



FRÜHERKENNUNG GEHACKTER WEBSEITEN.



Innovative IT Sicherheit aus Oberösterreich.

- Entwickelt seit mehr als vier Jahren nimbusec Webseitenwächter
- Internationale Partner im Webhosting Bereich von Finnland bis in die USA
- Enterprise-Kunden aus unterschiedlichen Wirtschaftssektoren (Finanz, Konsumgüter, Bildung, Politik, usw.)
- Mehrfach ausgezeichnet: futurezone.at Start-Up Preis 2014, Jungunternehmerpreis 2015 & Constantinus IT Preis 2015



Alexander Mitter
Geschäftsführung

Die Geschäftsmodelle der Hacker

Warum werden Webseiten angegriffen?

Global

- “Cybercrime is a growth industry. The returns are great, and the risks are low.
- We estimate that the likely annual cost to the global economy from cybercrime is more than \$400 billion.”

<http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf>

Großbritannien

- “81% of large companies had reported some form of security breach,
- costing each organisation on average between £600,000 and £1.5m.”

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf

Deutschland

- Die häufigsten Verbreitungswege von Schadprogrammen sind „Drive-by-Exploits“ → Infektionen durch bösartige Webseiten
- **4% aller deutschen Webseiten sind infiziert!**

http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/bsi-lagebericht-it-sicherheit.pdf?__blob=publicationFile

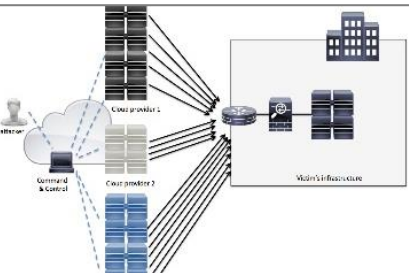
Warum werden Webseiten gehackt?

Die Herausforderung



... um **interne Systeme** zu erreichen

... um **Computerviren** zu verteilen



... um **andere Webseiten** anzugreifen

... aus reinem **Geltungsdrang**



... um Unternehmen zu **erpressen**

... um **illegale Daten** zu verbreiten



SPAMHAUS

“The current situation is the result of vast numbers of webservers running old, unmaintained and vulnerable web applications; applications that are exploited and used to install abusive software including - but not limited to - spamware.

Since these machines are usually servers hosted in datacenters instead of end-user machines sitting behind slow ADSL connections, the amount of spam they can pump out is way higher. That higher bandwidth easily explains why relatively few spam sources can contribute so heavily to the global quantity of spam. “

<http://www.spamhaus.org/news/article/718/stop-spammers-from-exploiting-your-webserver>

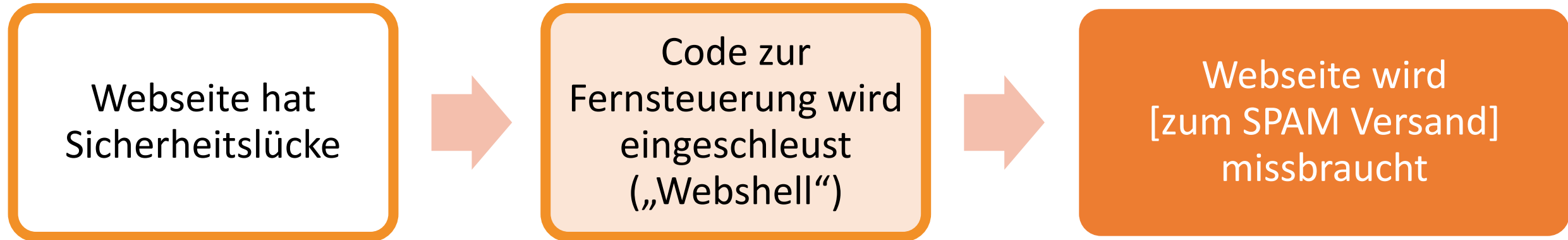
Server im Internet betreiben **massenhaft verwundbare Software**. Diese Sicherheitslücken werden ausgenutzt um schädliche Programme – beispielsweise zum Spamversand – zu installieren.

Da diese Server meist in Hochleistungs-Rechenzentren betrieben werden, ist es möglich, **mit verhältnismäßig wenigen Maschinen einen großen Beitrag zum weltweiten Spamaufkommen** zu leisten

