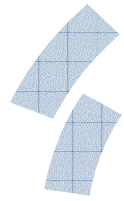


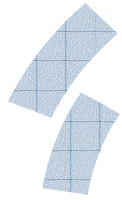
Spammer und ihre Würmer

Status Quo und
Zukunftsaussichten



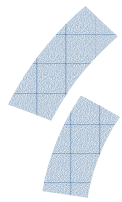
Spammer und ihre Würmer ...

- Was ist Spam und wer verschickt Spam?
- Was treibt Spammer an?
- Lohnt sich Spamming überhaupt?
- Gibt es einen Zusammenhang zwischen Viren, Würmern und Spam-Mails?
- Welche Tendenzen sind erkennbar?
- Wie kann man sich schützen

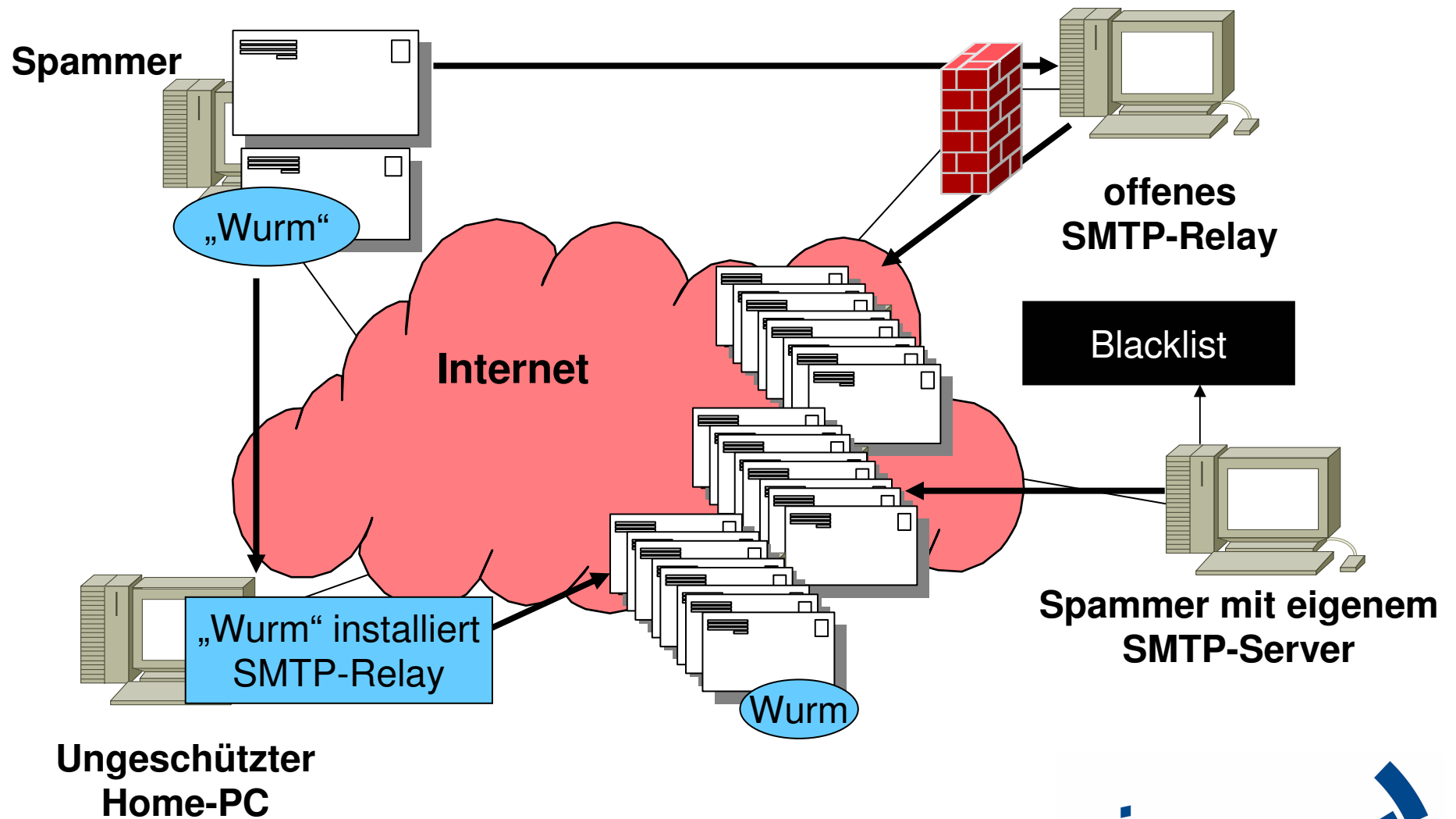


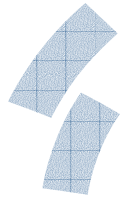
Warum überhaupt Spam durch Emails?

