherheit empfindet. Nutzt beispielsweise ein gewalttätiger Ex-Mann ein legales Spyware-Programm, um alle E-Mails und Chat-Konversationen seiner Ex-Frau zu überwachen und ihr dadurch große Angst einzujagen, begeht er wahrscheinlich Stalking nach dem Gesetz seines Bundesstaates. Die Überwachung der Internetnutzung eines zwölfjährigen Kindes durch einen Elternteil fällt hingegen wahrscheinlich nicht unter den Tatbestand des Stalkings.

Spyware erkennen

Es kann schwierig sein, Spyware auf dem eigenen Computer zu erkennen. Am besten sucht man mit einem der zahlreichen Anti-Spyware-Programme, die kostenlos heruntergeladen oder gekauft werden können, um Spyware aufzuspüren und vom Computer zu entfernen. Viele dieser Programme erkennen zwar eine Vielzahl von Spyware-Arten, dennoch ist es wichtig zu wissen, dass kein Anti-Spyware-Programm alle Spyware-Programme identifizieren und entfernen kann. In einem Testbericht der besten Anti-Spyware-Programme des PC World Magazine (Ausgabe April 2005) entfernten nur zwei Programme mehr als 80 Prozent der Adware- und Spyware-Infektionen. Die

übrigen getesteten Programme schnitten deutlich schlechter ab. Wie Antivirenprogramme können auch Anti-Spyware-Programme schnell veralten, da täglich neue Spyware-Programme, viele davon mit Anti-Erkennungsmechanismen, auftauchen. Experten empfehlen daher, mindestens zwei Spyware-Erkennungsprogramme zu kaufen oder herunterzuladen, diese stets aktuell zu halten und regelmäßig zu verwenden. Wichtig ist auch, zu verstehen, dass es sich um einen schnell wachsenden Markt handelt und neue Entwicklungen im Bereich Spyware und Anti-Spyware häufig vorkommen.

Was tun, wenn Sie glauben, Spyware auf Ihrem System zu haben?

Als Erstes sollten Sie Ihren Computer nicht mehr für Aktivitäten nutzen, die Ihre Sicherheit oder Privatsphäre gefährden könnten. Wenn Sie E-Mails senden oder das Internet nutzen müssen, sollten Sie einen öffentlichen Computer verwenden, bis Sie sicher sind, dass Ihr Computer sicher und frei von Spyware ist. Die Entscheidung, ob Spyware gelöscht werden soll, ist komplex. Die automatische Entfernung erkannter Spyware bedeutet, Beweise für Überwachung und möglicherweise Stalking zu beseitigen. Zudem ist die Entfernung der Software unter Umständen nicht hilfreich, da der Stalker oder ein anderer unbefugter Nutzer bereits umfangreiche persönliche Daten erlangt haben könnte. Sobald er oder sie bemerkt, dass das Programm gelöscht wurde, könnte dies den Stalker dazu veranlassen, seine oder ihre Bemühungen zu intensivieren und die Sicherheit des Opfers zu gefährden. Die Sicherheit hat jedoch oberste Priorität, und Opfer, die den Missbrauch sensibler Daten befürchten, sollten die Software möglicherweise sofort löschen. Wer vermutet, durch Spyware gestalkt zu werden, sollte sich an eine örtliche Opferberatungsstelle und an die zuständige Ermittlungsstelle für Stalking, häusliche Gewalt oder Computerforensik der örtlichen Polizei wenden. Zwar verfügen nicht alle Polizeibehörden über solche spezialisierten Ressourcen, die meisten Landespolizeien jedoch schon.

Da wir in unserem privaten und beruflichen Leben immer stärker auf Computer angewiesen sind, werden wir anfälliger für den Missbrauch von Programmen wie Spyware. Die Strafverfolgungsbehörden werden immer besser darin, kriminelle Missbräuche zu erkennen und lernen, wie sie elektronische Beweismittel in Stalking- und anderen Strafverfahren sammeln und nutzen können. Immer häufiger beziehen Opferhilfsorganisationen die Computerüberwachung routinemäßig in ihre Sicherheitspläne ein. Für Stalking-Opfer und die Öffentlichkeit ist das Verständnis der Funktionsweise von Spyware und der Schutz davor die beste Verteidigung.

Weitere Informationen zu Spyware erhalten Sie beim Stalking Resource Center unter (202) 467-8700 oder www.ncvc.org/src oder beim Safety Net Project des National Network to End Domestic Violence Fund unter www.nnedvfund.org . Das Stalking Resource Center analysiert das Problem fortlaufend und freut sich über Ihre Meldungen zu Spyware-Fällen.

Anhang: So schützen Sie sich im Internet.

Alle Rechte vorbehalten. Copyright © 2005 National Center for Victims of Crime. Diese Informationen dürfen frei verbreitet werden, sofern die Verbreitung kostenlos erfolgt. von der Gebühr, in ihrer Gesamtheit und einschließlich dieses Urheberrechtshinweises.

Ein alarmierender Anstieg von GPS-gestützter Belästigung

Im Jahr 2003 wurde Paul Seidler aus Kenosha, Wisconsin, wegen Stalkings seiner Ex-Freundin zu neun Monaten Haft verurteilt. Seine Masche war die Nutzung eines neu verfügbaren Echtzeit-Ortungsdienstes. Dieser basierte auf einem GPS-Gerät, das er in ihrem Auto versteckt hatte und das ihm per SMS ihren Standort mitteilte, sodass er mehrmals täglich neben ihr anhalten konnte.

Verfolgt von Satelliten

Von John Voelcker

Ein alarmierender Anstieg von GPS-gestützter Belästigung

Als Albert Belle im Februar wegen Stalkings seiner Ex-Freundin verhaftet wurde, war es nicht die von ihm eingesetzte Technologie, die ihn in die Schlagzeilen brachte, sondern sein Ruhm als ehemaliger Baseballprofi der Major League [siehe Foto, „ Ball's Belle "]. Sollte er jedoch verurteilt werden, würde sich der fünfmalige All-Star-Outfielder in die wachsende Liste derer einreihen, die GPS-Geräte missbraucht haben, um ehemalige Partner zu verfolgen und zu quälen.

Laut Polizeibericht aus Scottsdale, Arizona, fiel Ende Januar ein Gegenstand vom Mercedes-Benz seiner Ex-Freundin, nachdem diese über eine Bodenwelle gefahren war. Als sie anhielt, um nachzusehen, was es war, fand sie eine kleine schwarze Box mit zwei daran befestigten Magneten und einem handyähnlichen Gerät darin. Sie gab gegenüber der Polizei an, Belle sei häufig zu ungewöhnlichen Zeiten und an seltsamen Orten aufgetaucht, und sie vermutete, er verfolge sie. Nachdem sie Telefongespräche aufgezeichnet hatte, in denen Belle sie offenbar bedrohte, wurde er festgenommen und wegen Stalkings unter Verwendung eines GPS-Geräts angeklagt.

Dieser Fall, nur einer von vielen, ist ein dramatisches Beispiel dafür, wie eine ansonsten harmlose Technologie mit vielen wunderbaren Anwendungsmöglichkeiten in den falschen Händen zu einer echten Bedrohung werden kann.

GPS, ursprünglich vom US-Verteidigungsministerium entwickelt, wird seit etwa zehn Jahren auch zivil genutzt. Eine der bekanntesten Anwendungen ist OnStar von General Motors, das Autofahrer zu ihrem Ziel leitet. Nachrüstversionen, die nur die Ortung ermöglichen, sind für unter 1000 US-Dollar erhältlich und können direkt an das 12-Volt-Bordnetz des Fahrzeugs angeschlossen werden.

Die in Systemen wie OnStar verwendeten mobilen GPS-Ortungsgeräte basieren auf einem streichholzschachtelgroßen Sensor, der Signale von Satelliten empfängt. Eine Verarbeitungslogik trianguliert die Signale, um den Standort des Geräts auf etwa zwei Meter genau zu bestimmen. Frühere Versionen solcher Nachrüstgeräte mussten aus dem Fahrzeug ausgebaut und an einen Computer angeschlossen werden, um die Daten herunterzuladen. Neuere Modelle hingegen verfügen über einen Mobilfunksender, der die Standortdaten an einen Server überträgt. Nutzer können das Fahrzeug über ständig aktualisierte Webseiten verfolgen oder sich die Standortdaten per SMS auf ihr Mobiltelefon senden lassen – angesichts der lückenhaften Gesetzeslage eine große Versuchung für Stalker, die ihren Ex-Partnern nachgehen wollen.

Die Regelungen für den Missbrauch dieser Technologien variieren in den USA stark von Bundesstaat zu Bundesstaat. Viele Staaten haben allgemeine Gesetze gegen Stalking oder

Belästigung, aber weitaus weniger befassen sich explizit mit GPS-Ortung, Mobiltelefonen, Internet-Spionagesoftware und anderen neueren Entwicklungen im Bereich der Verbrauchertechnologie.

Die erste dokumentierte Anklage wegen GPS-Stalkings fand im Oktober 2000 in Boulder, Colorado, statt. Robert Sullivan wurde wegen Belästigung verurteilt, weil er seine jugendlichen Söhne dazu gebracht hatte, in Ann Arbor, Michigan, ein von Bluewater Security vertriebenes Ortungssystem der Firma TravelEyes in den Oldsmobile seiner von ihm getrennt lebenden Ehefrau einzubauen. Er wurde zu drei Jahren Haft verurteilt, nachdem das Gericht entschieden hatte, dass der Begriff „überwacht“ im Stalking-Gesetz des Bundesstaates auch elektronische Überwachung umfasst. Obwohl seine Haftstrafe später reduziert wurde, wurde er wegen mehrfacher Bewährungsauflagenverstöße erneut verhaftet und inhaftiert.

Im Jahr 2003 wurde Paul Seidler aus Kenosha, Wisconsin, wegen Stalkings seiner Ex-Freundin zu neun Monaten Haft verurteilt. Seine Masche war die Nutzung eines neu verfügbaren Echtzeit-Ortungsdienstes. Dieser basierte auf einem GPS-Gerät, das er in ihrem Auto versteckt hatte und das ihm per SMS ihren Standort mitteilte, sodass er mehrmals täglich neben ihr anhalten konnte.

Belästigung und Stalking sind kein Spaß. Laut einer Abteilung der US-amerikanischen Zentren für Krankheitskontrolle und -prävention (CDC) ist häusliche Gewalt für zwei Millionen Verletzungen und fast 1300 Todesfälle bei US-amerikanischen Frauen ab 18 Jahren verantwortlich. (Cindy Southworth, Technologiedirektorin des National Network to End Domestic Violence in Washington, D.C., erklärt, dass keine verlässlichen Daten zur Anzahl der Stalking-Fälle vorliegen, da es kein einheitliches Meldesystem bei den Strafverfolgungsbehörden gibt.)

Wer vermutet, Opfer von GPS-Stalking zu sein, dem rät Southworth zu einem überraschend einfachen Rat: Vertrauen Sie zunächst Ihrem Bauchgefühl. Wenn jemand Ihre Fahrstrecken wiederholt erkennt, seien Sie misstrauisch. Zweitens: Sollten Sie befürchten, dass Ihr Fahrzeug geortet wird, wenden Sie sich an die örtliche Polizei oder einen Tankstellenleiter. Sowohl die Polizei als auch eine Werkstatt können Ihr Fahrzeug durchsuchen. Wird dabei ein verdächtiges Gerät gefunden, muss die Werkstatt es unberührt lassen, damit es als Beweismittel für die Polizei sichergestellt werden kann.

Southworth befürchtet, dass GPS-Stalking zunehmen wird, da Sensoren und Sender immer kleiner werden und weniger Strom verbrauchen. Da zudem alle neuen US-Mobiltelefone voraussichtlich GPS-Positionsdaten an das Notrufsystem 911 übermitteln werden, kann jedes Telefon geortet werden, sofern der Mobilfunkanbieter diesen Service anbietet. Es gibt kein nationales Gesetz, das vorschreibt, dass Mobilfunkkunden über die Standortverfolgung informiert werden müssen, und ihre Einwilligung zur Aufzeichnung dieser Daten ist nicht erforderlich.

