nimbusec
webseitenwächter

FRÜHERKENNUNG GEHACKTER WEBSEITEN.

Nimbusec

Das Unternehmen

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?

Statusaufnahme

International

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!**

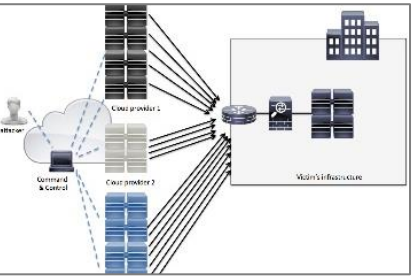
http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/bsi-lagebericht-it-sicherheit.pdf?__blob=publicationFile

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

Die Geschäftsmodelle der Hacker

SPAM-Versand

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. “

Server im Internet betreiben massenhaft verwundbare Software. Diese Sicherheitslücken werden ausgenützt 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

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

Die Geschäftsmodelle der Hacker

SPAM-Versand

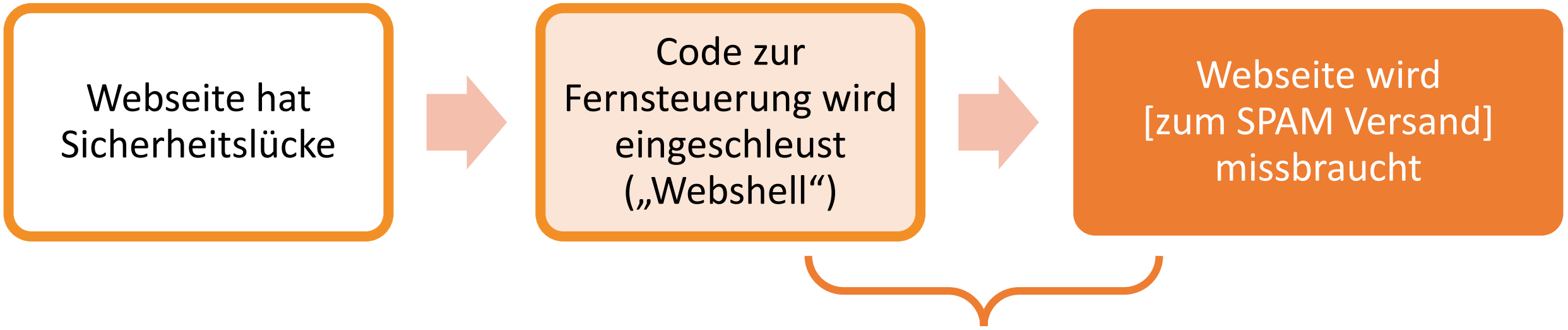
SPAMHAUS

Webseite hat Sicherheitslücke → Code zur Fernsteuerung wird eingeschleust („Webshell“) → Webseite wird [zum SPAM Versand] missbraucht

