



mitp



Jayson E.
Street

Kent
Nabors

Brian
Baskin

Forbieten Network

Anatomie eines Hacks

Kapitel

1

Erkundung

Kurz und knapp auf den Punkt gebracht bezeichnet man als *Erkundung* (engl. *recon* für *reconnaissance*, also die militärische Aufklärung eines Zielobjekts) die Fähigkeit, still und heimlich ein Ziel zu lokalisieren, das einen Angriff lohnt. In der physischen Welt gibt es diesen Prozess schon seit Jahrhunderten. Im Laufe der Zeit wurde er sowohl von Angreifern^a als auch Verteidigern immer weiter perfektioniert.

Kriminelle haben viele Ziele, die sie irgendwann ausbeuten können. Der englische Fachausdruck dafür lautet *Exploit*. Zwar führen viele Exploits oft nur zu wenigen Schätzen, aber durch einen glücklichen Treffer lohnt sich der ganze Angriffsprozess. In der physischen Welt würde zu einer solchen Erkundung gehören, ein potenzielles Ziel sorgfältig zu beobachten und dabei den Aufwand auf ein Ziel fokussieren, das geringes Risiko, aber hohen Erfolg verspricht. Das begann mit den Räufern, die sich in den Bäumen über Handelsstraßen versteckten, und führt heutzutage zum Einsatz technologischer Errungenschaften wie Teleskope und Ferngläser, um aus der Distanz etwas auszukundschaften. Außerdem erlauben die technischen Fortschritte ferngesteuerte Überwachungskameras, Geräte zum Entdecken von Funknetzen und Infrarot-Wärmescanner. Das Aufkommen des sozialen Zeitalters hat dies noch weiter vereinfacht. Jetzt kann man verfolgen, wie die überwachten Zielpersonen auf Twitter und Facebook ihre Urlaubspläne beschreiben, und man kontrolliert FourSquare-Konten auf sekundenschnelle, automatische Standort-

191

a. Die in diesem Buch beschriebenen Vorgänge lassen sich im Prinzip auf deutsche Verhältnisse übertragen, doch viele Details funktionieren nur im amerikanischen Kontext. In diesem Fall dient die Darstellung amerikanischer Hintergründe den interessierten deutschen Lesern, die sich an eigene Recherchearbeiten machen wollen. Darum wurde darauf verzichtet, für die Quellen aus dem englischen Sprachraum deutsche Entsprechungen zu finden, und nur gelegentlich ein Hinweis auf deutsche Gegebenheiten integriert. (A.d.Ü.)

taktualisierungen. Letzteres Beispiel wurde kürzlich auf der Site *www.PleaseRobMe.com* vorgeführt. Hier wurden automatisch Benutzerkonten aufgelistet, die über Twitter oder FourSquare zeigen, wer gerade von zu Hause abwesend ist.

In der digitalen Welt sind viele dieser Erkundungsaktionen tatsächlich sehr ähnlich. Ein Angreifer sucht sich Ziele, die unter leicht ausbeutbaren Schwachstellen leiden und viele wertvolle Informationen enthalten könnten. Das können Kreditkarten, Passwörter oder auch Schaltpläne für einen Helikopter sein, auf die ein Angreifer abzielt, und er ist ständig auf der Pirsch nach Zielen, die er überfallen kann. Egal was Ihre Firma herstellt oder in welcher Branche sie tätig ist, irgendwo auf der Welt wird es mindestens eine Person geben, die liebend gerne Ihre internen Daten hätte.

In diesem Kapitel werden alle Aspekte der Erkundung erläutert, die in der Geschichte vorgestellt wurden. Wir untersuchen, wie Sie, Ihre Firma oder Ihre Organisation sich gegen Angreifer schützen können, die es auf Ihre Daten abgesehen haben.

Anmerkung

Wir haben für den Teil von STAR (Security Threats Are Real) als Begleitung eine alternative Realität ins Internet gestellt. Sie können nachverfolgen, wie die Erkundung von 3DNF erfolgt. Viele der im Buch vorkommenden Personen verfügen auch im Internet über Präsenzen. Sie werden viele Hintergrundinformationen über das Unternehmen 3DNF und die Charaktere des Buches finden. Vergessen Sie nicht, den Namen Ihrer Firma, Ihren eigenen Namen oder von anderen, die Ihnen nahestehen, einzusetzen. Blättern Sie zum Ende dieses Kapitels: Dort erfahren Sie, wie Sie 3DNF selbst hacken können!

Die Firmenpräsenz von 3DNF:

- <http://www.3dnf.net>
- <http://blog.3dnf.net>
- <http://twitter.com/3dnf>

Personen aus *FORdb1dd3n Network – Anatomie eines Hacks* auf Twitter:

- http://twitter.com/Underground_Bob
- http://twitter.com/l_30N
- http://twitter.com/M4x_St34L
- http://twitter.com/Rudy_HTown
- http://twitter.com/Da_Dobbs
- <http://twitter.com/P4v3l>
- <http://twitter.com/MResol>

SOCIAL NETWORKING

Anatomie eines Hacks

Einer der Namen war nicht wie die anderen in schwarzer, sondern in roter Schrift. Michael Resol war für Stepan wohl irgendwie interessant. Dann folgten Links, die offenbar zu einem von Michael geschriebenen Blog führten. Es gab sogar Links auf Zocker-Seiten. Stepan hatte ein paar Dinge angemerkt:

Michael Resol ist das beste Ziel. Er ist seit fünf Jahren Netzwerk-administrator für 3DNF. Er wurde bei Beförderungen übergangen und redet in seinem Blog zuviel über seinen Arbeitgeber. Sowohl im Blog und auch auf seinen Facebook-Seiten verweist er auf seine bevorzugten Zocker-Seiten. Ich glaube, er steckt finanziell in der Klemme - siehe Link weiter unten.

Michaels technische Position, seine lange Beschäftigung bei 3DNF und Geldsorgen machen ihn zu einem guten Kandidaten für die Umsetzung unserer Zwecke. (Seite 35).

Wenn man ein Unternehmen angreift, egal ob real oder übers Internet, ist das ein sehr riskanter Prozess. Angreifer können in vielerlei Hinsicht abgewehrt werden, außer sie haben einen vollkommen kugelsicheren Plan. Allerdings gibt es eine Trumpfkarte, die viele Angreifer gut zu nutzen gelernt haben: den Insider. In vielen Fällen liefert ein Insider in der Zielfirma zahlreiche Informationen, die beim Angriff helfen können, und sei es unwissentlich.

In unserer Geschichte konnten Vlad und seine Kumpane für ihre Zwecke bei 3DNF einen Insider nutzen, um den Angriff vorzubereiten, und zwar Michael Resol. Michael hat ein paar kritische Sicherheitsfehler begangen, die ihn für Überredung oder gar Erpressung anfällig machten: Er ist ein zwanghafter Spieler, äußert sich detailliert in einer Internetpräsenz über seine Arbeit und kommentiert darin öffentlich seinen Unmut über seinen Arbeitgeber. Das prädestiniert ihn für Vlad als Ziel und löst viele der Geschehnisse im Buch aus.

