Der Nutzer im Fokus des Angreifers

... und was man dagegen tun kann

9. Tagung DFN-Nutzergruppe Hochschulverwaltung

12. Mai 2009, Leipzig

Klaus-Peter Kossakowski, Marcus Pattloch

(cert@dfn.de)

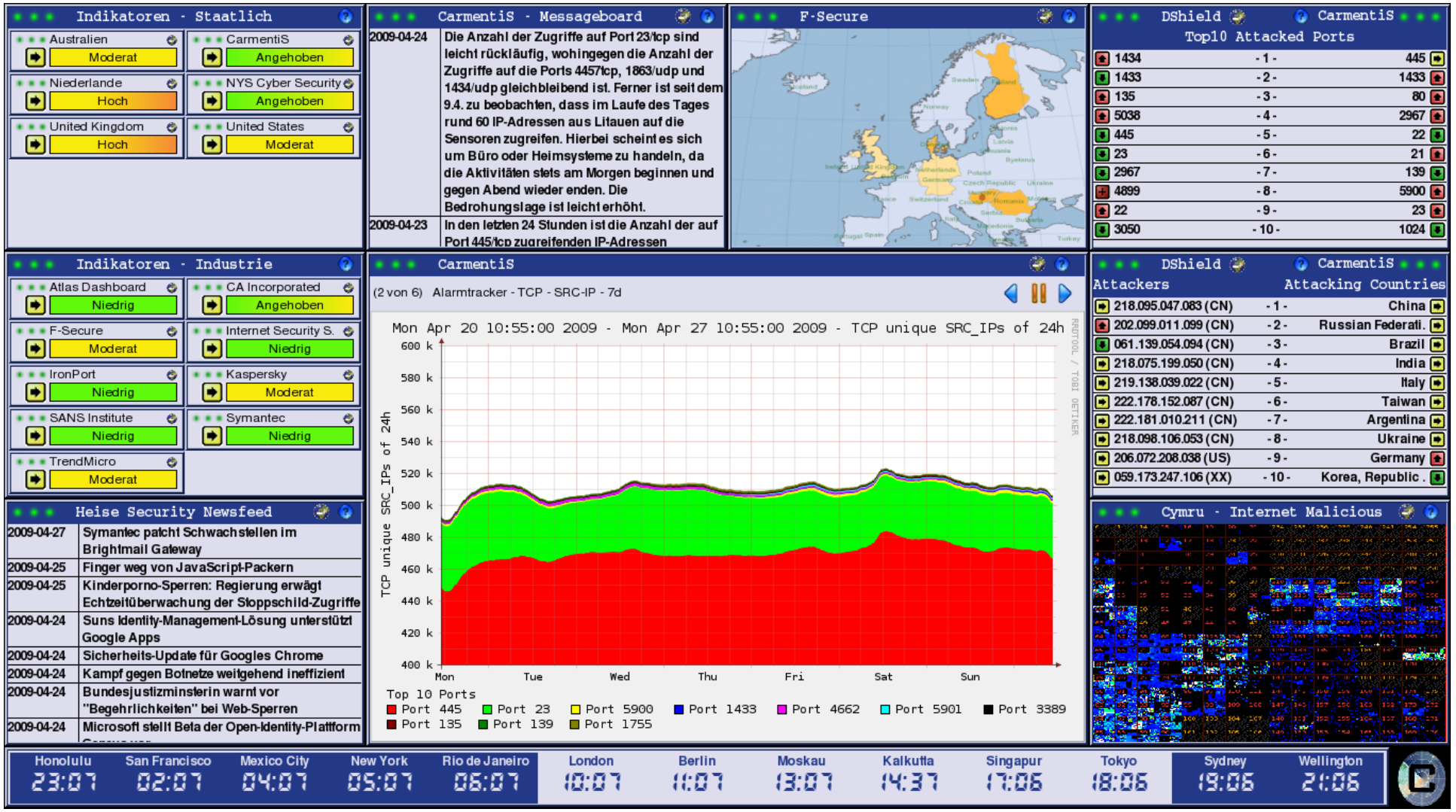
Übersicht

- Der Nutzer im Fokus des Angreifers
  - Unsicherheit im Netz
  - Conficker ABC
  - Angriffe 2.0 und 3.0
- ... und was man dagegen tun kann
  - „Einfache“ lokale Maßnahmen
  - Automatische Warnmeldungen
  - Das neue DFN-CERT Portal
- Fazit

Unsicherheit im Netz

CarmentiS Dashboard

DFN Deutsches Forschungsnetz



Immer wieder Lücken …

- **22. April 2009**
  - **Firefox 3.0.9 hat vier Lücken (mindestens)**
  - **Firefox kann zum Absturz gebracht werden**
    - Buffer Overflow, evtl. Potential für gezielte Ausnutzung gegeben
  - **Auch Thunderbird und SeaMonkey betroffen**

Immer wieder Lücken … (2)

- **24. April 2009**
  - **Chrome hat ein kritisches Problem im Zusammenhang mit dem Internet Explorer**

    JavaScript:

    ```
    document.location = \
    'chromehtml:"80 javascript: eval(
    'alert(\'JavaScript%20Code%20Execut
    ed\'); '));'
    ```

  - **Neuer Tab öffnet sich, der nicht durch Same Origin Policy geschützt ist**
    - z.B. Cookies Auslesen für Phishing-Angriffe ist populär

Conficker ABC

Microsoft RPC [MS08-067]

DFN Deutsches Forschungsnetz

- 23. Oktober 2008
  - Außer der Reihe – Patchday war schon – wird ein kritisches Update angekündigt:
    - Windows 2000 *)
    - Windows XP *)
    - Windows VISTA
    - Windows Server 2003 *)
    - Windows Server 2007
    - Windows 7 beta
  - Remote Exploit
    - *) ohne vorherige Authentisierung
  - Präparierte RPC-Requests mit Wurm-Potential

Microsoft RPC [MS08-067] (2)

- 25. Oktober 2008
  - Öffentlich verfügbarer Exploit-Code
  - Gestiegene Aktivitäten im gesamten Internet
  - Wurm Gimmiv.A wird im Internet gefunden
    - Erste Signaturen für Viren-Scanner und IDS
    - Allerdings kein Wurm, eher Trojaner, weil bisher die automatische Ausbreitung unterblieb
  - Windows Firewall nur bedingter Schutz
    - Datei- und Druckerfreigabe schaltet Ports frei!
  - Windows Dateiausführungsverhinderung bei XP und Server 2003 kein Schutz
    - Entsprechende Software nicht dafür compiliert!

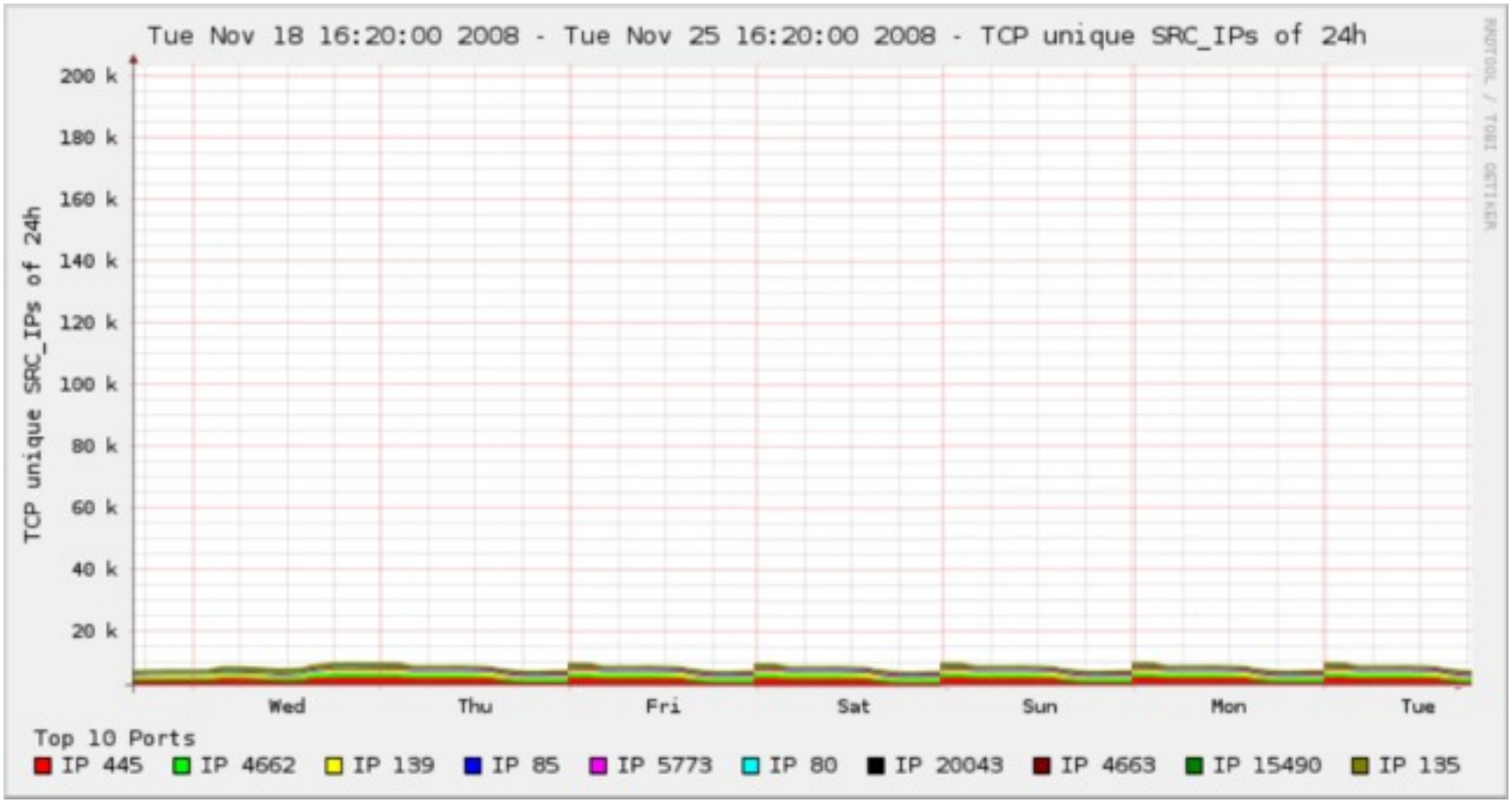
Microsoft RPC [MS08-067] (3)