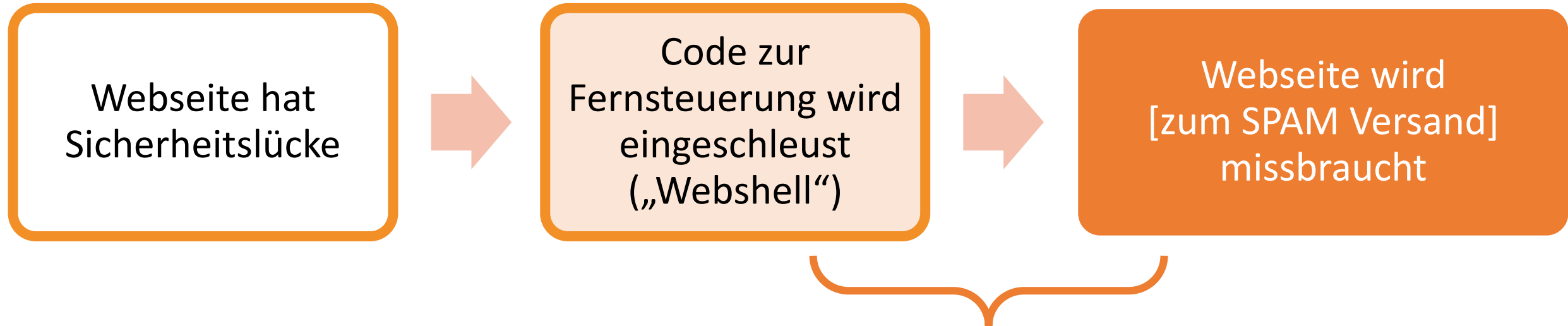
Die Geschäftsmodelle der Hacker

SPAM-Versand

SPAMHAUS



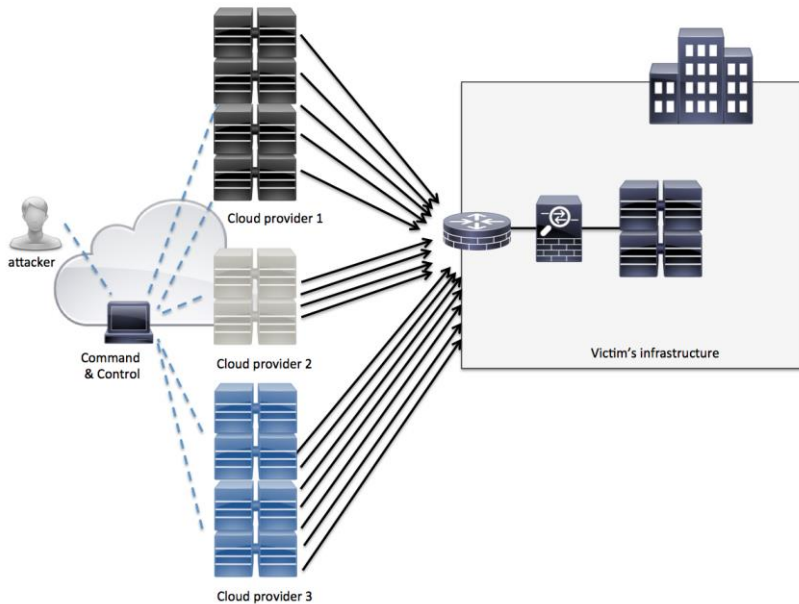
SPAMHAUS



Tage, Wochen, Monate

Die Geschäftsmodelle der Hacker

DDOS-Attacken



Angreifer

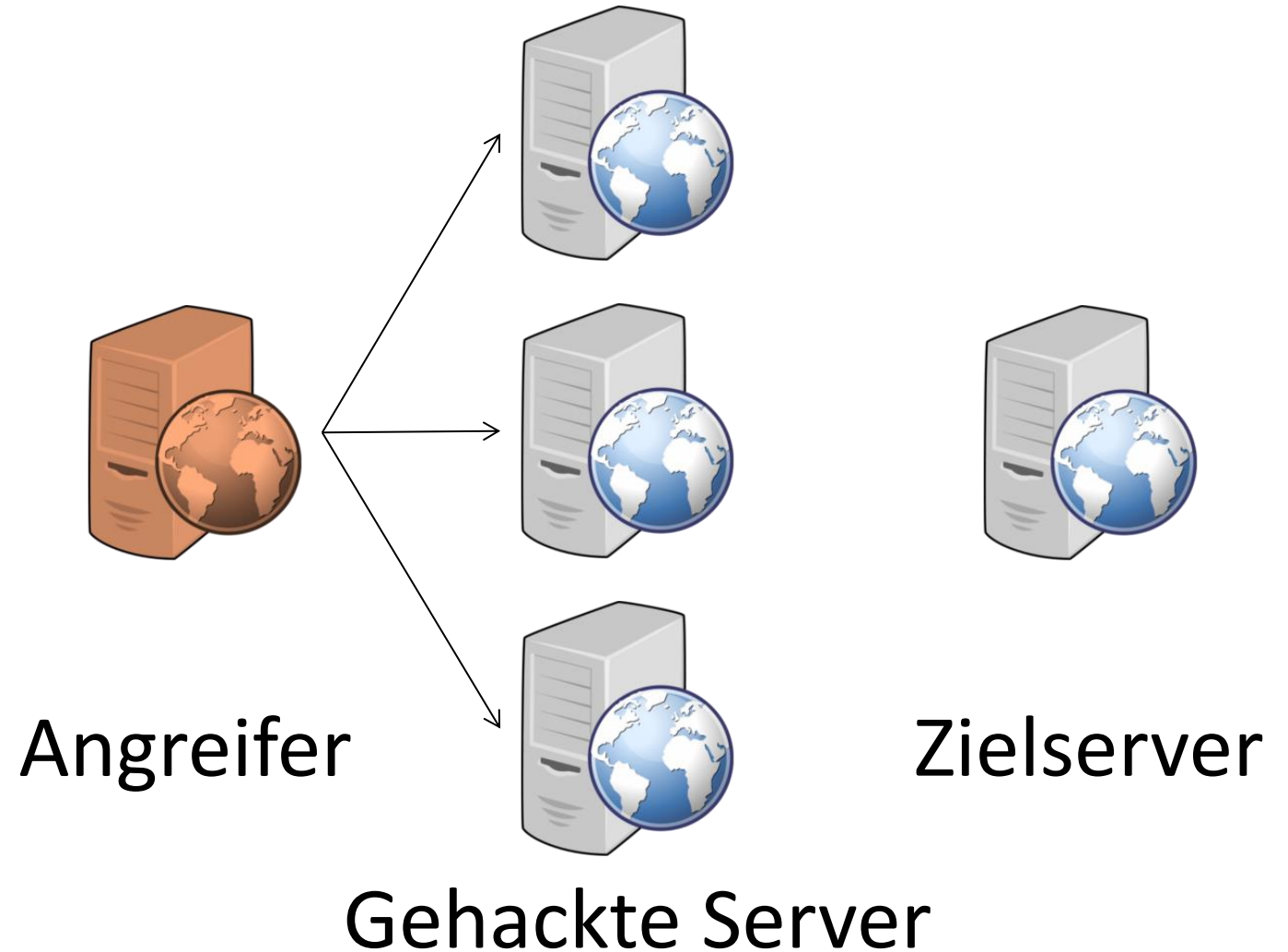
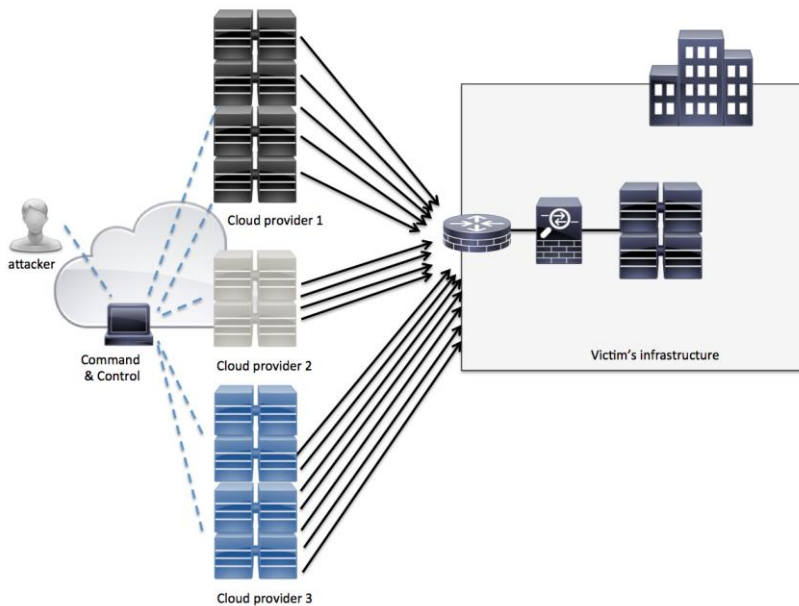