Damit liegt ein stetig wachsendes Problem unserer modernen Zeit auf der Hand. Nicht nur arbeiten immer mehr Menschen täglich mit dem Internet, sondern sie nutzen es auch, um mit anderen Gemeinschaften, sogenannte Communitys zu bilden. Diese Bewegung wird durch die Akzeptanz von Facebook und Twitter noch weiter beschleunigt. Darin können Nutzer ihre Gedanken und Ideen veröffentlichen, ohne Erfahrungen mit Publikationen im Web zu haben oder es vorab zu erlernen. In den frühen Tagen des Internet brauchte man wirkliches Wissen und Übung, um eine Online-Präsenz zu füh-

ren. Man musste sich einen Server suchen, auf dem die eigenen Webseiten gehostet wurden. Man musste lernen, wie man in HTML (Hypertext Markup Language) Inhalte erstellt und wie man diese dann mittels komplexer Tools und Utilities ins Internet hochlädt. Durch Schaffung solcher Hosts wie Geo-Cities wurde dieser Vorgang erleichtert, aber erst durch das Aufkommen von Sites wie MySpace und Blogger sank die Wissensschwelle tief genug, damit Webpublishing allen Nutzern zur Verfügung steht.

Durch Webpublishing konnten die User ihrer Umwelt immer die neuesten Updates über ihr persönliches Leben und ihre Erfahrungen kundtun – ein Absatz zurzeit. Viele Online-Karrieren wurden dadurch erfolgreich gestartet. Doch für manche Nutzer war es sogar eine zu hohe Hürde, einen oder gar zwei Absätze auf einmal zu schreiben. Ihre Gebete wurden erhört, als der Microblogging-Dienst (Twitter) erschien. Nun können sie in kurzen Botschaften mit 140 Zeichen flotte Meldungen aus ihrem Leben in die Welt senden.

Exploit-Techniken

Wenn wir darüber sprechen, wie dieses Material auszubeuten ist, meinen wir das in dem Kontext, schnell die öffentliche Repräsentation eines Angestellten finden und betrachten zu können, um für einen Angriff verwertbare Informationen zu finden. Das so erkundete Material kann direkt für einen Angriff benutzt werden, z.B. Informationen über Bauvorhaben, neue physische Sicherheitshardware oder neu umgesetzte Richtlinien. Mit solchen Informationen kann man auch Angestellte der Firma erschließen, die »umgedreht« werden können.

Angestellte ausbeuten

In unserer Geschichte fand Vlad mit öffentlich verfügbaren Informationen über die Firma einen der Netzwerkadministratoren von 3DNF und nutzte ihn aus, und zwar Michael Resol. Michael ist keinesfalls eine Ausnahme: Er sieht sich Versuchungen ausgesetzt, mit denen auch viele andere in der Welt fertig werden müssen. Er ist einer Online-Spielleidenschaft verfallen und unzufrieden mit seinem Job. Wir sind immer wieder mal mit unseren Jobs unzufrieden, das geht normalerweise vorüber oder bessert sich. Michaels Verhängnis war nicht nur, dass er Material online gepostet hat, sondern dass er selbst auch dafür gesorgt hat, für eine solche Ausnutzung anfällig zu sein. Außerdem fehlte die persönliche Charakterstärke, der Versuchung zu widerstehen. Er brauchte Geld, um seine Spielschulden zu bezahlen. Als er dann die Chance geboten bekam, auf einen Schlag seine Schulden loszuwerden, indem er einfach seinen ihm sowieso unsympathischen Arbeitgeber reinlegen konnte, griff er sogleich zu.

Angreifer suchen üblicherweise bei Firmenmitarbeitern nach solchen, deren Rüstung einen deutlichen Riss aufweist. Ein guter Bürger, dessen Vergangenheit mit etwas besonders Peinlichem belastet ist, kann erpresst werden, beispielsweise ein Pastor mit einer Leidenschaft für Online-Pornografie oder ein Manager der Leitungsebene mit einer früheren Drogenleidenschaft oder eben der unglückliche Netzwerktechniker, der süchtig nach Online-Zockereien ist.

Michaels Situation ist ein wenig überschaubarer als bei den anderen, denn er könnte durch eine schlichte Zahlung seine aktuellen Schulden loswerden, aber Vlad hätte ihn auch einfach damit unter Druck setzen können, den Arbeitgeber darüber zu informieren. Viele Arbeitgeber zögern, Personen mit außergewöhnlichen Schulden einzustellen. Tatsächlich ist das einer der zentralen Faktoren, die geklärt werden, wenn jemand eine Sicherheitsfreigabe für die Regierung bekommen will. Personen mit großen Schulden stehen möglicherweise vor der Entscheidung, ihren Patriotismus gegen die überwältigenden Schulden abzuwägen zu müssen, und einen solchen Kampf gewinnen meist die Schulden.

Hat ein Angreifer einen Mitarbeiter erst einmal am Haken, kann er ihn auch zu weiteren Informationen und Handlungen nötigen. Viele erpresste Angestellte sind sich nicht darüber im Klaren, dass ein solcher Deal in eine Einbahnstraße mündet. Auch wenn sie sich so wie Michael nur aus Finanzgründen auf eine Übereinkunft einlassen, gibt es keinen Ausweg. Wenn sie kalte Füße bekommen und die Abmachung neu verhandeln wollen, wird der Geldhahn zugedreht. Vlad hätte Michael dann gleich weiter erpressen können, dass er dem Arbeitgeber Details über die Firmenspionage mitteilt. In praktischer Hinsicht wäre, das für Vlad nicht von Vorteil, ist aber als Einschüchterungstaktik sehr effektiv, weil das Opfer in eine Position kommt, wo es sich zwischen seiner persönlichen Sicherheit und seiner Firma entscheiden muss.

Das Unternehmen ausbeuten

Für Angreifer ist es sogar noch einfacher, bloß darauf zu warten, dass der Angestellte Informationen im Internet verbreitet, als sich die Mühe zu machen, diesen Mitarbeiter aktiv auszubeuten. Das geschieht sehr häufig, indem Mitarbeiter sich im Internet über ihre Arbeitgeber oder Geschäftspartner beklagen. Schwer durchschaubare Kontrollen der Privatsphäre bei Social-Networking-Sites wie Facebook verkomplizieren das Problem, weil viele Nutzer sich nicht darüber im Klaren sind, dass ihre Privatbotschaften tatsächlich öffentlich in die ganze Welt gesendet werden. Obwohl viele dieser Botschaften dem Verfasser unschuldig und nichtig vorkommen mögen, kann ein Angreifer, der das Unternehmen ins Visier genommen hat, sich anhand dieser Informationen eine Vorstellung über interne Geschäftsangelegenheiten formen. Nehmen wir die folgenden Botschaften:

Mitarbeiter 1: »Neuer Exploit für Windows Server erschienen ... boah, ist das nervig«

Pressemitteilung des Unternehmens: »Wir werden an diesem Wochenende eine planmäßige Downtime vornehmen, um Wartungsarbeiten an unseren Servern durchzuführen.«

Mitarbeiter 2: »Hab grad ne Mail gekriegt, dass ich das Wochenende durcharbeiten darf. Adieu, schöne Angeltour!«

Jede dieser Nachrichten ist für sich genommen nur ein unschuldiges Posting im Internet. Dauernd nehmen Firmen zur regelmäßigen Wartung ihre Server vom Netz. Allerdings fügt ein Angreifer, der Mitarbeitern dieser Firma per Cyber-Stalking nachstellt, diese Teile zusammen und erkennt, dass die Server dieser Firma für einen gerade erschienenen Exploit anfällig sind und dass bis zum Wochenende gewartet werden soll, um die Patches zu installieren. Dieser Prozess wird *Inferenz* genannt und ist in der Informationssicherheitsbranche ein bekannter Angriffsvektor, einfach aufgrund der ungeheuren Mengen an Daten, die regelmäßig veröffentlicht werden.

Online erschienene Posts können einen Mitarbeiter sogar noch heimsuchen, lange nachdem der Sicherheitsvorfall passiert ist. Anfang 2010 wurde ein Zivilprozessverfahren gegen einen Schulbezirk in Pennsylvania wegen der nicht bestimmungsgemäßen Nutzung von Laptops angestrengt, die den Schülern ausgehändigt wurden¹. Die Laptops enthielten eine Überwachungssoftware, mit dem das Schulsystem jederzeit jede Webcam einschalten und Bilder des vor dem Laptop sitzenden Nutzers machen konnte. Das führte zu einem Vorfall, bei dem ein Schüler unter dem Vorwurf illegalen Drogenkonsums gemäßregelt wurde. Später stellte sich heraus, dass es ein Schokoriegel gewesen war. Obwohl an sich schon interessant, ist dieser Fall außerdem deswegen besonders bemerkenswert, weil die Online-Präsenz des Netzwerktechnikers der Schule und seine Rolle in dieser Situation mit hineinspielen. Einem unabhängigen Forscher zufolge betreibt dieser Netzwerktechniker ein eigenes Blog und verfügt »online über einen großen Webforum-Footprint«², was bedeutet, dass man ihn in vielen Online-Diskussionsforen finden kann. Der Techniker hatte viele öffentliche Postings und Interviews über seine Beteiligung bei den Laptop-Webcams vorgenommen. Allermindestens wird durch diese Online-Information seine Faszination und Leidenschaft für die Nutzung der Technologie deutlich, mit denen er Schülern hinterherspioniert und jene fangen will, die illegale Handlungen ausführen. Wer in diesem Fall recht und wer unrecht hat, konnte zur Drucklegung dieses Buches noch nicht geklärt werden. Doch die Menge des Materials, das öffentlich von einem in den Fall verwickelten Techniker gepostet wurde, hat die Arbeit der juristischen Verteidigung der Schule deutlich erschwert.

Anatomie eines Hacks

Michael Resol ist das beste Ziel. Er ist seit fünf Jahren Netzwerk-administrator für 3DNF. Er wurde bei Beförderungen übergangen und redet in seinem Blog zuviel über seinen Arbeitgeber. Sowohl im Blog und auch auf seinen Facebook-Seiten verweist er auf seine bevorzugten Zocker-Seiten. (Seite 35)

Facebook ist zwar eigentlich nicht zu übersehen, wird aber von vielen Organisationen gerne komplett ignoriert. Anfänglich wurde es einfach als eine weitere Blogging-Site betrachtet, etwa auf gleicher Ebene wie MySpace, aber Facebook ist mittlerweile zu einer der gewaltigsten und mächtigsten Sites der Welt geworden. Man kann sich nur schwerlich die wahre Größe und den Umfang der Tätigkeiten von Facebook vorstellen. Auf seiner eigenen Statistikseite veröffentlicht Facebook die folgenden Zahlen (Stand März 2010)³:

Anmerkung

- Über 400 Millionen aktive Nutzer
- 50 % unserer aktiven Nutzer loggen sich täglich bei Facebook ein.
- Über 35 Millionen Nutzer aktualisieren ihren Status täglich.
- Über 60 Millionen Status-Updates werden jeden Tag gepostet.
- Mehr als 3 Milliarden Fotos werden monatlich auf die Site hochgeladen.
- Über 5 Milliarden Inhalte (z.B. Weblinks, Nachrichten, Blog-Posts, Notizen, Fotoalben etc.) werden jede Woche weitergegeben.
- Jeder Nutzer hat durchschnittlich 130 Freunde auf der Site.
- Jeder Nutzer verbringt im Mittel täglich 55 Minuten auf Facebook.
- Jeder Nutzer schreibt durchschnittlich monatlich 25 Kommentare über Facebook-Inhalte.
- Jeder Nutzer ist durchschnittlich Mitglied von 13 Gruppen.

Liest man diese Informationen, stellt sich ein klares Bild der Nutzeraktivitäten auf einer solchen Site dar. Der durchschnittliche Nutzer verbringt täglich fast eine Stunde auf Facebook, und viele loggen sich während der Arbeit ein. Der durchschnittliche Nutzer schreibt an seine Kontakte auch jeden Monat etwa 25 Kommentare über seinen Alltag.

Die Gefahr bei Facebook besteht nicht nur in den geposteten Inhalten selbst, sondern auch, wer diese Postings lesen kann. Die meisten Nutzer ver-

stehen die Sicherheitseinstellungen von Facebook nicht oder wie man Inhalte nur für enge Freunde freigibt. Überdies hat Facebook sich große Mühe gegeben, dass die Nutzer nicht klar durchblicken und ihre Konten so eingestellt lassen, dass Inhalte für »Alle« veröffentlicht werden. Eine kürzlich erfolgte Modifikation der Einstellungen für die Privatsphäre auf Facebook vom Dezember 2009 war so schwer verständlich, dass viele Nutzer die Settings für Online-Inhalte auf »für alle sichtbar und lesbar« eingestellt haben.

Die Gefahren solcher Änderungen verdeutlicht beispielhaft die Suspendierung einer College-Professorin in Pennsylvania Anfang 2010, weil sie angeblich Bedrohungen gegenüber ihren Studierenden gepostet haben soll.⁴ Die Professorin führte ein sehr privates Facebook-Profil und hat ihre Einträge nur auf ihre Freunde beschränkt. Sie lehnte gewohnheitsmäßig außerdem freundschaftliche Beziehungen zu ihren Studierenden ab und hielt ihr berufliches Leben getrennt von ihrem Privatleben. Änderungen an den Privatsphäreneinstellungen, die sie ohne rechtes Verständnis vorgenommen hatte, führten dazu, dass ihre Studierenden in ihr privates Profil schauen konnten und dort abfällige Bemerkungen über sich fanden.