Obwohl Telefongesellschaften höchstwahrscheinlich nicht absichtlich Ortungsdaten ohne die Zustimmung ihrer Kunden an Dritte weitergeben würden, berichtet Southworth von Fällen, in denen es jemandem gelang, Ortungsdaten eines getrennt lebenden Ehepartners zu erlangen. Um nicht selbst Opfer zu werden, wird empfohlen, sich bei seinem Mobilfunkanbieter zu erkundigen, ob die Ortung aktiviert ist und wohin die Ortungsdaten gesendet werden, und alle Passwörter für die Zugangsdaten zu ändern.

Wenn Sie sich gefährdet fühlen, denken Sie daran, dass Stalking oft eine tiefsitzende und hartnäckige Obsession ist. Der Baseballspieler Belle wurde am 17. Mai erneut verhaftet, weil er dieselbe Frau weiterhin belästigte. Berichten zufolge hatte er dutzende Anrufe getätigt, bei denen er sofort wieder auflegte, und belästigende Kommentare abgegeben, obwohl ihm gerichtlich jeglicher Kontakt untersagt war. Er bleibt nun bis zu seiner Verhandlung in Haft.

Belle muss auf die harte Tour lernen, dass sich das Blatt wendet: Das elektronische Überwachungsgerät, das er vor seiner zweiten Verhaftung am Knöchel tragen musste, nutzte ebenfalls GPS-Daten, um den Standort seines Trägers zu berechnen.

Eine Untersuchung des räuberischen Verhaltens im Cyberspace

In den letzten Jahren haben Regierungen, Strafverfolgungsbehörden und Medien einen Anstieg von Online-Belästigung festgestellt. Obwohl „Offline-Stalking“ bereits umfassend erforscht wurde, existiert bisher keine systematische Studie, die Cyberstalker klassifiziert. Ziel dieser Studie war es, durch Befragung von Opfern eine Klassifizierung von Cyberstalkern zu entwickeln. 24 Teilnehmer wurden interviewt und ihre Antworten anhand einer 76-Punkte umfassenden Checkliste zu Cyberstalking-Vorfällen dokumentiert. Anschließend wurde eine Typologie von Cyberstalkern erstellt.

Eine Untersuchung des räuberischen Verhaltens im Cyberspace: Auf dem Weg zu einer Typologie von Cyberstalkern von Leroy McFarlane und Paul Bocij

In den letzten Jahren haben Regierungen, Strafverfolgungsbehörden und Medien einen Anstieg von Online-Belästigung festgestellt. Obwohl „Offline-Stalking“ bereits umfassend erforscht wurde, existiert bisher keine systematische Studie, die Cyberstalker klassifiziert. Ziel dieser Studie war es, durch Befragung von Opfern eine Klassifizierung von Cyberstalkern zu entwickeln. 24 Teilnehmer wurden interviewt und ihre Antworten anhand einer 76-Punkte umfassenden Checkliste zu Cyberstalking-Vorfällen dokumentiert. Anschließend wurde eine Typologie von Cyberstalkern erstellt.

Inhalt

Einführung

Methodik

Ergebnisse

Diskussion

Die Auswirkungen von Stalking auf die Opfer sind gut dokumentiert. Monate- oder gar jahrelange, ununterbrochene Konfrontation mit unerwünschter Aufmerksamkeit und/oder Bedrohungen führt häufig dazu, dass Opfer ihre täglichen Gewohnheiten ändern und sogar psychische Traumata erleiden. Fremouw et al. (1997) fanden in ihrer Studie mit 600 Psychologiestudierenden heraus, dass einige Opfer bereit waren, ihre gewohnten Abläufe zu unterbrechen, um ihrem Stalker zu entkommen. Manche waren sogar bereit, Pfefferspray, ein Messer oder eine Schusswaffe bei sich zu tragen. Pathé und Mullen (1997) stellten in ihrer Untersuchung fest, dass über 75 Prozent der Opfer von Gefühlen der Ohnmacht berichteten und ein Viertel der Befragten zugab, ernsthaft an Selbstmord gedacht oder einen Selbstmordversuch unternommen zu haben. Eine Studie von Sheridan et al. (2001), in der 95 Stalking-Opfer in Großbritannien befragt wurden, ergab, dass 59 Prozent der Befragten angaben, Angst zu haben, und 44 Prozent ihr Verhalten infolge des Stalkings veränderten.

Trotz mehr als zehn Jahren Forschung zum Thema Stalking existiert noch immer keine eindeutige Definition dieses Phänomens. Meloy und Gothard definieren es als „ein abnormes oder langfristiges Muster von Bedrohung oder Belästigung gegenüber einer bestimmten Person“ [1]. Pathé und Mullen beschreiben es als „eine Konstellation von Verhaltensweisen, bei denen eine Person eine andere wiederholt unerwünschten Eingriffen und Kontaktaufnahmen aussetzt“ [2]. Zu diesen Verhaltensweisen gehören unter anderem „… das Verfolgen, Herumlungern in der Nähe, die Überwachung und die Kontaktaufnahme … [per] Brief, Telefon, E-Mail, Graffiti oder Notizen, die beispielsweise am Auto des Opfers angebracht werden“ [3]. Westrup schlug Stalking als „eine oder mehrere Verhaltensweisen aus einer Konstellation vor, die (a) sich wiederholt direkt gegen eine bestimmte Person (das Ziel) richten, (b) vom Ziel als unerwünscht und aufdringlich empfunden werden und (c) beim Ziel Angst oder Besorgnis auslösen“ [4].

Mit der Entwicklung der Informations- und Kommunikationstechnologie (IKT) beobachten wir eine neue Form der Belästigung – *Cyberstalking.* Um Stalking von Offline-Stalking zu unterscheiden, wird es im Folgenden als Offline-Stalking bezeichnet . Einige Autoren vertreten die Ansicht, Cyberstalking sei lediglich eine natürliche Erweiterung des Stalkings (Ogilvie, 2000; Petherick, 2001; Burgess und Baker, 2002). Bocij und McFarlane (2002) widersprechen dieser Ansicht jedoch. In ihrer Arbeit liefern sie eine ausführlichere Diskussion; kurz gesagt, führen sie aus, dass manche Definitionen von Stalkern fälschlicherweise psychische Probleme unterstellen, da ihr Verhalten gegenüber dem Opfer als „zwanghaft“ beschrieben wird. Sie beschreiben jedoch auch andere Motive für Cyberstalking, beispielsweise wenn Organisationen Einzelpersonen, Gruppen oder andere Organisationen aus Profitgründen oder zur Erlangung von Wettbewerbsvorteilen verfolgen. Sie stellen auch die Frage, wie sich die Tatsache erklären lässt, dass viele Cyberstalker ihre Opfer ausschließlich über das Internet belästigen, wenn Cyberstalking nichts anderes als eine Erweiterung des Offline-Stalkings ist. Beispielsweise erließ ein amerikanisches Gericht eine einstweilige Verfügung gegen Herrn Kevin Massey, der Robert Maynard, CEO von Internet America, und seine Frau und Mitbegründerin Teresa Maynard belästigte (D'Amico, 1997).

Monate- oder sogar jahrelange, ununterbrochene Konfrontation mit unerwünschter Aufmerksamkeit und/oder Bedrohungen führt oft dazu, dass die Opfer ihre täglichen Gewohnheiten ändern und sogar psychische Traumata erleiden.

Die Autoren führen außerdem an, dass in allen Klassifizierungen zum Offline-Stalking (z. B. Zona et al., 1993; Mullen et al., 1999; Sheridan et al. [5], 2001) viele Täter ihre Obsession aufgrund des Zeit- und Energieaufwands für die Überwachung ihres Ziels dazu neigen, sich jeweils auf ein Opfer zu konzentrieren. Diese Typologien (ebenso wie andere Offline-Klassifizierungen) erklären jedoch nicht die von Bocij et al. (in Vorbereitung) vorgestellte Fallstudie, in der der Cyberstalker mehrere Opfer online belästigte. Sollte die Ansicht, dass Cyberstalking eine natürliche Erweiterung des Stalkings darstellt, aufrechterhalten werden, müssen diese (und weitere im Artikel angeführte) Punkte berücksichtigt werden.

Zur Erklärung des Phänomens Cyberstalking wurden verschiedene Definitionen vorgeschlagen. Petherick (2001) erklärte, dass Cyberstalking „... eine Erweiterung des physischen Stalkings darstellt, bei dem elektronische Medien wie das Internet genutzt werden, um andere unaufgefordert zu verfolgen, zu belästigen oder zu kontaktieren.“ Deirmenjian (1999) definierte Cyberstalking als „... Belästigung im Internet unter Verwendung verschiedener Übertragungswege wie E-Mail, Chatrooms, Newsgroups, Mailboxing-Dienste und das World Wide Web.“

Bocij und McFarlane (2002) haben versucht, eine umfassendere Definition vorzulegen:

> „Belästigung bezeichnet Verhaltensweisen, bei denen eine Einzelperson, eine Gruppe von Personen oder eine Organisation Informationstechnologie nutzt, um eine oder mehrere Personen zu belästigen. Zu diesen Verhaltensweisen gehören

> unter anderem die Übermittlung von Drohungen und falschen Anschuldigungen, Identitätsdiebstahl, Datendiebstahl, Beschädigung von Daten oder Geräten, Computerüberwachung und die Anbahnung sexueller Kontakte mit Minderjährigen. Belästigung wird definiert als ein Vorgehen, das nach Einschätzung einer vernünftigen Person, die über dieselben Informationen verfügt, bei einer anderen vernünftigen Person seelisches Leid verursacht.“

Der dramatische Anstieg von Cyberstalking lässt sich nicht auf offizielle Kriminalitätsstatistiken zurückführen, sondern auf die Aufmerksamkeit der Medien, die andere Institutionen zum Handeln veranlasst hat. Erstens war die US-Regierung so besorgt über die Situation des Cyberstalkings, dass Vizepräsident Al Gore 1999 den Justizminister mit einem Bericht in Auftrag gab, der Empfehlungen zum Schutz aller Bürger enthielt (National Institute of Justice, 1999). Zweitens nehmen Strafverfolgungsbehörden diese Beschwerden inzwischen ernster. In Großbritannien hat der National Criminal Intelligence Service (NCIS) seine Operationen ausgeweitet, um Fälle von Cyberstalking zu untersuchen. In den USA hat das FBI immer mehr Fälle an die Staatsanwaltschaft zur weiteren Bearbeitung weitergeleitet. Schließlich haben auch mehrere Opferhilfsorganisationen den Anstieg von Cyberstalking festgestellt. Mitarbeiter des National Center for Victims of Crime in den USA, die zahlreiche Anrufe zu verschiedenen Straftaten – von Diebstahl bis Mord – erhalten, berichten von einem starken Anstieg der Fälle von Cyberstalking (Techtv, 2001). Im Jahr 2000 berichtete Working to Halt Online Abuse (WHOA), eine in den Vereinigten Staaten ansässige Organisation für Online-Sicherheit, dass sie durchschnittlich 100 Opfermeldungen pro Woche erhielt.

Um Informationen über die Anzahl von Cyberstalking-Fällen zu gewinnen, erhob WHOA demografische Daten von Betroffenen, die ihre Fälle gemeldet hatten. Der Durchschnitt der Zahlen von 2000 und 2001 ergab, dass 14,45 Prozent der Männer und 83,58 Prozent der Frauen online belästigt wurden (1,97 Prozent der Befragten machten keine Angaben zu ihrem Geschlecht). Bezüglich des Alters der Betroffenen waren 30,54 Prozent der Befragten zwischen 18 und 30 Jahre alt, 16,58 Prozent zwischen 31 und 40 und 6,90 Prozent gaben an, 41 Jahre und älter zu sein (45,98 Prozent machten keine Angabe zu ihrem Alter). Die überwiegende Mehrheit der Betroffenen waren Weiße (57,47 Prozent). Die nächstgrößte ethnische Gruppe, die Cyberstalking-Fälle meldete, waren Asiaten (1,97 Prozent). Afroamerikanische Opfer machten 0,82 Prozent aus, hispanische 1,81 Prozent, indigene 1,15 Prozent und sonstige 0,82 Prozent (WHOA, 2002). Die hier erhobenen Daten sind nicht repräsentativ, geben aber Einblick in ein wenig erforschtes Phänomen. Es besteht ein dringender Bedarf an einer formellen Untersuchung der jährlichen Anzahl von Cyberstalking-Fällen.