Die Geschäftsmodelle der Hacker

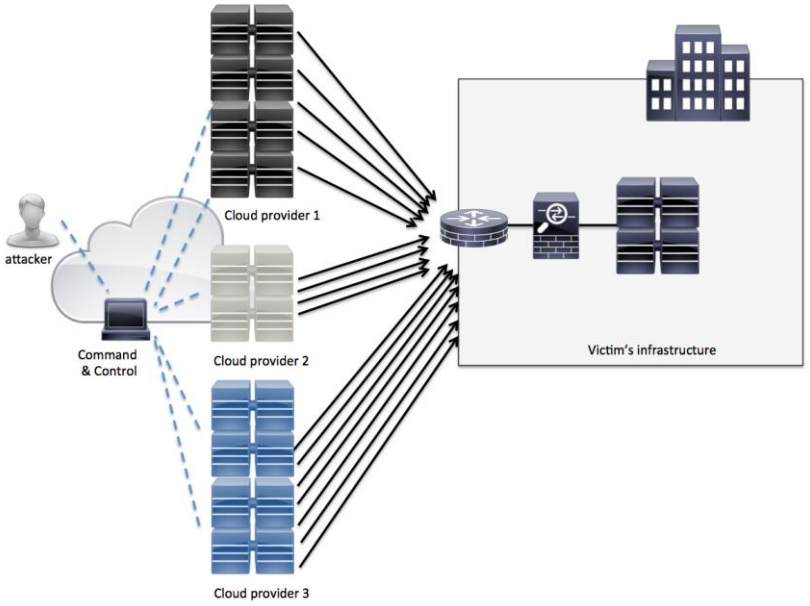
SPAM-Versand

SPAMHAUS



Die Geschäftsmodelle der Hacker

DDOS-Attacken



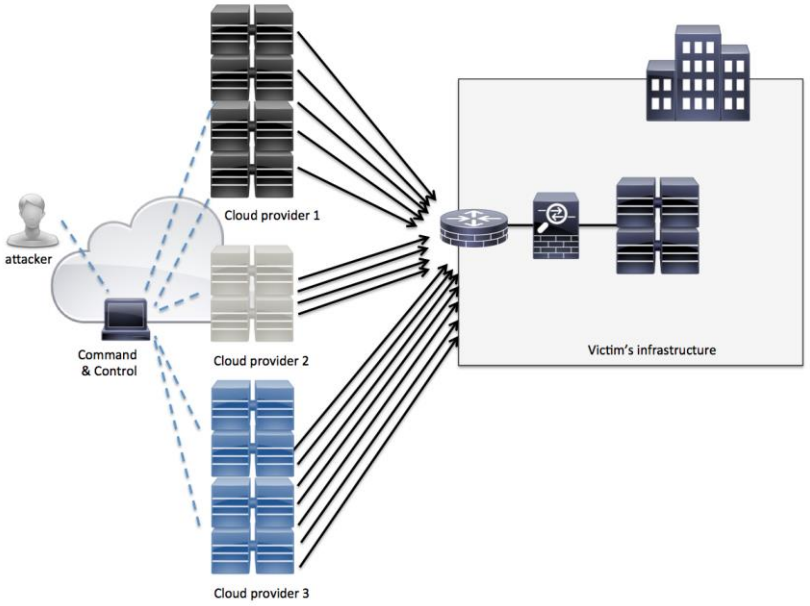
Angreifer