Twitter

Anatomie eines Hacks

»Ich hab' dir doch gesagt, das waren FBI-Leute!« versuchte Bob es erneut.

»Das wissen wir doch nicht«, antwortete Leon und gähnte. »Genau das hat Dobbs aber gerade getwittert. Hast du was im Code gefunden?« (Seite 123)

»Darum kümmer dich jetzt. Ich muss noch ein paar Sachen checken, und dann sende ich ein paar DMs auf Twitter. Ich will nicht twittern, falls das FBI oder wer uns da verfolgt zuhört.« (Seite 139)

Obwohl Twitter auf keinen Fall an die immense Größe von Facebook heranreicht, wurde es zu einer Microblogging-Site, die viele Internet-Analysiker überrascht hat. Von vielen belächelt, ist Twitter schnell zu einer der beliebtesten Sites mit immer größerer Community gewachsen.

Bei Twitter kann man in kurzen Status-Updates in 140 Zeichen wie mit einer SMS öffentliche Botschaften an die ganze Welt senden. Die User können auch anderen folgen, die sie interessieren, und schaffen damit eine Welt kurzzeitiger Berühmtheit, in der viele Nutzer daran gemessen werden, wie viele »Follower« sie haben. Alle von Nutzern eingestellten Status-Updates, die

sogenannten »Tweets«, sind frei und offen zugänglich und können von jedem gelesen oder gesucht werden. Ausgenommen sind Nutzer, die ihr Profil auf »Geschützt« gesetzt haben. Da können weiter alle die Basisinfos über das Profil sehen, auch die Freunde des Nutzers, aber nicht die eigentlichen Tweets.

Twitter wurde zu einer neuen Form des Instant Messagings (IM) unter Freunden und Kollegen. Anders als Standard-IM-Clients wie Microsoft Messenger oder AOL Instant Messenger gibt es keine zustandsbezogene (*stateful*) Verbindung zu Twitter. Der Empfänger einer Nachricht muss nicht online sein, um die Nachricht zu erhalten. Empfänger lesen sie einfach dann, wenn sie beschließen, ihre Nachrichten anzuschauen. Man kann nicht genau bestimmen, wann jemand bei Twitter angemeldet ist und wann nicht, außer mit Blick auf die Zeiten der Tweets. Twitter wurde oft als weltgrößter Chatraum bezeichnet, in dem alle an ihrer Tastatur herumhängen.

In unserer Story nutzt Dobbs Twitter, um Leon eine Botschaft zu senden, dass er gerade Besuch vom FBI (Federal Bureau of Investigation) bekommen hat. Später bittet Bob über Twitter mit einer privaten DM (Direct Message) seinen Freund um Hilfe. DMs werden privat auf Twitter von einem Nutzer zu einem anderen gesendet, ohne dass jemand sie lesen kann. Sie sind eine der wenigen Einschränkung für die Privatsphäre, die in diesem Dienst genutzt werden.

Best Practices

Es gibt keine Möglichkeit, Ihre Angestellten daran zu hindern, irgendetwas im Internet zu publizieren, das alle lesen können. Allerdings gibt es effektive Wege, um das Risiko zu senken. Dazu muss man den Einstellungsprozess der Firma anpassen und interne Sicherheitsschulungen vornehmen.

Den Hintergrund der Mitarbeiter prüfen

Um Angriffe gegen seine Mitarbeiter zu verhindern, muss ein Unternehmen weitere Sicherheitsmaßnahmen einsetzen, um die persönliche Integrität der einzustellenden Personen zu gewährleisten. Allerdings ist das schwerer, als es klingt. Viele Unternehmen führen bei neuen Bewerbern keine Referenzanrufe durch und treffen ihre Entscheidungen einzig aufgrund eigener Erfahrungen mit dem Bewerber bzw. der Bewerbungsunterlagen. Noch weniger Firmen nutzen sogenannte »Background Checks«, um sich den Hintergrund eines Bewerbers vor der Einstellung anzusehen, und somit abschätzen zu können, ob sie für Bestechung oder Ausbeutung anfällig sein könnten. Ferner wird nur ein sehr kleiner Prozentsatz den finanziellen Aufwand für eine vollständige Sicherheitsfreigabe in Kauf nehmen.

Für Deutschland gilt: Falls Sie in Ihrer Firma Informationen besitzen, verarbeiten oder lagern, die einen Verschlusssachengrad haben, sollten Sie beim Bundesministerium für Wirtschaft eine Geheimschutzbetreuung erbitten. Dort bekommen Sie Auskünfte, wie Sie ggf. Angestellte gesetzeskonform überprüfen können (<https://bmwi-sicherheitsforum.de>).^b

Schulungen

Nach außen sickernde Informationen, die für Ihr Unternehmen abträglich sein können, kann man weitgehend dadurch mildern, dass Ihre Nutzer und Angestellten geschult werden. Eine solche Schulung muss weiter gehen als die simple Aufforderung, »Zurückhaltung« zu üben und Richtlinien der Form »Das darf man nicht« zu veröffentlichen. Moderne User wollen Informationen online posten und werden empört sein, wenn dieses Privileg eingeschränkt werden soll. Stattdessen sollten Sie mit ihnen wie mit Gleichberechtigten arbeiten. Stellen Sie Usern tatsächliche Fälle vor, bei denen Informationen aus Firmen gesickert sind, und gehen Sie gemeinsam durch, wie man das Risiko senken kann. In den weiter oben als Beispiel gebrachten Botschaften hätte Mitarbeiter 1 den Exploit von seiner persönlichen Arbeit getrennt halten können, indem er einfach feststellt, dass ein neuer Exploit erschienen ist, ohne das wehklagend zu kommentieren. Angreifer suchen andauernd danach, wie unschuldige Botschaften mit persönlichen Aktivitäten im Alltag einer Person verknüpft werden können. Erleichtern Sie nicht deren Arbeit, indem Sie öffentlich verkünden, dass oder ob ein Sicherheitsproblem sich auf Sie oder Ihre Firma auswirken wird.

Schulen Sie Kolleginnen und Kollegen, wie man Online-Einstellungen zur Privatsphäre korrekt vornimmt. Wenn sie Twitter nutzen, sollten sie ihr Konto »schützen«, um außer bei Freunden Einzelheiten privat zu halten. Bei Facebook gehen Sie mit den Nutzern die Einstellungen zur Privatsphäre durch und erklären alles im Detail. Für jede Art von Daten, die auf Facebook gepostet werden, gibt es ein Setting, das steuert, wer sie sehen darf. Damit wird kontrolliert, ob Ihre Daten sichtbar sind für »Alle«, »Freunde von Freunden«, »Nur Freunde« oder ob Sie eine benutzerdefinierte Einstellung vornehmen wollen.⁵ Erklären und demonstrieren Sie, warum keine der Privatsphäreinstellungen so gesetzt sein sollten, dass Informationen für »Alle« sichtbar sind.