Es wurden bereits einige formale Studien zum Thema Cyberstalking durchgeführt. Spitzberg und Hoobler (2002) befragten 235 Studierende zu ihren Erfahrungen mit Cyberstalking und stellten fest, dass 59 Prozent der Befragten angaben, Opfer von Cyberstalking geworden zu sein. Davon fühlten sich 19,6 Prozent bedroht oder fürchteten um ihre persönliche Sicherheit. Burgess und Baker (2002) untersuchten Offline- und Online-Stalking mit 656 Teilnehmenden einer Universität an der Ostküste der USA und fanden heraus, dass 11 Prozent belästigt worden waren. Die Mehrheit der Betroffenen war weiblich (61 Prozent), und das Alter reichte von 17 bis 42 Jahren, wobei 55 Prozent 20 Jahre oder jünger waren.

Es wurden verschiedene Typologien zum Thema Stalking vorgeschlagen. Zona et al. (1993) erstellten die erste Analyse von strafrechtlichem Stalking anhand von 74 Fällen, die von der Threat Management Unit des Los Angeles Police Department untersucht wurden. In ihrer Klassifizierung orientierten sie sich eng am Diagnostic and Statistical Manual of Mental Disorders (DSM-5) und unterschieden drei Arten von Stalkern: Erotomaniker, Liebesbesessene und einfache Obsessionen. *Erotomaniker* sind wahnhaft davon überzeugt, dass das Ziel ihrer Begierde, meist eine Person von höherem Status, in den Stalker verliebt ist. Fälle von *Liebesbesessenheit* zeichnen sich dadurch aus, dass zwischen dem Stalker und dem Opfer (meist Prominente) keine Beziehung besteht, der Stalker aber eine fanatische Liebe zu der Person hegt. Diese Stalker leiden häufig an Schizophrenie, einer bipolaren Störung oder einer anderen psychischen Erkrankung. Die letzte Gruppe bilden die *einfachen Obsessionen,* bei denen der Stalker in der Regel ein Ex-Partner des Opfers ist und möglicherweise die Beziehung wiederbeleben möchte oder das Opfer aus Rache belästigt.

Harmon et al. (1995) entwickelten ihre eigene Typologie, nachdem sie die Fallakten von Tätern ausgewertet hatten, die an die forensisch-psychiatrische Klinik des New Yorker Straf- und Obersten Gerichtshofs überwiesen worden waren. Sie charakterisierten Stalker anhand zweier Kriterien: der Art der Bindung zwischen Opfer und Stalker (klassifiziert als liebevoll/verliebt oder verfolgend/wütend) und der Art der vorherigen Beziehung zwischen Stalker und Opfer (d. h. persönlich, beruflich, Beschäftigung, Medien, Bekanntschaft, keine oder unbekannt). Es wurde festgestellt, dass *liebevolle/verliebte* Belästiger häufig erotomanische Züge aufwiesen und dass die Mehrheit der Stalker von Ex-Partnern narzisstische und paranoide Persönlichkeitsmerkmale besaß. *Verfolgende/wütende* Belästiger stalkten nicht nur Einzelpersonen, sondern auch große Institutionen, die ihnen (tatsächlich oder vermeintlich) Unrecht getan hatten (Mullen et al., 2000).

Kienlen et al. (1997) untersuchten die Akten von 25 Personen, die wegen Stalking-Delikten angeklagt waren. Diese Personen wurden zu diesem Zeitpunkt im Auftrag der Gerichte psychiatrisch begutachtet. Die Autoren schlugen eine Klassifizierung vor, die Stalker in *psychotische* (mit Symptomen wie Schizophrenie, wahnhafter Störung mit erotomanischen Zügen und bipolarer Störung) und *nicht-psychotische* (mit Störungen wie affektiven Störungen, Alkohol- und Drogenmissbrauch und Persönlichkeitsstörungen) unterteilte.

Wright et al. (1996) entwickelten eine weitere Klassifizierung. Ihr System basierte auf Tatort- und allgemeinen forensischen Befunden, Stalking-Fällen, Erfahrungsberichten, Zeitungsberichten über Stalking sowie Interviews mit Stalking-Opfern. Ihre Kategorisierung bezog sich auf Folgendes:

- Art der Beziehung zwischen Opfer und Stalker *(häuslich* oder *nichthäuslich);*
- der Inhalt der Mitteilungen *(nicht wahnhaft* oder *wahnhaft);*
- das Risiko für das Opfer in Bezug auf Aggression *(niedrig, mittel, hoch);*
- das Motiv des Stalkers *(Verliebtheit, Besitzgier, Wut/Rache, Sonstiges);* und
- Der Ausgang des Verfahrens für den Stalker *(juristisch, Suizid, psychiatrisch, Sonstiges).*

Mullen et al. (1999) entwickelten eine mehrachsige Typologie, indem sie verurteilte Stalker in einer australischen psychiatrischen Klinik untersuchten. Die Achsen umfassten die Untersuchung der Hauptmotivation der Stalker und des Kontextes, in dem das Stalking stattfand, Informationen über die Art der vorherigen Beziehung zum Opfer sowie schließlich eine psychiatrische Diagnose. Sie

klassifizierten fünf Stalker-Typen:

- Der *abgewiesene Stalker* hatte eine intime Beziehung zum Opfer (wobei es sich gelegentlich auch um ein Familienmitglied oder einen engen Freund handeln kann) und empfindet die Beendigung dieser Beziehung als inakzeptabel. Sein Verhalten ist von einer Mischung aus Rache und dem Wunsch nach Versöhnung geprägt.
- *Menschen, die nach Nähe suchen,* versuchen, eine Beziehung zu einer Person aufzubauen, die ihre Wünsche geweckt hat und von der sie fälschlicherweise annehmen, dass sie diese Zuneigung erwidert.
- *Unfähige Verehrer* versuchen zwar, Beziehungen aufzubauen, halten sich aber nicht an die gesellschaftlichen Regeln der Partnersuche. Sie sind meist intellektuell beschränkt und/oder sozial inkompetent.
- *Verbitterte Stalker* belästigen ihre Opfer mit der gezielten Absicht, Angst und Schrecken zu erzeugen, aus dem Wunsch nach Vergeltung für eine tatsächliche oder vermeintliche Verletzung oder Demütigung heraus.
- *Stalker mit räuberischen Absichten* , die zum Zweck der Informationsbeschaffung oder zur Fantasievorstellung im Vorfeld eines sexuellen Übergriffs stalken.

Bislang liegen keine Studien zur Klassifizierung von Cyberstalkern vor [6]. Petherick (2001 verwendete lediglich die von Zona et al. (1993) entwickelte Typologie für Offline-Stalker und wandte sie auf Cyberstalking an. Die vorliegende Studie untersucht, ob die diskutierten Typologien für Offline-Stalking auch auf Cyberstalking anwendbar sind.

Diese qualitative Studie nutzte einen halbstrukturierten Fragebogen. Der verwendete Fragebogen war eine modifizierte Version der Stalking Incident Checklist von Wright et al. (1996). Diese modifizierte Version wurde erweitert, um Aspekte der Informations- und Kommunikationstechnologie (IKT) zu integrieren. Die ursprüngliche Stalking Incident Checklist ist ein fünfteiliger, 46 Items umfassender Interviewfragebogen, der zur Erstellung einer Stalker-Typologie entwickelt wurde. Er basiert auf Forschungsergebnissen zu Viktimologie, Tatortbefunden, Tatortindikatoren, Ermittlungsaspekten, Empfehlungen für Durchsuchungsbefehle, gängigen forensischen Befunden und Interviews mit Stalking-Opfern (Wright et al., 1996). Für die Zwecke dieser Studie wurde Cyberstalking analog zum Protection from Harassment Act (1997) in England und Wales definiert, d. h. als zwei oder mehr Verhaltensweisen, die zur Belästigung einer anderen Person führen.

Zusätzlich wurde das Computerprogramm *Copernic* eingesetzt, um im Internet nach 50 Fällen von Cyberstalking zu suchen. Diese Fälle wurden analysiert, und die Methoden der Belästigung über Informations- und Kommunikationstechnologien (IKT) dienten als Grundlage für die Überarbeitung der Checkliste. Die finale Checkliste für Cyberstalking-Vorfälle enthielt 30 weitere Punkte und umfasste somit einen 76-teiligen Interviewfragebogen. Der fünfte Abschnitt der ursprünglichen Stalking-Checkliste wurde nicht verwendet, da befürchtet wurde, dass dieser die Ergebnisse zugunsten der ursprünglichen Studie verfälschen würde. In jedem Abschnitt wurde Platz für zusätzliche Informationen der Teilnehmenden vorgesehen.

Die Checkliste für Cyberstalking-Vorfälle besteht aus vier Hauptabschnitten. Der erste Abschnitt erfasst die Hintergrundinformationen des Opfers und des Täters. Zu den hier zu erhebenden Daten gehören die Initialen der befragten Person (um die Vertraulichkeit zu gewährleisten), Alter, Geschlecht, ethnische Zugehörigkeit, Erwerbsstatus, Familienstand, Wohnort, höchster Bildungsabschluss, lokale/nationale Bekanntheit sowie eine *subjektive* Einschätzung der Computerkenntnisse von Opfer und Täter (1 = gering, 2 = eher gering, 3 = mittel, 4 = eher hoch, 5 = hoch). Das Opfer wurde außerdem gebeten, Hintergrundinformationen zum Cyberstalker anzugeben, z. B. zu früheren Übergriffen, psychiatrischen Erkrankungen, Vorstrafen und früheren Opfererfahrungen – jedoch nur, sofern diese Informationen bekannt waren.

Im zweiten Abschnitt wurden die Anzahl der Cyberstalking-Vorfälle und die Dauer der Online-Belästigung untersucht. Außerdem wurden die ersten und letzten Kontaktwege über Informations- und Kommunikationstechnologien (IKT) erfasst: E-Mail, Netzwerkzugang, Webseiten/Gästebücher, persönliche Chatdienste (z. B. ICQ, MSN Messenger), Chatrooms, Webdiskussionsgruppen (z. B. Usenet, Foren), Online-Dating-Portale und Internetspiele. Falls Offline-Stalking stattfand, wurde das Opfer gemäß der Checkliste für Stalking-Vorfälle nach dem ersten und letzten Vorfall befragt. Zu den erfassten Verhaltensweisen von Offline-Stalking zählten der Arbeitsplatz, der Wohnort, das Verhalten im Freien, Anzeichen von Diebstahl, Anzeichen von Überwachung, unbefugtes Betreten der Wohnung des Opfers durch den Täter und das Verfolgen des Opfers mit dem Auto. Sowohl im IKT- als auch im Offline-Teil dieses Abschnitts wurde der Teilnehmer gefragt, ob der Cyberstalker versucht hatte, ihn gegenüber anderen zu diskreditieren oder über Dritte weitere Informationen über ihn zu erlangen. Die dritte Studie untersuchte den Grad der Aggression im ersten und letzten Fall von Cyberstalking und Offline-Stalking.

Abschnitt vier (ähnlich der Checkliste für Stalking-Vorfälle) erfasste die Art des Kontakts (z. B. per IKT, Telefon, persönlich oder schriftlich). Auch Stil und Inhalt der Kommunikation bei Cyberstalking- und Offline-Stalking-Vorfällen wurden dokumentiert. Dazu zählten: Computerviren, versuchte Einschleusung/Einschleusung von Trojanern [7], Spamming [8], Mailbombing [9], Identitätsdiebstahl [10], Verwendung von Multimedia-Inhalten und/oder Fotos, Videos und Tonaufnahmen, plötzliches Auflegen/plötzliche Unterbrechungen, Zurschaustellung detaillierter Kenntnisse über das/die Opfer, Liebesbekundungen und/oder Heiratsdrohungen, Geschenke, sexuelle Kommentare, Drohungen, Opfer und/oder andere zu verletzen, das Tragen einer Waffe, die Androhung des Waffengebrauchs, der Waffengebrauch, wirre Gespräche/Schriften, bizarre, unklare oder zusammenhanglose Kommentare sowie andere, nicht in der Checkliste aufgeführte Verhaltensweisen.