- Menschen sind neugierig!
 - Ungewöhnliches und Verbotenes reizt, mehr darüber herauszufinden ...
- „Email“ ist eine weit verbreitete, sehr schnelle Technologie zum Informationsaustausch
- Emails sind heute ein hervorragendes Trägermedium für schädliche Inhalte
 - Attachements mit Viren und Würmern
 - HTML-Mails mit Script-Inhalten
 - HTML-Mails mit Links zu einschlägigen Websites
 - ...



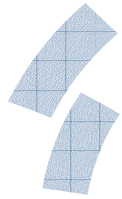
Woher kommen Spam-Mails?





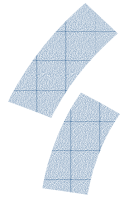
Wie tarnen sich Spammer und wie finden sie ihre „Opfer“?

- Die Absenderadresse existiert nicht und wird zufällig erzeugt
 - lucy121@hotmail.com, lucy271@hotmail.com, ...
- Eine existierende Emailadresse wird als Absenderadresse missbraucht
 - z.B. Auslesen von öffentlichen Verzeichnissen
 - Diebstahl von Mailinglisten
- Existierende Zieladressen werden missbraucht
 - z.B. Auslesen von öffentlichen Verzeichnissen
 - ...
- Die Zieladresse wird zufällig erzeugt
 - z.B. Bekannte Adressschema eines Unternehmens
 - a.miller@adomain.com, b.miller@adomain.com, c.miller@adomain.com, ...



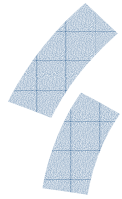
Spam durch Spam?

- Emails mit falschen Absender- oder Zieladressen erzeugen Rückmeldungen!
 - Mail mit existierender Absenderadresse an eine nicht existierende Zieladresse hat eine Unzustellbarkeitsnachricht zur Folge ...
 - Mail mit gefälschter Absenderadresse an nicht existierende Zieladresse hat eine Unzustellbarkeitsnachricht zur Folge ...
- Folge: Es wird viel unnötiger Traffic erzeugt!
- Konsequenz: Für das unnötigerweise übertragene Datenvolumen muss zusätzlich bezahlt werden und es entsteht jede Menge Arbeit, d.h. es entsteht finanzieller Schaden!



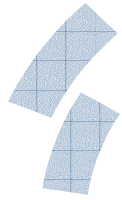
Wonach suchen Spammer?

- Webseitenbesucher, die „Hits Counter“ in die Höhe treiben
 - Viele Zugriffe bedeuten mehr Geld für Werbebanner
- Ausfindigmachen von Namen, Adressen, Kreditkarteninformationen, ...
 - Missbräuchliche Nutzung dieser Informationen bringt Geld
- Opfer für Betrügereien
 - Würden Sie zugeben, dass Sie die bestellten und bereits bezahlten „Magic Penis Enlargement Pills“ nie bekommen haben?
- Kunden, die Spam-Services nutzen wollen
 - Spammer versenden Spam für Dritte („Email-Werbeagenturen“) ...
 - Spammer verkaufen Emailadressen ...
 - Spammer verkaufen „Spam-Software“ ...



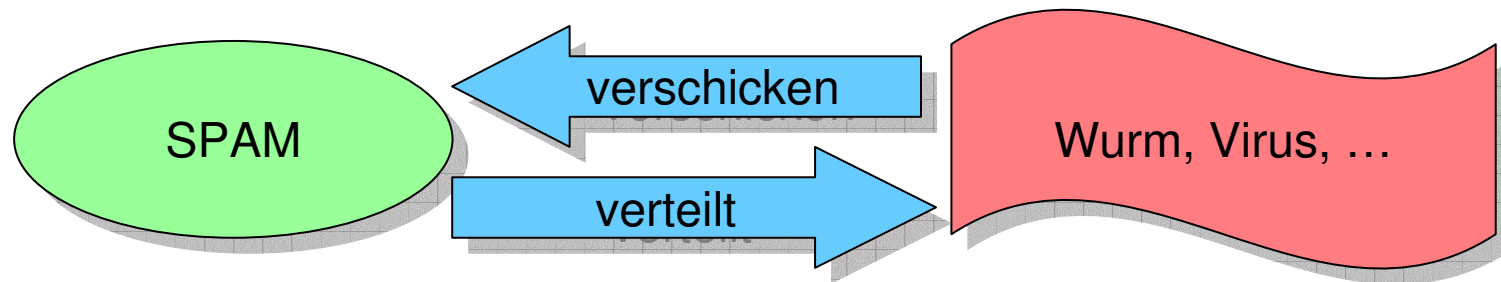
Wie kommen Spammer an das Gesuchte?