ZUSAMMENFASSUNG

Wie in der Geschichte demonstriert, war der Auslöser für die ganze Kette der Reaktionen und Ereignisse ein beeinflussbarer Mitarbeiter, der zu viele

b. Dank an Frank Hitzke, Hanse Computer Service, www.hcs-net.com, für diesen Hinweis.

persönliche Details über sich selbst und seine Arbeit im Internet gepostet hat, die dann für alle einsehbar waren. Vlad und seine Kumpane haben diese Details aufgegriffen und diesen Angestellten als Ziel genommen, indem sie ihn mit einer großen Summe bestochen haben, damit er ein paar einfache Aufgaben innerhalb des 3DNF-Büros ausführt.

Das Problem der Online-Lecks von Unternehmens- und persönlichen Informationen wächst immer mehr, weil Millionen Menschen täglich über ihre Lebens- und Arbeitsgewohnheiten Updates ins Netz stellen. Das kann eine Ausbeutung sowohl des Mitarbeiters als auch des Unternehmens, für das er tätig ist, zur Folge haben. Solche Angriffe entschärft man am besten, indem man grundsätzlich verhindert, dass sie überhaupt geschehen können. Setzen Sie in Ihren Bewerbungsverfahren bessere Auswahlverfahren ein, um zu verhindern, dass anfällige Mitarbeiter angeworben werden. Schulen Sie Ihre Nutzer über die Gefahren, öffentliches Material online zu posten. Informieren Sie sie auch darüber, wie sie bei den Online-Systemen, die sie regelmäßig nutzen, die Einstellungen zur Privatsphäre korrekt gesetzt werden.

WEITERE INFORMATIONEN

Die Welt des Social Networkings wächst und entwickelt sich immer weiter. Manche Sites verändern sich im Laufe der Jahre dramatisch, und aktuelle Sicherheitsrichtlinien müssen sich anpassen, um den steigenden Risiken zu begegnen. Damit Sie mehr Material darüber bekommen, wie Sie Ihre Informationen und Ihr Netzwerk absichern können, geben wir hier eine Reihe von zusätzlichen lesenswerten Links an. In diesen Links finden Sie Ressourcen über korrekte Sicherheitsaktionen, die Sie heute schon implementieren können. Außerdem werden Sie zu Experten in diesem Thema geführt, die Sie bei Ihren Bemühungen um eine bessere Sicherheit unterstützen können.

- Das Twitter-Verzeichnis von Security Twits:
<https://twitter.com/securitytwits/lists>
- This you?? What's the point of phishing a Twitter account?:
www.f-secure.com/weblog/archives/00001893.html
- US-CERT: Staying Safe on Social Network Sites:
www.us-cert.gov/cas/tips/ST06-003.html
- Sophos Social Media Threat Beaters: *www.sophos.com/lp/threatbeaters/*
- Social Media Security Podcast: *<http://socialmediasecurity.com>*
- »How cybercriminals invade social networks, companies«:
www.usatoday.com/tech/news/computersecurity/2010-03-04-1Anetsecurity04_CV_N.htm

GOOGLE-HACKING

Anatomie eines Hacks

Dann hatte Stepan ein paar Namen und E-Mail-Adressen aufgelistet, die zur Domäne 3dnf.com gehörten. Vlad konnte nur vermuten, dass Stepan den Domänennamen gegoogelt hatte, um diese Adressen abzugreifen. War das der Fall, dann war Stepan bei seinen Recherchen ziemlich einfallsreich. (Seite 34)

Praktisch allen in der Informationssicherheitsbranche tätigen Profis ist das Problem des Google-Hackings bekannt. Doch obwohl »googeln« bereits ein akzeptiertes Verb in der Alltagssprache ist, ist das Konzept des Google-Hackings für viele außerhalb dieser Branche immer noch Neuland.

Der Begriff Google-Hacking wurde von Johnny Long geprägt und perfektioniert. Dieser bekannte Sicherheitsforscher ist auch Gründer der »Hackers for Charity« und Autor einer Reihe von Büchern zu diesem Thema. Das aktuelle Werk heißt *Google Hacking for Penetration Testers, Volume 2*, ISBN 978-1-59749-176-1, Syngress). Er entdeckte, dass sorgfältig formulierte Google-Anfragen Suchergebnisse zurückgeben können, die zeigen, dass auf dem Ziel anfällige Software läuft, die nur darauf wartet, angegriffen zu werden. So schuf Johnny Long die Google Hacking Database (GHDB), zu finden unter www.hackersforcharity.org/ghdb/, die durch die Hunderte von Einreichungen durch Johnny Long und seinen Freiwilligenteams schnell wuchs.

Google-Hacking arbeitet mit bestimmten Schlüsselwörtern oder Phrasen, die nur innerhalb von Websites zu finden sind, auf denen anfällige Software läuft. Es zielt auch auf Schlüsselbegriffe sensibler Daten selbst ab, z.B. Kreditkarten- und Sozialversicherungsnummern. In manchen Fällen erlauben die spezifischen Google-Suchanfragen einem User sogar, die Sicherheitskontrollen einer Website zu umgehen und sich direkt als Administrator einzuloggen.

Obwohl es beim Google-Hacking ursächlich nur um die Lokalisierung von Schwachstellen und Datenlecks geht, wird der Begriff jetzt allgemeiner genutzt, um sich auf jede Art von Suchanfragen zu beziehen, mit denen man Informationen über eine Person oder Firma herausfinden kann, die eigentlich nicht für die Öffentlichkeit gedacht waren. Diese Nutzung hört allerdings nicht mit Google auf. Google war ursprünglich vielleicht die einzige Suchmaschine, die solch komplexe Anfragen erlaubte, doch jetzt unterstützen auch Yahoo! und Bing viele dieser Operatoren und können die gleichen Suchfunktionen ausführen. Aus Gründen der Einfachheit werden wir den Vorgang weiter als Google-Hacking bezeichnen, doch sollten Sie einfach im Hinterkopf behalten, dass die meisten der Operationen auch bei Ihrer bevorzugten Suchmaschine funktionieren.

Exploit-Techniken

Google und alle großen Suchmaschinen verfügen über sehr leistungsfähige Funktionalitäten, die Trillionen Webseiten durchsuchen können – und auch seitenübergreifend suchen. Wir werden in diesem Abschnitt verschiedene Wege vorstellen, um mit Google ein Ziel zu erkunden, und konzentrieren uns auf die in unserer Story genutzten Ansätze. Da bekam Vlad von Stepan eine Liste von Namen und E-Mail-Adressen, was den gewieften Verbrecher schwer beeindruckte. Vlad erwähnt, dass Stepan 3DNF »gegoogelt« hat, um die Informationen zu finden, was tatsächlich möglich ist, und wir stellen diesen Vorgang hier vor.

