Kurs „Internet-Sicherheit und Internet-Banking“

Teil 2

Sparkasse Dortmund

PING e.V.
Weiterbildungsveranstaltung
in Zusammenarbeit mit der
Sparkasse Dortmund, Medialer Vertrieb

Daniel Borgmann (PING e.V.)
Dr. med. Arthur Pranada (PING e.V.)
Karin Glodde (Sparkasse Dortmund)

Virenlawine ...

Sparkasse Dortmund

news 17.05.2005 12:08

WM-Wurm Sober.O ist Auslöser der Spam-Welle

Die Vermutung über den Zusammenhang zwischen dem **WM-Ticket-Wurm Sober.O[1]** und der **Welle von Mails mit teilweise rechtsgerichtetem Inhalt[2]** hat sich bestätigt. So stoppte Sober.O Mitte der letzten Woche seine eigene Verbreitungsroutine, um infizierte Windows-PCs zu Spam-Bots umzufunktionieren. Dazu lud er von diversen Servern ein Programm nach, das die Hersteller von Antivirensoftware Sober.P getauft haben. Sober.P startete dann am vergangenen Samstag den Versand von Mails in großem Umfang mit gefälschter Absenderadresse.

FAZ 2003-06-06
Computer
Virenlawine durch "Bugbear.B"
"Bugbear.B" ist wie sein Vorganger "Bugbear" auf Pin-Nummern von Kreditkarten und Paßwörter aus. Die neue Variante des Computervirus vereint ...

FAZ 2003-08-22
Sobig.F schlägt alle Rekorde
Der schnellste Computerwurm
HAMBURG, 21. August (dpa). Der erstmals am Dienstag in Umlauf gebrachte neue E-Mail-Wurm Sobig.F hat am Donnerstag einen Geschwindigkeitsrekord ...

FAZ 2004-06-04
Computer
Neuer PC-Wurm stiehlt Paßwörter fürs Online-Banking
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor einem neuen Computerwurm. Besonders brisant: "Korgo", so der Name des ...

FAZ 2004-06-05
Der Computerwurm Sasser legt Millionen Rechner lahm
Urheber vermutlich in Rußland / Viren werden immer schneller entwickelt / Von Holger Schmidt
FRANKFURT, 5. Mai. Stundenlange Verspätungen bei British Airways, eine lahmgelegte Küstenwache und Handbetrieb an den Postschaltern: Der Computerwurm ...

Sparkasse Dortmund

news 22.11.2005 09:23

Neuer Sober-Wurm tarnt sich als Mail des Bundeskriminalamts

Kaum ist die letzte Sober-Welle abgeklungen, tritt eine neue Variante auf den Plan und versucht, die Windows-Systeme von Anwendern zu infizieren. Anders als bei seinen **Vorgängern Sober.V/.W[1]** sind die Nachrichtentexte von Sober.Y/.Z sehr viel raffinierter. Unter anderem tarnt sich der

Übersicht

Sparkasse Dortmund

- Was ist ein Virus?
- Wie fing das alles an?
- Wie viele Viren gibt es heute eigentlich?
- Wie kann sich mein Computer infizieren?
- Können Viren Schäden anrichten?
- Wie kann ich mich schützen?

- Vorsicht! Abzocker und Betrüger im Internet
  - Phishing, Pharming, Geldwäsche

Was ist ein Virus?

Sparkasse Dortmund

Viren in der Medizin

- das Virus
  - *lat. / Sanskrit:* Schleim oder Gift
- Definition
  - obligat intrazelluläre Parasiten (= müssen in einer Zelle leben)
  - Vermehrung: nicht selbständig, nur durch Wirte
  - Eigenschaften: Verändern Erbgut

Computerviren

- Computerprogramm
  - mit Verbreitungs- und Infektionsfunktion
- Definition
  - Benötigt/infiziert andere (harmlose) Programme und nutzt diese als Wirt
  - Vermehrung: durch das Wirtsprogramm
  - Eigenschaften: Verändern Programmcode

Definition Computer-Viren, Würmer und Trojaner

Sparkasse Dortmund

- Ein Virus ist ein Programm, das sich verbreitet, indem es andere (harmlose) Programme benutzt.
- Ein Wurm ist ein Programm, das sich eigenständig verbreitet.
- Ein Trojaner ist ein Programm, das sich als harmloses Programm tarnt.

Wie fing das alles an?

