Proseminar

Ethische Aspekte der Informationsverarbeitung

Thema:

Phishing, Pharming, DNS Spoofing,DNS Poisoning

(15.01.07 Christian Krüger)

Phishing, Pharming, Spoofing, DNS Poisoning

- Phishing
  - Definition und Geschichte von Phishing
  - Arten von Phishing Attacken
  - Gegenmaßnahmen
  - Soziales Phishing
- DNS Spoofing und DNS Poisoning
  - Begriffsdefinition
  - Technische Grundlagen
  - Arten von DNS Attacken
  - Gegenmaßnahmen der Provider
  - Gegenmaßnahmen der Benutzer
- Pharming

Definition und Geschichte von Phishing

- Phishing stellt eine Form des Internetbetruges dar, bei dem versucht wird, von Personen vertrauliche Daten zu erlangen, um diese Daten dann später selber zu verwenden und sich als der Benutzer auszugeben.
- Die Bezeichnung Phishing wird verwendet da die Betrüger nach persönlichen Daten der Kunden im Meer des Internets fischen.
- Häufig wird dies durch gefälschte E-Mails und Webseiten aber auch Trojaner getätigt.
- Der erste dokumentierte Phishing-Versuch fand am 2. Januar 1996 in der Usenet-Newsgroup alt.online-service.america-online statt. Ziel war es an Kundenkonten von dem Internetprovider AOL zu gelangen.
- Erster dokumentierter Angriff gegen das Online Banking wurde im Juni 2001 registriert.
- Bis 2003 wurde Phishing bevorzugt per E-Mail durchgeführt. Ab 2003 wurden zahlreiche Domainnamen registriert die große Ähnlichkeit mit den Adressen bekannter Unternehmen aufwiesen.
- Ab 2004 geht man beim Phishing von organisierter Kriminalität aus die weltweit agiert.
- seit ca 2006 werden bei Phishingangriffen Scriptsprachen und Fehler in Browsern genutzt um z.B. in der Adressleiste die Original Adresse anzuzeigen obwohl man auf einer gefälschten Seite ist.
- Rechtlich ist Phishing nicht verboten, erst wenn man die Informationen nutzt die es erbracht haben ist es Betrug.

Geschichte des Phishing

- **Statistik erfasst von der APWG**
- **Anzahl der E-Mail Attacken**
  - Januar 2006 17877 Meldungen
    - Anstieg von September 2005 – 2006 um 36%
    - Anstieg von September 2006 – 2007 um 28%

- **Anzahl der Gefälschten Internetseiten**
  - Januar 2006 9715 Seiten
    - Anstieg von September 2005 – 2006 285%
    - Anstieg von September 2006 – 2007 290%

- **Betroffene Industrie zweige**
  - 2006 92% Finanzwesen, 5% ISP
  - 2007 91% Finanzwesen, 2% ISP, 3% Regierungsseiten

- **Länder aus denen die Phishing Attacken getätigt wurden**
  - 2006 52% USA, 13% China, 11% Korea, 5% Deutschland
  - 2007 28% USA, 15% China, 6% Thailand, 6% Russland, 2,8% Deutschland
  - 1.1.2008 - 14.1.2008 26% USA, 11,5% Russland, 7,5% Rumänien

Arten von Phishing Angriffen

- Generell treffen folgende Schritte auf alle Attacken zu:
  - Zu Beginn der Phishing Attacke muss der Betrüger über E-mail Adressen von potentiellen Opfern verfügen
  - Er muss eine E-Mail erstellen die dem Opfer glaubwürdig erscheint. z.B. über Ähnlichkeit mit einem tatsächlich existierendem Unternehmen
  - Am häufigsten verwendete Vorwände beziehen sich auf Aktualisierungen von Kundendaten oder eingegangene Rechnungen die storniert werden können, wenn man den Anweisungen folgt
  - Auswahl der Opfer entweder intelligent oder per Massenmail

→ **Angriffsmöglichkeit Download bösartiger Software**

- Der Kunde wird aufgefordert den Anhang der Mail zu öffnen da diese die Sicherheit der Transaktion zum Unternehmen erhöhen soll.
- Im Anhang enthalten sind aber Viren, Würmer, Spyware oder Trojaner. Diese versuchen die Kommunikation mit dem Unternehmen zu protokollieren oder die gespeicherten Zugangsdaten zu ermitteln.
- Im Anschluss werden die Daten an den Betrüger übermittelt.