Erweiterte Suchoperatoren

Für die wichtigste Google-Hacking-Technik muss man die Nuancen der verschiedenen erweiterten Suchoperatoren verstehen, die von einer Suchmaschine unterstützt werden. Jeder kennt die grundlegenden Suchoperatoren wie + und -. Wenn ein Wort auf jeden Fall vorhanden sein soll, stellt man ihm ein + voran, z.B. *+Hacking*. Wenn entsprechend ein bestimmtes Wort nicht vorkommen soll, kommt ein - davor, z.B. *-Google*. Eine Anfrage mit *+Hacking -Google* gibt jede Seite aus, die sich mit Hacking beschäftigt, aber nicht das Wort »Google« enthält.

Wenn man nach einer Phrase oder einem Satz sucht, setzt man ihn in Anführungszeichen, z.B. *Hack the Planet* (dieses Zitat ist manchen vielleicht noch aus dem Film *Hackers – Im Netz des FBI* bekannt). Diese Suche gibt Seiten aus, die sich dem Konzept »Hack the Planet« widmen, das der Computerforscher Wes Felter⁶ formuliert hat.

Für die Mehrheit der Internetnutzer reichen diese Basisoperatoren, aber ihnen mangelt es an den subtilen Fähigkeiten, die von einem Meistersucher gefordert werden. Solche Suchanfragen zu formulieren, die Trillionen potenzieller Webergebnisse nehmen und sie auf genau jene Resultate limitieren, nach denen man sucht, ist eine Kunst, die Übung und Sorgfalt erfordert. Um diese Macht zielgerichtet einzusetzen, braucht man weitere Suchoperatoren, z.B. jene, die in Tabelle 1.1 gezeigt werden.

Sie können all diese Operatoren selbst ausprobieren, während Sie weiterlesen. Machen Sie einfach mal beim Lesen eine Pause und nutzen Sie mit Ihren neu gewonnenen Kenntnissen Google. Als Erstes schauen wir uns den Operator *site:* an. Dieser Operator beschränkt die Ergebnisse nur auf den angegebenen Domänennamen. Wenn Sie also eine Basisuche nach *site:microsoft.com* durchführen, erhalten Sie eine Liste von Webresultaten, die alle von *www.microsoft.com* und deren verschiedener Subdomänen stammen. Wenn Sie das weiter auf eine Subdomäne wie z.B. *http://store.microsoft.com*

einschränken wollen, passen Sie die Suchanfrage an und schreiben *site:store.microsoft.com*. Dann können Sie nach einem bestimmten Item suchen, an dem Sie interessiert sind, und wissen, dass nur der Microsoft Store erscheinen wird. Probieren Sie einmal diese Suche nach dem Microsoft Flugsimulator: *site:store.microsoft.com flight simulator*.

Der Operator *inurl*: erweist sich bei vielen Suchen als immens hilfreich. Manchmal geht es bei den gesuchten Daten nicht nur um den Text einer Seite, sondern stattdessen um den Text, der im URL (Uniform Resource Locator) einer bestimmten Seite erscheint. Auf der Suche nach E-Mail-Adressen, Postanschriften oder Telefonnummern einer Site können Sie probieren, direkt nach einer häufig vorkommenden Seite namens »Kontakt« oder »contact« zu suchen. Abhängig von der auf dem Webserver eingesetzten Software kann diese Datei verschiedene Erweiterungen haben, z.B. *contact.htm*, *contact.html*, *contact.asp*, *contact.php* etc. Eine generische Suche nach *inurl:contact* wird all diese Ergebnisse ausgeben. Viele Sites haben für diese bestimmte Seite unterschiedliche Namen, manche nennen sie auch »ueberuns« (»aboutus«). Wenn man nur nach Seiten mit »contact« im Namen sucht, könnten einem diese anders benannten Seiten entgehen.

Tabelle 1.1: Operatoren für erweiterte Suche

Suchoperator	Beschreibung
site:	Beschränkt alle Suchergebnisse auf einen einzigen Domännennamen und die darin enthaltenen Seiten.
inurl:	Sucht im URL (Uniform Resource Locator) der Webseite nach dem Suchwort.
intitle:	Sucht das Suchwort im Titel der Webseite.
intext:	Legt fest, dass das Suchwort innerhalb des Textes der Webseite erscheinen <i>muss</i> .
inanchor:	Sucht das Suchwort nur innerhalb der HTML-Anker (Hypertext Markup Language), also den Seitenlinks.
link:	Sucht nach Webseiten, die auf den angegebenen URL verweisen.
ext:	Sucht nach Webdokumenten, die die angegebene Dateierweiterung tragen.
cache:	Sucht im archivierten Cache von Google nach dem angegebenen URL.

Gehen Sie nun zu Google und geben Sie *inurl:aboutus.htm* ein. Sie sollten mehrere Hunderttausende Treffer bekommen, die Sie durchsehen können.

Kombinieren wir das nun mit anderen Suchoperatoren, um die Resultate einzuschränken. Wir nehmen uns einmal vor, nur nach Behörden der US-Regierung mit dieser Seite zu suchen: `inurl:aboutus.htm site:gov`. In diesem Beispiel nehmen wir den Operator `site:` und begrenzen die Ergebnisse auf die Top-Level-Domain `.gov`. Schränken wir das noch mehr ein, indem wir nach Regierungsbehörden suchen, die Adressen in Washington, DC, haben, indem Folgendes eingegeben wird: `inurl:aboutus.htm site:gov "Washington, DC"`. Dann erkennen Sie, dass die Ergebnisse deutlich leichter zu überschauen sind (siehe Abbildung 1.1).

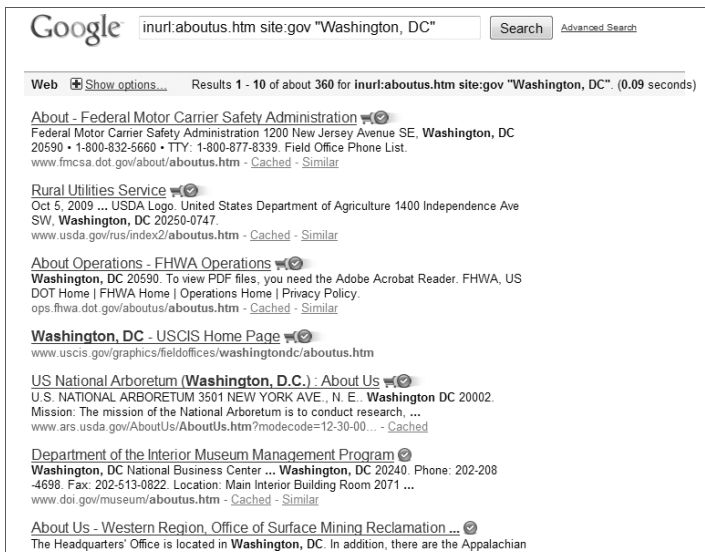


Abbildung 1.1: Suchergebnisse bei Google anhand von erweiterten Operatoren

In den vergangenen Jahren haben die Fähigkeiten von Google deutlich zugenommen. Anfangs konnte man nur einfache Textdokumente und Webseiten suchen, doch nun stehen einem auch Medieninhalte wie Microsoft Word-Dokumente, Tabellenkalkulationen und PDF-Dokumente (Portable Document Format von Adobe) zur Verfügung. Vor wenigen Jahren noch konnte man über solche Suchanfragen viele sensible und vertrauliche Dokumente aufspüren, die im ganzen Internet öffentlich sichtbar eingestellt worden waren. Nehmen wir z.B. Tabellenkalkulationen (Spreadsheets), in denen große Mengen geordneter Informationen gespeichert sind und die für Echtzeitberechnungen von Preisen und Zahlen eingesetzt werden. Kurz gesagt