Sparkasse Dortmund

- 1982
  - Der 15-jährige Rich Skentra stellt ein Programm vor, das sich auf Apple-II-Rechnern verbreitet und bei jedem 50. Mal ein Gedicht präsentiert
- 10. November 1983
  - Fred Cohen stellt erstes Computervirus vor
  - für Betriebssystem Unix
  - Teil einer Forschungsarbeit / Doktorarbeit: „Programme, die andere Programme infizieren indem sie diese verändern um möglicherweise eine verbesserte Version von sich selbst einzubauen"
- 19. Januar 1986
  - Der erste Bootsektor-Virus für das Betriebssystem MS-DOS gelangt in die Freiheit
  - Entwickelt von Basit und Amjad Alvi aus Lahore, Pakistan
  - Copyright-Hinweis auf Disketten beim Kopieren

Wie viele Viren gibt es heute eigentlich?

Sparkasse Dortmund

- Heute morgen am 28. August 2007
  - 1.036.264 bekannte Viren
    - Ca. 80.000 Hauptstämme
    - Aktuell 1.958 Viren „in the wild"

- 14.07.2007: 921.159 bekannte Viren
- 12.12.2006: 579.398 bekannte Viren
- 29.07.2006: 466.393 bekannte Viren
- 18.05.2006: 387.551 bekannte Viren
- 01.12.2005: 252.806 bekannte Viren

Wer schreibt denn nun Viren und warum?

- Der „typische Virenprogrammierer“
  - Unter 25 Jahren
  - Männlich
  - „keine Freunde“ – sucht Anerkennung im Cyberspace
  - Nutzt Phantasienamen aus Fantasyromanen
  - Es gibt auch IT-Spezialisten, die Viren programmieren

Wie kann sich mein Computer infizieren?

- Der Virus muss auf meinen PC gelangen
  - Speichermedien (z.B. CD, DVD, USB-Sticks)
  - Netzwerk (z.B. Internet)
- Der Viruscode muss ausgeführt werden
  - Programm starten
  - eMail und/oder Anhang öffnen
  - Webseite öffnen

Können Viren Schäden anrichten? Sind Viren wirklich ein Problem?

- Daten verändern (XM/Compatable)
- Daten löschen (Michelangelo)
- Daten ausspionieren (Loveletter)
- Fremdzugriff ermöglichen (Back Orifice 2000)
- Arbeit unmöglich machen (NightShade / Blaster)
- Computer zerstören (Chernobyl)

- Direkte Kosten (Telefonkosten 0190, Reparatur, Arbeitszeit, Bankkonto)
- Geschäftsschädigung
- Rufschädigung (Rassistische eMails)

Beispiel: MyDoom-Varianten

Sparkasse Dortmund

FAZ 2004-01-31
Microsoft setzt 250 000 Dollar auf "Mydoom"-Urheber aus
Kaspersky: Programmierer stammt wohl aus Rußland / Bisher rund 2,6 Milliarden Dollar Schaden
mwe./ht. MOSKAU/FRANKFURT, 30. Januar. Der Softwarekonzern Microsoft hat 250 000 Dollar Kopfgeld auf den Programmierer des E-Mail-Wurms "Mydoom" ...

FAZ 2004-07-27
Computer-Viren
Neue "MyDoom"-Version lähmt Suchmaschinen
Ein Computerwurm hat am Montag zeitweilig die Funktionen bekannter Internet-Suchmaschinen beeinträchtigt. Der Wurm - ein Nachfolger des berüchtigten ...

FAZ 2004-07-28
Internet-Wurm Mydoom legte Suchmaschine Google lahm
Vierschreiber ließ nach neuen E-Mail-Adressen suchen / Ausbreitung gestoppt
ht. FRANKFURT, 27. Juli. Die neueste Variante des Internet-Wurms Mydoom hat in den vergangenen Tagen nicht nur E-Mail-Postfächer überflutet, ...

Tagesschau 2004-07-27
Neue MyDoom-Version
Internetwurm stört Suchmaschinen

Ein so genannter Internetwurm hat Experten zufolge die Funktion von Internet-Suchmaschinenen beeinträchtigt. Der Wurm sei anscheinend auch für den zweitweiligen Ausfall der Suchmaschine Google in den USA und einigen Ländern Europas verantwortlich. "Die jüngste Version von MyDoom, die verstärkt auf Mailboxen eingelaufen ist, benutzt die Suchmaschinen, um sich weiter zu verbreiten", teilte der US-Sicherheitsforschungsdienst SANS mit. Einige Suchmaschinen-Betreiber hätten sich über eine Beeinträchtigung der Leistung ihrer Großrechner beklagt.