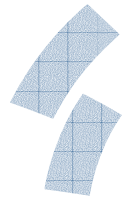
- Aufgedeckt im Februar 2004:
Trojaner als Spam-Roboter
- Dem Magazin c't ist der Nachweis gelungen,
dass Virenschreiber die Adressen von mit
Trojanern infizierten Rechnern gegen
Bezahlung an Spammer weitergeben.
Spammer nutzen die befallenen Systeme,
um unbemerkt illegal Werbemails zu
verteilen.
- Ahnungslose User fallen auf die „Angebote“
der Spammer rein.



Wie kommen Spammer an das Gesuchte?

- Schlussfolgerung:
Es besteht ein Zusammenhang zwischen der gezielten Entwicklung von Schadensroutinen, wie Viren und Würmern zur weiteren Verbreitung von Spam

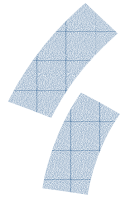




Spam heute und was kommt morgen?

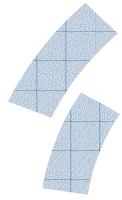
- Laut der dem Marktforschungsunternehmen Radicati Group werden heute bereits täglich mehr als 2.3 Milliarden Spam-Mails verschickt
- Für 2006 wird sich die Zahl auf schätzungsweise 15 Milliarden Spam-Mails pro Tag erhöhen!

Quelle: <http://www.radicati.com>



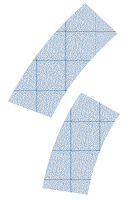
Wie kann man Spam heute eindämmen?

- Heute leider meist nur reaktiv ...
- Spam-Filter als Teil von Mailscannern
 - Erkennung an zentralem Gateway schwierig, da Merkmale von Spam meist sehr „weich“ sind
- SMTP-Gateways sicher machen
 - z.B. Prüfen, ob Absender/Empfänger existiert
- Gesetzliche Vorgaben ...
 - National vielleicht umsetzbar, aber international?



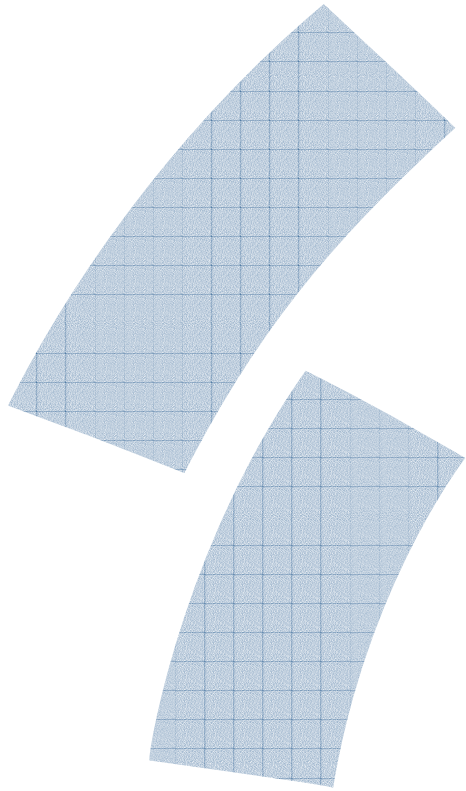
Wichtige Aspekte zur Produktauswahl von Spam-Filtern

- Wer bestimmt was Spam ist?
 - Administratoren an einem Gateway?
 - Kann der Benutzer selbst und einfach Ausnahmen definieren?
 - Wie sieht es mit dem Datenschutz aus?
- Wie bekommt der Benutzer Informationen über als Spam erkannten Mails?
- Welche Erkennungsmethode und Erkennungsrate weist das Produkt auf?
- Wo verbleiben die Spam-Mails?



Wie kann man Spam in Zukunft eindämmen?

- Heute nur reaktiv ...
- Idee: Der Sender „bezahlt“ für die Zustellung der Email
 - Microsoft z.B. arbeitet an entsprechenden Konzepten
- Emails werden nur von vertrauenswürdigen Sendern angenommen
 - „Web of Trust“
- Bessere Verfolgung von Gesetzesverstößen
 - Aber: Gesetze allein reichen nicht!
 - Ohne Anzeige ist keine Aktion der Staatsorgane möglich!



Fragen?