Die Checkliste für Cyberstalking-Vorfälle wurde forensischen und Forschungspsychologen sowie einem IT-Berater zur Begutachtung vorgelegt. Auf Grundlage der Kommentare der Gutachter wurde die Checkliste überarbeitet. Für die Studie wurde eine Stichprobe von 24 Teilnehmenden herangezogen, die über Online- und Offline-Opferhilfegruppen Kontakt zum Autor aufgenommen hatten. Alle Befragten erklärten sich ohne Gegenleistung zur Teilnahme bereit. Die Teilnehmenden stammten aus verschiedenen Ländern, darunter Großbritannien, die USA, Kanada und Neuseeland. 22 der Teilnehmenden waren weiblich, zwei männlich.

Die Teilnehmer wurden anhand der 76-Punkte umfassenden Cyberstalking-Checkliste befragt. Diese erfasste die von den Teilnehmern erlebten Belästigungen und lieferte demografische Informationen zum Täter. Die Teilnehmer konnten nach jedem Abschnitt zusätzliche Angaben machen. Da einige Teilnehmer in verschiedenen Ländern lebten und die unterschiedlichen Zeitzonen zu einem für sie passenden Zeitpunkt vereinbart werden mussten, wurden die Interviews ausschließlich vom Erstautor durchgeführt. Die Interviews fanden persönlich, telefonisch oder per Chat statt.

Die Datenanalyse erfolgte nach Abschluss aller Fragebögen. Die beiden Forscher trafen sich regelmäßig, um die Ergebnisse zu besprechen und festgestellte Muster zu überprüfen. Nach Abschluss der Interviews führten die Forscher weitere Treffen durch, um die Themen zusammenzufassen und die Fachliteratur nach bestätigenden Informationen zu durchsuchen.

Analyse

Die in dieser Studie angewandten Schritte der Datenanalyse umfassten die Datenreduktion, bei der die Daten ausgewählt, fokussiert und präzisiert wurden, um Kodierkategorien zu entwickeln. Die Kodierkategorien wurden im Zuge der Datenanalyse durch die Forschenden verfeinert und definiert. Der zweite Analyseschritt war die Datenvisualisierung. Computerdateien und Datentabellen dienten der Organisation der Daten, der Identifizierung von Lücken und der Erkennung erster Zusammenhänge innerhalb der Kategorien.

Die Schlussfolgerung und Verifizierung bildeten den dritten Schritt der Datenanalyse. Feldnotizen und Memos, die vorläufige Interpretationen der Daten erarbeiteten, trugen zur Schlussfolgerung bei. Während der Datenerhebung und -analyse wurde ein Experte für Informations- und Kommunikationstechnologie (IKT) und qualitative Forschungsmethoden hinzugezogen. Der Prüfpfad umfasste den Forschungsantrag mit seinen Zielsetzungen, die Rohdaten (Fragebögen und Computerdateien, Kodierungskategorien mit Definitionen, Datendarstellungstabellen und Feldnotizen) sowie die vom Forscher während der Datenerhebung und -analyse geführten Memos.

Die zusammenfassenden Statistiken werden in drei Tabellen dargestellt. Tabelle 1 untersucht die intrinsischen Merkmale von Opfern und Tätern, während Tabelle 2 die extrinsischen Merkmale von Opfern und Tätern untersucht. Tabelle 3 veranschaulicht die Beziehungsfaktoren zwischen Opfern und Tätern.

Tabelle 1: Intrinsische Merkmale von Opfern und Cyberstalkern.

Themen (N=24)	Opferdaten	Täterdaten
Durchschnittsalter	32,0	41,0
Reichweite	Mindestens: 14; Maximal: 53	Mindestens 18; Maximal 67
Prozentuales Alter		
<17 [11]	4.2	—
18-30	45,8	23.1
31-40	25.0	34,6
41+	25.0	42.3
Prozentuales Rennen		
Weiß	100,0	100,0
Prozentuale Geschlechterverteilung		
Weiblich	91,0	15.4
Männlich	9.0	84,6

Dauer und Art des Cyberstalking-Verhaltens

Die Dauer des Cyberstalkings reichte von einem Tag bis zu fünf Jahren, mit einer durchschnittlichen Dauer von 11,5 Monaten. In einem Fall, der einen Tag andauerte, kam es zu Offline-Stalking mit mehrtägigen Telefonanrufen und körperlichen Bedrohungen des Opfers. Abgesehen von diesem Fall dauerte der kürzeste Fall von Cyberstalking 17 Tage.

Die häufigste Methode der ersten Kontaktaufnahme durch Cyberstalker über Informations- und Kommunikationstechnologien (IKT) war E-Mail (10 Fälle), gefolgt vom Netzwerkzugang am Arbeitsplatz (sechs Fälle) und Webdiskussionsforen wie Usenet oder Bulletin Boards (sechs Fälle). Weitere Kontaktmethoden waren elektronische Dating-Portale und Chatrooms (jeweils ein Fall). In 13 Fällen von Online-Belästigung gab es auch Fälle von Offline-Stalking; sechs Opfer wurden zu Hause, drei an ihrem Arbeitsplatz, drei an öffentlich zugänglichen Orten und ein Opfer berichtete von Überwachung (z. B. durch Kameras, Abhörgeräte usw.).

Bedrohungen und Gewalt

Elf der Cyberstalker bedrohten das Opfer, vier von ihnen bedrohten auch Dritte. Insgesamt bedrohten acht Cyberstalker nur das Opfer, einer nur die Dritten und drei beide Gruppen. Es kam zu keinen körperlichen Angriffen auf die Opfer, jedoch wurde das Eigentum zweier Opfer – ihre Autos – beschädigt.

Tabelle 2: Äußere Merkmale von Opfern und Tätern.

Themen	Opferdaten	Täterdaten
Prozentualer Familienstand		
Einzel	58,3	52.3
Geschieden	8.3	13.0
Getrennt	4.2	4.3
Verheiratet	29.2	21,7
Unbekannt	—	8,7
Prozentuale Computerkenntnisse		
Niedrig	12,5	—
Ziemlich niedrig	20.8	4,5
Medium	29.2	41,0
Ziemlich hoch	20.8	27.3
Hoch	16.7	22,7
Unsicher	—	4,5
(Hinweis: Dies ist eine subjektive Bewertung.)		
Prozentuale Belegungsquote		
Professioneller Beitrag	37,5	50,0
Büroangestellte	20.8	4.6
Unqualifizierter Handwerker	4.2	4.6
Student	20.8	8.3
Im Ruhestand		4.6
Arbeitslos	16.7	18.2

Unbekannt		9,7
Prozentuale Bildung		
Abschlüsse	25.0	27.3
A-Level/Hochschule	50,0	22,7
GCSEs/O-Levels/Gymnasium	20.8	9.1
Keine formalen Qualifikationen	4.2	4,5
Unbekannt		36,4

Identitätsdiebstahl

In acht Fällen gab sich der Täter online als das Opfer aus. Viermal wurde die Identität des Opfers in E-Mails an Familie/Freunde/Usenet-Gruppen missbraucht, dreimal wurde die Identität auf elektronischen Dating-Plattformen oder in Chatrooms nachgeahmt, und im letzten Fall wurden die Kreditkartendaten des Opfers für Online-Einkäufe verwendet und dessen Identität in Usenet-Gruppen imitiert.

Vorgeschichte mit Opfererfahrungen, aggressivem Verhalten, psychiatrischen Einweisungen und strafrechtlichen Verurteilungen

Die Opfer berichteten, dass acht der Cyberstalker bereits zuvor andere Opfer über Informations- und Kommunikationstechnologien (IKT) belästigt hatten und vier der Cyberstalker in der Vergangenheit wegen Körperverletzung vorbestraft waren (d. h. ohne Strafverfolgung). Nur ein Täter war in einer psychiatrischen Klinik untergebracht. Die Opfer gaben außerdem an, dass sechs der Cyberstalker Vorstrafen hatten: drei wegen Eigentumsdelikten, eine wegen Verstoßes gegen Bewährungsauflagen (ursprünglich wegen Offline-Stalking), eine wegen unerlaubten Waffenbesitzes und eine wegen Körperverletzung.

Tabelle 3: Beziehungen zwischen Opfern und Tätern.

Prozentuales Verhältnis	
Ex-Partner	12.0

Arbeitskontakte/Kollegen	12.0
Bekannte	16.7
Professionelles Netzwerk (z. B. Gesundheitsdienstleister, Anwälte, Lehrer)	4.0
Ich habe mich vor Kurzem/vor sehr kurzer Zeit kennengelernt über Informations- und Kommunikationstechnologie (IKT)	33.3
Völlig fremder Mensch	22.0
Stalking-Verhalten	
Stalking zwischen Männchen und Weibchen	75,0
Stalking durch gleichgeschlechtliche Beziehungen	25.0
	(50 Prozent männlich-männlich; 50 Prozent weiblich-weiblich)

Die Motivation des Cyberstalkers

Aus den Daten ließen sich vier Hauptthemen im Zusammenhang mit der Beziehung beim Cyberstalking ableiten: die „rachsüchtigen“, die „überlegten“, die „kollektiven“ und die „intimen“ Cyberstalker.

Rachsüchtiger Cyberstalker

Diese Gruppe verdankt ihren Namen der Brutalität, mit der sie ihre Opfer verfolgt. Sie bedrohten ihre Opfer häufiger als jede andere Gruppe und stalkten sie in den meisten Fällen auch offline. Ein Drittel der Täter war bereits vorbestraft, und zwei Drittel hatten schon zuvor andere Opfer gemacht.

In der Hälfte der Fälle gaben die Betroffenen an, dass die Belästigung mit einer belanglosen Diskussion begann, die völlig eskalierte. In einem Drittel der Fälle gab es keinen erkennbaren Grund, und die übrigen Opfer berichteten von einem heftigen Streit zwischen beiden Parteien. Die Opfer schätzten die Computerkenntnisse der Cyberstalker als mittel bis hoch ein. Der rachsüchtige Cyberstalker nutzte mehr IKT-Methoden zur Belästigung seines Opfers (z. B. Spam, Mailbombing und Identitätsdiebstahl) als jede andere Gruppe. Er war auch die einzige Gruppe, die Trojaner einsetzte, um sich Zugang zu den Rechnern ihrer Opfer zu verschaffen und/oder diese mit Viren zu infizieren. Drei Viertel der Opfer gaben zudem an, verstörende Nachrichten von dieser Gruppe erhalten zu haben, beispielsweise bizarre Kommentare, wirre Gespräche, unklare und zusammenhanglose Äußerungen sowie bedrohliche Multimedia-Bilder und/oder -Töne (z. B. Totenköpfe, Leichenbilder, Schreie usw.). Diese Nachrichten deuten möglicherweise auf schwere psychische Probleme hin.

Zusammengesetzter Cyberstalker

Der sogenannte Cyberstalker wird so genannt, weil man annimmt, dass seine Handlungen darauf abzielen, seine Opfer ständig zu belästigen und zu quälen. Diese Cyberstalker versuchen nicht, eine Beziehung zu ihren Opfern aufzubauen, sondern wollen ihnen Leid zufügen. Solche Täter sprechen in der Regel Drohungen aus.

Insgesamt schätzten die Teilnehmer die Computerkenntnisse dieser Cyberstalker als mittel bis hoch ein. Nur einer der Cyberstalker dieser Gruppe war vorbestraft, und nur einer war bereits Opfer eines Verbrechens geworden. Keiner der Täter hatte eine psychiatrische Vorgeschichte; dennoch verfolgten drei von ihnen ihre Opfer auch auf herkömmliche Weise.

Intimer Cyberstalker

Diese Gruppe versuchte, die Gefühle und/oder die Aufmerksamkeit ihrer Opfer zu gewinnen. Die Teilnehmer schätzten die Computerkenntnisse dieser Cyberstalker im Vergleich zur vorherigen Gruppe als deutlich breiter gefächert ein – von eher gering bis hoch. Sie nutzten E-Mail, Online-Diskussionsforen und Online-Dating-Portale. Zudem verfügten sie über detaillierte Kenntnisse ihrer Opfer.