Zielserver

http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html

Die Geschäftsmodelle der Hacker

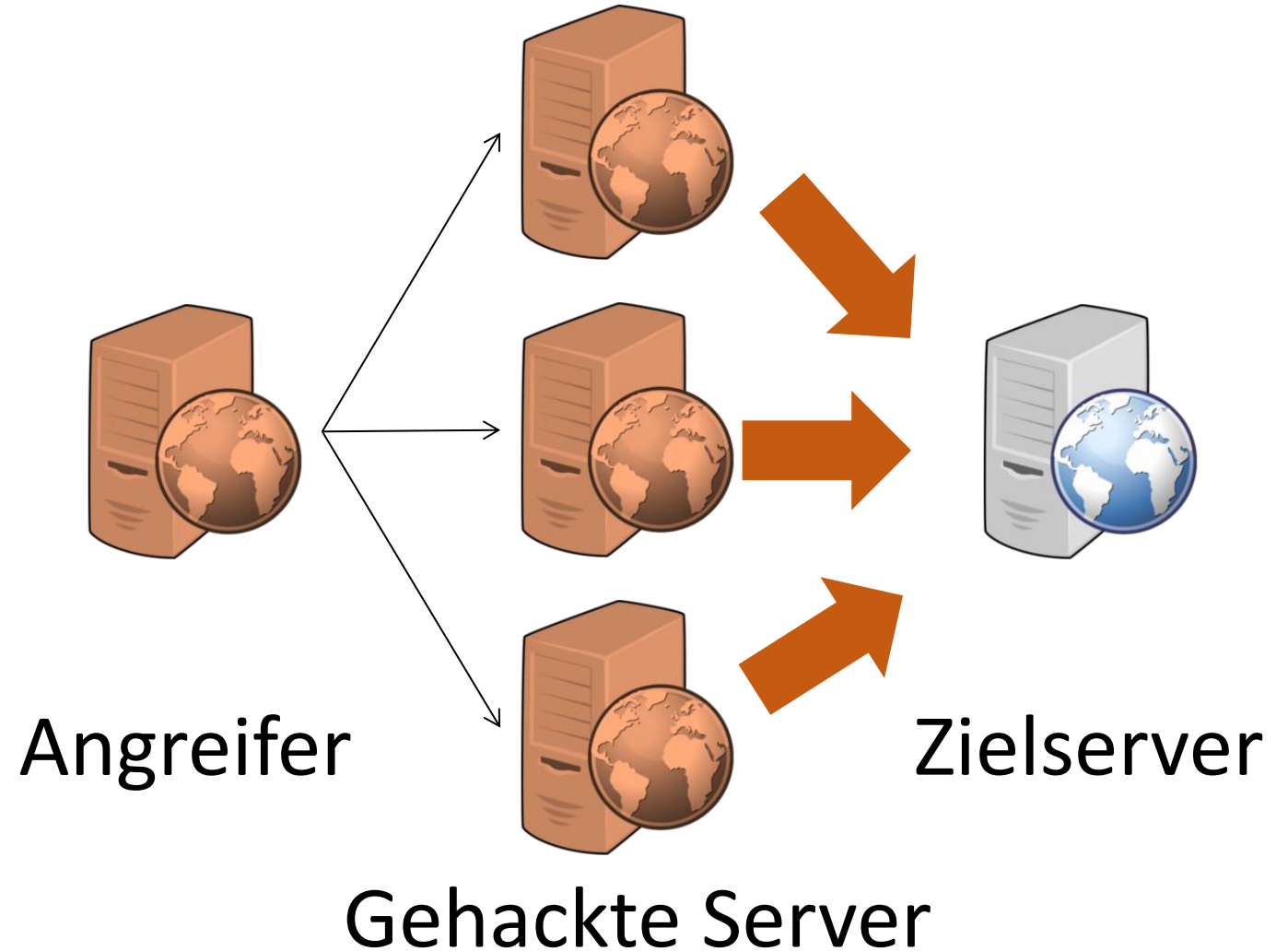
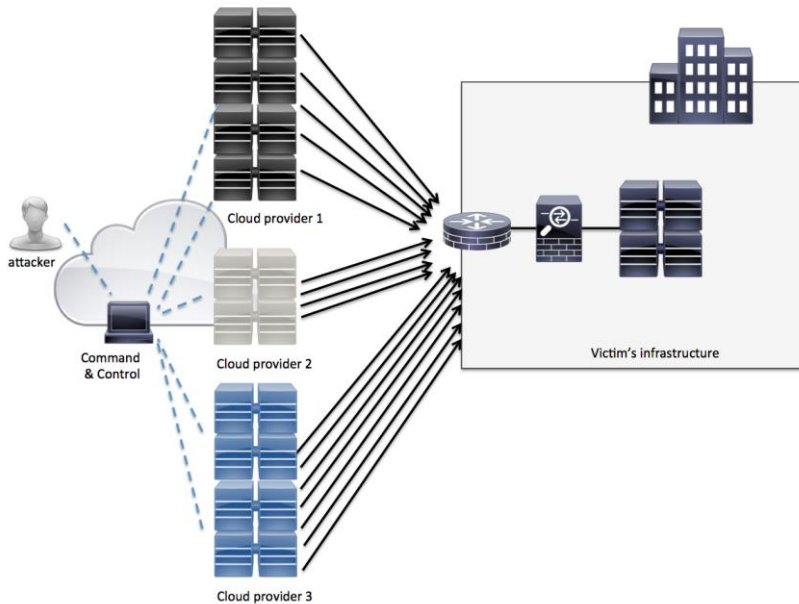
DDOS-Attacken



http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html

Die Geschäftsmodelle der Hacker

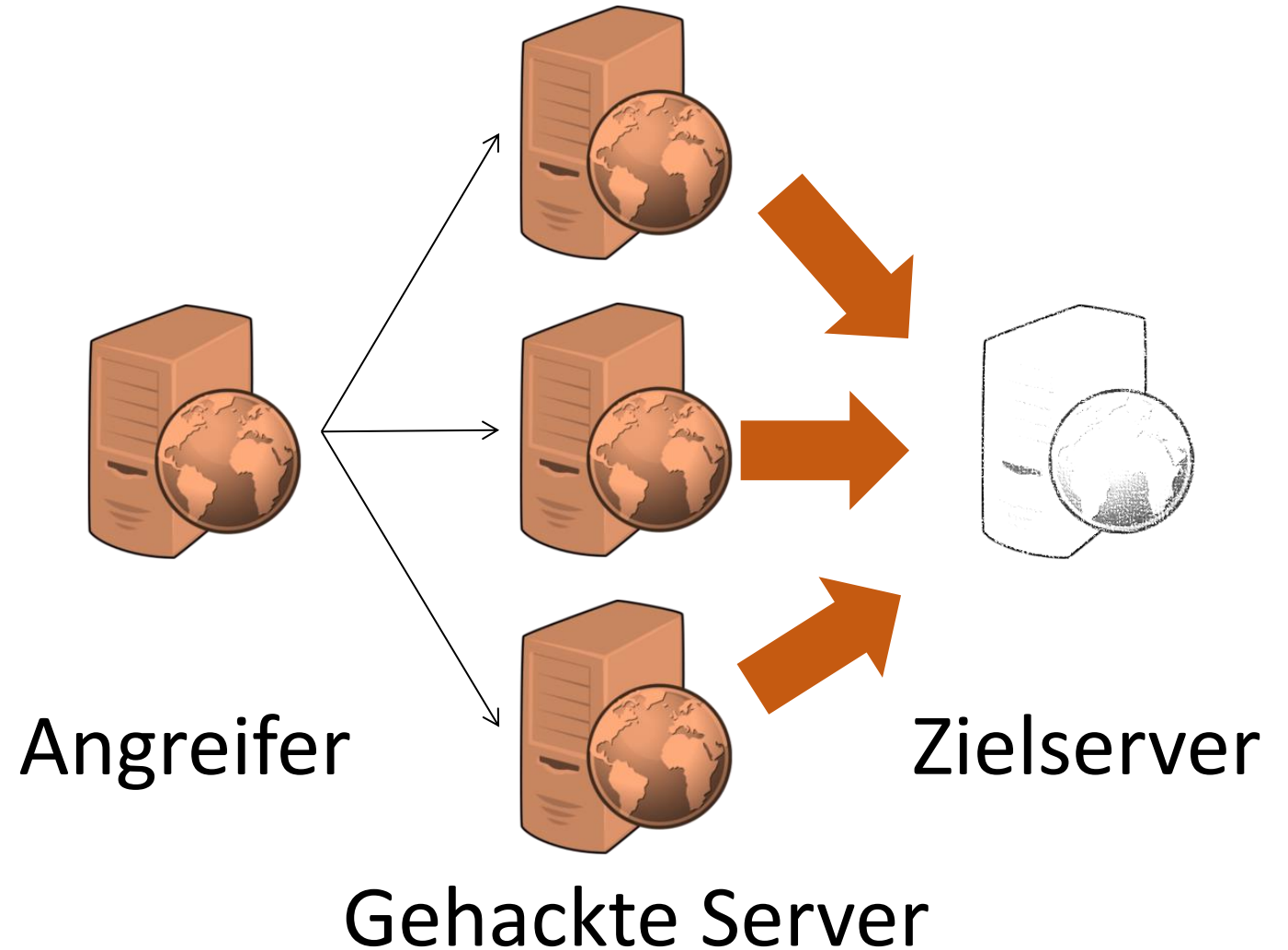
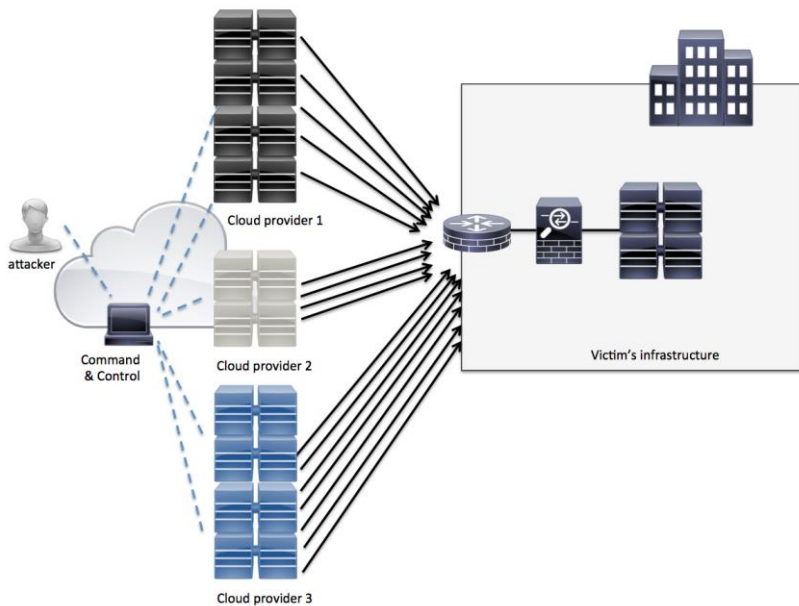
DDOS-Attacken