- 03. November 2008
  - ISC SANS berichtet über Exploits
- 14. November 2008
  - Microsoft meldet, dass 50 verschiedene Exploits identifiziert wurden, die die Schwachstelle ausnutzen
  - Kommerzielle Angriffswerkzeuge aus China:

    http://www.avertlabs.com/research/blog \
    /index.php/2008/11/14/exploit-ms08-067 \
    -bundled-in-com mercial-malware-kit/

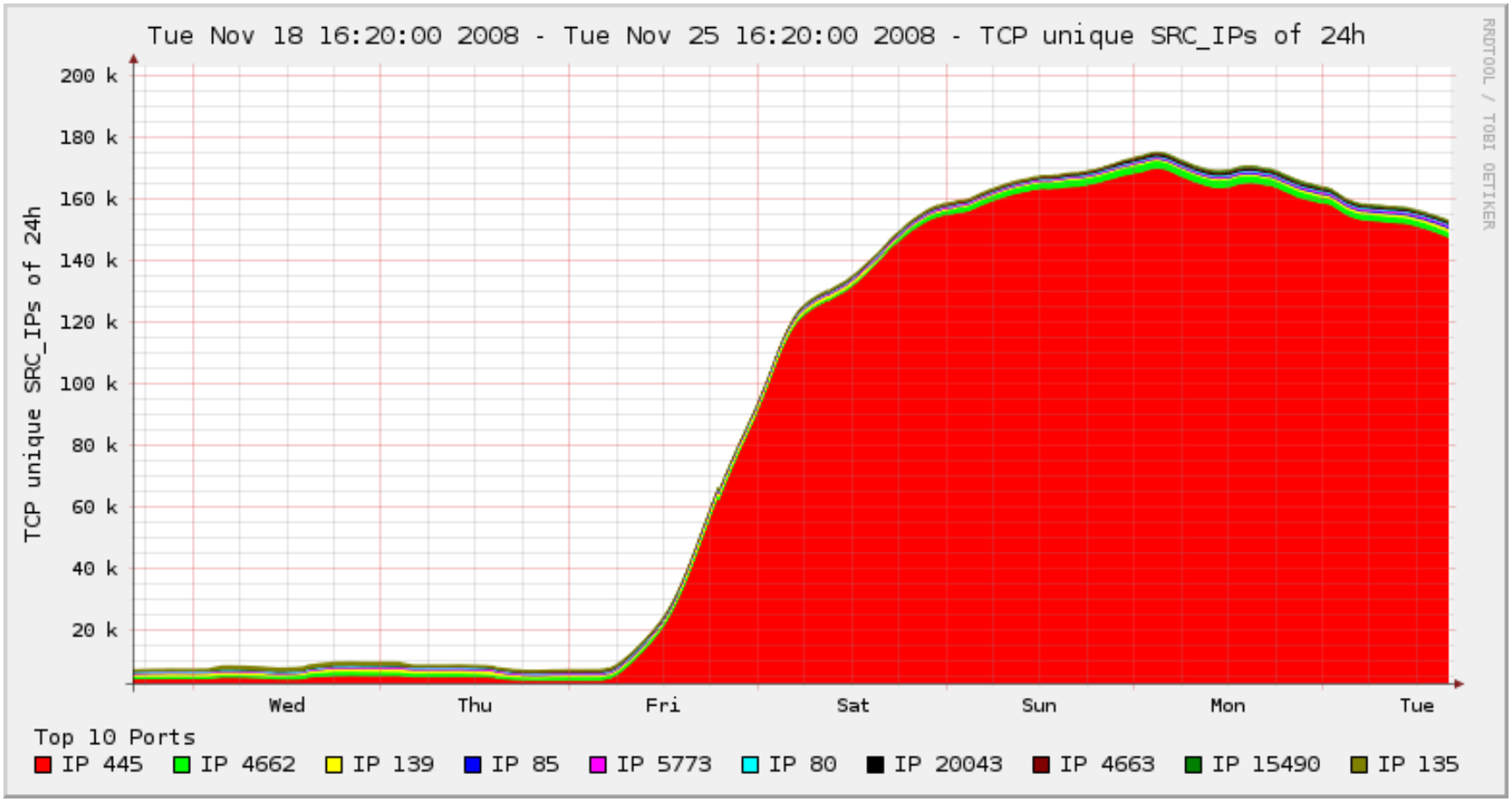
14. November 2008

- Alles ist ruhig ...