Eine genauere Untersuchung des Verhaltens dieser Gruppe ergab, dass sie sich in zwei Untergruppen einteilen lässt: *Ex* -Partner oder ehemalige Bekannte des Cyberstalkers, die sich als „Ex-Partner“ bezeichneten, und *Personen* , die auf der Suche nach einer intimen Beziehung waren. *Die Ex-Partner* zeigten ein breites Spektrum an Verhaltensweisen, von Nachrichten zur Wiederherstellung der Beziehung bis hin zu Drohungen gegen ihren ehemaligen Partner oder Freund. Zur Verdeutlichung gaben diese Opfer an, dass die Belästigung *online begann* . In einigen Fällen gaben sich die Ex-Partner online als ihre ehemaligen Partner oder Bekannten aus und agierten dabei beispielsweise in Chatrooms als Ex-Partner oder nutzten Kreditkartentransaktionen. Interessanterweise gab es keine Fälle von Offline-Stalking im Anschluss an Cyberstalking.

Die *Verliebten* strebten allesamt eine engere Beziehung zum Opfer an. Ihre Kommunikation war deutlich intimer als die der vorherigen Untergruppe, doch nach einer Zurückweisung fielen ihre Nachrichten bedrohlicher aus. In einem Fall stalkte ein Verliebter sein Opfer sogar offline. Zusammenfassend lässt sich sagen, dass die Untergruppen insgesamt den von Mullen et al. (1999) definierten Kategorien des abgewiesenen Stalkers, des Nähesuchenden und des inkompetenten Verehrers sehr ähnlich sind.

Kollektive Cyberstalker

Diese letzte Gruppe zeichnet sich dadurch aus, dass zwei oder mehr Personen ihre Opfer über Informations- und Kommunikationstechnologien (IKT) verfolgen. Die Computerkenntnisse der Personen in dieser Untergruppe reichten von recht hoch bis sehr hoch. Die Täter sprachen zahlreiche Drohungen aus und nutzten Spamming, Mailbombing, Identitätsdiebstahl und einschüchternde Multimedia-Inhalte, um ihre Opfer zu belästigen. Diese Gruppe versuchte außerdem, Informationen über ihr Ziel zu erlangen.

Innerhalb dieser Gruppe wurde eine weitere Untergruppe festgestellt. Die Studie dokumentierte Fälle von Cyberstalking, die als *Unternehmens-Cyberstalking bezeichnet werden können.* Typischerweise wird eine Organisation für ihre Geschäftspraktiken kritisiert und fühlt sich dadurch angegriffen. Belästigungen werden eingesetzt, um das Opfer zu diskreditieren und/oder zum Schweigen zu bringen. In dieser Gruppe wird Identitätsdiebstahl genutzt, um sich als andere Personen auszugeben und die Opfer zu diskreditieren. *Auch Gruppen-Cyberstalking* wurde in der Studie beobachtet. Hierbei glauben zwei oder mehr Täter, ihnen sei *Unrecht geschehen,* und wollen *das Opfer bestrafen* . Es ist nicht auszuschließen, dass diese Gruppe von Cyberstalkern versucht, weitere Personen zu rekrutieren, um das Opfer auch offline zu belästigen. In einem Fall gelang es einer Tätergruppe sogar, andere Täter zu rekrutieren, indem sie ihnen die Adresse des Opfers mitteilte.

Diese Studie untersuchte die Antworten der Opfer mithilfe eines Fragebogens und versuchte, eine Typologie des Cyberstalkings zu entwickeln. In der Einleitung wurde die Frage aufgeworfen, ob die Studie eine Klassifizierung von Cyberstalkern liefern würde, die mit den zuvor diskutierten Kategorisierungen des Offline-Stalkings übereinstimmt. Die Ergebnisse zeigen, dass dies nicht der Fall ist. Es wurden vier Typen von Cyberstalkern identifiziert: der gelassene, der intime, der kollektive und der rachsüchtige. Die Studie mag aufgrund ihrer geringen Stichprobengröße kritisiert werden; unseres Wissens ist sie jedoch die erste Studie zum Thema Cyberstalking, die versucht, eine Klassifizierung dieser Täter zu formulieren.

Rachsüchtige Cyberstalker geben besondere Anlass zur Sorge, da die Opfer berichteten, dass es in manchen Fällen keinen Grund für die Belästigungen gab und dass diese Art von Cyberstalkern sie auch offline weiter verfolgten. Diese Sorge wird dadurch verstärkt, dass die Opfer vermuteten, dass diese Cyberstalker psychische Probleme hätten; so waren beispielsweise E-Mails und Anhänge besonders aggressiv und sadistisch. Der Umgang dieser Gruppe mit Informations- und Kommunikationstechnologien (IKT) erwies sich als ausgefeilt. Viren wurden eingesetzt, um Rechner zu infizieren, Identitätsdiebstahl war weit verbreitet, und sogar Trojaner kamen zum Einsatz (was in der Regel relativ gute Computerkenntnisse voraussetzt). Es wird vermutet, dass diese Cyberstalker mittelschwere bis schwere psychische Probleme haben könnten, beispielsweise eine diagnostizierbare Persönlichkeitsstörung.

Cyberstalker ist schwierig *Ein Vergleich mit einem gelassenen* – in der Literatur zum Offline-Stalking findet sich schlichtweg nichts Vergleichbares. Die zentrale Frage ist: Warum begeht jemand Cyberstalking? Eine Möglichkeit wäre, dass die Anonymität des Internets zu einer ungehemmten Kommunikation und Handlungsweise führt. Warum greifen sie nicht zu drastischeren Methoden wie Trojanern oder Viren? Möglicherweise empfinden sie solche Mittel als übertrieben. Dieser Typus des Cyberstalkings bedarf weiterer Forschung.

Ebenso *ist kollektives Cyberstalking* mit Stalking im realen Leben nicht vergleichbar. Während man offline üblicherweise einen Stalker und ein Opfer beobachtet, verfolgen hier zwei oder mehr Personen eine oder mehrere Personen. *Unternehmensbezogenes Cyberstalking* zielt primär darauf ab, Informationen über das Ziel zu sammeln, um es zu diskreditieren und zu belästigen. Dabei werden sowohl konventionelle Mittel (z. B. Telefonbücher oder Wählerverzeichnisse) als auch

Informations- und Kommunikationstechnologien (z. B. 192.com, ein elektronisches Telefonbuch) eingesetzt. Es ist jedoch möglich, dass auch illegale Mittel zur Belästigung des Opfers eingesetzt werden (z. B. Identitätsdiebstahl und Betrug). *Gruppen-Cyberstalking* ist ein faszinierendes Thema, das weiterer Forschung bedarf. Es entsteht wahrscheinlich aus einer Auseinandersetzung, die zur Parteinahme führt (daher ist anzunehmen, dass Gruppenstalking mehrere Opfer umfassen kann). Es besteht auch die Möglichkeit, dass andere zum Cyberstalking gezwungen oder aus Angst vor Vergeltungsmaßnahmen zum Nichtstun gezwungen werden. Auch diese passive Form des Gruppen-Cyberstalkings muss weiter untersucht werden.

Wie bereits erwähnt, ähnelte die Untergruppe der Cyberstalker mit intimer Beziehungsorientierung stark den Offline-Stalker-Klassifizierungen von Mullen et al. (1999). Die Antworten der Opfer deuteten darauf hin, dass die „Ex-Partner“ der von Mullen und seinen Kollegen beschriebenen Gruppe der abgewiesenen Stalker (die eine beendete Beziehung wiederbeleben möchten) ähnelten. Auch die „Verliebten“ wiesen Ähnlichkeiten mit der Gruppe der intimitätssuchenden/unfähigen Verehrer auf (die versuchen, eine Beziehung zu einer Person aufzubauen, die ihr Interesse geweckt hat und von der sie fälschlicherweise annehmen, dass diese Zuneigung erwidert wird, oder die eine Beziehung anstreben, aber die sozialen Regeln der Partnersuche missachten).

Obwohl viele Menschen über die Studie informiert wurden, nahm nur eine Minderheit teil. Dabei sollte nicht außer Acht gelassen werden, dass dies an den Gefühlen von Angst, Scham, Verlegenheit oder Wut liegen könnte, die die Betroffenen möglicherweise noch während oder sogar nach dem Vorfall empfinden. Eine Betroffene (die später aus der Studie ausschied) schilderte am Ende ihres Berichts die intensiven Gefühle, die sie empfand: Sie war wütend und gleichzeitig extrem beschämt über ihre Erfahrung mit Cyberstalking. Zukünftige Forscher sollten die möglicherweise komplexen und intensiven Gefühle berücksichtigen, die eine solche Erfahrung hervorrufen kann und die die Teilnahme an zukünftigen Studien zu Cyberstalking negativ beeinflussen können.

Unser Wissen über Cyberstalker ist derzeit noch sehr begrenzt, aber die Autoren dieser Studie hoffen, dass sie andere dazu anregen wird, dieses Gebiet genauer zu untersuchen.

Über die Autoren

Leroy McFarlane ist forensischer Psychologe und arbeitet in einem Gefängnis in den East Midlands (Großbritannien). Zuvor war er als Universitätsdozent tätig und verfügt über einen Hochschulabschluss im Bereich Kriminologie. Seine Forschungsschwerpunkte umfassen Stalking und Cyberstalking, Risikobewertung, Brandstiftung und Strafvollzugslehre. Er wurde von Mitarbeitern des britischen Justizvollzugsdienstes (Her Majesty's Prison and Probation Services) zu Stalking und Cyberstalking konsultiert. Aufgrund seiner umfangreichen Forschungsarbeit in diesem Bereich hat er kürzlich mehrere Publikationen zu Belästigungsverhalten und den Auswirkungen von Cyberstalking auf die Opfer mitverfasst.

Paul Bocij ist ein ehemaliger Universitätsdozent, der heute als freiberuflicher Autor und Berater tätig ist. Als Autor hat er über zwanzig Bücher verfasst oder daran mitgewirkt, darunter zahlreiche Fachbücher. Er ist einer der Autoren von „ *Business Information Systems“,* dem meistverkauften Lehrbuch für Wirtschaftsinformatik in Großbritannien, und hat außerdem an der Entwicklung eines begleitenden Online-Kurses mitgewirkt, der mittlerweile landesweit in Großbritannien eingesetzt wird. Darüber hinaus hat er zahlreiche Artikel, Kolumnen, wissenschaftliche Abhandlungen, Schulungsunterlagen und weitere Materialien zu Informationssystemen und Informationstechnologie verfasst. Er forscht aktiv und beschäftigt sich vor allem mit den Auswirkungen von Technologie auf die Gesellschaft, insbesondere mit abweichendem Verhalten wie Belästigung. In seiner Tätigkeit als unabhängiger Berater unterstützt er regelmäßig Einzelpersonen und Organisationen in vielfältigen Fragen der Computersicherheit. Er war zudem in mehrere Fälle von Cyberstalking involviert und hat zahlreichen Betroffenen geholfen, mit Belästigungen im Internet umzugehen.

Kommentare bitte direkt an: mail@pbocij.demon.co.uk .

Danksagungen

Die Autoren möchten Jayne Hitchcock, Präsidentin von Working to Halt Online Abuse (WHOA), und der National Anti-Stalking and Harassment Campaign and Support Association (NASH) für ihre Unterstützung danken, sowie allen, die an der Studie teilgenommen haben.

Anmerkungen

1. Meloy und Gothard, 1995, S. 259.

2. Pathé und Mullen, 1997, S. 12.

3. *Ebenda.*

4. Westrup, 1998, S. 276.

5. Die Autoren räumen ein, dass Autoren wie Sheridan et al. (2001) die Vorstellung eines Serienstalkers akzeptieren, aber keiner scheint die Möglichkeit in Betracht gezogen zu haben, dass ein Stalker mehrere Opfer gleichzeitig ins Visier nehmen könnte.

6. Obwohl Hatcher (2001) anhand von anekdotischen Beschwerden an die Gruppe eine Typologie von Cyberstalkern entwickelte, scheint diese nicht auf formaler akademischer Forschung zu beruhen.

7. Ein Trojanisches Pferd ist ein Programm, das von Hackern und anderen genutzt wird, um in ein Computersystem einzudringen. Viele Trojaner dienen der Überwachung eines Computersystems und versenden regelmäßig Berichte, die vertrauliche Informationen wie beispielsweise alle vom Computer gesendeten oder empfangenen E-Mails enthalten.