http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html

Die Geschäftsmodelle der Hacker

DDOS-Attacken



http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html

Die Geschäftsmodelle der Hacker

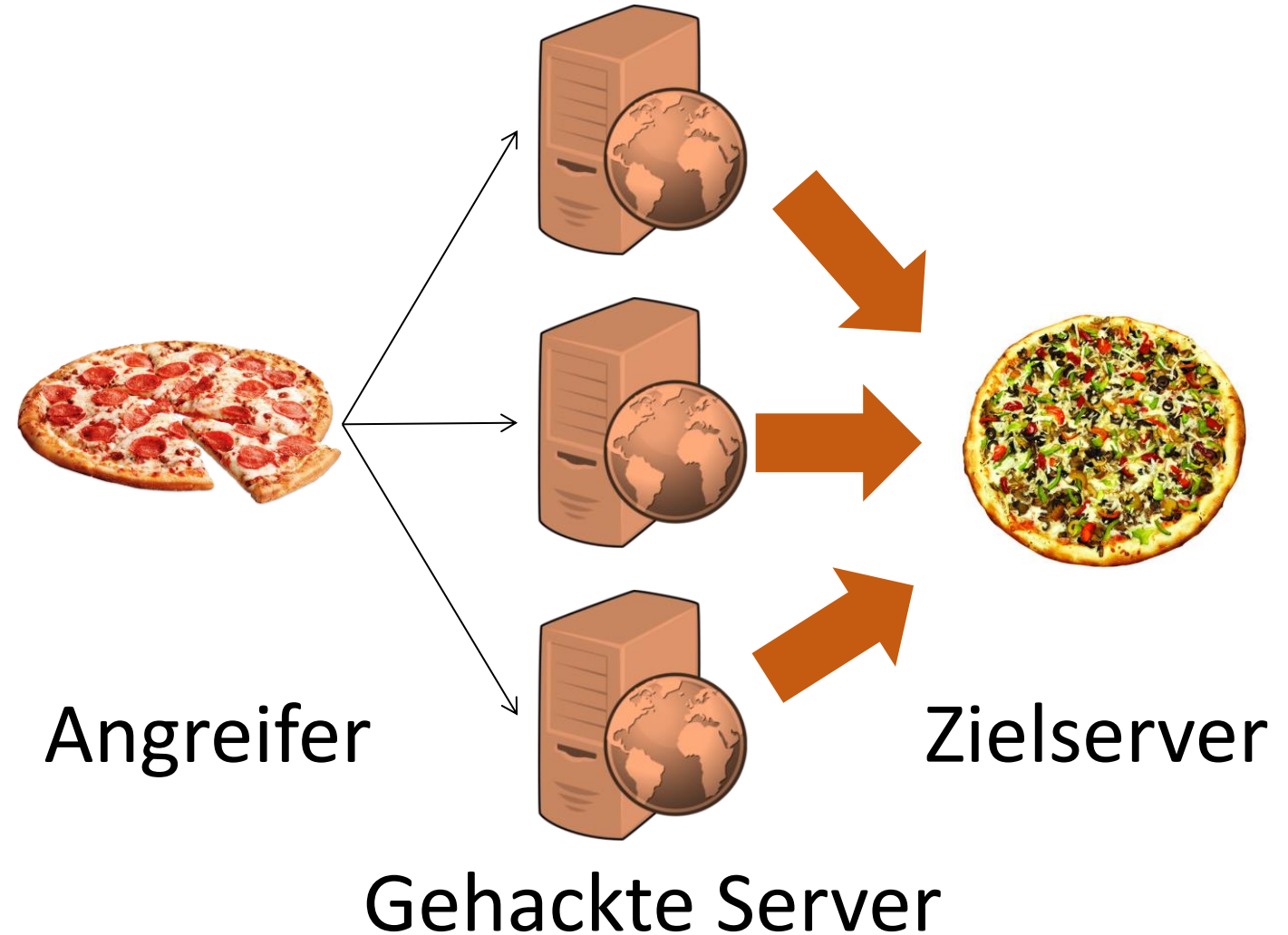
DDOS-Attacken

DER SPIEGEL

22. April 2012, 08:33 Uhr

Razzia bei Berliner Bestellplattform Lieferheld

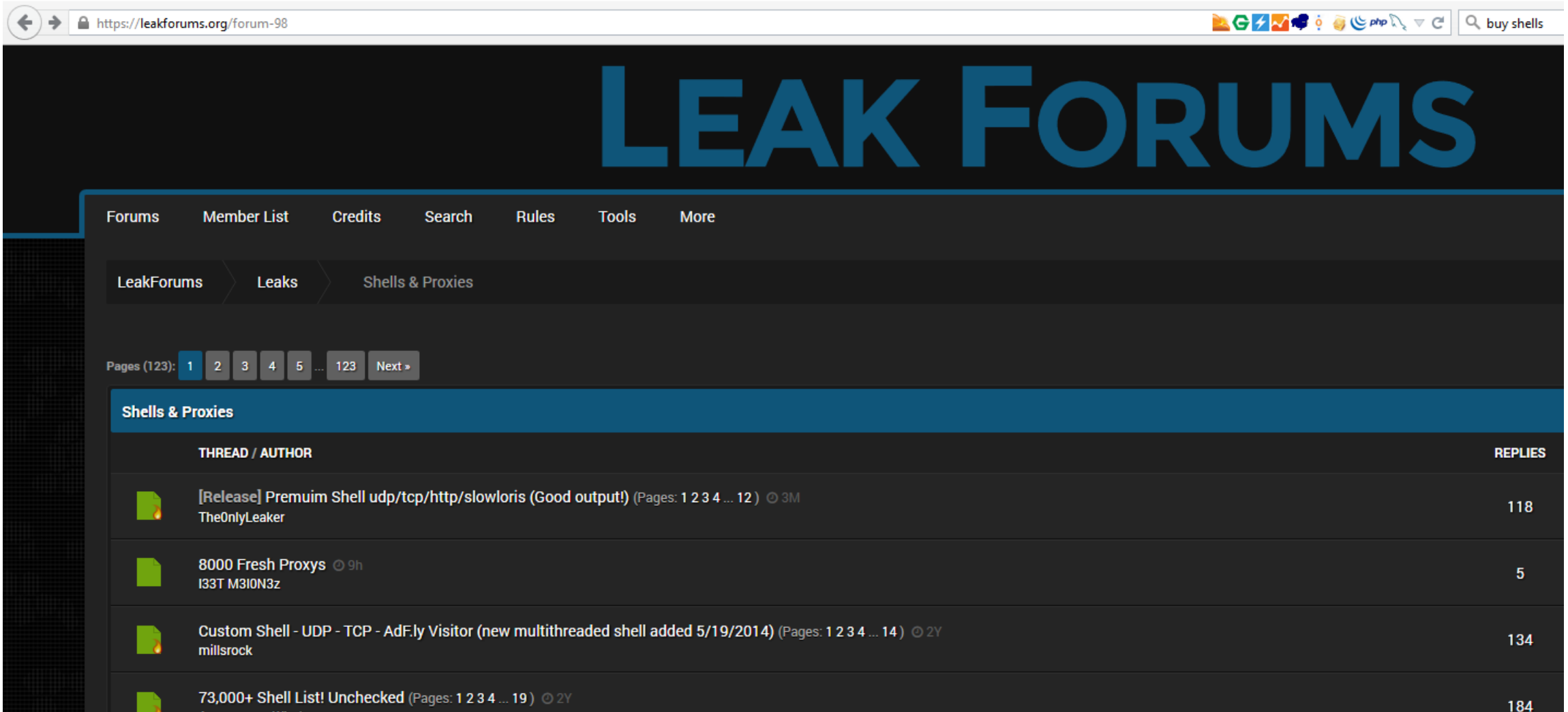
Die Berliner Staatsanwaltschaft ermittelt gegen die vier Geschäftsführer der Online-Bestellplattform Lieferheld wegen des Verdachts auf Computersabotage. Am Mittwoch durchsuchten Beamte des Landeskriminalamts Berlin die Geschäftsräume des 2010 gegründeten Unternehmens, das nach eigenen Angaben bereits mehr als eine Million Essensbestellungen über 5600 angeschlossene Lieferservices abwickelte. Laut Durchsuchungsbeschluss soll das Unternehmen mittels Internetattacken "mehrfach" seinen ebenfalls in Berlin ansässigen Konkurrenten Lieferando für dessen Kunden unreachbar gemacht haben. Der dadurch entstandene Schaden belaufe sich auf "mindestens 75000 Euro". Die Lieferando-Macher hatten bei einer besonders gravierenden und gezielten Attacke im Dezember 2011, die zum mehrstündigen Ausfall der Plattform zur abendlichen Hauptbestellzeit führte, die angreifenden Adressen analysiert. Eine habe sie direkt zu einem von Lieferheld angemieteten Server geführt, so Lieferando-Geschäftsführer Christoph Gerber. Die Vorwürfe, den Wettbewerber mittels Cyber-Attacken lahmgelegt zu haben, bezeichnet der mitbeschuldigte Lieferheld-Geschäftsführer Fabian Siegel als "völlig absurd". "Ich bin doch nicht so dumm, mich für einen möglichen Nachteil eines wesentlich kleineren Mitbewerbers strafbar zu machen." Er erklärt den Vorgang mit einem von Lieferheld eingesetzten Crawler der automatisiert überprüfe ob die vom Konkurrenten Lieferando







<http://www.spiegel.de/spiegel/vorab/a-828910.html>

Die Geschäftsmodelle der Hacker

DDOS-Attacken



The screenshot shows a web browser window with the URL <https://leakforums.org/forum-98>. The page title is "LEAK FORUMS". The navigation menu includes "Forums", "Member List", "Credits", "Search", "Rules", "Tools", and "More". The breadcrumb trail is "LeakForums > Leaks > Shells & Proxies". The page number is 1 of 123. The forum thread list is as follows:

THREAD / AUTHOR	REPLIES
 [Release] Premuim Shell udp/tcp/http/slowloris (Good output!) (Pages: 1 2 3 4 ... 12) ⌚ 3M TheOnlyLeaker	118
 8000 Fresh Proxys ⌚ 9h I33T M3ION3z	5
 Custom Shell - UDP - TCP - AdF.ly Visitor (new multithreaded shell added 5/19/2014) (Pages: 1 2 3 4 ... 14) ⌚ 2Y millsrock	134
 73,000+ Shell List! Unchecked (Pages: 1 2 3 4 ... 19) ⌚ 2Y AnonymousWhut	184

AP Twitter hack causes panic on Wall Street and sends Dow plunging

Market recovers after hackers tweeted from the official AP feed that two explosions had hit the White House



 The panic, however brief, demonstrates how tightly intertwined Wall Street has become with Twitter.
Photograph: Spencer Platt/Getty Images

Wall Street collided with social media on Tuesday, when a false tweet from a trusted news organization sent the US stock market into freefall.

<http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall>

AP Twitter hack causes panic on Wall Street and sends Dow plunging

Market recovers after hackers tweeted from the official AP feed that two explosions had hit the White House



 The panic, however brief, demonstrates how tightly intertwined Wall Street has become with Twitter.
Photograph: Spencer Platt/Getty Images

Wall Street collided with social media on Tuesday, when a false tweet from a trusted news organization sent the US stock market into freefall.

<http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall>

Einbruch in Unternehmenswebseite
ist erfolgt, aber vorerst noch kein
Missbrauch.

AP Twitter hack causes panic on Wall Street and sends Dow plunging

Market recovers after hackers tweeted from the official AP feed that two explosions had hit the White House

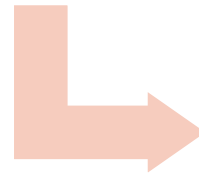


 The panic, however brief, demonstrates how tightly intertwined Wall Street has become with Twitter.
Photograph: Spencer Platt/Getty Images

Wall Street collided with social media on Tuesday, when a false tweet from a trusted news organization sent the US stock market into freefall.