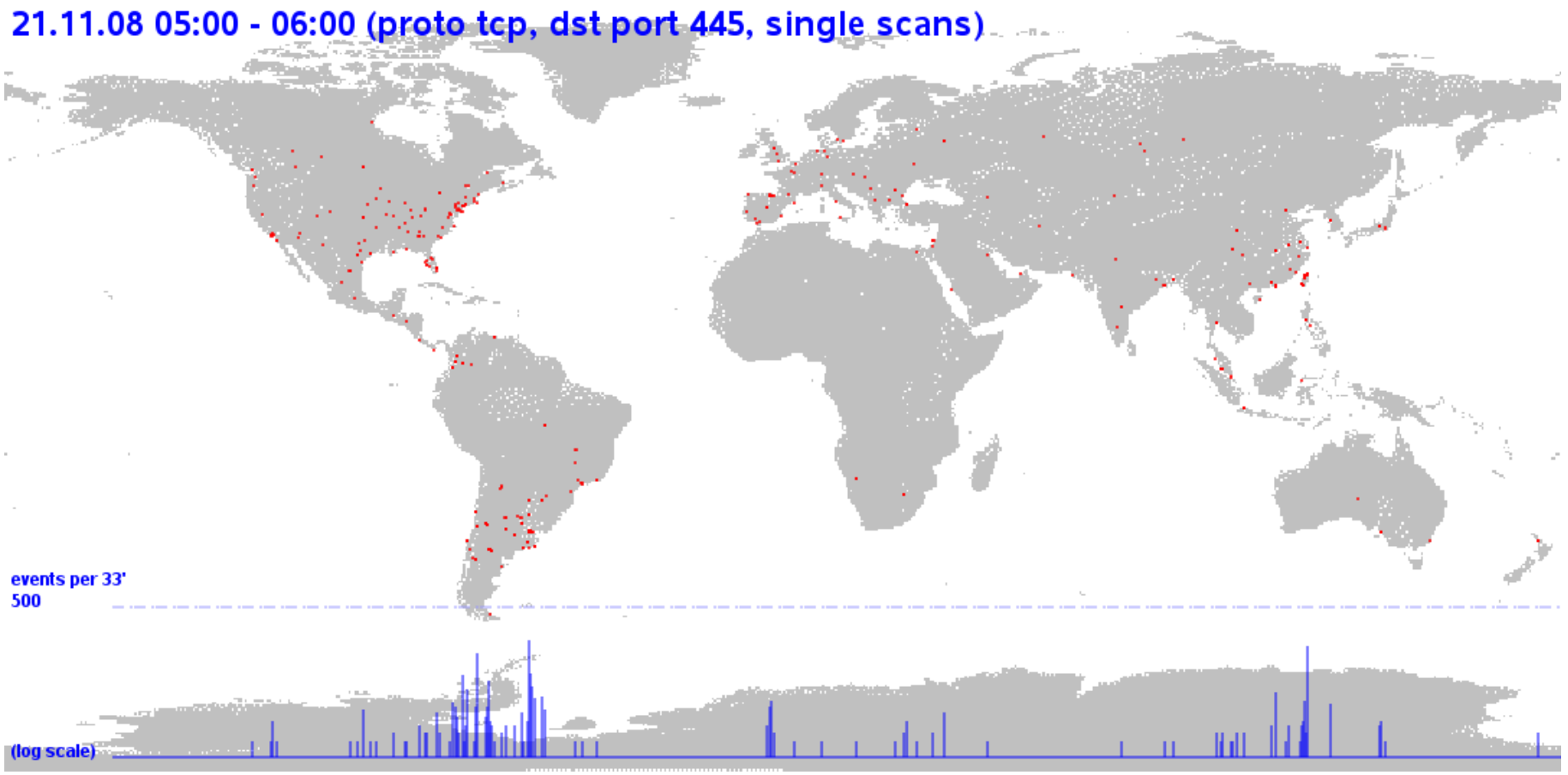


21. November 2008

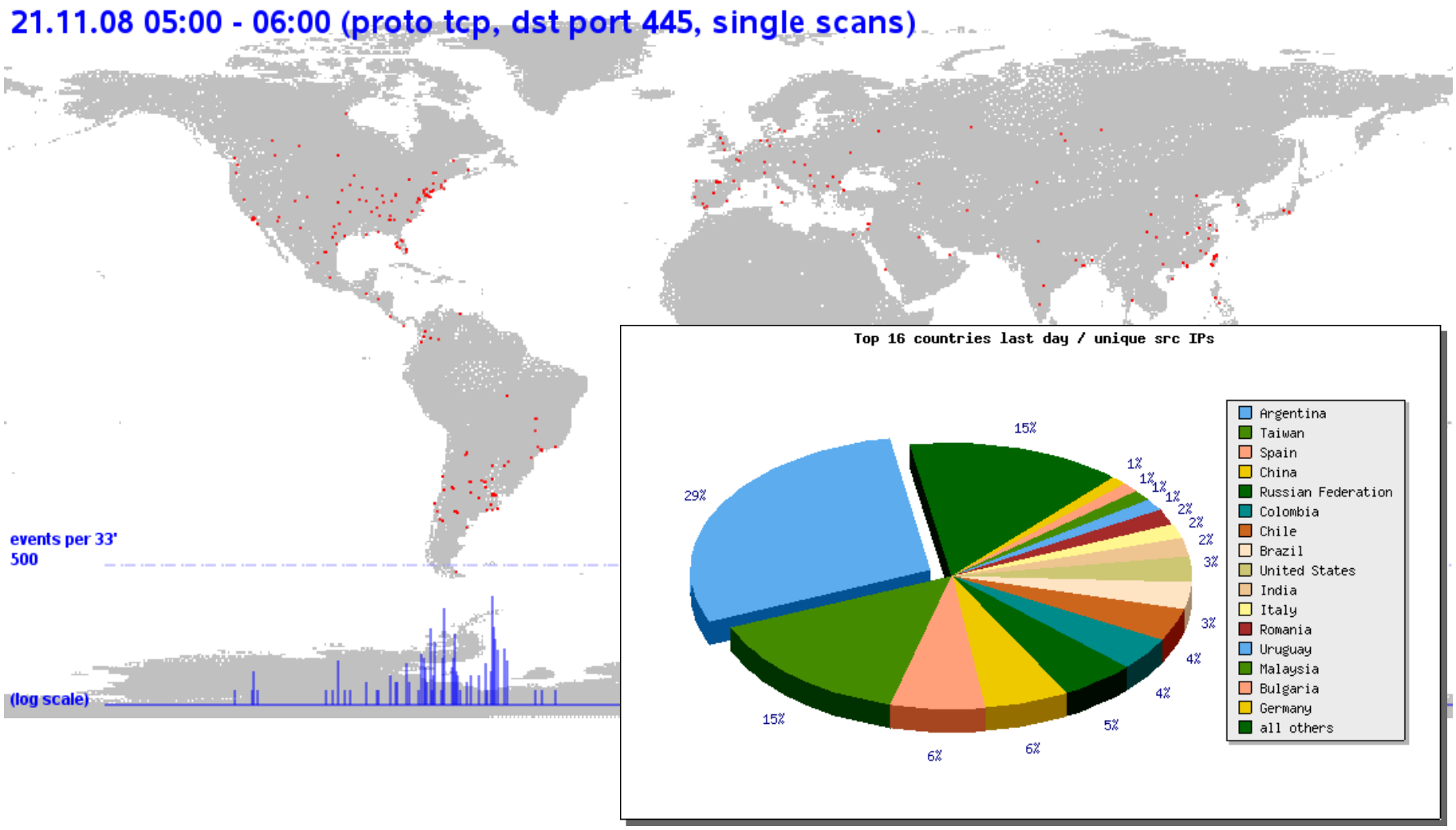
- CarmentiS stellt herausragendes Ereignis fest!



21. November 2008 (2)



21. November 2008 (3)

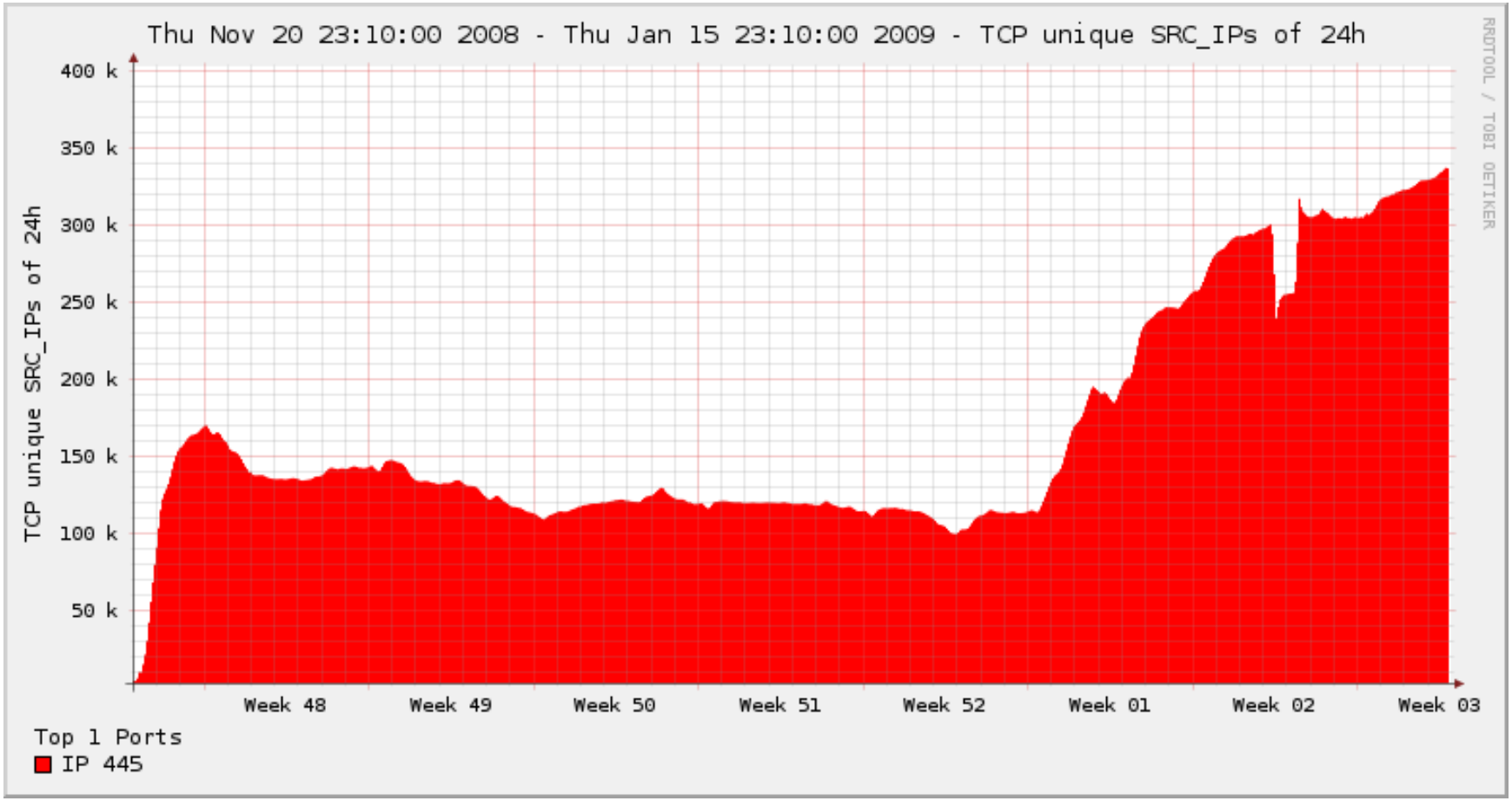


Interessante Details

- Nachladen von Software
  - Täglich werden 250 neue Domainnamen zufällig erzeugt
- Selbstkontrolle
  - Zerstört sich selbst, wenn ukrainische Rechner identifiziert werden

... und die folgenden Wochen

- Im Januar 2009 geht es dann richtig los!



Eskalation in 2009

- Nutzung von USB-Sticks und anderen externen Medien
  - Durchschlagender Erfolg!
  - Auch kritische Infrastrukturen gefährdet!
  - Medien überschlagen sich in ihren Berichten!
- AUTORUN-Problem bei Microsoft
  - Abschalten nicht ohne weiteres möglich
  - Weiteres Update (24. Januar 2009) nötig
  - Bis dahin weitere Ausbreitung
- Über 100 Varianten ...

Warum auf den Benutzer?

DFN Deutsches Forschungsnetz

- Firewalls gehören heute zum „Best Practice“
  - Seit SP2 auch bei XP eine Firewall dabei!
- Zugriffskontrollen in Netzen funktionieren dennoch auf einem „Alles oder Nichts“ Prinzip
  - Technisch auf Level 3 (IP) bzw. 4 (TCP/UDP)
  - Syntax und Semantik auf Level 7 und höher?

Warum auf den Benutzer? (2)

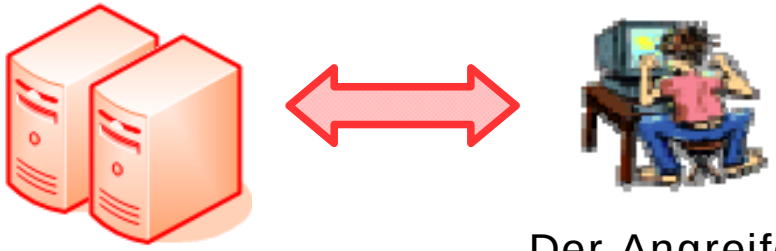
- Email geht immer!
  - Universelles, billiges, skalierbares Trägermedium
- Web geht immer!
  - Web-Browser als universelles Benutzertool im Netz überhaupt
    - Java, Javascript, ActiveX, Plugins inclusive

=> Aber bisherige Unsicherheiten und Angriffe bleiben bestehen!