8. Spam kann als unerwünschte E-Mail beschrieben werden, die oft auch als „Junk-E-Mail“ bezeichnet wird.

9. Beim Mailbombing wird eine riesige Menge an E-Mails an eine bestimmte Person oder Website gesendet, um das Zielsystem zu überlasten.

10. Hierbei handelt es sich um die Nachahmung einer anderen Person, in der Regel mit der Absicht, Schaden anzurichten oder Betrug zu begehen.

11. In diesem Fall wurde das Interview von der Mutter des Opfers durchgeführt.

Referenzen

P. Bocij und L. McFarlane, 2002. „Online-Belästigung: Auf dem Weg zu einer Definition von Cyberstalking“, *Prison Service Journal,* Band 139, S. 31-38.

P. Bocij und L. McFarlane, 2003. „Sieben Irrtümer über Cyberstalking“, erscheint im *Prison Service Journal,* Band 149.

P. Bocij, H. Bocij und L. McFarlane, 2003. „Cyberstalking: Eine Fallstudie über wiederholte Belästigung in Großbritannien“, *British Journal of Forensic Practice,* Band 5, Nummer 2 (Mai), S. 25-32.

A. W. Burgess und T. Baker, 2002. „Cyberstalking“. In: J. Boon und L. Sheridan (Hrsg.). *Stalking und psychosexuelle Obsession: Psychologische Perspektiven für Prävention, Polizeiarbeit und Behandlung.* Chichester: Wiley.

M. D'Amico, 1997. „Das Gesetz versus Online-Stalking“, unter

http://www.madcapps.com/writings/faqabout.htm , abgerufen am 9. Dezember 2001.

JM Deirmenjian, 1999. „Stalking im Cyberspace“, *Journal of American Academy of Psychiatry and Law,* Band 27, S. 407-413.

WJ Fremouw, D. Westrup und J. Pennypacker, 1997. „Stalking auf dem Campus: Die Verbreitung und Strategien zum Umgang mit Stalking“, *Journal of Forensic Science,* Band 42, S. 666-669.

G. Hatcher, 2001. „Warum stalken Cyberstalker?“ unter http://www.cyberangels.org , abgerufen am 3. Juli 2001.

KK Kienlen, DL Birmingham, KB Solberg, JT O'Regan und JR Meloy, 1997. „Eine vergleichende Studie über psychotisches und nicht-psychotisches Stalking“, *Journal of the American Academy of Psychiatry and the Law,* Band 25, S. 317-334.

PE Mullen, M. Pathé und R. Purcell, 2000. *Stalker und ihre Opfer.* Cambridge: Cambridge University Press.

PE Mullen, M. Pathé, R. Purcell und GW Stuart, 1999. „Eine Studie über Stalker“, *American Journal of Psychiatry,* Band 156, S. 1244-1249.

National Institute of Justice, 1999. „Cyberstalking: Eine neue Herausforderung für Strafverfolgungsbehörden und Wirtschaft. Ein Bericht des Generalstaatsanwalts an den Vizepräsidenten“, abrufbar unter http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm , abgerufen am 1. Juli 2001.

E. Ogilvie, 2000. „Cyberstalking“, *Trends & Issues in Crime and Criminal Justice,* Nummer 166, S. 1-6.

M. Pathé und PE Mullen, 1997. „Die Auswirkungen von Stalkern auf ihre Opfer“, *British Journal of Psychiatry,* Band 170, S. 12-17.

W. Petherick, 2001. „Cyberstalking: Obsessional pursuit and the digital criminal“, unter http://www.crimelibrary.com/criminology/cyberstalking/index.html , abgerufen am 3. Juli 2001.

L. Sheridan, GM Davies und JCW Boon, 2001. „Der Verlauf und das Wesen des Stalkings: Eine Opferperspektive“, *Howard Journal of Criminal Justice,* Band 40, S. 215-234.

BH Spitzberg und G. Hoobler, 2001. „Cyberstalking und die Technologien des zwischenmenschlichen Terrorismus“, *New Media & Society,* Band 4, S. 71-92.

Techtv, 2001. „Stalking goes online“, unter http://www.techtv.com/cybercrime/print/0,23102,3014794,00.html , abgerufen am 3. März 2003.

Working to Halt On-line Abuse, 2001. „Online harassment statistics For 2000“, unter http://www.haltabuse.org/resources/stats/index.shtml , abgerufen am 3. Juli 2001.

JA Wright, AG Burgess, AW Burgess, AT Laszlo, GO McCrary und JE Douglas, 1996. „Eine Typologie des zwischenmenschlichen Stalkings“, *Journal of Interpersonal Violence,* Band 11, S. 487-502.

M. Zona, K. Sharma und J. Lane, 1993. „Eine vergleichende Studie von erotomanischen und zwanghaften Personen in einer forensischen Stichprobe“, *Journal of Forensic Sciences,* Band 38, S.

894-903.

Redaktionsgeschichte

Manuskript eingegangen am 24. April 2003; angenommen am 7. August 2003.

Copyright © 2003, *First Monday*

Copyright © 2003, Leroy McFarlane und Paul Bocij

Eine Untersuchung des räuberischen Verhaltens im Cyberspace: Auf dem Weg zu einer Typologie von Cyberstalkern von Leroy McFarlane und Paul Bocij
Erster Montag, Band 8, Nummer 9 (September 2003),

URL: Erster Montag

Gefahren auf der Informationsautobahn

Obwohl es keine allgemein anerkannte Definition von Cyberstalking gibt, bezeichnet der Begriff im Allgemeinen die Nutzung des Internets, von E-Mails oder anderen Telekommunikationstechnologien zur Belästigung oder Verfolgung anderer Personen. Es handelt sich nicht um bloße Belästigung durch unerwünschte E-Mails. Cyberstalking ist methodisch, vorsätzlich und anhaltend. Die Kommunikation, ob von bekannten oder unbekannten Absendern, reißt selbst dann nicht ab, wenn der Empfänger den Absender aufgefordert hat, jeglichen Kontakt einzustellen, und enthält oft unangemessene und mitunter verstörende Inhalte. Im Grunde ist Cyberstalking eine Erweiterung des physischen Stalkings.

Von: Trudy M. Gregorie, Ausbildungsleiterin des Nationalen Zentrums für Opfer von Straftaten

Obwohl es keine allgemein anerkannte Definition von Cyberstalking gibt, bezeichnet der Begriff im Allgemeinen die Nutzung des Internets, von E-Mails oder anderen Telekommunikationstechnologien zur Belästigung oder zum Stalking einer anderen Person. Es handelt sich nicht um bloße Belästigung durch unerwünschte E-Mails. Cyberstalking ist methodisch, vorsätzlich und anhaltend. Die Kommunikation, ob von einer bekannten oder unbekannten Person, reißt auch dann nicht ab, wenn der Empfänger den Absender gebeten hat, jeglichen Kontakt einzustellen, und ist oft mit unangemessenen und mitunter verstörenden Inhalten gefüllt. Im Wesentlichen ist Cyberstalking eine Erweiterung des physischen Stalkings. Die meisten Landes- und Bundesgesetze gegen

Stalking setzen voraus, dass der Stalker eine direkte Gewaltdrohung gegen das Opfer ausspricht, während einige lediglich verlangen, dass das Verhalten des mutmaßlichen Stalkers eine implizite Drohung darstellt. Auch wenn manche Formen des Cyberstalkings, die belästigendes oder bedrohliches Verhalten beinhalten, nach geltendem Recht noch nicht als Stalking gelten, können solche Verhaltensweisen ein Vorbote für Stalking und Gewalt im realen Leben sein und sollten daher ernst genommen werden. Cyberstalking birgt das Potenzial, von einer URL-Adresse auf eine reale Adresse überzugehen – vom Virtuellen ins Reale. In einem Bericht des US-Justizministeriums aus dem Jahr 1999 mit dem Titel „Cyberstalking: Eine neue Herausforderung für Strafverfolgung und Wirtschaft“ wird Cyberstalking als wachsendes Problem identifiziert. (1) Laut diesem Bericht haben derzeit über 80 Millionen Erwachsene und 10 Millionen Kinder in den Vereinigten Staaten Zugang zum Internet. Selbst wenn man annimmt, dass der Anteil der Cyberstalking-Opfer nur einen Bruchteil des Anteils derjenigen ausmacht, die in den vorangegangenen zwölf Monaten Opfer von Offline-Stalking geworden sind, schätzt der Bericht, dass es in den Vereinigten Staaten potenziell Zehntausende oder sogar Hunderttausende von Cyberstalking-Opfern geben könnte.

kriminelles Verhalten

Auch erfahrene Staatsanwälte beginnen, die Gefahren des Internets zu erkennen. Linda Fairstein, Leiterin der Abteilung für Sexualdelikte in der Staatsanwaltschaft von Manhattan und Vorstandsmitglied des National Center for Victims of Crime, erklärte: „Durch den Einsatz neuer Technologien und Geräte, die sich nicht mit herkömmlichen Methoden kontrollieren lassen, hat Cyberstalking traditionelle Formen des Stalkings und der Belästigung abgelöst. Zudem hat Cyberstalking zu Gewalttaten außerhalb des Internets geführt. Polizei und Staatsanwaltschaft müssen sich der steigenden Zahl dieser Vorfälle bewusst sein und Strategien entwickeln, um diese Probleme mithilfe des Strafrechtssystems zu lösen.“ (2) Opfer von Cyberstalking, die sich an das National Center for Victims of Crime wenden, beklagen sich häufig darüber, nicht ernst genommen oder von den kontaktierten Strafverfolgungsbehörden gar nicht erst als Opfer anerkannt zu werden. Auf die Beschwerde eines Opfers mit Aussagen wie „Im Internet kann Ihnen nichts passieren – es sind doch nur Worte“ oder „Schalten Sie einfach Ihren Computer aus“ zu reagieren, ist weder akzeptabel noch verantwortungsvoll. Es ist unzumutbar, von Opfern von Cyberstalking zu erwarten, dass sie ihre Online-Aktivitäten, die unter Umständen ihre berufliche Laufbahn beeinträchtigen, aufgeben, um solchen Problemen zu entgehen. Online-Belästigung und -Bedrohungen sind genauso beängstigend und belastend wie Belästigung und Bedrohungen im realen Leben. Ein kürzlich im Cyberstalking-Bericht des US-Justizministers beschriebener Vorfall verdeutlicht beispielhaft den Mangel an Schulung und Fachwissen bei den Strafverfolgungsbehörden, der für Opfer so frustrierend sein kann. (3) Eine Frau erstattete Anzeige bei der örtlichen Polizei, weil ein Mann im Internet Informationen veröffentlicht hatte, in denen er behauptete, ihre neunjährige Tochter sei für sexuelle Dienstleistungen zu haben, und seine private Telefonnummer mit der Aufforderung, rund um die Uhr anzurufen, angab. Es gingen zahlreiche Anrufe ein. Obwohl die Familie jeden Anruf der örtlichen Polizei meldete, riet der Polizist ihnen lediglich, ihre Telefonnummer zu wechseln. Daraufhin wurde das FBI eingeschaltet, das Ermittlungen aufnahm. Das FBI stellte fest, dass die örtliche Polizeibehörde keinen Computerexperten beschäftigte und der zuständige Polizist noch nie im Internet unterwegs

gewesen war. Die mangelnde Vertrautheit und die unzureichenden Ressourcen der örtlichen Behörde könnten dazu geführt haben, dass die Ernsthaftigkeit des Problems und die Handlungsmöglichkeiten der Strafverfolgungsbehörden nicht erkannt wurden. Fehlende moderne Technologie und ausreichend geschultes, erfahrenes Personal zählen zu den größten Herausforderungen für Strafverfolgungsbehörden und Staatsanwälte bei der Untersuchung und Verfolgung von Cyberkriminalität. Die Justiz muss sensibler auf Anzeigen wegen Cyberstalking und die damit verbundene reale Bedrohung reagieren und die notwendigen Schulungen und Ressourcen bereitstellen, um eine ordnungsgemäße Untersuchung und Strafverfolgung zu ermöglichen.