<http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall>

Einbruch in Unternehmenswebseite ist erfolgt, aber vorerst noch kein Missbrauch.



Angreifer setzt auf fallenden Börsenkurs.

Die Geschäftsmodelle der Hacker

Fehlinformationen

AP Twitter hack causes panic on Wall Street and sends Dow plunging

Market recovers after hackers tweeted from the official AP feed that two explosions had hit the White House

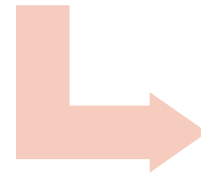


 The panic, however brief, demonstrates how tightly intertwined Wall Street has become with Twitter.
Photograph: Spencer Platt/Getty Images

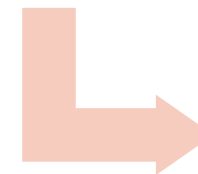
Wall Street collided with social media on Tuesday, when a false tweet from a trusted news organization sent the US stock market into freefall.

<http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall>

Einbruch in Unternehmenswebseite ist erfolgt, aber vorerst noch kein Missbrauch.



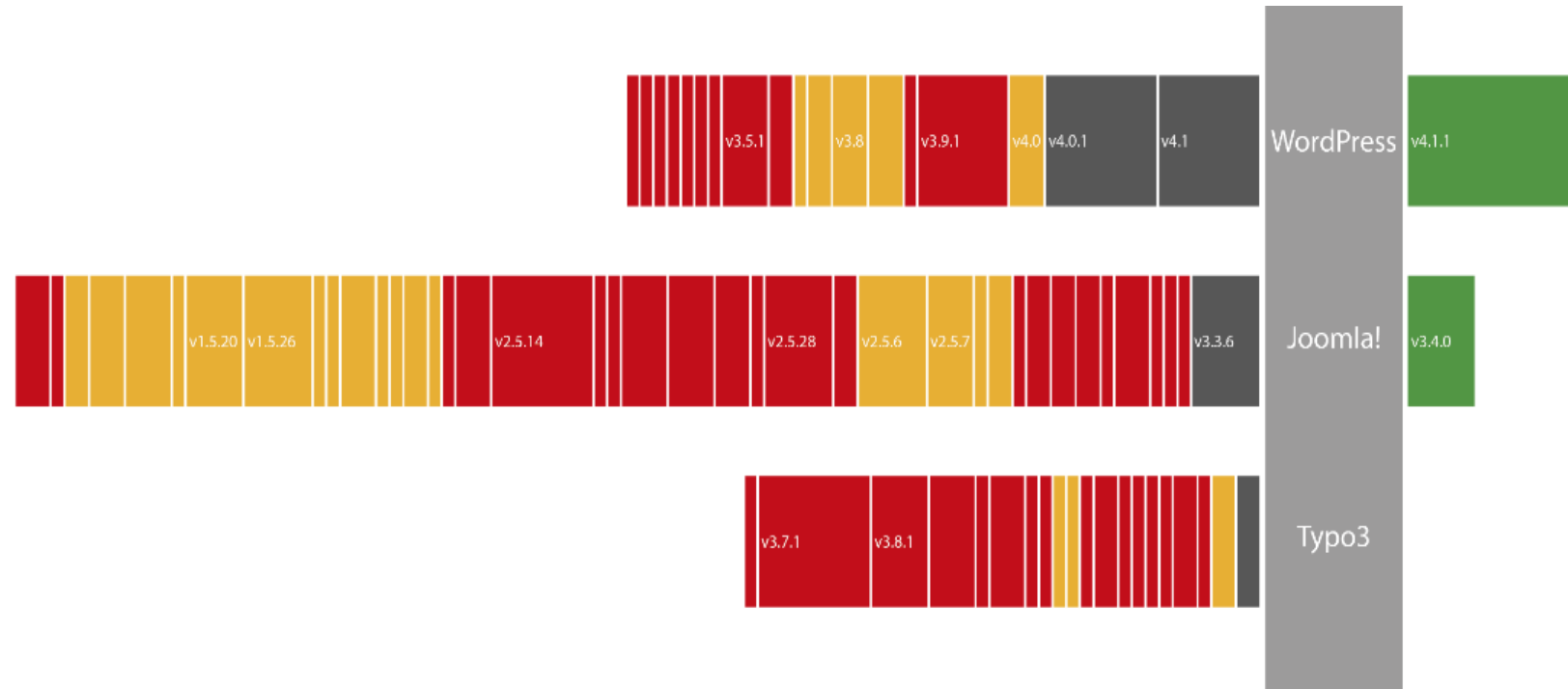
Angreifer setzt auf fallenden Börsenkurs.



Über die angreifbare Webseite werden Fehlinformationen gestreut.

Wie wurden Cyberattacken ein Massenproblem?