werden Spreadsheets normalerweise für interne Datenberechnungen eingesetzt und meist nicht außerhalb einer Organisation weitergegeben. Durch den Operator *ext:* können wir unsere Ergebnisse direkt auf eine bestimmte Dateiart eingrenzen, z.B. Microsoft Excel-Tabellen. Suchen Sie nach *ext:xls site:mil* oder *ext:xlsx site:mil*. Diese Suchanfrage sucht nach allen öffentlichen Excel-Tabellen mit der Dateiendung *.xls* bzw. *.xlsx*, die sich auf Webservern des Militärs befinden (».mil«). Obwohl die Ergebnisse dieser Anfrage meistens harmloses Material ergibt, holten sich in den Kindertagen des Internet viele Organisationen ein blaues Auge, weil kritische Informationen hier unabsichtlich gepostet wurden und durchgesickert sind.

Archivierte Webseiten

Wenn man Webseiten nach für Angriffe relevanten Informationen durchsucht, ist es auch wichtig, die zeitliche Dimension einer Website zu berücksichtigen. Die Seite, die Sie heute sehen, könnte eine andere sein als die, die gestern oder im vergangenen Jahr zu sehen war. Informationen ändern sich andauernd, und manche Sites beginnen, aus Angst vor einem Angriff die veröffentlichten Informationen schlicht zu reduzieren. Allerdings hilft diese Reduktion ihnen nicht gegen Archivierungsdienste im Internet, z.B. Google und die Wayback Machine des Internet-Archivs, die sich unter www.archive.org/web/web.php befindet.

Google Cache speichert die letzte Kopie einer gefundenen Website auf den Google-Servern und ist außerordentlich hilfreich für den Fall, dass eine Website aus Wartungsgründen aus dem Netz genommen wurde. Sie kann außerdem von Online-Suchern genutzt werden, um Informationen herauszuziehen, die vielleicht gerade von einer Website entfernt oder modifiziert wurde, bevor Google die Chance hatte, die Website erneut zu indexieren und die gecachete Version zu ändern.

Um die gecachete Version einer Website aufzurufen, suchen Sie einfach nach der fraglichen Seite und klicken auf den Link Im Cache direkt unter dem Ergebnis (siehe Abb. 1.2). Durch Klick auf diesen Link wird die Webseite gezeigt, aber sie kommt direkt von einem Google-Server statt vom eigentlichen Server der Website. Wenn diese Aussage Ihr Herz höher schlagen lässt, haben Sie wahrscheinlich gemerkt, welch prima Chance das für weitere Erkundungsarbeiten bietet.

Indem Sie eine direkte Verbindung mit der Website eines Unternehmens aufbauen, wie wir es in diesem Abschnitt erläutert haben, verraten Sie Ihr Vorgehen. Die Aktivitäten werden fortlaufend in einem Weblog protokolliert, und zwar auf dem Webserver des Unternehmens für jede einzelne aufgerufene Seite, und auch die IP-Adresse (Internet Protocol) des Computers, der sie angefordert hat.

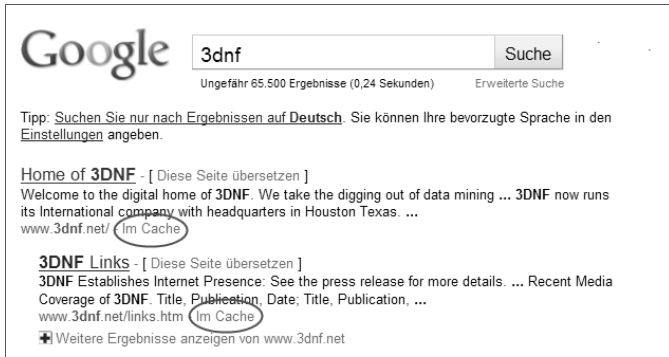


Abbildung 1.2: Der Link auf den Google-Cache

Die meisten Angreifer werden darauf achten, die IP zu verschleiern, indem sie die Verbindung im Netz über Proxies aufbauen, doch dafür kann auch der Google Cache genutzt werden. Indem wir unsere Suchanfragen auf den Google Cache konzentrieren, können wir bergeweise Informationen über das Ziel herausfinden, ohne jemals auf den Server des Ziels zuzugreifen. Allerdings ist das nicht vollständig narrensicher. Google cachet nur den eigentlichen Textinhalt der Seite, keine Bilder oder Multimedia-Inhalte. Diese liefert weiterhin der Server des Ziels direkt, und Ihre Anwesenheit fällt dem Ziel immer noch auf, wenn Sie versuchen, Grafiken, Bilder und Videos von der Seite herunterzuladen. Wenn Sie die Version einer Seite im Google Cache betrachten, sehen Sie einen großen Kasten oben auf der Seite (siehe Abb. 1.3). Unten rechts in diesem Kasten finden Sie einen Link, der Sie direkt zu einer reinen Textversion dieser Seite führt. Durch Klick auf diesen Link wird nur den Text der Seite selbst direkt vom Google-Server aufgerufen. Auf manchen Seiten sind Textinhalte nicht vollkommen getrennt, aber Sie haben gute Chancen, auf der großen Mehrheit von Websites die Seitendetails passiv anschauen zu können, ohne je auf den Server des Ziels zugreifen zu müssen.



Abbildung 1.3: Seitenbanner des Google-Cache mit Link auf die Nur-Text-Version

Diese Aktion kann auch manuell vorgenommen werden, ohne sich durch die verschiedenen Google-Links zu klicken. Sie können direkt die Version einer Website aus dem Google-Cache entnehmen, wenn Sie die Google-Suche mit

dem Operator *cache:* vornehmen. Wenn Sie beispielsweise nach *cache:3DNF.net* suchen, werden Sie direkt auf die gecachete Version geleitet. Wenn Sie dann die Bilder nicht haben wollen und nur den Text brauchen, klicken Sie in die Adresszeile des Browsers und ergänzen den URL-Text mit dem Argument *&strip=1*. Durch diese Zeichenfolge wird Google aufgefordert, die Seite erneut zu laden, aber alle Bilder und Multimediainhalte wegzulassen. Durch eine manuelle Ausführung dieser Aktionen greifen Sie beim ersten Cache-Request auf den realen Server der Webseite zu und bekommen die zu modifizierende Suchanfrage. Somit entfällt der Bedarf, beim zweiten Request die auf dem eigentlichen Server der Webseite gehosteten Inhalte wegzulassen. Diese Aktionen können allerdings auch automatisch durch verschiedene Browser-Add-ons ausgeführt werden, z.B. Passive Cache für Mozilla Firefox. Damit klicken Sie mit der rechten Maustaste auf einen URL und bekommen sofort die bereinigte Cache-Version. Passive Cache kann bei <https://addons.mozilla.org/en-US/firefox/addon/977> heruntergeladen werden.