Sofortiger Zugriff

Alles, was ein Cyberstalker braucht, ist ein Computer und ein Modem. Aufgrund der enormen Menge an persönlichen Informationen im Internet kann er mit wenigen Mausklicks oder Tastatureingaben leicht private Daten über ein potenzielles Opfer finden. Wissen ist Macht, und bei jeder Form von Stalking geht es um Macht und Kontrolle. Online gibt es kaum Sicherheit. Schon das Einschalten eines Computers kann jeden Belästigungen aussetzen. Jeder, der E-Mails empfängt oder das Internet nutzt, ist anfällig für Cyberstalking. Besonders gefährdet sind Internetnutzer in Bereichen des Internets, in denen sie mit anderen interagieren. Dazu gehören Chats, Foren und Newsgroups, in denen Nutzer Nachrichten austauschen, sowie ihre E-Mail-Postfächer. Belästigungen per E-Mail beginnen meist mit dem ersten Kontakt in einem Live-Chat oder einer Newsgroup.

Techniken

Cyberstalker nutzen verschiedene Techniken. Zunächst suchen sie im Internet nach ihren Opfern und verfolgen diese. Anschließend versenden sie unerwünschte E-Mails, darunter Hass-, Obszön- oder Droh-E-Mails. Belästigungen in Live-Chats erfolgen direkt oder durch elektronische Sabotage (z. B. durch das Überfluten des Chatkanals, um die Unterhaltung des Opfers zu stören). In Newsgroups können Cyberstalker Beiträge über das Opfer verfassen oder Gerüchte streuen, die sich über das Forum verbreiten. Sie können auch eine Webseite über das Opfer erstellen, die persönliche oder fiktive Informationen oder Anfragen an die Leser enthält. Eine weitere Technik besteht darin, online, beispielsweise in Chatrooms, die Identität des Opfers anzunehmen, um dessen Ruf zu schädigen, Details über das Opfer zu veröffentlichen oder unerwünschte Kontakte zu erzwingen. Komplexere Formen der Belästigung umfassen Mailbomben (Massen-E-Mails, die das E-Mail-System des Opfers durch Überlastung praktisch lahmlegen), das Versenden von Computerviren oder Spam. Es besteht ein deutlicher Unterschied zwischen der Belästigung durch unerwünschte E-Mails und Online-Belästigung. Unerwünschte E-Mails sind gelegentlich zu erwarten. Cyberstalking hingegen ist ein über einen längeren Zeitraum andauerndes Verhalten mit wiederholten, vorsätzlichen Versuchen, dem Opfer Leid zuzufügen. Auch Menschen ohne Internetzugang oder die bewusst auf das Internet verzichten, sind vor Cyberkriminalität nicht gefeit. Datenbanken mit persönlichen Daten im Internet ermöglichen es einem Stalker, den

Benutzernamen eines Opfers mit dessen echtem Namen, Adresse, Telefonnummer und anderen persönlichen Informationen in Verbindung zu bringen oder sich online als das Opfer auszugeben. Der Täter kann das Opfer dann am Computer per E-Mail oder zu Hause per Post, Telefonanrufen oder sogar durch persönliches Erscheinen am Wohnort oder Arbeitsplatz belästigen. Telekommunikationstechnologien erleichtern es Cyberstalkern zudem erheblich, Dritte zur Belästigung und/oder Bedrohung des Opfers anzustiften. So erreichte die Staatsanwaltschaft von Los Angeles im ersten erfolgreichen Verfahren nach dem neuen kalifornischen Cyberstalking-Gesetz beispielsweise ein Geständnis eines 50-jährigen ehemaligen Wachmanns, der das Internet nutzte, um eine Frau, die seine Annäherungsversuche zurückwies, zur Vergewaltigung aufzufordern. Der Angeklagte terrorisierte sein 28-jähriges Opfer, das noch nie online gewesen war und nicht einmal einen Computer besaß, indem er sich in verschiedenen Internet-Chatrooms und Online-Foren als sie ausgab und dort – zusammen mit ihrer Telefonnummer und Adresse – Nachrichten veröffentlichte, in denen sie von einer Vergewaltigung fantasierte. Mindestens sechsmal, teils mitten in der Nacht, klopften Männer an die Tür des Opfers und boten ihr Vergewaltigung an, nachdem sie eine Kontaktanzeige im Internet geschaltet hatte. Der Angeklagte bekannte sich im April 1999 in einem Fall von Stalking und in drei Fällen der Anstiftung zu sexueller Nötigung für schuldig. Infolge der Taten des Stalkers wurde das Opfer schließlich aus ihrer Wohnung vertrieben, verlor ihre Arbeit, erlitt einen erheblichen Gewichtsverlust und entwickelte Angst, ihr Haus zu verlassen. (4) Die meisten der strafrechtlich verfolgten Fälle von Cyberstalking betrafen keine technisch komplexen Formen des Stalkings, und E-Mail wurde lediglich als alternative Kommunikationsform genutzt. Dies ist jedoch nicht immer der Fall. Die Verfügbarkeit von Anonymisierungssoftware bietet Stalkern einen hohen Schutz, da sie ihre Spuren effektiver verwischen können. Beispiele für solche Technologien sind „anonyme Remailer“, die die Identität des Absenders automatisch durch Pseudonyme verschleiern und die E-Mail über Server senden, die digitale Spuren sofort löschen, um einen späteren Zugriff durch Dritte, selbst durch Strafverfolgungsbehörden, zu verhindern. Ein weiteres Beispiel ist Stratfors Shredder, ein Softwareprogramm für Windows 95, das wie ein elektronischer Aktenvernichter funktioniert und gelöschte Dateien, einschließlich aller routinemäßigen Computer-Backups, automatisch überschreibt. (5) Je komplexer Software und Computertechnologien werden, desto einfacher können Cyberstalker anonym agieren und desto schwieriger wird es für Strafverfolgungsbehörden, zu ermitteln und genügend Beweise für eine Anklage zu sammeln. Um Cyberstalking zu bekämpfen, ist es entscheidend, Stalking im Allgemeinen zu verstehen. In vielen Fällen ist Cyberstalking lediglich eine weitere Phase in einem umfassenderen Stalking-Muster oder reguläres Stalking-Verhalten unter Nutzung neuer technologischer Werkzeuge. Daher lassen sich Strategien und Interventionen, die zur Bekämpfung von Offline-Stalking entwickelt wurden, oft auch auf Online-Stalking-Situationen übertragen. Es gibt Strafverfolgungsbehörden auf Bundes-, Landes- und lokaler Ebene, die sich verstärkt mit Stalking befassen, und einige haben vor Kurzem spezielle Arbeitsgruppen zur Bekämpfung von Cyberstalking eingerichtet.

Auswirkungen

Wie bei jeder Form von Stalking besteht das größte Trauma im anonymen Terror, den es im Leben des Opfers auslöst – rund um die Uhr, sieben Tage die Woche. Das Internet wird zu einem elektronischen Vorhang, hinter dem sich der Stalker versteckt und das Opfer zu Hause, am

Arbeitsplatz, im Freundes- und Nachbarnkreis und gegenüber unzähligen Menschen terrorisiert, die das Opfer gar nicht kennt. Cyberstalker können sich am anderen Ende der Welt, im selben Bundesstaat, auf der anderen Straßenseite oder im Nachbarbüro befinden. Es kann sich um einen ehemaligen Freund oder Partner handeln, um einen völlig Fremden aus einem Chatroom oder einfach um einen Teenager, der einen Streich spielt. Die Unfähigkeit, die Quelle der Belästigungen oder Drohungen zu identifizieren, ist einer der beunruhigendsten Aspekte dieses Verbrechens für ein Cyberstalking-Opfer. Die Tatsache, dass Cyberstalking keinen physischen Kontakt beinhaltet, kann fälschlicherweise den Eindruck erwecken, es sei weniger bedrohlich oder gefährlich als physisches Stalking. Cyberstalking ist jedoch genauso beängstigend und potenziell gefährlich wie ein Stalker vor der Haustür des Opfers. Die psychische Belastung ist sehr real, selbst wenn keine konkrete physische Bedrohung vorliegt. Sie stört das Leben und den Seelenfrieden des Opfers massiv. Cyberstalking führt zu einer Reihe von physischen, emotionalen und psychischen Traumata, die beim Opfer auftreten können.

- Schlafstörungen;
- Wiederkehrende Albträume;
- Störungen des Essverhaltens;
- Hypervigilanz;
- Hohes Stressniveau;
- Das Gefühl, die Kontrolle zu verlieren; und/oder
- Ein allgegenwärtiges Gefühl des Verlusts der persönlichen Sicherheit.

Aktuelle Antworten

In einer Grundsatzrede am 10. Januar 2000 beschrieb die US-Justizministerin Janet Reno das Internet und andere Informationstechnologien als enorme Vorteile für die Gesellschaft, gleichzeitig aber auch als Quelle neuer Möglichkeiten für kriminelles Verhalten. Sie schlug ein rund um die Uhr besetztes Netzwerk von Strafverfolgungsbeamten zur Bekämpfung von Cyberkriminalität, regionale Computerforensiklabore zur Analyse beschlagnahmter Computer auf Hinweise auf illegale Aktivitäten sowie eine sichere Online-Informationsplattform vor, die es Bundes-, Landes- und Kommunalbehörden ermöglichen sollte, Informationen über Cyberfälle auszutauschen. (6) Im Rahmen des Gesetzes gegen Gewalt gegen Frauen aus dem Jahr 2000 erweiterte der Kongress das Bundesgesetz gegen Stalking über Staatsgrenzen hinweg auf Cyberstalking (18 USC § 2261 A). Ebenfalls im Jahr 2000 verabschiedete der Kongress das Amy-Boyer-Gesetz (42 USC § 1320 B-23 (PL 106-553)), welches den Verkauf oder die öffentliche Zurschaustellung der Sozialversicherungsnummer einer Person, einschließlich des Verkaufs über das Internet, ohne deren ausdrückliche, elektronisch oder schriftlich übermittelte Einwilligung verbietet. Das Gesetz ermöglicht es einer Person, die durch die unrechtmäßige Weitergabe einer Sozialversicherungsnummer geschädigt wurde, den Verkäufer oder die Zurschaustellerin vor einem US-Bezirksgericht auf Unterlassung und Schadensersatz zu verklagen. Darüber hinaus kann der Sozialversicherungsbeauftragte gegen jeden solchen Verstoß eine Zivilstrafe von 5.000 US-Dollar verhängen, die sich bei Verstößen, die eine gängige Geschäftspraxis darstellen, auf bis zu 50.000 US-Dollar erhöhen kann. Dieses neue Gesetz gilt für Verstöße, die am 21. Dezember 2002, zwei

Jahre nach seinem Inkrafttreten, wirksam wurden. Das Amy-Boyer-Gesetz ist nach einer jungen Frau benannt, die ermordet wurde, nachdem ihr Stalker ihre Sozialversicherungsnummer im Internet erworben hatte. Mit diesen Informationen konnte er ihr Autokennzeichen und ihren Arbeitsplatz ausfindig machen. Er beschrieb seine Mordpläne detailliert auf einer Website, die unter ihrem Namen veröffentlicht wurde. Nur wenige Minuten nach seinem letzten Website-Besuch fuhr er zu ihrem Arbeitsplatz und erschoss sie, als sie in ihr Auto stieg. Auch die Bundesstaaten haben begonnen, auf Cyberstalking zu reagieren, indem sie ihre bestehenden Gesetze gegen Stalking und Belästigung um Bestimmungen ergänzt haben, die „Stalking mit elektronischen Mitteln“ oder „die Nutzung von Computern zum Zwecke des Stalkings“ unter Strafe stellen. (7) Etwa die Hälfte der Bundesstaaten enthält derzeit Formulierungen in ihren Gesetzen, die sich speziell mit belästigender elektronischer, Computer- oder E-Mail-Kommunikation befassen. Die Gesetze anderer Bundesstaaten enthalten weit gefasste Formulierungen, die so interpretiert werden können, dass sie auch Cyberstalking umfassen. Einige Bundesstaaten haben Gesetze, die Belästigung über Computerkontakt verbieten, während andere Gesetze gegen Stalking haben, die auch elektronische Kommunikation umfassen. Einige wenige haben Gesetze, die sowohl Stalking als auch Belästigung unter Strafe stellen und elektronische Kommunikation einschließen. Andere Bundesstaaten haben Gesetze, die – unabhängig von Stalking oder Belästigung – Computerkommunikation oder E-Mail-Missbrauch unter Strafe stellen. Manche haben Gesetze, die Drohungen per E-Mail oder „elektronisch übermittelte Nachrichten“ verbieten.