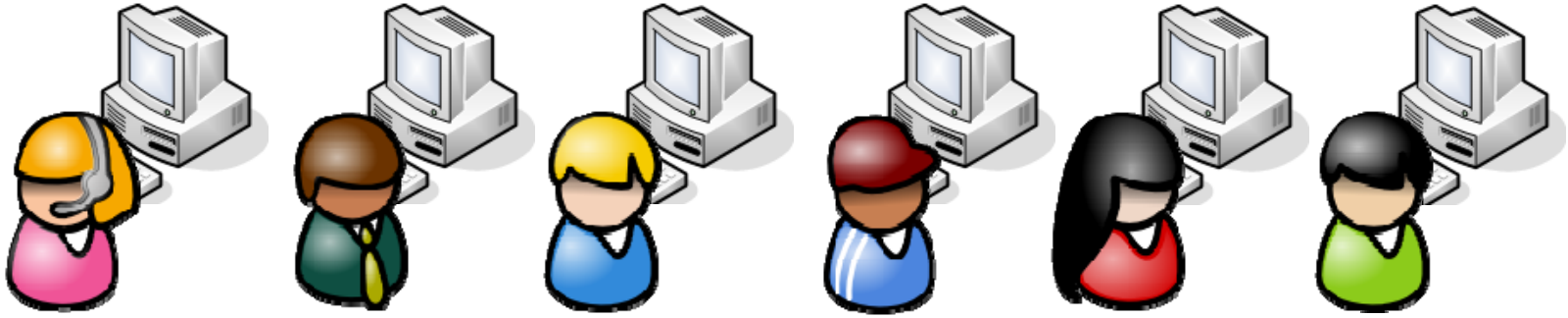
Angriffe 2.0

Attack 2.0

<- prepare



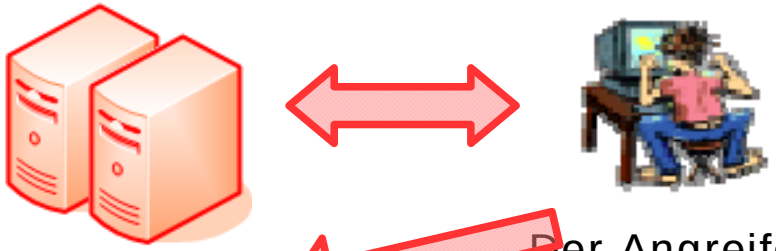
Der Angreifer richtet seine Server ein.



Web-Benutzer machen nichts anderes, als normal das Netz zu benutzen.

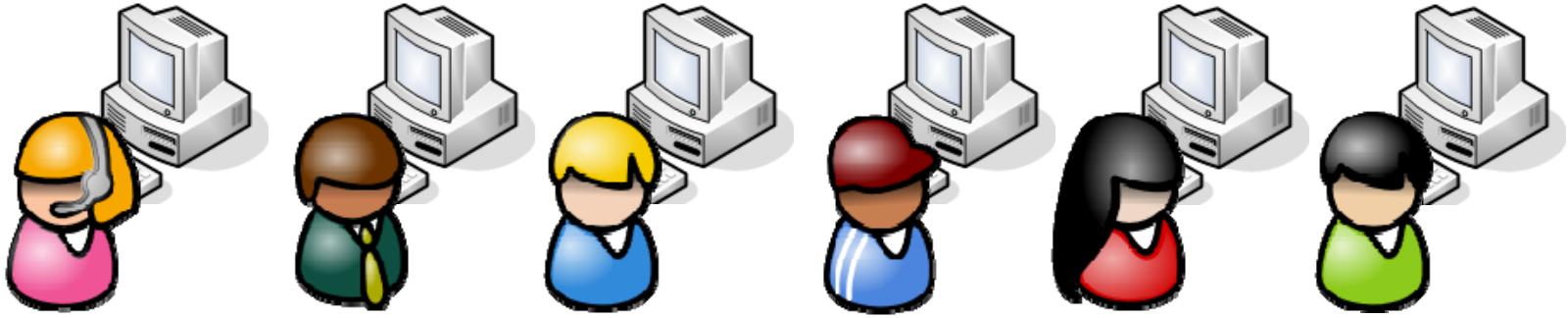
Attack 2.0 (2)

<- prepare



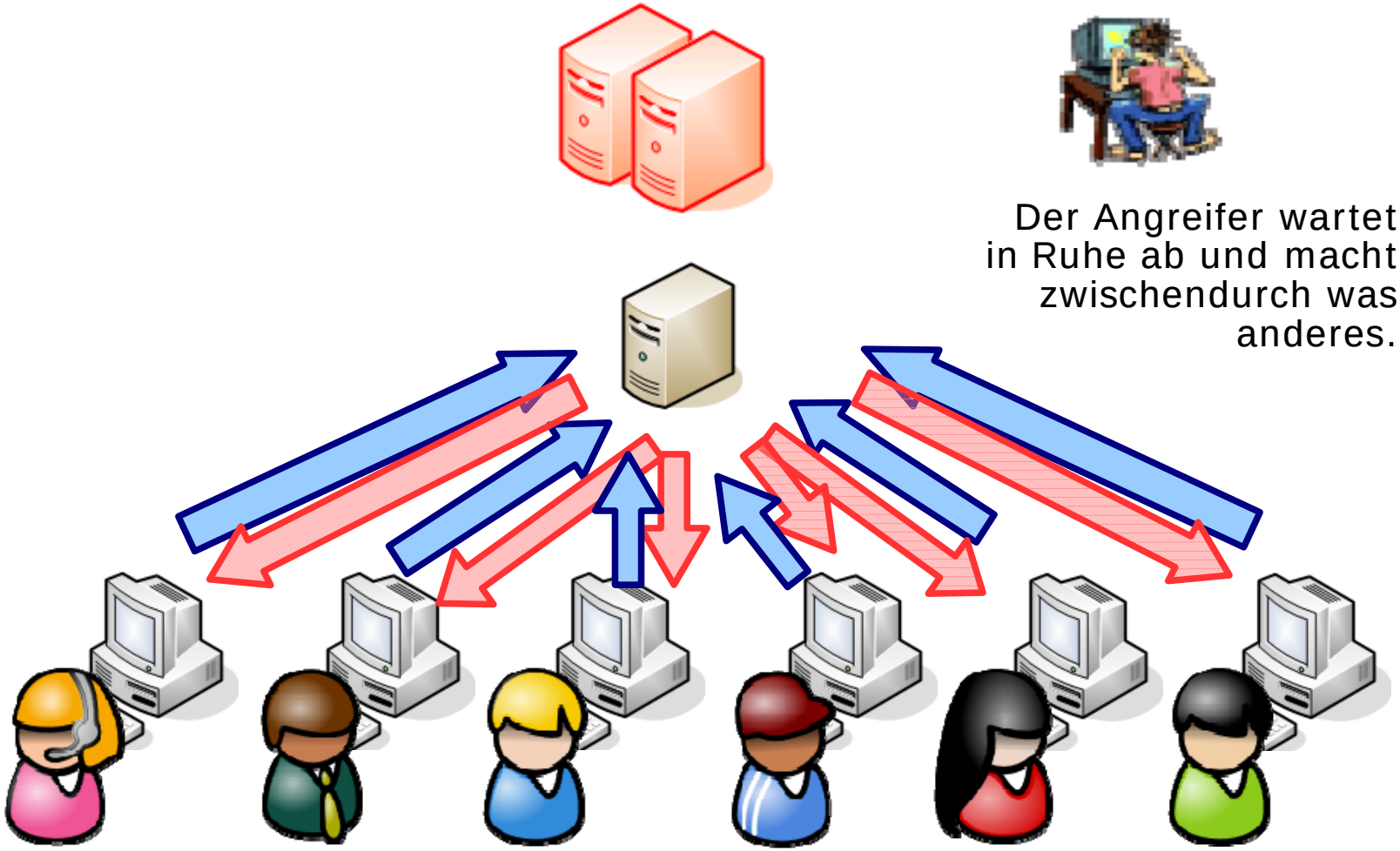
Der Angreifer richtet den Angriffsserver ein.

Der Angreifer stellt Inhalte über kontroverse Themen zusammen, bietet Bilder an, etc.



Web-Benutzer machen nichts anderes, als normal das Netz zu benutzen.

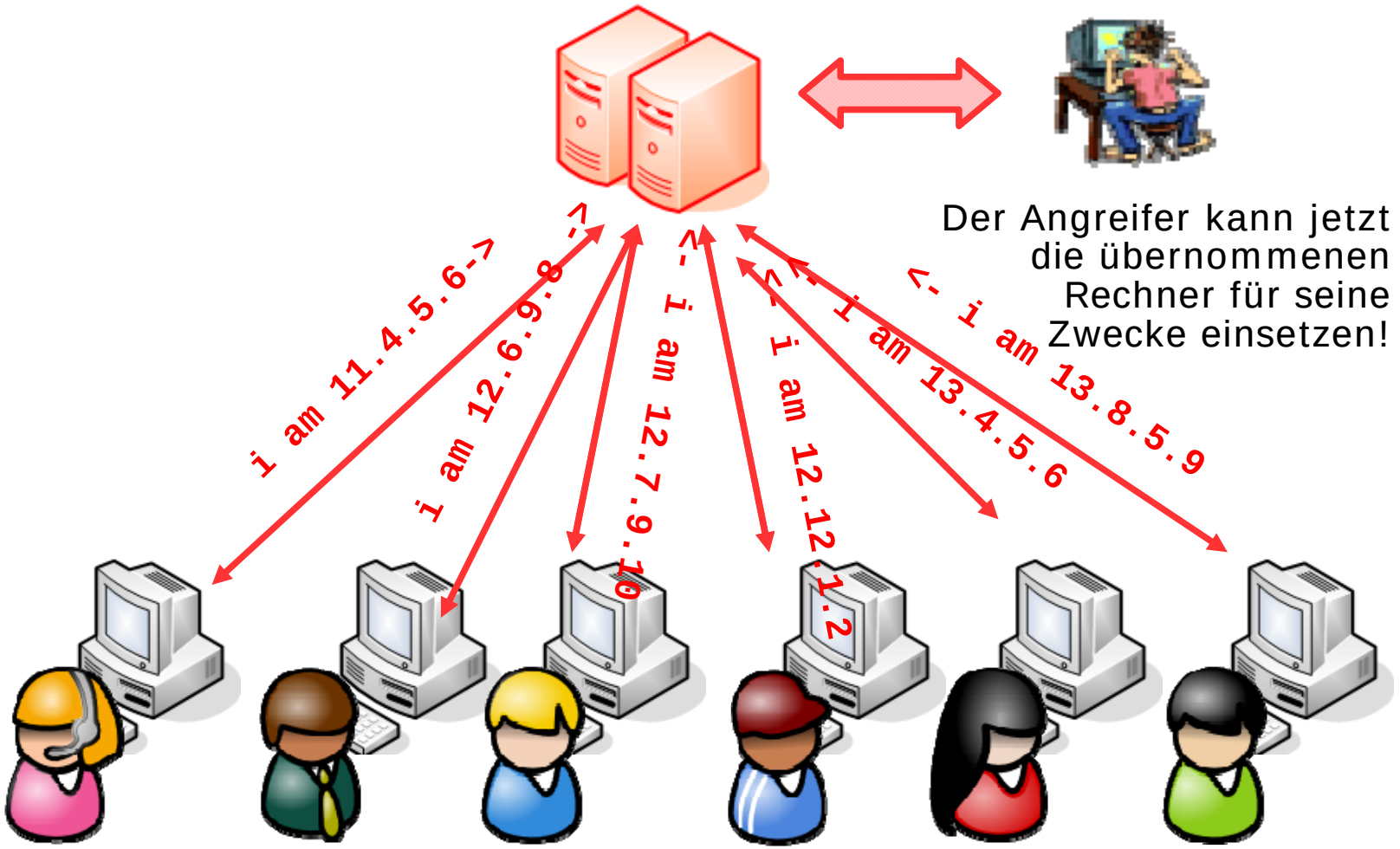
Attack 2.0 (3)



Der Angreifer wartet in Ruhe ab und macht zwischendurch was anderes.