Der Wurm MyDoom hatte Anfang Februar bereits weltweit für Aufregung gesorgt, als er unter anderem die Web-Seiten der US-Softwarefirma SCO lahm gelegt hatte. Experten hatten am Montag eine deutliche Verlangsamung der Performance bei verschiedenen Internet-Seiten festgestellt, als deren Ursache sie Viren-Attacken oder anders geartete Angriffe auf das Internet nicht ausgeschlossen hatten.

Internet-Sicherheit und Internet-Banking

Beispiel: Rufschädigung durch Sober

Sparkasse Dortmund

Tagesschau 2004-06-11

Online-Kriminalität

Computerkriminalität: Wurm verbreitet Hetz-Mails

Von Werbemails verstopfte E-Mail-Postfächer sind inzwischen traurige Realität. Immer häufiger kommen in den letzten Monaten dazu auch massenweise Mails, die von so genannten Würmern ohne das Wissen der Computerbesitzer verschickt werden. Wer diese Mails oder darin enthaltene Anhänge öffnet, fängt sich den Wurm in der Regel ebenfalls ein und wird so zur unfreiwilligen Versendestation.

Ausländerfeindliche Botschaften

Genau dieses Prinzip haben sich jetzt die Urheber eines Wurms zunutze gemacht, um rechtsradikale Hetz-Mails zu verbreiten. Sie griffen dabei auf einen bereits bekannten Schädling zurück: Sober. Die Mails enthalten Verweise zu rechtsradikalen Webseiten sowie ausländerfeindliche und rassistische Texte, die oft wie Nachrichten oder auch Leserbriefe formuliert sind.

Die Betreffzeilen haben meist klar ausländerfeindliche Bezüge. Einige Beispiele: "Bankrott des Gesundheitswesens durch Ausländer!", "Ausländer erschleichen sich zunehmend Sozialleistungen", "MULTI-KULTI-BANDE TYRANNISIERTE MITSCHUELER" oder "ASYLANTEN BEGRABSCHTEN DEUTSCHES MAEDCHEN".

Ahnungslos werden Computerbesitzer zum Versender rechter Hetz-Mails.

Internet-Sicherheit und Internet-Banking

Wie kann ich mich schützen?

- Informiert sein (Weiterbildung)
- Keine fremden Datenträger nutzen
- Sicherheitseinstellungen (Browser) auf höchster Stufe
- Aktuelle Sicherheitsupdates installieren
- Einen Virenscanner installieren
- Immer die aktuelle Signaturen für den Virenscanner haben
- Personal Firewall installieren, bzw. eingebaute Firewall nutzen
- Weniger anfällige E-Mail-Clients und Browser verwenden
- E-Mail-Clients „sicher“ konfigurieren
- Mails von unbekannten Absendern löschen
- Keine E-Mail-Anhänge ausführen
- Gesundes Misstrauen haben

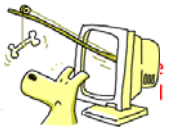
Vorsicht! Abzocker und Betrüger im Internet ...

Sparkasse Dortmund

Internet-Banking
Phishing
Geldwäsche

Internet-Sicherheit und Internet-Banking

Phishing – „Passwort Fishing“



- Gefälschte E-Mails von Betrügern, die den Nutzer verleiten sollen, Zugangsdaten sowie andere geheime Informationen freiwillig preiszugeben
  - Online-Banking: Kontonummer, PIN, TAN
  - Kreditkartendaten
  - Zugangsdaten zu Online-Shops oder anderen kostenpflichtigen Diensten

Wie gehen die „Phisher“ vor?

Sparkasse Dortmund

- Nutzung fremder Rechner zum Versand der Mail
- Spiel mit der Angst und Unsicherheit der Anwender
  - „Sicherheitsüberprüfung“
  - Neues „Sicherheitssystem“
- Absender der E-Mails ist gefälscht
  - security@[bankname].com
- E-Mail beinhaltet Erkennungsmerkmale der Bank
  - Logo / Kontaktadressen
- Sicherheitslücken in Browser/Betriebssystem werden genutzt
- Anwender wird auf gefälschte Anmeldeseite gelockt, die der echten Seite täuschend ähnlich sieht
  - Beschriftung von Links in der E-Mail stimmt nicht mit der tatsächlichen Adresse überein
  - Oft handelt es sich um „gehackte Rechner“

Beispiele für Phishing

Sparkasse Dortmund

Wie Betrüger an Ihr Geld kommen wollen ...

Wie schütze ich mich vor „Phishern“?