Ressourcen

Opfer von Online-Belästigung und -Bedrohungen mussten, oft in Zusammenarbeit mit Opferhilfsorganisationen, die Lücke an verfügbaren Ressourcen und Unterstützungsangeboten schließen, indem sie eigene informelle Unterstützungsnetzwerke und Informationswebseiten aufbauten, um Strategien zum Umgang mit diesen Straftaten auszutauschen. Ein solches Programm ist „Working to Halt Online Abuse“ (WHOA), das von Frauen gegründet wurde, um die Internet-Community über Online-Belästigung aufzuklären. WHOA schult die Online-Community außerdem in der Entwicklung von Webseiten-Ressourcen, darunter die Erstellung einer Liste sicherer und unsicherer Seiten, damit Internetnutzer fundierte Entscheidungen treffen können, und bietet Informationen darüber, wie sich Nutzer vor Online-Belästigung schützen können.

Webseite: http://www.haltabuse.org/

E-Mail-Adresse: whoa@haltabuse.org

Weitere Online-Ressourcen umfassen

- CyberAngels: Eine gemeinnützige Organisation, die Opfern von Online-Belästigung und Stalking hilft. http://www.cyberangels.org
- Safety Ed International: Eine gemeinnützige Organisation, die die Internet-Community unterstützt und Opfern von Online-Belästigung oder -Stalking konkrete Ratschläge, Ressourcen und Informationen bietet.
  safetyed.org

- Privacy Rights Clearinghouse: Ein gemeinnütziges Verbraucher- und Interessenvertretungsprogramm, das Verbrauchern die Möglichkeit bietet, zu erfahren, wie sie ihre Privatsphäre schützen können. Zu den Dienstleistungen des PRC gehört eine Hotline, über die Verbraucher Datenschutzverletzungen melden und Informationen zum Schutz ihrer Privatsphäre anfordern können. Das PRC hat außerdem Informationsblätter zu Datenschutzthemen veröffentlicht, darunter Informationsblatt Nr. 14 mit dem Titel „Werden Sie gestalkt? Tipps zu Ihrem Schutz“ und Informationsblatt Nr. 18 mit dem Titel „Datenschutz im Internet“. safetyed.org
- Online Privacy Alliance: Ein Zusammenschluss von über 80 globalen Unternehmen und Verbänden, die sich für den Schutz der Online-Privatsphäre einsetzen. Ziel ist es, Datenschutzrichtlinien für das neue elektronische Medium zu definieren und ein Online-Umfeld zu fördern, das die Privatsphäre der Verbraucher respektiert. Auf dieser Website finden Sie Informationen für Verbraucher, Muster-Datenschutzrichtlinien für das Internet sowie aktuelle Nachrichten zu Datenschutzverstößen und -problemen im Internet. privacyalliance.com
- Network Solutions bietet mit WHOIS einen Internetdienst an, der Abfragen in seiner Registrar-Datenbank durchführt, um Nutzern zu helfen, den Inhalt eines Domainnamen-Registrierungsdatensatzes im Header einer empfangenen E-Mail zu ermitteln. Das Ergebnis liefert die Kontaktinformationen des Internetdienstanbieters des Absenders. networksolutions.comprivacyalliance.com
- Bundeshandelskommission (FTC), Abteilung Verbraucherschutz: Eine Informationsseite der US-Bundesregierung für Verbraucher, inklusive Kontaktinformationen für Betroffene von Identitätsdiebstahl, Missbrauch der Sozialversicherungsnummer oder betrügerischen Kreditkartenkonten. FTC-Hotline: 877-IDTHEFT
  Hotline für Betrug mit Sozialversicherungsnummern: 800-269-0271

Empfehlungen für Opfer von Online-Stalking
Wenn Sie online belästigt werden, sollten Sie Folgendes tun:

Wenn du unter 18 bist, erzähle deinen Eltern oder einer anderen erwachsenen Person, der du vertraust, dass du belästigt oder bedroht wirst. Behalte das nicht für dich. Deine Eltern müssen wissen, was los ist, damit sie dir helfen und dich unterstützen können.

Wenn Sie belästigende E-Mails erhalten, erstellen Sie ein neues Konto oder fordern Sie bei Ihrem Internetanbieter einen neuen Benutzernamen und ein neues Passwort an. Schließen Sie Ihr altes Konto. Informieren Sie sich, wie Sie die Filterfunktionen Ihres E-Mail-Programms nutzen können, um E-Mails von bestimmten Absendern zu blockieren.

Speichern Sie jede Nachricht, die Sie vom Cyberstalker erhalten. Sichern Sie alle verfügbaren Header-Informationen, falls es sich um eine E-Mail oder einen Newsgroup-Beitrag handelt. Drucken Sie eine Kopie aus und speichern Sie die Nachricht zur Dokumentation auf einem Datenträger.

Führen Sie ein Protokoll jeder Kommunikation, in dem Sie die Situation detaillierter beschreiben. Dokumentieren Sie, wie sich die Belästigung auf Ihr Leben auswirkt und welche Schritte Sie unternehmen, um sie zu beenden.

Nehmen Sie einmalig direkt Kontakt mit Ihrem Belästiger auf und fordern Sie ihn in klaren, deutlichen und formellen Worten auf, Sie nicht weiter zu kontaktieren und/oder nichts über Sie zu veröffentlichen. Machen Sie deutlich, dass die Kontaktaufnahme unerwünscht und unangemessen ist und dass Sie weitere Schritte einleiten werden, falls dies nicht aufhört. Senden Sie eine Kopie per E-Mail an den Systemadministrator Ihres Internetanbieters. Speichern Sie Kopien dieser Nachrichten und vermerken Sie, dass Sie sie gesendet haben.

Wenn Sie belästigende Online-Nachrichten erhalten und deren Ursprung zurückverfolgt werden kann, obwohl Sie den Absender darüber informiert haben, dass Sie nicht kontaktiert werden möchten, sollten Sie erwägen, den Online-Stalker Ihrem Internetanbieter (ISP) zu melden. Viele ISPs haben Richtlinien, die die Nutzung ihrer Dienste zur Belästigung oder zum Missbrauch anderer Personen verbieten. Einige ISPs sind möglicherweise bereit, das Konto des Stalkers zu sperren. Wenn Sie beleidigende E-Mails erhalten, ermitteln Sie die Domain (die Buchstaben nach dem @-Zeichen) und kontaktieren Sie Ihren ISP. Die meisten ISPs bieten eine E-Mail-Adresse wie abuse@[Domainname] oder postmaster@[Domainname] für Beschwerden an. Sollte dies nicht funktionieren, finden Sie die Kontaktadressen in der Regel unter www.networksolutions.com/cgi-bin/whois/whois (führen Sie eine „Whois“-Abfrage für den jeweiligen ISP durch). Wenn Beschwerden per E-Mail nicht zum Erfolg führen, rufen Sie an. Bewahren Sie Kopien dieser Kommunikation auf und notieren Sie alle Kontakte in Ihrem Protokoll.

Bedenken Sie jedoch, dass dies nur eine kurzfristige Lösung sein kann oder die Situation sogar verschlimmern kann, wenn der Stalker herausfindet, dass Sie Ihren Internetanbieter informiert haben. [In diesem Fall könnte er/sie versuchen, sich an Ihnen zu rächen oder Sie offline zu stalken. Unabhängig davon, ob das Online-Stalking aufhört, sollten Sie sich bewusst sein, dass der Stalker möglicherweise persönliche Informationen über Sie über das Internet oder andere Quellen erhalten hat und Sie daher weiterhin dem Risiko von Offline-Stalking ausgesetzt sind. In diesem Fall sollten Sie entsprechende Sicherheitsvorkehrungen treffen.]

Wenden Sie sich an Ihre örtliche Polizei. Melden Sie jeden Vorfall von Online-Missbrauch und übergeben Sie der Polizei Kopien aller gesammelten Beweise. Bewahren Sie Kopien aller Polizeiberichte auf und vermerken Sie jeden Kontakt mit den Strafverfolgungsbehörden in Ihrem Protokoll. Falls sich der Stalker außerhalb Ihres Bundeslandes befindet, sollten Sie sich zusätzlich an die örtliche Niederlassung des FBI wenden.

Wenden Sie sich an die Computerkriminalitätsabteilung des FBI in Ihrer Region. [Der Federal Interstate Stalking and Prevention Act, 18 USC § 2261A, wurde im Jahr 2000 geändert, um neben Stalking per Telefon und Post auch Online-Stalking zu erfassen. Darüber hinaus können einige Fälle von Online-Stalking unter 18 USC § 875, Interstate Communications (Drohungen mit körperlicher Gewalt oder Entführung einer anderen Person in der Kommunikation zwischen Bundesstaaten sind ein Verbrechen) oder 47 USC § 223, Obscene or Harassing Telephone Calls in Interstate Communications fallen.]

Um sich online besser zu schützen:

1. Verwenden Sie einen geschlechtsneutralen Benutzernamen.
2. Geben Sie Ihr Passwort niemals an Dritte weiter, insbesondere nicht an Personen, die Ihnen eine Sofortnachricht (IM) senden.
3. Geben Sie Ihre Kreditkartennummer oder andere Identifikationsdaten nicht als Altersnachweis an, um auf eine Webseite eines Ihnen unbekannten Unternehmens zuzugreifen oder sich dort anzumelden.
4. Weisen Sie Kinder darauf hin, dass sie ihren richtigen Namen, ihre Adresse oder ihre Telefonnummer nicht ohne Erlaubnis im Internet preisgeben sollen.
5. Nutzen Sie ein kostenloses E-Mail-Konto wie Hotmail (www.hotmail.com) oder YAHOO! (www.yahoo.com), um Nachrichten in Newsgroups und Mailinglisten zu versenden, Chatrooms zu betreten, Formulare auszufüllen oder mit jemandem zu korrespondieren, den Sie nicht gut kennen.
6. Gib deine primäre E-Mail-Adresse niemals an Unbekannte weiter.
7. Verbringen Sie Zeit in Newsgroups, Mailinglisten und Chatrooms als „stiller“ Beobachter, bevor Sie „sprechen“ oder Nachrichten veröffentlichen.
8. Wenn Sie online teilnehmen, schreiben Sie nur das, was Sie jemandem persönlich sagen würden.
9. Antworten Sie nicht auf E-Mails von Fremden; mit einer Antwort bestätigen Sie dem Absender Ihre E-Mail-Adresse.
10. Geben Sie regelmäßig (mindestens einmal im Monat) Ihren Namen in Internetsuchmaschinen ein, um zu sehen, ob und welche Informationen angezeigt werden. Um Ihren Namen aus Verzeichnissen entfernen zu lassen, kontaktieren Sie jede Suchmaschine, bei der Sie gelistet sind, und bitten Sie um Löschung. (Die Tipps 1–8 wurden 1999 von den Beratungsstellen für Opfer sexueller Gewalt der George Mason University entwickelt.)

Endnoten

1. US-Justizministerium. (August 1999). Cyberstalking: Eine neue Herausforderung für Strafverfolgungsbehörden und Wirtschaft – Ein Bericht des Generalstaatsanwalts an den Vizepräsidenten. Washington, DC: US-Justizministerium, S. 2, 6.
2. Ebenda, S. 8.
3. Ebenda, S. 8.
4. Los Angeles Times, 23.01.1999.
5. Riveira, Diane. (September/Oktober 2000). „Internetkriminalität gegen Frauen“, Sexual Assault Report, 4(1), S. 14.
6. Pressemitteilung des US-Justizministeriums. (Veröffentlicht am 10. Januar 2000). „Generalstaatsanwältin Reno schlägt neue Maßnahmen zur Bekämpfung von Cyberkriminalität vor.“ Washington, DC: US-Justizministerium.

Alle Rechte vorbehalten. Copyright © 2003 National Center for Victims of Crime. Diese Informationen dürfen frei verbreitet werden, sofern die Verbreitung kostenlos erfolgt. von der Gebühr, in ihrer Gesamtheit und einschließlich dieses Urheberrechtshinweises.

Revision #2
Created 10 November 2025 01:56:03 by investigatione
Updated 10 November 2025 02:01:10 by investigatione