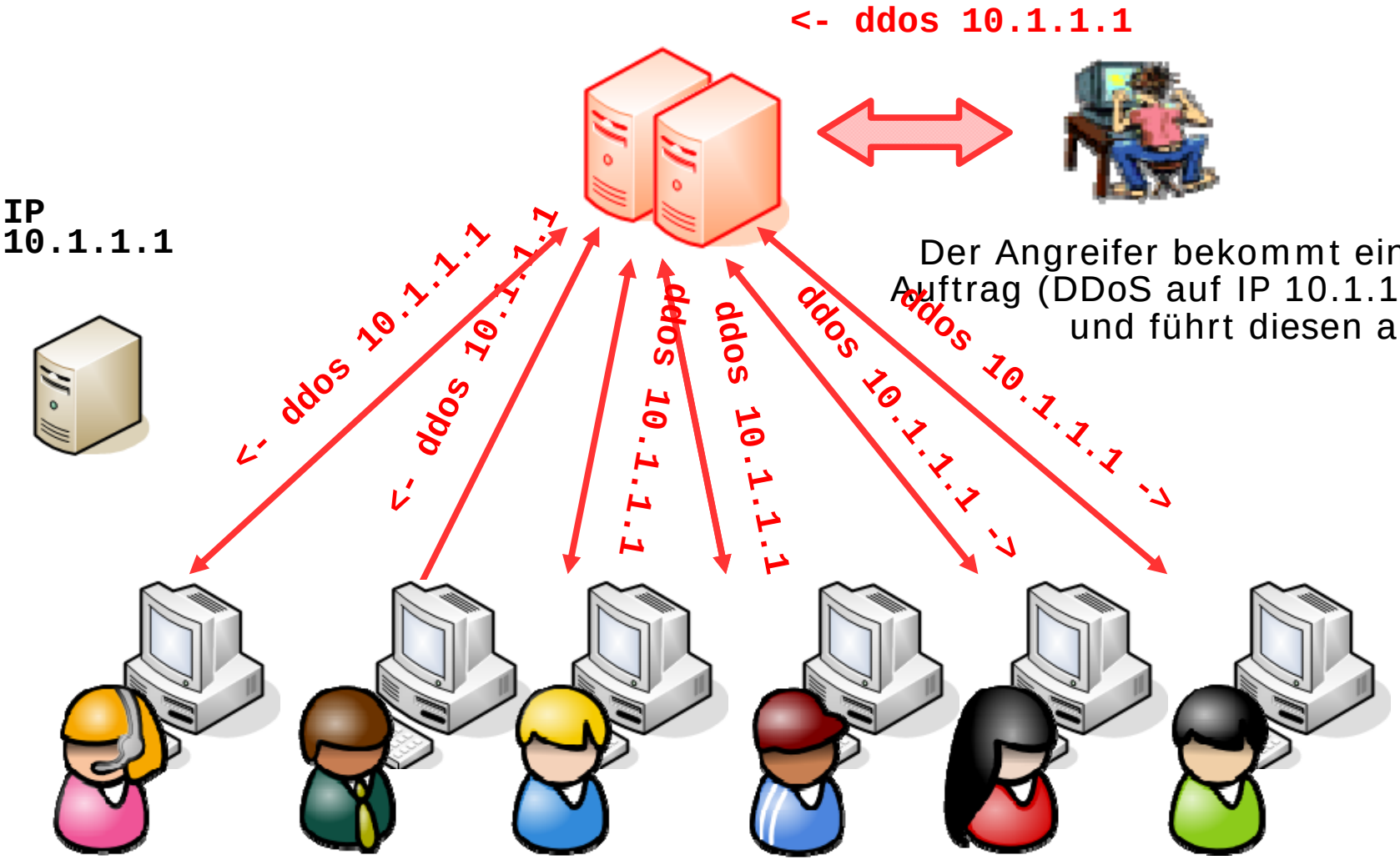
Die Web-Benutzer werden auf die vom Angreifer angebotene Web-Seite aufmerksam und nutzen diese eifrig, empfehlen die sogar weiter.

Attack 2.0 (4)



Die Web-Seiten sehen wieder langweilig aber unauffällig aus. Im Hintergrund geschieht jedoch mehr, als der Web-Benutzer merkt.

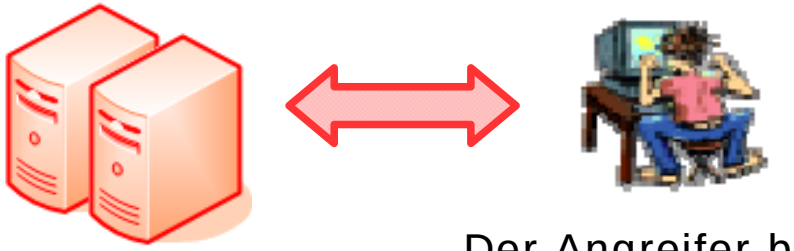
Attack 2.0 (5)



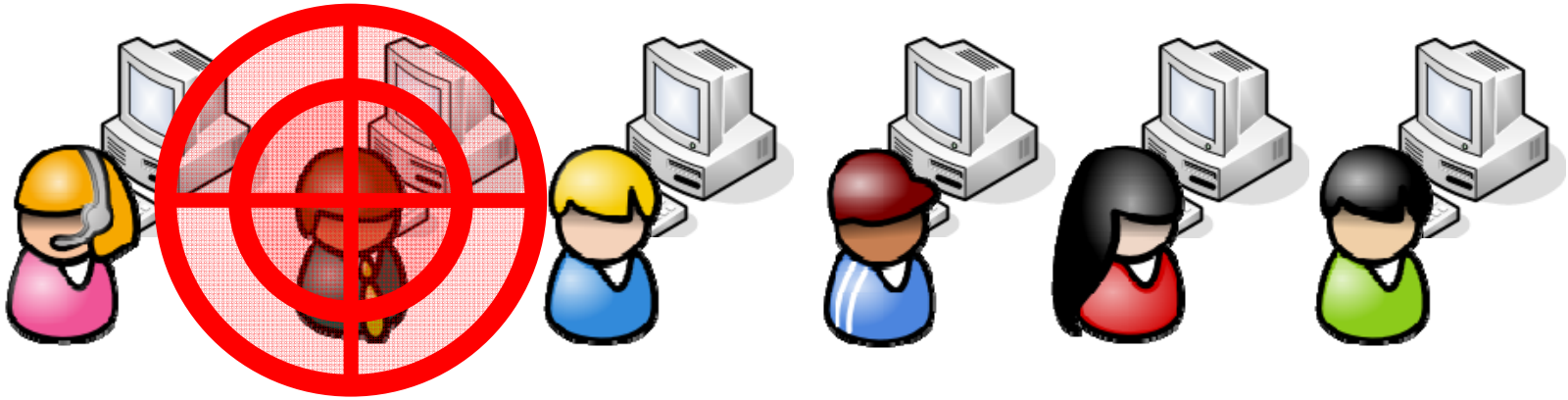
Die übernommenen Rechner erhalten “ihren” Auftrag und führen diesen in der Folge aus. Rückmeldungen erlauben ein Management des Angriffs.

Angriffe 3.0

Attack 3.0



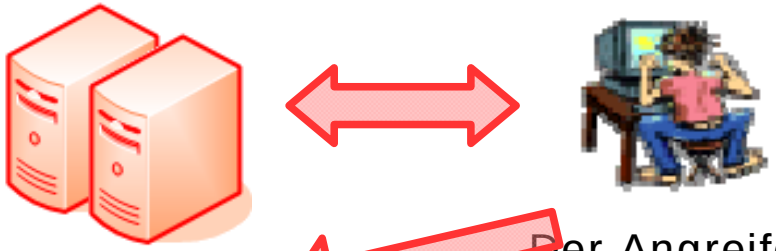
Der Angreifer bekommt ein neues Ziel.



Alle Benutzer machen nichts anderes, als normal das Netz zu benutzen.