Arten von Phishing Angriffen

- **Angriffsmöglichkeit Dateneingabe in E-Mails**

- Abfrage der Kontendaten und des Passwortes per E-Mail, um die Glaubwürdigkeit zu erhöhen. Es wird oft von notwendige Datenaktualisierung gesprochen.
- In den E-Mails stehen Eingabefelder zur Verfügung die ausgefüllt werden sollen und dann an den Betrüger geschickt werden sollen.

- **Angriffsmöglichkeit Verweis auf falsche Internetseite**

- In den E-Mail verweist eine Weiterleitung auf eine Internetseite des Betrügers die der Seite des vorgetäuschten Unternehmens ähnlich ist.
- Dies ist schwieriger für den Betrüger da er nicht nur eine glaubhafte E-Mail verfassen muss sondern auch eine Webseite erstellen muss.
- Dank Fehlern im Webbrowser wiegt sich das Opfer in Sicherheit. Man kann die Seite in einem Pop-up Fenster öffnen um die Adressbar abzuschalten, oder mit Javascript den Zugriff auf den Quellcode zu verbieten.

- **Erlangen von Glaubwürdigkeit der Angriffe**

- Anpassen des Erscheinungsbildes, der Absenderadresse, der Webadresse und des Textes an die eines Unternehmens
- Alle Links auf der Webseite des Betrügers führen zu der Seite des Unternehmens, außer die für sie interessanten.
- Passwörter, Logins werden gegen geprüft ob das Opfer sich nicht vertippt hat oder Scherzangaben gemacht hat.

Gegenmaßnahmen

- **Sensibilisierung der Kunden**
  - Kunden sollten E-Mails gegenüber skeptischer sein.
  - Das Unternehmen sollte gleich bleibende Layouts und Verhaltensmuster benutzen, oder Änderungen rechtzeitig bekannt geben.
  - Verzicht auf Links in E-Mails der Unternehmen
  - Unternehmen sollen keine Datenerfassung in E-Mails machen, dies ist für die Kunden sicher wenn auch für Ihn aufwendiger.

- **Verifizierungmöglichkeiten für den Kunden**
  - Unternehmen können ihre E-Mails digital Signieren, der Kunde kann dann mit dem öffentlichen Schlüssel die Echtheit prüfen.
  - Personalisierung der E-Mails
  - Sequentielle Nummerierung der E-Mail vom Unternehmen

- **Technische Hilfsmittel für den Kunden**
  - Blockieren von Phishingmails durch Spamschutz.
  - Antivirenschutz und Anti-Phishing-Toolbars um die Anhänge zu überprüfen, oder die Echtheit der Seiten.
  - Übertragung der Daten der Kunden verschlüsselt um die Datensammlung der Betrüger zu erschweren.
  - Unorthodoxe Methoden Spammer zuspammen. Blue Security hat dies von 2004 an versucht und ist im Mai 2006 daran gescheitert, da die Spammer mit Viren Rechner von Privatleuten befallen haben und von dort aus Spammten.

- **Verifizierungsmöglichkeiten für die Unternehmen**
  - Die Verifizierung sollte nicht nur am Benutzernamen festmacht werden.
  - Authentifizierungsmerkmale können sein
    - Was eine Person weiß z.B. Passwörter
    - Was eine Person besitzt z.B Token
    - Merkmale einer Person z.B. Fingerabdrücke

- **Ein-Faktor Authentifizierung**
  - Identifizierung der Kunden durch nur ein Authentifizierungsmerkmal

- **Zwei-Faktor Authentifizierung**
  - Identifizierung durch zwei Authentifizierungsmerkmal z.B. Bankautomaten Kreditkarte und PIN

- **Weitere Authentifizierungsarten**
  - Grundsätzlich, Kunden wollen durch die Vorgehensweise nicht in irgendeiner erdenklichen Art an der Kontobenutzung gehindert werden.
  - Kunden sollen nicht alle Teile zur Authentifizierung wissen. Damit können sie auch nicht alles verraten.

Gegenmaßnahmen

- **Token-Authentifizierung**
  - Kunden wissen einen Teil ihres Passwort nicht, dieser Teil des Passwort wird auf einer Hardwarekomponente gespeichert.
  - Die Hardwarekomponente generiert regelmäßig neue Passwörter.
  - Hardware Token sind z.B USB-Sticks, Smart Cards
  - Software Token werden in Online-Banking Software benutzt, diese haben den Nachteil das diese Software wenig verbreitet ist.
  - Karten Token sind sehr verbreitet und werden von den Nutzern akzeptiert, siehe Bankkarten.
- **Biometrische Authentifizierung**
  - Daten die einen Kunden eindeutig identifizieren, diese werden im Unternehmen aufgezeichnet. Um eine Charakteristik der aufgezeichneten Daten zu bestimmen gibt es Algorithmen.
  - Diese Daten können nicht als einziges Authentifizierungsmerkmal verwendet werden da es Messungenauigkeiten geben kann und minimalen Variationen.
  - Mögliche Biometrische Verfahren
    - Fingerbilderkennung ist sicher, da einzigartig aber da Personen den Fingerabdruck überall hinterlassen auch unsicher.
    - Gesichtserkennung, spezieller Iriserkennung, machbar über Webcam, aber zu viele Einflussfaktoren verschlechtern die Erkennung.
    - Spracherkennung

- **Geographische Authentifizierung**
  - viele der Phishing Attacken stammen aus fremden Ländern, siehe Statistiken.
  - Die Wahrscheinlichkeit ist hoch, das Kontenzugriffe aus dem Ausland illegal sind, diese Zugriffe werden vom System verweigert
  - Dies ist ein Nachteil für Leute die viel reisen, die also legaler weise auf ihr Konto zugreifen können.

- **Social Phishing**
- Soziales Phishing ist Phishing, bei den der Angreifer sich als eine vertrauenswürdige Person oder Firma ausgibt und auch Informationen über diese hat
- Umso mehr der Angreifer von seinem Opfer weiß, umso eher bekommt man die Informationen die man will. Wenn jemand Persönlich angeredet wird wird er auch eher antworten auf Anfragen.
- Kommen Anfragen von persönlichen Kontakten werden diese auch wahrscheinlicher gelesen als von Fremden, analog zum ILOVEYOU Virus
- Um an die persönlichen Informationen zu kommen reicht das Internet. Plattformen wie "myspace", "studivz", "facebook", "Blogs" usw. reichen um den Freundeskreis des Opfers aufzuzeichnen.

Soziales Phishing

- Testversuch einer Universität. Sie haben ihren eigenen Studenten ein normale Phishingmail geschickt oder eine Mail die auf Soziale Kontakte der Studenten basierte. Sie wurden dabei aufgefordert ein Link zu drücken, der Sie ins Universitätsnetz führte und Sie aufforderte ihre persönlichen Daten einzugeben.
- Die Studenten bei den Soziales Phishing durchgeführt wurde haben zu 72% den Link in der Mail gedrückt und ihren Universitätslogin und Password bekannt eingegeben. Bei normalen Phishing hatte die Universität nur 16% Erfolg verzeichnet.
- Erfolgreiche Eingabe der Daten hat zu keinem Ziel geführt, die Opfer sollten es später nochmal probieren. Einige Studenten haben es über 80mal probiert, ohne verdacht zu schöpfen das etwas nicht stimmte mit der Mail.
- Als über den Test aufgeklärt wurde reagierten die Studenten verärgert, gar nicht, oder verstanden den gemachten Test nicht einmal.
- Eine andere Variante des Sozial Phishing: man nutzt die Faulheit der Menschen aus. Man macht eine legale, interessante Seite an denen sich Nutzer anmelden müssen. Mit den so gesammelten Daten testet man ob die Nutzer auf bekannten Seiten wie „eBay“ , „gmx“ usw. dieselben Logins oder Passwörter haben.
- Als Schutz müsste man die Nutzer Sensibilisieren, das Sie nicht einmal Mails ihrer Freunde blind vertrauen. Sowie regelmäßig Passwörter zu ändern und auf unterschiedlichen Webseiten unterschiedliche Passwörter haben.

- **Begriffsdefinition**
  - Von DNS Spoofing ist die Rede wenn es einem Angreifer gelingt die Zuordnung zwischen einem Rechnername und der zugehörigen IP zu fälschen.
  - DNS Poisoning ist eine effektive DNS Spoofing Attacke welche Sicherheitsmängel im DNS Konzept ausnutzt, um den Cache der DNS Server überschreibt.
- **Technische Grundlagen**
  - Domain Name System (DNS) werden dazu verwendet um die Übersetzung von Domainnamen in IP-Adressen vorzunehmen.
  - Die Domains werden Hierarchisch verwaltet. Das obere Ende dieser Namens Hierarchie bilden mehrere Rootserver. Die nur die unter ihnen liegenden DNS Server kennen welche dann wiederum alle Hosts in ihren Zonen kennen.
  - Muss ein Client ein Domainname auflösen fragt dieser bei dem nächstgelegen DNS-Server nach, dieser dann beim nächst höheren bis die Domain aufgelöst ist.
  - Um die Netzlast zu reduzieren merkt sich jeder DNS-Server alle ermittelten IP-Adressen temporär in einem DNS Cache.
  - Entscheidend ist die Tatsache das jeder DNS-Server den Antworten von anderen DNS-Servern Blind vertraut. Es gibt keine Authentifizierung zwischen den Servern

Arten von DNS Attacken

- DNS-Spoofing kann zum Umleiten auf falschen Webservern verwendet werden.
- Die meisten Internet Protokolle verlassen sich sich auf Korrektheit der DNS-Server Auflösung.
- Ziel der Attacken ist, daß der DNS-Server nach dem Angriff falsche IP's an die Clients liefert.

➔ **Sicherheitsmängel in der DNS Software**

- Ein Spoofing Angriff auf die Zonendatenbank eines DNS-Servers wird mit Hilfe von Expliots durchgeführt
- Man trifft alle Nutzer eines DNS-Servers mit einem Angriff.
- Funktioniert auch gegen den Resolver auf den Clients, betrifft dann aber nur den Nutzer des Rechners.

➔ **Domain Hijacking**

- Man versucht an den Registrierungsstellen unberechtigte Änderungen existierender Domains zu beantragen, dabei wird für eine Domain der zugehörige Nameserver geändert.
- Für einige Stunden werden die Anfragen auf fremde Server umgeleitet. Bis der Fehler entdeckt wurde und behoben.

Arten von DNS Attacken

➔ **Manipulation der Hosts Datei**

- Die hosts-Datei liegen auf jedem Client und lösen die Anfragen des Clients direkt auf ohne das der Client bei einem DNS-Server nachfragen muss.
- Der Angreifer kann mit Hilfe von Viren, Würmer und Backdoors diese Datei gezielt manipulieren.
- Das Opfer verwendet dann diese, ohne bei einem DNS-Server nachzufragen.

➔ **DNS Poisoning**

- DNS Poisoning infiziert den Cache eines DNS-Server, der diesen dann wiederum gutgläubig verteilt.
- Es werden dazu nur fehlende Sicherheitsaspekte im DNS-Protokoll ausgenutzt, um Einträge in den Cache aufzunehmen z.B. Ausgabe als anderer DNS-Server dem immer zu trauen ist.

➔ **Man in the Middle**

- Wegen fehlender Authentifizierungskontrolle der DNS-Server kann man sich als Angreifer zwischen Client und Server setzten und den Datenverkehr zwischen den beiden protokollieren oder, und verändern.
- Die Opfer bekommen von einer MitM Attacke nichts mit da das Protokoll auf Hardwareebene realisiert wurde.

Gegenmaßnahmen der Provider

Verantwortlichkeit liegt bei den Providern

- **DNSSEC**
  - DNS Nachrichten werden digital signiert um ihre Authentizität und Integration zu sichern. Innerhalb des DNS Netzwerks muss dazu eine Public-Key Infrastruktur aufgebaut werden.
  - Planungen für DNSSEC laufen seit 1999, aber sind bis heute nicht flächendeckend verfügbar. Im Oktober 2005 wurde mit der schwedischen SE-Domain erstmals eine Top Level Domain digital unterschrieben. Die Verantwortlichen anderer Top Level Domains verzichteten bisher auf die Einführung von DNSSEC, da einige Problem noch nicht gelöst sind z.B. die Anfälligkeit gegen DoS-Attacken und dem DNSSEC Walking.