Man kann sich ältere Details einer Site auch in deren Eintrag in der Wayback Machine vom Internet Archive anschauen. Auf dieser Site werden über 150 Milliarden Seiten nach Adresse und Datum archiviert. So können Sie z.B. die Website von Apple aus dem Jahr 1996 anschauen – lange bevor Apple international populär wurde. Sie können sich wahrscheinlich ausmalen, wie leistungsfähig diese Suchmaschine ist. In ihren Kindertagen werden viele Unternehmen unglaublich detaillierte Informationen auf ihren Webseiten posten, um dem Geschäft auf die Sprünge zu helfen. Im Laufe der Zeit tritt der Bedarf nach operationaler Sicherheit in den Vordergrund, während der Druck, neue Geschäftsfelder zu erschließen, sich verringert, und somit werden auch die Details auf den Webseiten weniger. Mit der Wayback Machine von Archive.org können Sie Seiten finden, die scheinbar schon längst aus dem Internet entfernt wurden.

Ein bemerkenswertes Beispiel eines Datenlecks stammt vom United States Postal Service (USPS) aus dem Jahre 2004. Damals installierte ein Abteilungsleiter von USPS auf seinem Bürocomputer Kazaa und gab versehentlich die gesamte Festplatte frei.⁷ Das wurde von einem zufälligen P2P-User entdeckt, der Hunderte von Seiten disziplinarischer Berichte voller persönlicher Informationen herunterladen konnte. Diese Informationen wurden dann für alle lesbar in einem öffentlichen Forum gepostet. Mittlerweile wurde die Website vom Netz genommen und das Forum eingestellt. Diese Site kann nicht mehr aufgerufen werden und existiert nirgends ... außer in der Wayback Machine. Wenn man den URL in der Wayback Machine eingibt, kann man sich die gecachete Version des gesamten Forum-Postings anschauen und alle Details lesen (siehe Abb.1.4). Diese Funktionalität wird auch vom Add-on Passive Cache für Mozilla Firefox automatisiert.

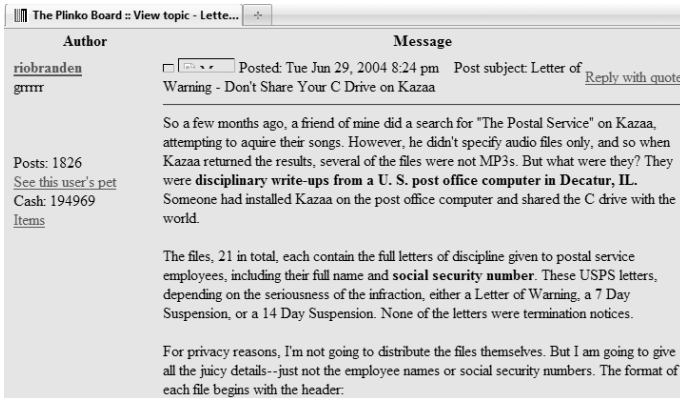


Abbildung 1.4: Darstellung einer gelöschten Website bei Archive.org

Advanced Dork

Obwohl Sie für diese Aktionen eigentlich nur Ihre Lieblings-Suchmaschine brauchen, gibt es einige zusätzliche Software-Tools, um den Prozess zu beschleunigen und leichter zu gestalten. Viele dieser Applikationen sind eigentlich kostenlose Add-ons für Browser, die weitere Funktionalitäten installieren, da die gesamte Welt des Google-Hackings innerhalb eines Browsers abläuft.



Abbildung 1.5: Die Erweiterung Advanced Dork für Mozilla Firefox

Ein bemerkenswertes Add-on ist Advanced Dork für Mozilla Firefox, entwickelt von CP (erhältlich unter <https://addons.mozilla.org/en-US/firefox/addon/2144>). CP ist ebenfalls Koautor des bekannten *Google Hacking for Penetration*

Testers, Volume 2 (ISBN: 978-1-59749-176-1, Syngress). Mit Advanced Dork klicken Sie einfach mit der rechten Maustaste auf einen URL in einer Website und bekommen eine Gruppe erweiterter Google-Suchoperatoren, um sich Suchanfragen maßzuschneidern. Sie können auch auf einen markierten Textstrich rechtsklicken und den in Ihren Suchanfragen nutzen (siehe Abb. 1.5).

Best Practices

Als Firma müssen Sie davon ausgehen, dass jemand es gegen Sie verwenden wird, dass im Internet Unmengen verfügbares Material bereitstehen. Als Fingerübung sollten Sie Google-Hacking regelmäßig gegen Ihr eigenes Unternehmen einsetzen, um abschätzen zu können, welche Art Material der Öffentlichkeit im Internet zur Verfügung gestellt wird. Suchen Sie nach bestimmten Schlüsselwörtern Ihrer Firmenprodukte und schränken Sie die Resultate nur auf Ihre Domain ein, indem Sie den Operator *site:* verwenden. Suchen Sie auf Ihrer eigenen Site nach Details Ihrer Angestellten, um zu sehen, wie leicht verfügbar diese Informationen sind. Und vergessen Sie nicht, auch die archivierten Seiten der Wayback Machine von Archive.org zu durchsuchen, ob dort immer noch kritische Informationen verfügbar sind.

ZUSAMMENFASSUNG

In dem Maße, wie das Internet durch seine Trillionen von Webseiten immer weiter wächst, werden auch Einsatzbreite und Leistungsfähigkeit solcher Suchmaschinen wie Google zunehmen. Eine gut formulierte Suchanfrage kann dabei helfen, sehr exakte und spezifische Resultate für gesuchte Informationen zu finden, womit Google-Hacking fast zu einer chirurgischen Fähigkeit wird. Um darin kompetent zu werden, muss man den Einsatz der verschiedenen erweiterten Suchoperatoren zu üben, die innerhalb der Suchmaschinen wie Google, Yahoo! und Bing verfügbar sind.

WEITERE INFORMATIONEN

Google-Hacking ist zu einem sehr komplexen und äußerst effizienten Weg geworden, im Internet nach Informationen zu suchen, die nicht für die Öffentlichkeit gedacht sind. Im Zusammenhang dieses Buches konzentrierten wir uns nur auf eine sehr kleine Portion seiner Leistungsfähigkeit. Dazu gibt es noch sehr viel mehr Quellen (einige davon sind weiter unten aufgeführt), aus denen Sie lernen können, wie man in Google spezifische Begriffe für die Suche nach Material über Ihre Site zu formuliert.

- *Google Hacking for Penetration Testers, Volume 2* (ISBN: 978-1-59749-176-1, Syngress)