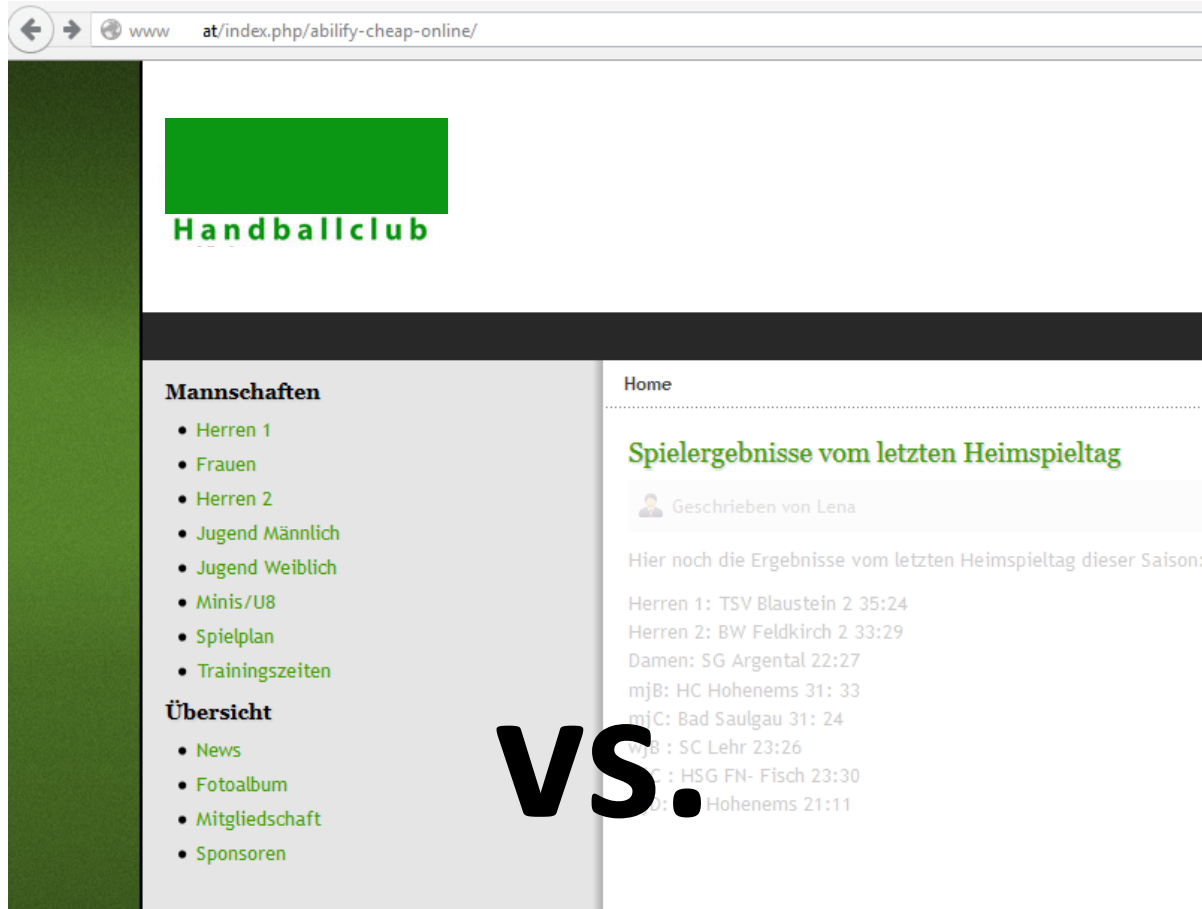
Die Herausforderung



89% der Webseiten sind **unzureichend gewartet** und dadurch anfällig für **automatisierte Cyberattacken**.

Die Geschäftsmodelle der Hacker

„Pharma-Shop“ Angriff



www at/index.php/abilify-cheap-online/

Handballclub

Mannschaften

- Herren 1
- Frauen
- Herren 2
- Jugend Männlich
- Jugend Weiblich
- Minis/U8
- Spielplan
- Trainingszeiten

Übersicht

- News
- Fotoalbum
- Mitgliedschaft
- Sponsoren

Home

Spielergebnisse vom letzten Heimspieltag

Geschrieben von Lena

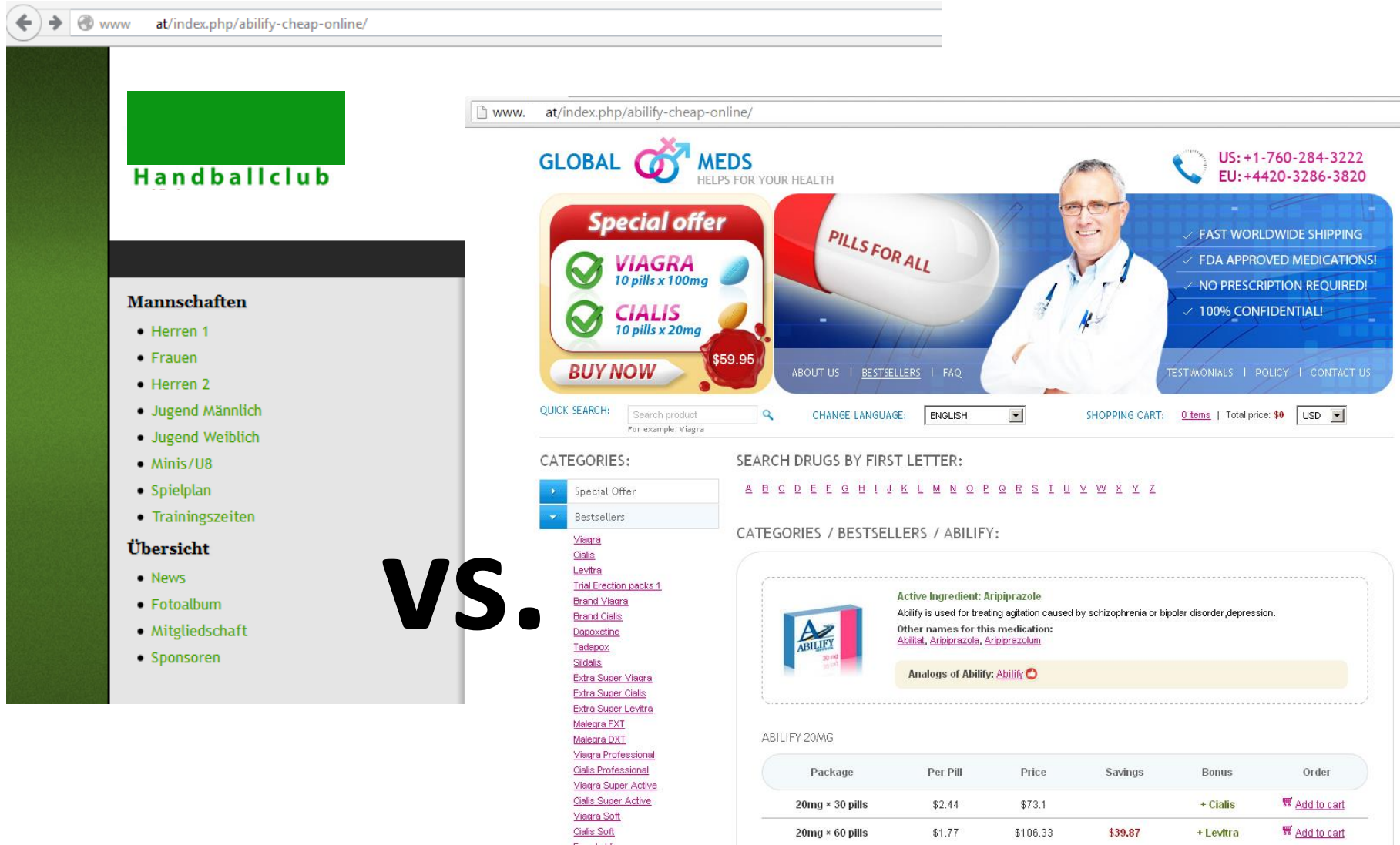
Hier noch die Ergebnisse vom letzten Heimspieltag dieser Saison:

Herren 1: TSV Blaustein 2 35:24
Herren 2: BW Feldkirch 2 33:29
Damen: SG Argental 22:27
mjB: HC Hohenems 31: 33
mjC: Bad Saulgau 31: 24
mjB : SC Lehr 23:26
mjC : HSG FN- Fisch 23:30
mjD: Hohenems 21:11

VS.

Die Geschäftsmodelle der Hacker

„Pharma-Shop“ Angriff



The image shows a comparison between a legitimate sports club website and a fraudulent pharmacy website. On the left, a sidebar for 'Handballclub' lists various team categories. On the right, a screenshot of 'GLOBAL MEDS' features a 'Special offer' for Viagra and Cialis, a doctor's image, and a list of benefits like 'FAST WORLDWIDE SHIPPING' and 'NO PRESCRIPTION REQUIRED!'. Below the pharmacy ad, there is a 'VS.' watermark and a list of various Viagra and Cialis products.

Handballclub

Mannschaften

- Herren 1
- Frauen
- Herren 2
- Jugend Männlich
- Jugend Weiblich
- Minis/U8
- Spielplan
- Trainingszeiten

Übersicht

- News
- Fotoalbum
- Mitgliedschaft
- Sponsoren

GLOBAL MEDS
HELPS FOR YOUR HEALTH

Special offer

- ✓ **VIAGRA**
10 pills x 100mg
- ✓ **CIALIS**
10 pills x 20mg

BUY NOW \$59.95

PILLS FOR ALL

FAST WORLDWIDE SHIPPING
FDA APPROVED MEDICATIONS!
NO PRESCRIPTION REQUIRED!
100% CONFIDENTIAL!