- **IPv6**
  - IPv6 ist der Nachfolger von IPv4. Das neue Protokoll verwendet Erweiterungsheader um die fehlenden Sicherheitsaspekte von IPv4 zu beheben.
  - Es beherrscht symmetrische und asymmetrische Verschlüsselung um die Authentizität und die Vertraulichkeit der Pakete zu wahren.
  - IPv6 ist vollständig standardisiert, aber die vollständige Umsetzung wird noch einige Jahre dauern, da Software und Hardware IPv6 unterstützen müssen.

- **Präparierte Hosts Dateien**
  - Nur Benutzer können ihre hosts Dateien ändern, um Domains hinzufügen.
  - Dies ist eine mühsame Vorgehensweise und nur bei einer geringen Anzahl von Domains praktikabel.
- **SSL-Zertifikate zur Authentifizierung**
  - Webserver nutzen SSL-Zertifikate beim Verbindungsaufbau. Der Nutzer muss dann deren Echtheit prüfen.
  - Aufgrund fehlendem Fachwissen der meisten Anwender ignorieren diese oft SSL Warnungen des Browsers.
- **Zweiseitige Authentifizierung auf Anwendungsebene**
  - SSL- Zertifikate vom Webserver zum Nutzer
  - Token vom Nutzer an den Webserver, siehe Phishing

Pharming

- Der Begriff Pharming wird momentan für Angriffe verwendet bei denen das Ziel dadrin besteht, eine Vielzahl von Benutzern eine gefälschte Webseite zu präsentieren. DNS-Spoofing bezieht sich allgemein auf das Fälschen von DNS Einträgen.
- Pharming nutzt Techniken des Spoofing um Phishing zu erzielen.
- Unterschiede zwischen Pharming und Phishing

Phishing	Pharming
Benutzer Klickt auf den Link in einer E-Mail und Landet auf dem Webserver des Angreifers	Benutzer landet auch dann Auf dem Webserver des Angreifers wenn er die Adresse im Browser eingibt
Phishing ist Erkennbar	Pharming ist nicht erkennbar
Phishing betrifft nur einzelne Nutzer die an die die E-Mail gesendet wurde	Pharming betrifft alle Nutzer eines DNS-Servers, Providers
Phishing nutzt die Naivität der Benutzer aus	Pharming nutzt die Fehler in DNS-Diensten aus

Danke Für die Aufmerksamkeit

Quellenverzeichnis

Quellenangaben

- Martin Kraus, Dominik Herrmann, Michael Lang:
  Neue Bedrohungen im Bestiarium: Pharming, Domain Spoofing und DNS Poisoning. Hausarbeit,
  Universität Regensburg 2005
  http://blog.krausmartin.de
  (17.10.2007)

- Franz Müller:
  Gegenmaßnahmen zu Phishing-Attacken mit Hilfe von Zwei-Faktor- Authentifizierung. Bakkalaureatsarbeit,
  Wirtschaftsuniversität Wien, 2006,
  http://epub.wu-wien.ac.at/
  (17.10.2007)

- Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, Filippo Menczer:
  Social Phishing,
  Indiana University, Bloomington
  http://www.indiana.edu/~phishing/
  (17.10.2007)

- Thomas Fischermann:
  Die Herren der Cyber-Zombies. Die Zeit, 18. 5. 2006, S. 23
  http://www.llnet.de/
  (17.10.2007)

Quellenverzeichnis

- Phishing Activity Trends Report December, 2005
  http://www.antiphishing.org/reports/
  (07.01.2008)
- Phishing Activity Trends Report September, 2007
  http://www.anti-phishing.org/reports/
  (07.01.2008)
- Phishing and Crimeware Map
  http://www.anti-phishing.org/
  (14.01.2008)
- Informationspapier zur Problematik des Phishing
  http://www.bitkom.org/
  (27.12.2007)
- DNSSEC
  http://wikipedia.org/
  (28.12.2007)