Sparkasse Dortmund

- Gesundes Misstrauen!
  - Keine Bank fragt unaufgefordert nach Ihren geheimen Zugangsdaten
  - Niemals die PIN/TAN an Fremde geben
  - Informieren Sie sich, welche Zugangsdaten normalerweise von der Bank abgefragt werden!
  - Fragen Sie bei ungewöhnlichen Aktivitäten lieber bei Ihrer Bank nach!
- Niemals Links in E-Mails anklicken!
  - Adressen immer von Hand eingeben oder eigene Bookmarks benutzen!
- Überprüfen Sie auf welcher Seite Sie sich befinden!
- Prüfen Sie die SSL-Zertifikate!
- Melden Sie ungewöhnliche Aktivitäten Ihrer Bank!
- Provider kann ggf. gefälschte Massen-E-Mails filtern
- Aktuelle Sicherheitsupdates einspielen!

Pharming

Sparkasse Dortmund

- Weiterentwicklung des Phishing
- Domain-Name-System (Übersetzung von www.bankname.de in eine Computeradresse) wird manipuliert
- Benutzer wird so auf eine gefälschte Seite umgeleitet (obwohl im Browser www.bankname.de steht)
- Die Betrüger setzen unzählige gefälschte Server ein (=Server-Farmen)

Demonstration Pharming

Sparkasse Dortmund

Wie Betrüger Ihnen andere Internet-Adressen vorgaukeln...

„Phisher“ werden immer erfolgreicher

Sparkasse Dortmund

Wie Betrüger um Ihre Mithilfe bitten ...

Immer höhere Schäden durch Phishing und Identitätsdiebstahl...

Sparkasse Dortmund

news 02.04.2006 11:29

USA: Jährlich 6,4 Milliarden Schaden durch Identitätsdiebstahl

In den USA sei Privatpersonen 2004 ein geschätzter Schaden von 6,4 Milliarden US-Dollar durch Indentitätsdiebstahl entstanden. Das berichtet das US-amerikanische Justizministerium in seiner gerade veröffentlichten **jährlichen Kriminalstatistik[1]**. 3,6 Millionen beziehungsweise drei Prozent aller US-amerikanischen Haushalte haben demnach alleine im ersten Halbjahr 2004 finanziellen Schaden durch Identitätsklau erlitten.

Beinahe die Hälfte dieser Fälle ging der Statistik zufolge auf Missbrauch von Kreditkartendaten zurück. Bei 25 Prozent der Opfer habe das Erschleichen von Onlinebanking-Daten eine Rolle gespielt. Für seine Statistik befragte das Department of Justice alle sechs Monate rund 42.000 US-amerikanische Haushalte. In dem seit 30 Jahren erscheinenden Report wurde jetzt erstmalig Identitätsdiebstahl als eigenständige Delikt-Kategorie aufgenommen.

(**hob[2]**/c't) (hob/c't)

Immer mehr Phishing-Opfer ...

Sparkasse Dortmund

news 14.03.2006 21:09

Phisher schwimmen in gestohlenen Geheimnummern

Nach Erkenntnissen der Arbeitsgruppe Identitätsschutz im Internet (**a-i3[1]**) suchen Phisher derzeit massiv nach Geldwäsche-Helfern, weil sie sich mit betrügerischen E-Mails mehr Geheimnummern "erarbeiten", als sie für Überweisungen von fremden Konten nutzen können. Kontoinhaber sollten keinesfalls Aufträge annehmen, die darin bestehen, Überweisungen anzunehmen und das Geld (meist abzüglich einer verlockenden Provision) weiterzuleiten.

Obacht gilt es daher nicht nur beim Umgang mit Kontoauszügen walten zu lassen, sondern etwa auch bei eBay-Verkäufen: Phisher können sich auf einfache Weise Bankdaten beschaffen, indem sie dort Waren ersteigern. Wenn beim Verkäufer eine extrem überhöhte Bezahlung eingeht, gefolgt von der Bitte, die "versehentliche" Überbezahlung per Western Union oder auf andere Weise in bar zurückzuzahlen, besteht dringender Geldwäsche-Verdacht.

In ihrem Vortrag auf dem **Heise-CeBIT-Forum [2]** berichteten Christoph Wegener und Dennis Werner

Geldwäsche-Mails

Sparkasse Dortmund

- Phisher „bitten“ inzwischen um Mithilfe, um an das erbeutete Geld zu kommen
  - Über das Internet (E-Mail) werden „Finanzagenten“ oder „Mitarbeiter/Vertriebspartner“ angeworben
  - Diese sollen das erphishte Geld ins Ausland transferieren
  - Achtung: Geldwäsche ist strafbar!
    (AG Darmstadt, Urteil vom 11.1.2006, Az. 212 Ls 360 Js 33848/05)

Geldwäsche ist strafbar!