US: +1-760-284-3222
EU: +4420-3286-3820

ABOUT US | BESTSELLERS | FAQ | TESTIMONIALS | POLICY | CONTACT US

QUICK SEARCH: Search product For example: Viagra CHANGE LANGUAGE: ENGLISH SHOPPING CART: 0 items | Total price: \$0 USD

CATEGORIES:

- ▶ Special Offer
- ▶ Bestsellers

SEARCH DRUGS BY FIRST LETTER:
A B C D E E G H I J K L M N O P Q R S T U V W X Y Z

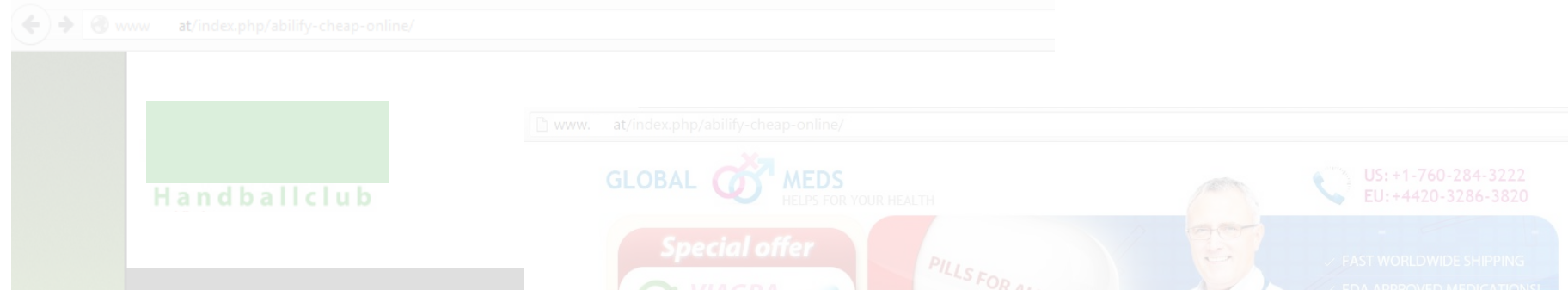
CATEGORIES / BESTSELLERS / ABILITY:

Active Ingredient: Aripiprazole
Ability is used for treating agitation caused by schizophrenia or bipolar disorder, depression.
Other names for this medication:
Abilitat, Aripiprazola, Aripiprazolum

Analogs of Ability: [Abilify](#)

ABILITY 20MG

Package	Per Pill	Price	Savings	Bonus	Order
20mg x 30 pills	\$2.44	\$73.1		+ Cialis	Add to cart
20mg x 60 pills	\$1.77	\$106.33	\$39.87	+ Levitra	Add to cart



Selbstversuch per Google Suche:
site:at cheap viagra

Übersicht

- News
- Fotoalbum
- Mitgliedschaft
- Sponsoren

VS.

Ability

Cialis
Levitra
Trial Fraction packs 1
Brand Viagra
Brand Cialis
Dapoxetine
Tadalafil
Sildenafil
Extra Super Viagra
Extra Super Cialis
Extra Super Levitra
Malegra FXT
Malegra DXT
Viagra Professional
Cialis Professional
Viagra Super Active
Cialis Super Active
Viagra Soft
Cialis Soft

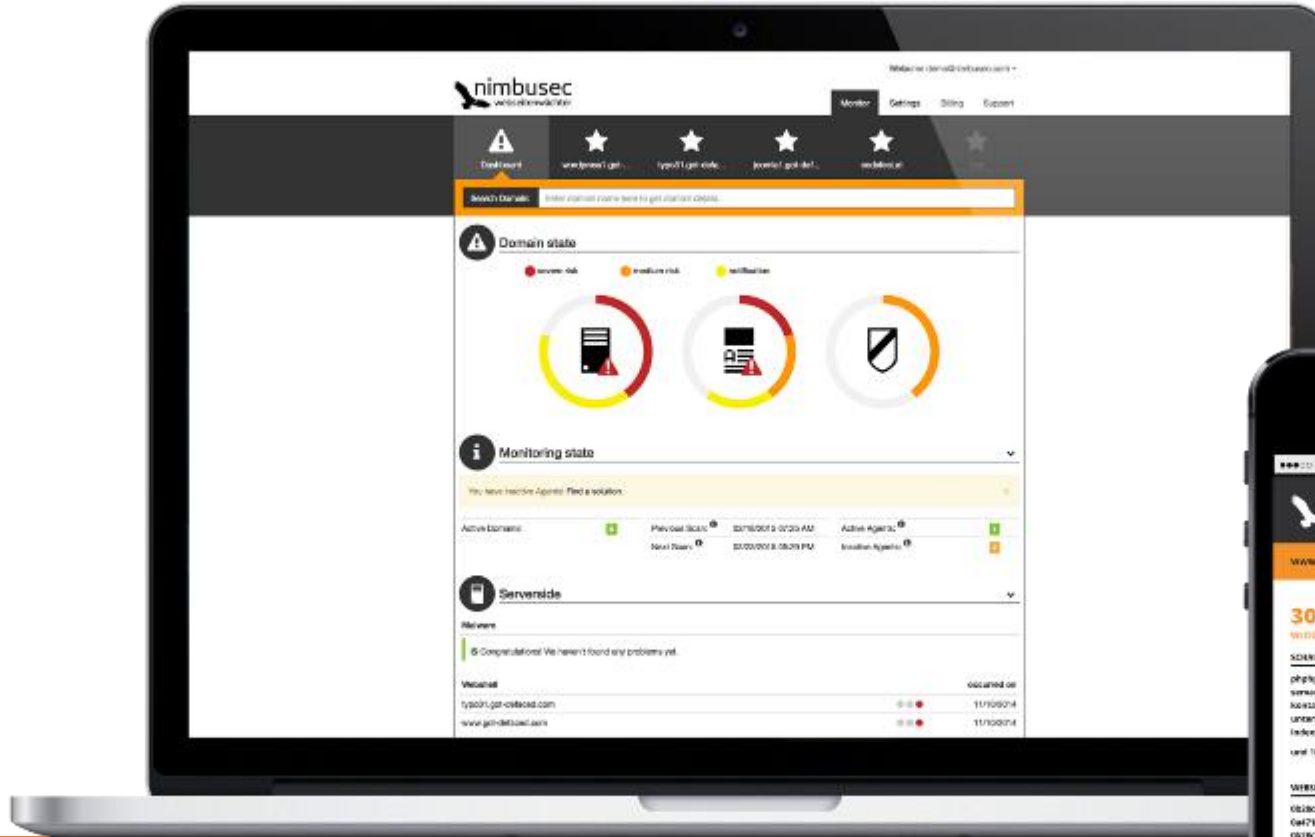
Active ingredient: Aripiprazole
Ability is used for treating agitation caused by schizophrenia or bipolar disorder, depression.
Other names for this medication:
[Abilif](#), [Aripiprazole](#), [Aripiprazolum](#)

Analogs of Ability: [Abilify](#)

ABILITY 20MG

Package	Per Pill	Price	Savings	Bonus	Order
20mg x 30 pills	\$2.44	\$73.1		+ Cialis	Add to cart
20mg x 60 pills	\$1.77	\$106.33	\$39.87	+ Levitra	Add to cart

Ausgezeichnet:



Im Einsatz:

