Man-in-the-Middle – die Zukunft des Phishings

Angriff und Verteidigung

Präsentation für den IISA-Stammtisch 8.3.2006

Philipp Schaumann
http://sicherheitskultur.at/

p.schaumann@bull.at

Agenda

- Problem: „ ... because that‘s where the money is“
- Phishing: You ain‘t see nothing yet
- Man-in-the-Middle Techniken
- E-Banking Absicherung – einstellbarer Paranoia-Level
- Konsequenzen für Mobile Computing der Firmen
- Ganz andere Lösungsansätze

Because that‘s where the money is

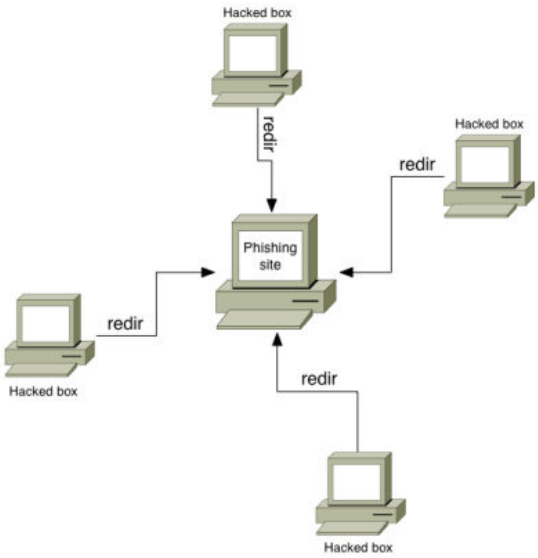
- As Willie Sutton the bank robber said when asked why he robbed banks,
  'because that's where the money is'."
- 2004: Die organisierte Kriminalität entdeckt, dass
  - der elektronische Bankraub viel einfacherer ist, als sie geglaubt hatten
  - sich der elektronische Bankraub automatisieren lässt
  - die Spezialisten, die dafür nötig sind, leicht zu finden sind
  - eine Steuerung eines solchen Bankraubs von einer tropischen Insel aus viel angenehmer und gefahrloser ist, als mit einer Pistole in der Schalterhalle zu stehen

Industrialisierung der Angriffe

- Spezialisierung und Arbeitsteilung mit gut abgestimmter zeitlicher Koordination
  - Suchen nach verwundbaren Rechnern, Handel der Listen
  - „Knacken“, infizieren und Integration in Bot-Netze
  - Vermietung/Leasing der Bot-Netze
  - Erstellen von Websites als Phishing Sites
  - „Harvesting“ von E-Mail-Adressen und online-Handel
  - Versenden von Spam
  - Durchführung von dDoS-Angriffen
  - Eintreiben von Erpressungsgeldern und Geldwäsche

Industrialisierung der Angriffe (2)

- Hochverfügbarkeit der Netze durch
  - multiple Deployment alles Komponenten
  - indirekte Adressierung über redir-Pointer



Gezielte Angriffe zwecks Industriespionage

- Myfip-B Wurm hat sehr geringe Verbreitung, aber er schickt „heim“, vermutlich Richtung China:
  - .pdf - Adobe Portable Document Format
  - .doc - Microsoft Word Document
  - .dwg - AutoCAD drawing
  - .sch - CirCAD schematic
  - .pcb - CirCAD circuit board layout
  - .dwt - AutoCAD template
  - .dwf - AutoCAD drawing
  - .max - ORCAD layout
  - .mdb - Microsoft Database

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1120855,00.html?track=NL-358&ad=525085

Phishing History
You ain‘t see nothing yet

- 2004: langsamer Start
- 2005: starke Zuwächse
- 2006: Konsolidierung
- 2007: Next Generation - MITM

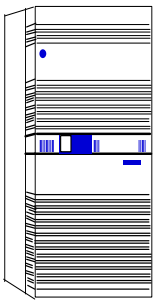
Quelle: Chaos Computer Congress Dez. 2004

Lösungen für Benutzerauthentifzierung im E-Banking

Lösung	Problematik
Passwort	**zu kurz, zu einfach, aufgeschrieben, vergessen**
One Time Passwort: TAN	**unbequem, lästig, liegen rum, sind am falschen Ort**
One Time Passwort: SMS	**nur für Handy-Besitzer, Zustellungsgarantie**
Fingerabdruck	**Kosten für Lesegerät(e), Installation, Administration**
digitales Zertifikat	**Kosten für Lesegerät(e), Installation, Administration**

Man-in-the-Middle Angriff (MITM)

Webserver



Angriffsmöglichkeiten durch MITM

- Mithören und Wiederverwenden von Passworten
- Einfügen von Links zu Trojanern in jegliche Webseiten
- Modifizieren von Überweisungsdaten
- Fortsetzung der Sitzung nach dem abgefangenen Logout des Anwenders

E-Banking Absicherung: Bruce Schneier und andere

- die Vertraulichkeit von Passworten und von Accounts wird nie zu garantieren sein
- die Überweisung ist der Schritt, der abgesichert werden muss, nicht nur das Einloggen
- Kreditkarten funktionieren praktisch ohne Authentisierung, trotzdem ist der Kreditkartenbetrug im erträglichen Umfang
  - Nilsen Report: 1992 - 15 cents pro 100$, 2004 - 5 cents pro 100$
- wer für die Schäden haftet, kümmert sich um die Absicherung

http://www.schneier.com/crypto-gram-0504.html#2
http://sicherheitskultur.at/haftung.htm#phishing

Transaktionssicherung auf 2 Ebenen

- Absicherung der Transaktionsdaten bei der Eingabe durch den Kunden
  - „Out of Band“-TAN
- Absicherung des Backend-Processing vor der entgültigen Überweisung auf das Zielkonto

Absicherung der Transaktionsdaten bei der Eingabe durch den Kunden - viele Verfahren

- Überweisung nur an Konten in der Vorlagenliste. Einrichtung eines neuen Zielkontos nur nach Freischaltung durch TAN per SMS
- Kunde gibt Überweisungsdaten ein, Bank errechnet aus Kontonummer, BLZ und Betrag eine Checksum, sendet diese per SMS. Kunde gibt Checksum ein

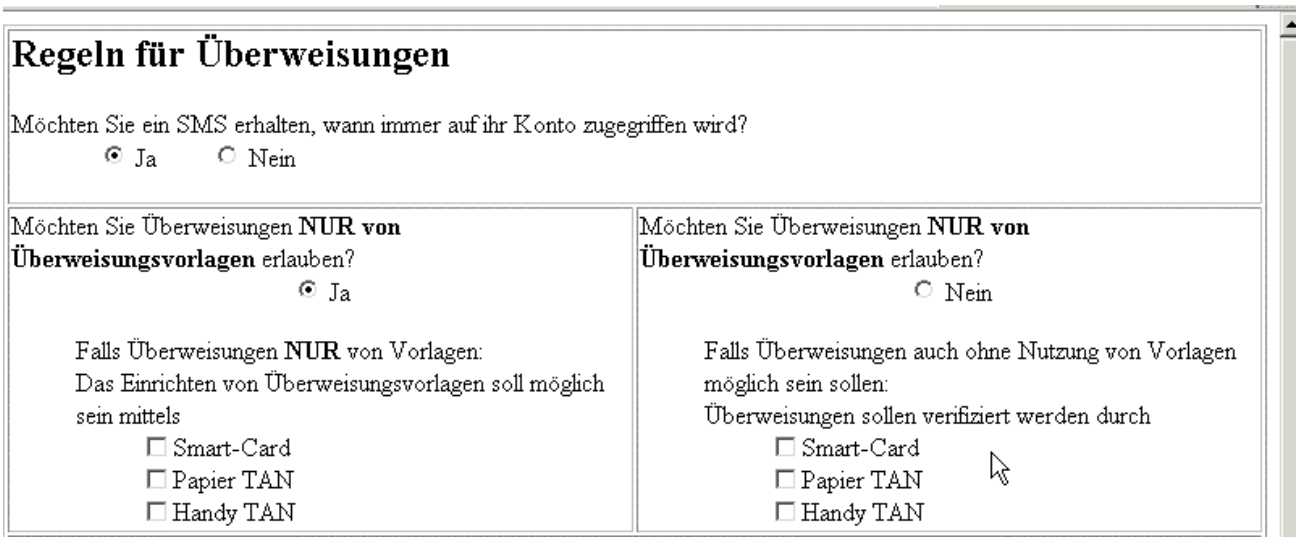
Absicherung des Backend-Processing Pattern über alle Kunden

- Überwachung von „bounced emails“ (Kundenanfragen an gefälschte Bankadresse)
- Überwachung des Webserver logs, z.B. viele referrals von 1 IP-Adresse
- viele Kunden kommen von 1 IP-Adresse
- Überweisungen von vielen Kunden an 1 Empfänger

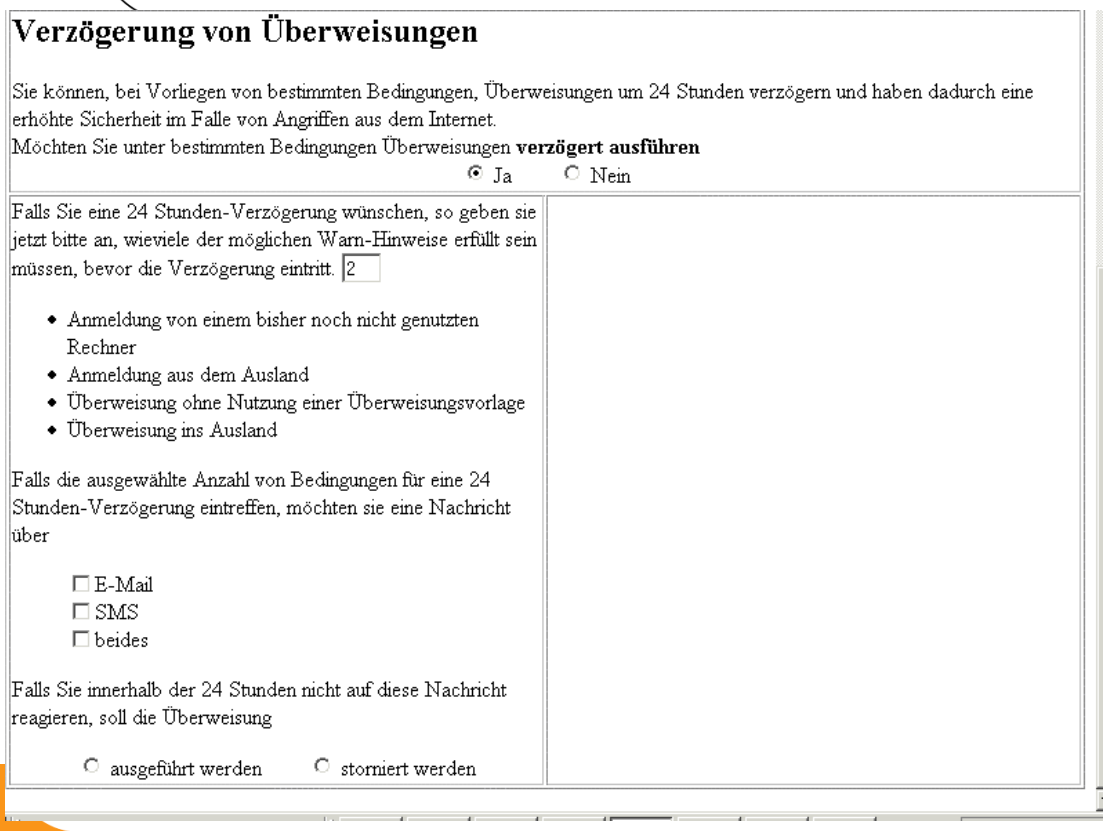
Paranoia-Level einstellbar

- Kunde wählt aus einer Liste von Sicherheitsvorkehrungen, z.B.
  - SMS-TAN,
  - verzögerte Überweisung, Verzögungszeit und -kriterien kunden-wählbar),
  - Rückfrage ab einer gewissen Höhe (out of band),
  - Email-Info für alle/gewisse Überweisungen
  - nur Überweisungen von Vorlagen,
  - Vorlagen-Einrichtung TAN gesichert,
  - Beschränkung auf bestimmte IP-Adressen
  - nur Login über Digitale Signatur

Einstellbare Paranoia (1)



Einstellbare Paranoia (2)



Mobile Geräte für Firmen – die Problemstellung

Geräte \ Verbindungen	untrusted	trusted
trusted	• Home Office mit Firmen-PCs	• Firmengeräte • im Firmen-Netz
untrusted	• Home Office mit Privat-PCs • Internetcafé • Fernwartung	• Fremdgeräte • im Firmen-Netz

Mobile Geräte für Firmen – die einzelnen Lösungen

Geräte \ Verbindungen	untrusted	trusted
trusted	VPN Zugang möglich mit sicherer Authentisierung	Verbesserung der Gerätesicherheit
untrusted	kein VPN Zugang! Präsentation ohne Datenspeicherung sichere Authentisierung	keine Fremdgeräte ins Firmen-Netz !

Sicherheit über Haftungsänderung ?

- Die Sicherheitsvorkehrungen der Kreditkarten-Unternehmen wurden drastisch verbessert, nachdem die Haftung der Kunden auf 50$ beschränkt wurde
- Theoretiker fordern, dass die Haftung für Schäden bei demjenigen liegen sollen, die die besten Möglichkeiten zur Behandlung des Risikos haben http://www.sims.berkeley.edu/~hal/people/hal/NYTimes/2000-06-01.html

Haftungsfragen

- Spyware Infection Rate von Heim-PCs:
  - 88 % of the consumer machines in the study harbored some form of unwanted program during the first quarter of 2005 **http://news.zdnet.com/2100-1009_22-5693730.html**
  - < 80 % bei Business-Desktops **http://downloadsrv.webroot.com/uploads/Webroot_SoS_Q2_05.pdf**
- Wer ist verantwortlich für den Benutzer-PC?
  - Customer vs. Bank of America: Who's to blame? **http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1062440,00.html 25 Feb 2005**

Vorschläge aus der juristischen Ecke

- Eine ausführliche Diskussion zur rechtlichen Situation und möglichen Lösungen: Douglas Barnes, Deworming the Internet. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=622364

1. Mandatory „bug bounties“ (einige 1000 $ pro gemeldete Sicherheitsschwachstelle)
2. Minimum quality standards mit Penalties bis zum erzielten Profit
3. „Lemon Law“ (Kunden bekommen Refunds for Software mit zu vielen Schwachstellen)
4. at least minimal penalties für Enduser (bzw. ISPs, um zu erreichen, dass sie strenger gegen infizierte Kunden durchgreifen können, ohne diese an die Konkurrenz zu verlieren)

Provokante Lösungsvorschläge (1) http://www.networm.org/faq/

- Make software vendors subject to product liability laws so that shipping flaws becomes much more costly to them.
- Set up a government agency to fine vendors who ship vulnerabilities. Recycle some of the money to independent bountyhunters that find new vulnerabilities and report them to the government agency.
- Require software engineers to be licensed like civil engineers. That way, guys just out of college won't be writing critical or widespread applications without a clue.

Provokante Lösungsvorschläge (2)
http://www.networm.org/faq/

- Have a government agency scan the national address space. Give fix-it tickets to people with vulnerable computers. Fine them if they haven't patched their system two weeks later.
- More research funding. In particular, worm containment research is still a very new field, and there is a lot more to be done. Funding should be allocated based on merit as determined by peer-review.
- Mandate that ISP's do not allow scanning out of their network. Also mandate egress filtering (filtering/blocking of outgoing traffic) - nur outbound-filtering „sieht“ random scans

Provokante Lösungsvorschläge (3)
http://www.networm.org/faq/

- Make sites liable for damage caused by compromised machines on their network, so they have an incentive not to get hacked.
- Mandatory disclosure laws for security incidents.
- Mandate worm containment technologies

„Most of these would make the Internet significantly safer, but would be MUCH LESS FUN than the current modus operandi (and likely less profitable for various parties also). They will not be politically feasible until the damage from worms has worsened significantly further.“

Fragen bitte

Skripten zu Sicherheitsthemen auf meiner Website:
http://sicherheitskultur.at/Eisbergprinzip.htm