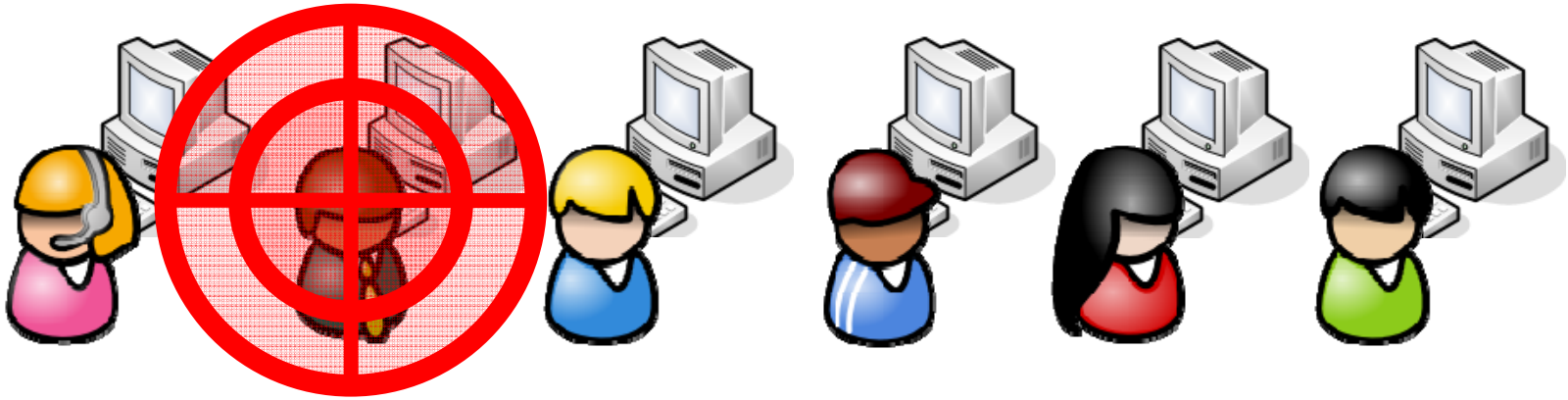
Attack 3.0 (2)

<- prepare



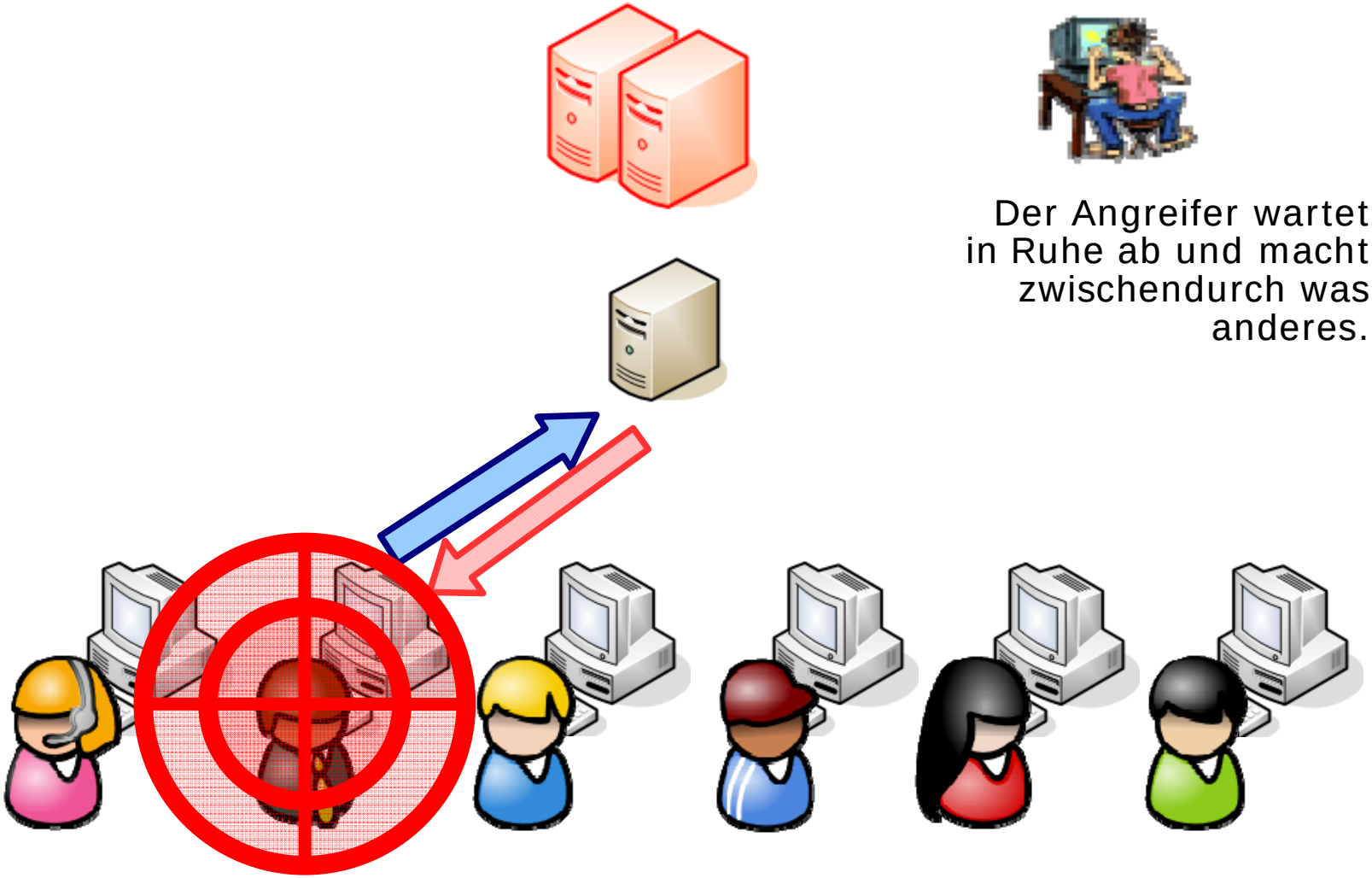
Der Angreifer richtet den Angriffsserver ein.

Der Angreifer stellt genau abgestimmte Inhalte zusammen. Dazu nutzt er quasi öffentliche Details aus sozialen Netzen!



Web-Benutzer machen nichts anderes, als normal das Netz zu benutzen.

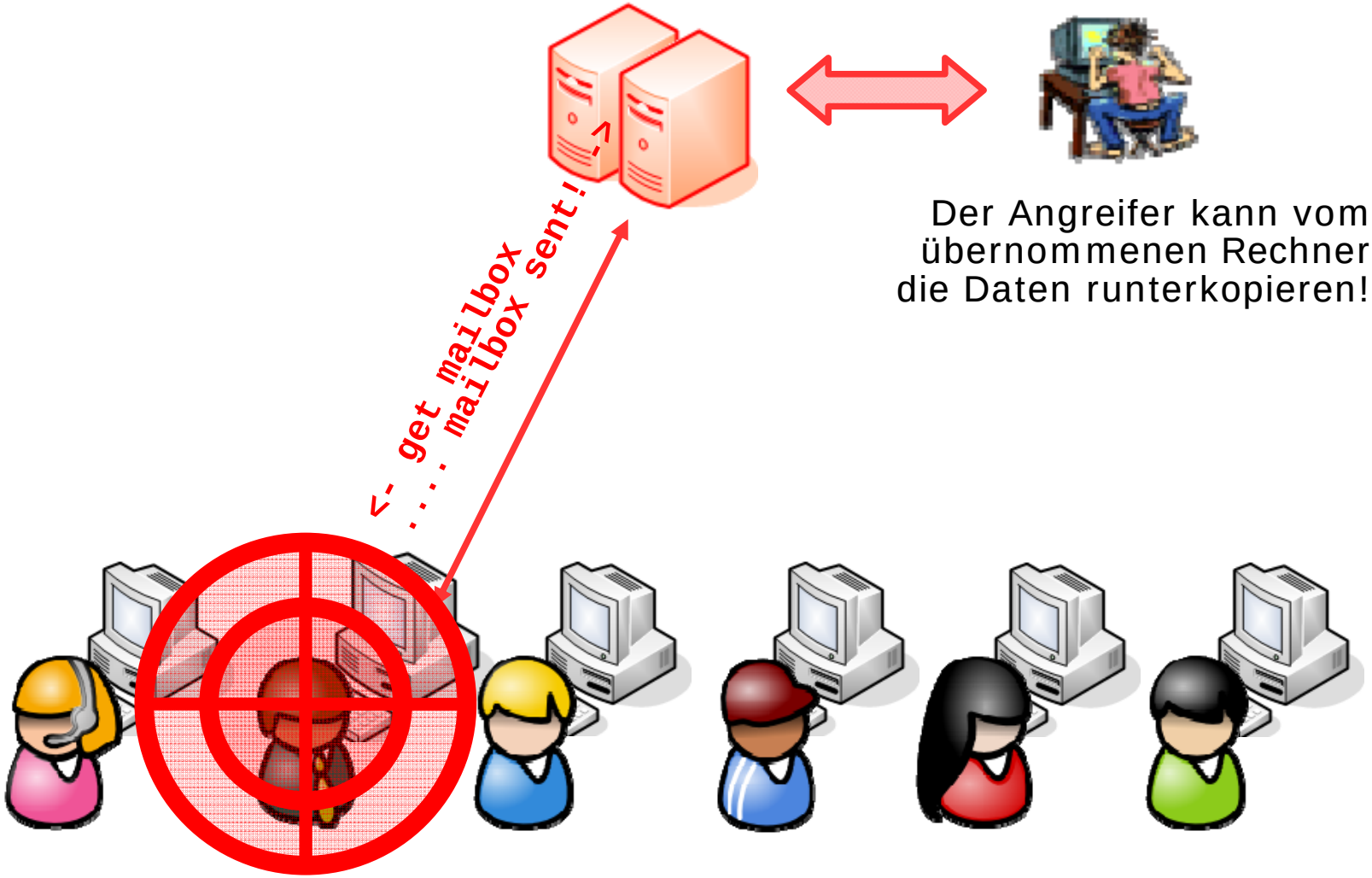
Attack 3.0 (3)



Der Angreifer wartet in Ruhe ab und macht zwischendurch was anderes.

Nur der angegriffene Nutzer greift auf den manipulierten Server zu!
Auf seinem Rechner ist danach ein Rootkit installiert.

Attack 3.0 (4)



Die Web-Seiten sehen wieder langweilig aber unauffällig aus. Im Hintergrund geschieht jedoch mehr, als der Web-Benutzer merkt.

Und nun?