Sparkasse Dortmund

news 19.04.2006 09:13

Phishing: Hohe Strafe gegen Finanzagenten

Das bundesweit zweite Urteil gegen einen so genannten Finanzagenten bei Phishing-Betrügereien liegt nun vor, teilte die "**Arbeitsgruppe Identitätsschutz im Internet[1]**" mit (AG Darmstadt, Urteil vom 11. 1. 2006, Az. 212 Ls 360 Js 33848/05 – **PDF-Datei[2]**).

Phishing, das "Abfischen" vertraulicher Daten wie etwa Bankzugangsdaten, Kreditkartennummern, eBay-Accounts und Ähnlichem, hat sich längst von einer irrlichternen Randerscheinung des Online-Bankings zum handfesten wirtschaftlichen Problem entwickelt. Nun rücken auch verstärkt die für die

Was kann getan werden?

Sparkasse Dortmund

Maßnahmen gegen Spam, Phishing, Pharming

Wie können Internet-Provider helfen?

Sparkasse Dortmund

- Scanning-Systeme für E-Mails
  - Viren
  - Spam
  - Phishing
- Mehrstufige Firewalls
- Information der Mitglieder/Kunden
- Weiterbildungsveranstaltungen

Informieren Sie sich...

Sparkasse Dortmund

- Arbeitsgruppe Identitätsschutz im Internet
  https://www.a-i3.org/
- Anti-Phishing Working Group
  http://www.antiphishing.org/
- Heise Security
  http://www.heise.de/security/
- Bundesamt für Sicherheit in der Informationstechnik
  http://www.bsi.de/
  http://www.bsi-fuer-buerger.de/

Neue Legitimationsmedien der Banken/Sparkassen

Sparkasse Dortmund

- iTan – indiziertes TAN-Verfahren
  - bestimmte TAN wird verlangt
- TAN-Generatoren (statisch oder dynamisch)
- Mobile TAN (via SMS)
- HBCI mit Chipkarte
  - Homebanking mit Chipkartenleser und spezieller Software

Weitere Sicherheitsmaßnahmen der Sparkassen (Banken?) (1)

Sparkasse Dortmund

- Einrichtung eines Sicherheits-Teams (S-CERT) für Sparkassen-Organisation
  - Konzentration von Know-How
  - Internationale Vernetzung
  - Hilfe bei Sicherheitsvorfällen (z. B. Phishing-Mails)
- Bündelung von Sicherheitsexperten beim Rechenzentrum
- Präventionsmaßnahmen

Weitere Sicherheitsmaßnahmen der Sparkassen (Banken?) (2)

Sparkasse Dortmund

- „Aufklärung“ unserer Kunden
  - über Sicherheitshinweise im Internet
  - durch Veranstaltungen wie diese
- denn:
  die Angriffe richten sich in der Regel auf das „schwächste Glied“ in der Kette
  => den Kunden-PC

Sicherheitsmaßnahmen der Kunden

Sparkasse Dortmund

- Wenn die während der Veranstaltung erwähnten Schutzmaßnahmen beachtet werden,

dann ist Online-Banking sicher!!!

Vielen Dank für Ihre Aufmerksamkeit!

Sparkasse Dortmund

Für Fragen stehen wir Ihnen gerne zur Verfügung!

Weitere Informationen auch in der Weiterbildungsveranstaltung „Viren, Würmer und Trojaner“

www.ping.de
Einfach mehr als nur Internet!

Kontakt

Sparkasse Dortmund

PING e.V.
Verein zur Förderung der privaten Internet Nutzung e.V.
Emil-Figge Str. 85
44227 Dortmund
Tel. 0231/9791 -0
FAX 0231/9791 -19
E-Mail: hotline@ping.de

Hotline-Zeiten:
Mittwochs 20 - 22 Uhr
Sonntags 19 - 21 Uhr

Weiterbildung:
www.ping.de/weiterbildung
weiterbildung@ping.de

Sparkasse Dortmund
Medialer Vertrieb

Freistuhl 2
44137 Dortmund
Tel. 0231/183-20220
FAX 0231/183-22298
E-Mail: info@sparkasse-dortmund.de

Erreichbarkeit:
Montags – Freitags 8 – 20 Uhr
Samstags 9 – 13 Uhr

Internet:
www.sparkasse-dortmund.de

Sie sind neugierig geworden und wollen noch mehr wissen? Dann besuchen sie auch die übrigen kostenlosen Weiterbildungsveranstaltungen des PING e.V.:

http://www.ping.de/weiterbildung/