DFN Deutsches Forschungsnetz

- **Browser Security Handbook**
  http://code.google.com/p/browsersec/wiki/

Test description	MSIE6	MSIE7	MSIE8	FF2	FF3	Safari	Opera	Chrome	Android
`Referer` header sent on HTTPS → HTTPS navigation?	YES	YES		YES	YES	YES	NO	YES	YES
`Referer` header sent on HTTPS → HTTP navigation?	NO	NO		NO	NO	NO	NO	NO	NO
Behavior on invalid certificates	prompt	interstitial		prompt	block	prompt	prompt	interstitial	prompt
Is EV SSL visually distinguished?	NO	YES*		NO	YES	NO	YES	YES	NO
Does mixing EV SSL and SSL turn off the EV SSL indicator?	n/a	NO		n/a	NO	n/a	NO	NO	n/a
Mixed content behavior on `<IMG>`	block	block		warn	warn	permit	permit	permit	permit
Mixed content behavior on `<SCRIPT>`	block	block		warn	warn	permit	permit	permit	permit
Mixed content behavior on stylesheets	block	block		warn	warn	permit	permit	permit	permit
Mixed content behavior on `<APPLET>`	permit	permit		permit	permit	permit	permit	permit	n/a
Mixed content behavior on `<EMBED>`	permit	permit		permit	permit	permit	permit	permit	n/a
Mixed content behavior on `<IFRAME>`	block	block		warn	warn	permit	permit	permit	permit

* On Windows XP, this is enabled only when KB931125 is installed, and browser's phishing filter functionality is enabled.

„Einfache“ lokale Maßnahmen

Motivation

- Beispiel USB-Stick
- Untersuchung in der Praxis hat gezeigt
  - wenn jemand irgendwo einen USB-Stick findet, dann würden mehr als 50% der Nutzer ihn in den eigenen Rechner stecken, um „mal zu gucken“, was drauf ist
- Frage: Wenn Sie eine Zahnbürste auf der Straße finden - würden Sie diese in Ihren Mund stecken?

Organisatorische Maßnahmen

- Nicht auf Mail-Attachments klicken
- Nicht auf „fragwürdige“ Webseiten gehen
  - schon das Anzeigen reicht aus
- Generell Vorsicht bei aktiven Inhalten
  - z.B. Excel-Makros
  - zunehmend mehr Programme: pdf, Bilder, ...
- Zwei goldene Regeln
  - Nicht alles was bunt ist, sollte installiert werden
  - Nicht alles was blinkt, sollte angeklickt werden

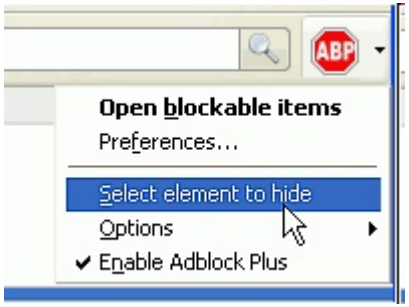
Technische Maßnahmen (1)

- Neben den üblichen Maßnahmen
  - aktueller Virenschutz, Patches einspielen, lokale Firewall, ...
- Abschalten (denn was nicht läuft, verursacht auch keine Probleme)
  - aktive Inhalte a la JavaScript so weit möglich verhindern
  - Autorun deaktivieren
    - Problem des USB-Sticks
    - wichtiger Ausbreitungsweg für Conficker

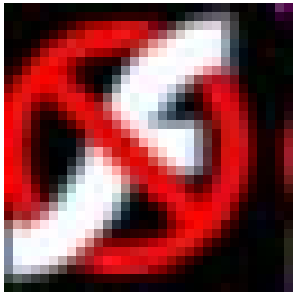
Technische Maßnahmen (2)

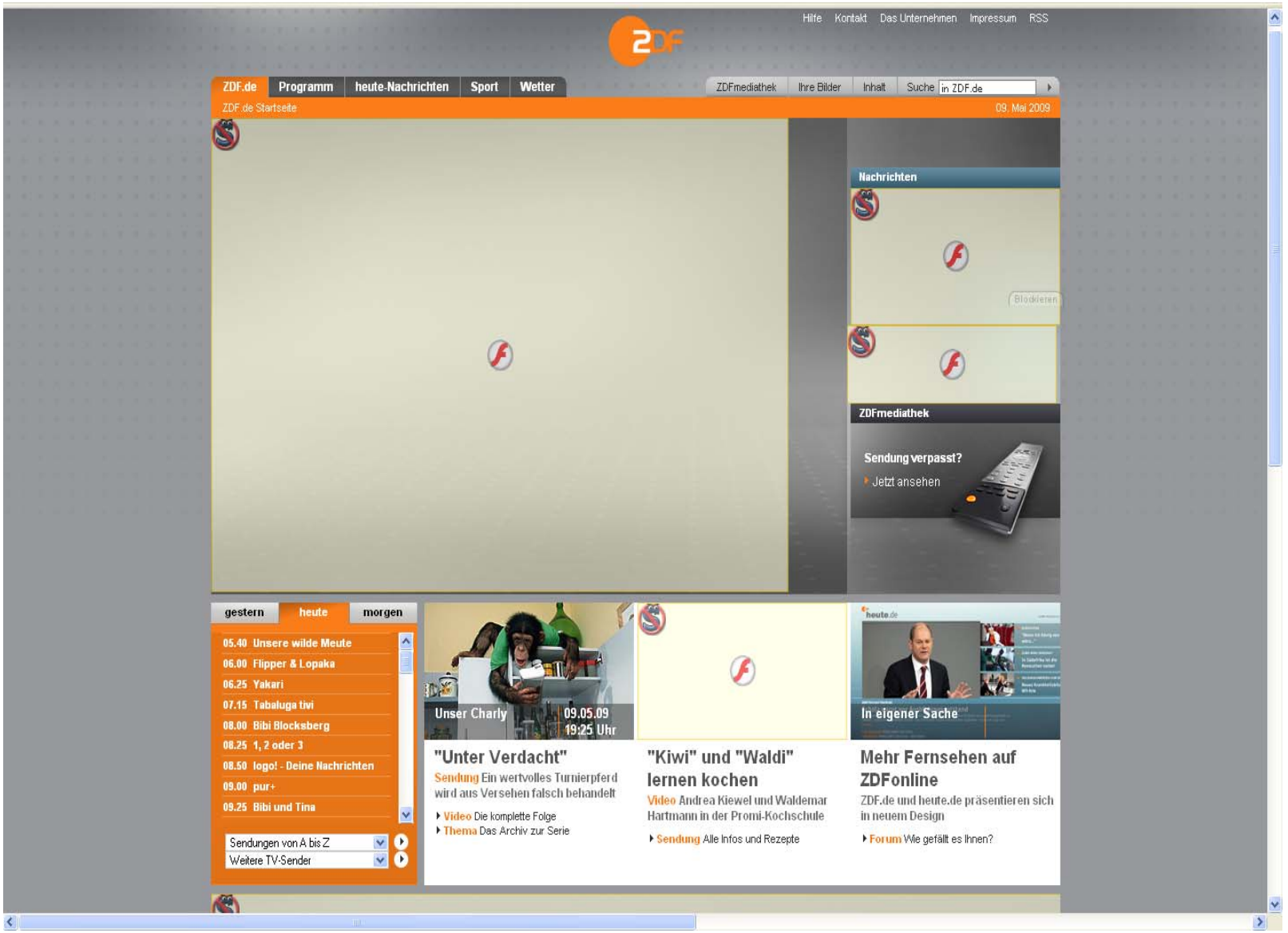
- Für Browser gibt es aus Sicht der Sicherheit sehr nützliche Erweiterungen
- NoScript

- Adblock Plus



- Flashblock




Hilfe Kontakt Das Unternehmen Impressum RSS
ZDF.de Programm heute-Nachrichten Sport Wetter
ZDFmediathek Ihre Bilder Inhalt Suche in ZDF.de
ZDF.de Startseite
09. Mai 2009
Nachrichten
Blockieren
ZDFmediathek
Sendung verpasst?
Jetzt ansehen
gestern heute morgen
05.40 Unsere wilde Meute
06.00 Flipper & Lopaka
06.25 Yakari
07.15 Tabaluga tivi
08.00 Bibi Blocksberg
08.25 1, 2 oder 3
08.50 logo! - Deine Nachrichten
09.00 pur+
09.25 Bibi und Tina
Sendungen von A bis Z
Weitere TV-Sender
Unser Charly
09.05.09
19:25 Uhr
"Unter Verdacht"
Sendung Ein wertvolles Turnierpferd wird aus Versehen falsch behandelt
Video Die komplette Folge
Thema Das Archiv zur Serie
"Kiwi" und "Waldi" lernen kochen
Video Andrea Kiewel und Waldemar Hartmann in der Promi-Kochschule
Sendung Alle Infos und Rezepte
In eigener Sache
Mehr Fernsehen auf ZDFonline
ZDF.de und heute.de präsentieren sich in neuem Design
Forum Wie gefällt es Ihnen?

Automatische Warnmeldungen
- ein Dienst des DFN-CERT -

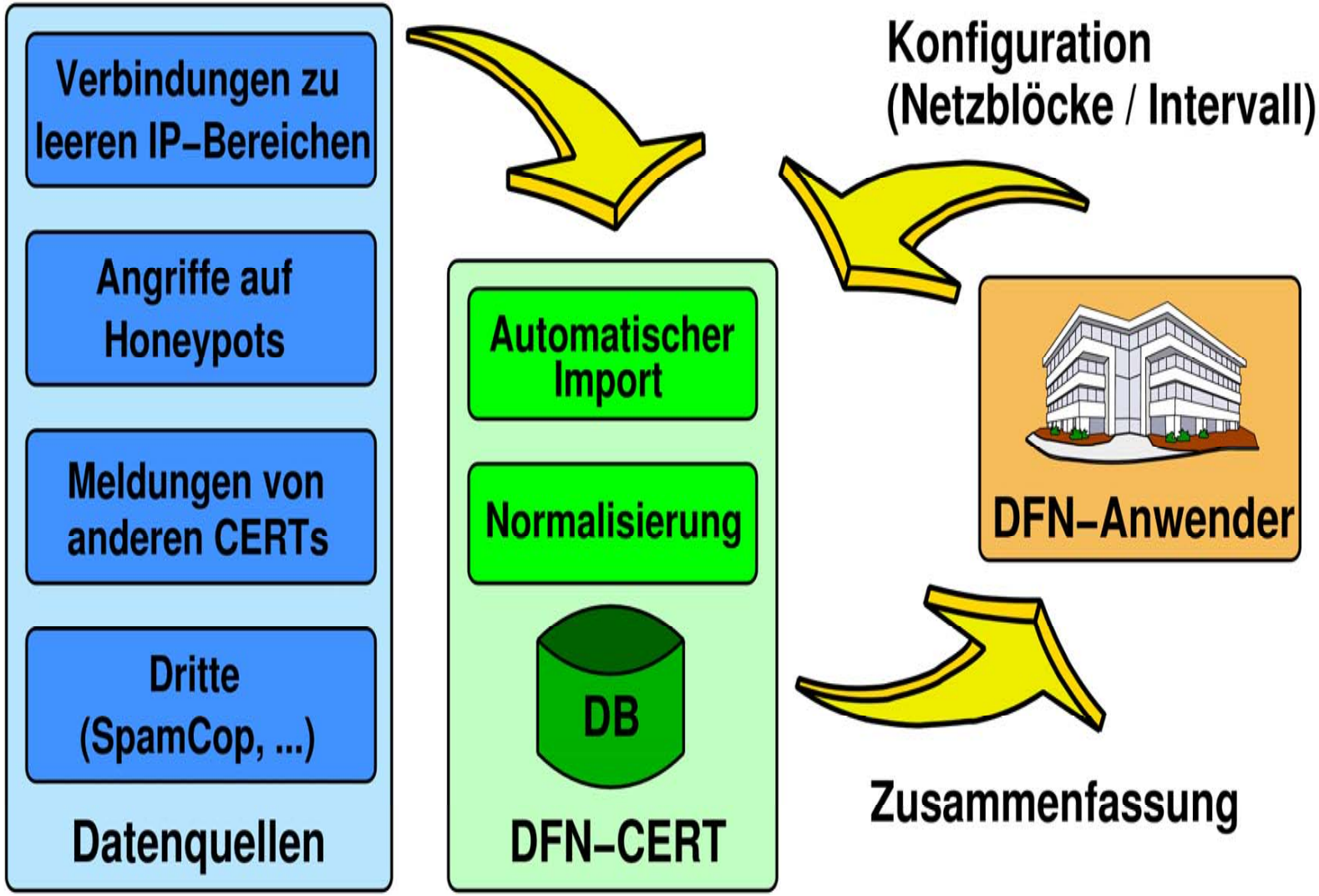
Ausgangslage

- DFN-CERT betreut Anwender bei Vorfällen
  - Anwender meldet Vorfall
  - Beratung per E-Mail / Telefon
  - Analyse des Vorfalls
  - Spuren in Logdateien sichern
  - System bereinigen
  - seit vielen Jahren etablierte Dienstleistung
- Seit einigen Jahren ändern sich die Vorfälle
  - oft von Anwendern gar nicht erkannt
  - Anzahl „nicht so kritischer“ Vorfälle steigt stark an
  - manuelle Bearbeitung nicht mehr möglich

Automatische Warnmeldungen

- Grundlegende Idee des Dienstes
  - das DFN-CERT sammelt Informationen zu möglichen Sicherheitsproblemen
    - Registrierung bei SPAM- / Security-Communities
    - Automatisierte Suche in Foren / Listen
    - Auswertung der Daten aus eigenen Sensoren
  - Überführung in einheitliches Format
  - Korrelieren und Zusammenfassen der Daten
  - Automatische Benachrichtigung betroffener DFN-Anwender

Schema des AW-Dienstes



Beispiel Warnmeldung (Teil 1)

Liebe Kolleginnen und Kollegen,

dies ist eine automatische Warnmeldung des DFN-CERT. In den letzten Tagen erhielten wir Informationen über mögliche Sicherheitsprobleme auf Systemen in ihrem Netzwerk.

IP	Meldungstyp	Zuletzt gesehen
xxx.xxx.149.100	Virus/Wurm: Stormworm	2009-01-29 09:00:01
xxx.xxx.149.33	Spam-Beschwerde	2009-01-29 19:20:03

Weitere Informationen zu den Meldungstypen finden Sie auf den Seiten des DFN-Vereins unter: www.cert.dfn.de/autowarn

Wir bearbeiten den Vorfall als DFN-CERT#33277 und stehen natürlich für Rückfragen unter <cert@dfn-cert.de> zur Verfügung.

Beispiel Warnmeldung (Teil 2)

Details zu den Meldungen pro IP:

System: xxx.xxx.149.100
Meldungstyp: Virus/Wurm: Stormworm
Zeitstempel: 2009-01-29 09:00:01 GMT+01 (Winterzeit)
Beschreibung: Das System fiel durch Such-Anfragen in Peer-2-Peer Netzwerken auf, die für die trojanische Schadsoftware StormWorm typisch sind. Evtl. ist das System infiziert.

Quellport	Zeitstempel (GMT+00)	Wahrscheinlichkeit
18239/udp	2009-01-29 08:00:01	hoch

Etwas Statistik

- DFN-Dienst „Automatische Warnmeldungen“
  - mehr als 120 Einrichtungen nehmen bisher teil
  - umfasst ca. 60% der IP-Adressen im X-WiN
  - Anwender über mehr als 10.000 Vorfälle informiert
- Wichtigste Kategorien von Vorfällen
  - übernommener Rechner ist aktiver Teil eines Botnetzes
  - übernommener Rechner versendet Spam
  - System ist mit einem Wurm/Virus verseucht

Erfahrungen

- Einrichtungen erfahren oft erst über diesen Dienst von lokalen Problemen
- Am Anfang 10-20 Vorfälle pro Tag, derzeit mehr als 100 Vorfälle / Tag (insb. Conficker)
  - d.h. jeden Tag finden wir mehr als 100 verseuchte **aktive** Rechner im DFN
  - tatsächliche Zahl weit höher (da hinter Proxy)
- Manche Einrichtungen möchten von den Problemen zunächst nichts wissen
  - enge Zusammenarbeit hilft, Hürden zu überwinden

Das neue DFN-CERT Portal

Portal (1)


DFN-CERT Portal
Automatische Warnmeldungen
DFN
Deutsches Forschungsnetz
Willkommen
Automatische Warnmeldungen
Hilfe
Übersicht
Konfiguration
Informationen
Automatische Warnmeldungen - AW-Dienst
• Bitte wählen Sie Konfiguration, um Ihre Netzbereiche für den AW-Dienst zu konfigurieren oder zu ändern. Kurze Erläuterungen zu den Möglichkeiten finden Sie als Tooltips in der Konfigurationstabelle.
• Bitte wählen Sie Informationen für weitere Informationen und eine ausführliche Anleitung zum AW-Dienst.
Impressum

Portal (2)

Name Ihrer Einrichtung: Uni Musterstadt

Netzbereiche verstecken

Folgende Netzbereiche sind nach Informationen des DFN-Vereins Ihrer Einrichtung zugeordnet:

Netzbereich	Erste Adresse	Letzte Adresse
10.0.0.0/8	10.0.0.0	10.255.255.255
192.168.0.0/16	192.168.0.0	192.168.255.255

Darin enthaltene, aber nicht Ihrer Einrichtung zugeordneten Netzbereiche:

Netzbereich	Erste Adresse	Letzte Adresse
192.168.100.0/29	192.168.100.0	192.168.100.7

Falls diese Angaben nicht zutreffend oder unvollständig sind, schicken Sie bitte eine E-Mail an cert@dfn.de.

Neue Regel einfügen

Die Regeln werden in der angegeben Reihenfolge von oben nach unten bearbeitet. Nur die erste passende Regel wird angewendet.

	Aktiv?	Netzbereiche	Intervall	Leermeldungen?	Empfänger	Betreff	
	Ja	Alle	Mo - Fr	Nein	ansprechpartner@uni-musterstadt.de		Ändern

Regel für diese IP finden

Portal (3)

Name Ihrer Einrichtung: Uni Musterstadt

Netzbereiche anzeigen

Neue Regel einfügen

Die Regeln werden in der angegeben Reihenfolge von oben nach unten bearbeitet. Nur die erste passende Regel wird angewendet.

	Aktiv?	Netzbereiche	Intervall	Leermeldungen?	Empfänger	Betreff	
⬇	Ja	192.168.222.222	Mo, Mi, Fr	Ja	ap300@uni-musterstadt.de	ap300	Ändern Löschen
⬆ ⬇	Ja	192.168.0.0/24	Mo	Nein	ap200@uni-musterstadt.de	ap200	Ändern Löschen
⬆	Ja	192.168.123.17 - 192.168.123.47 192.168.0.0/23	Mo - Fr	Nein	ap100@uni-musterstadt.de		Ändern Löschen
	Ja	**Alle übrigen**	**Mo - Fr**	**Nein**	**ansprechpartner@uni-musterstadt.de**		Ändern

Regel für diese IP finden

Fazit

Fazit

- Risiken nehmen zu
  - Software bietet immer neue (unnütze) Funktionen
  - Kenntnisstand der Nutzer wächst nicht mit
- Empfehlungen
  - Schulung der Nutzer (erst denken, dann klicken; USB-Stick; nicht frustrieren lassen)
  - „zwingen“ Sie Nutzer zu ihrem Glück (z.B. kein Autorun, Extensions im Browser)
  - Nutzung des DFN-CERT Portals und des AW-Dienstes (Mail an: cert@dfn.de)