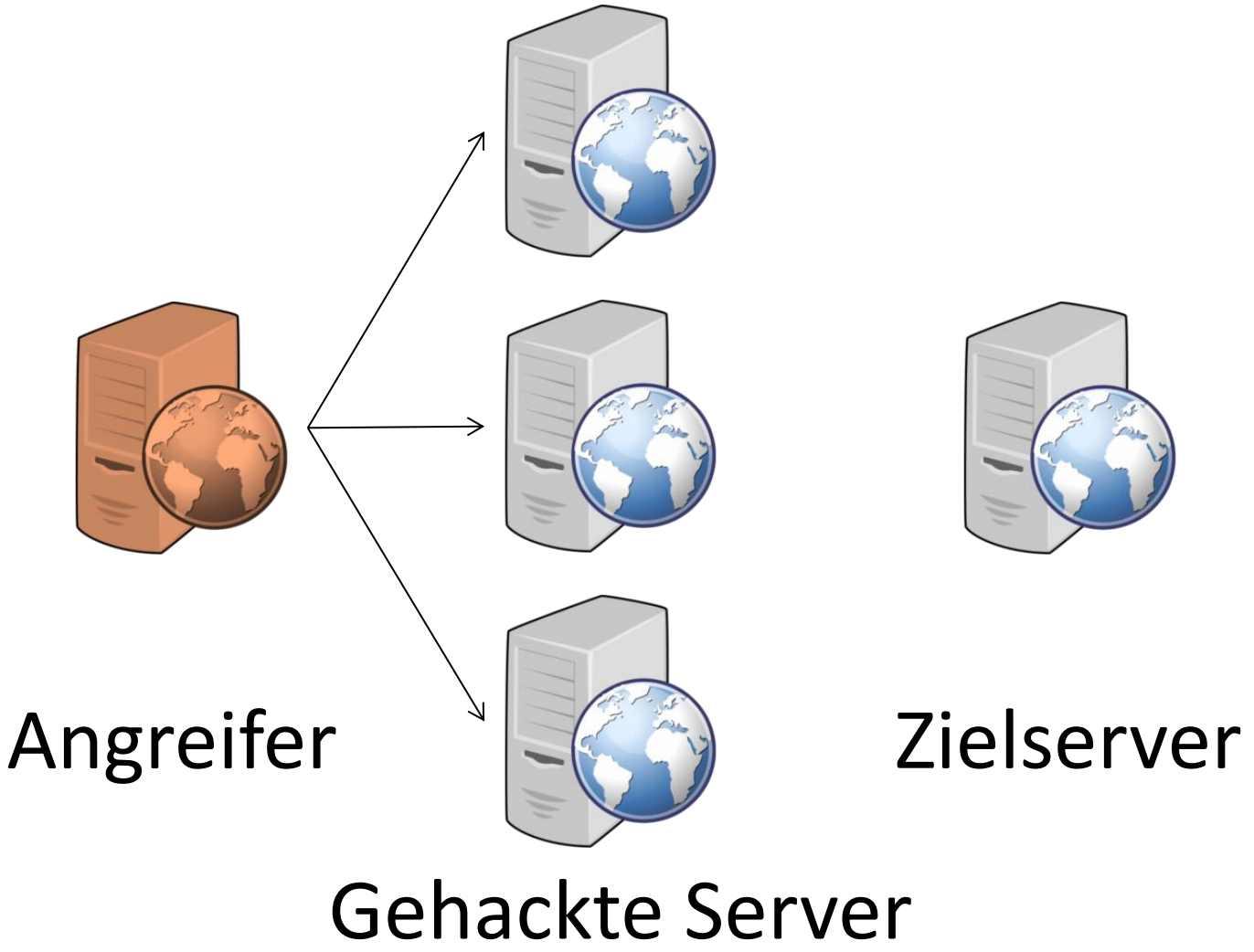
Zielserver

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

Die Geschäftsmodelle der Hacker

DDOS-Attacken

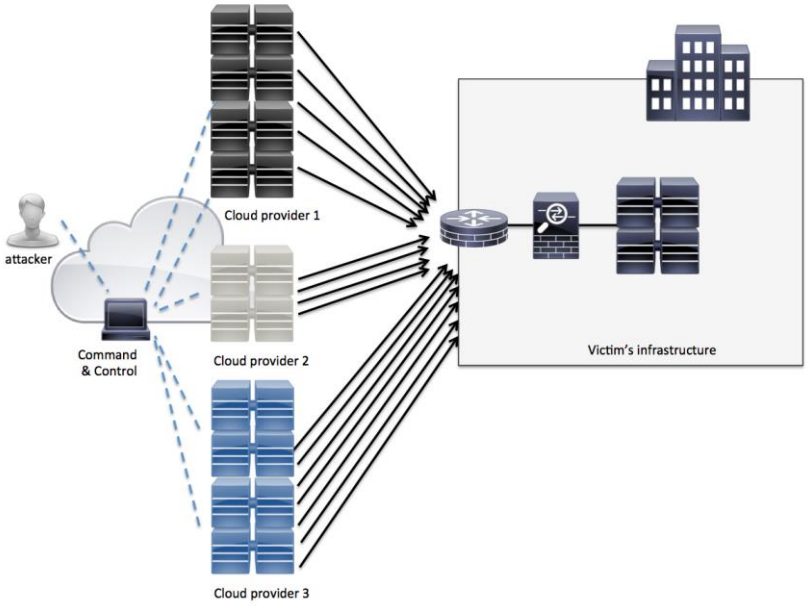


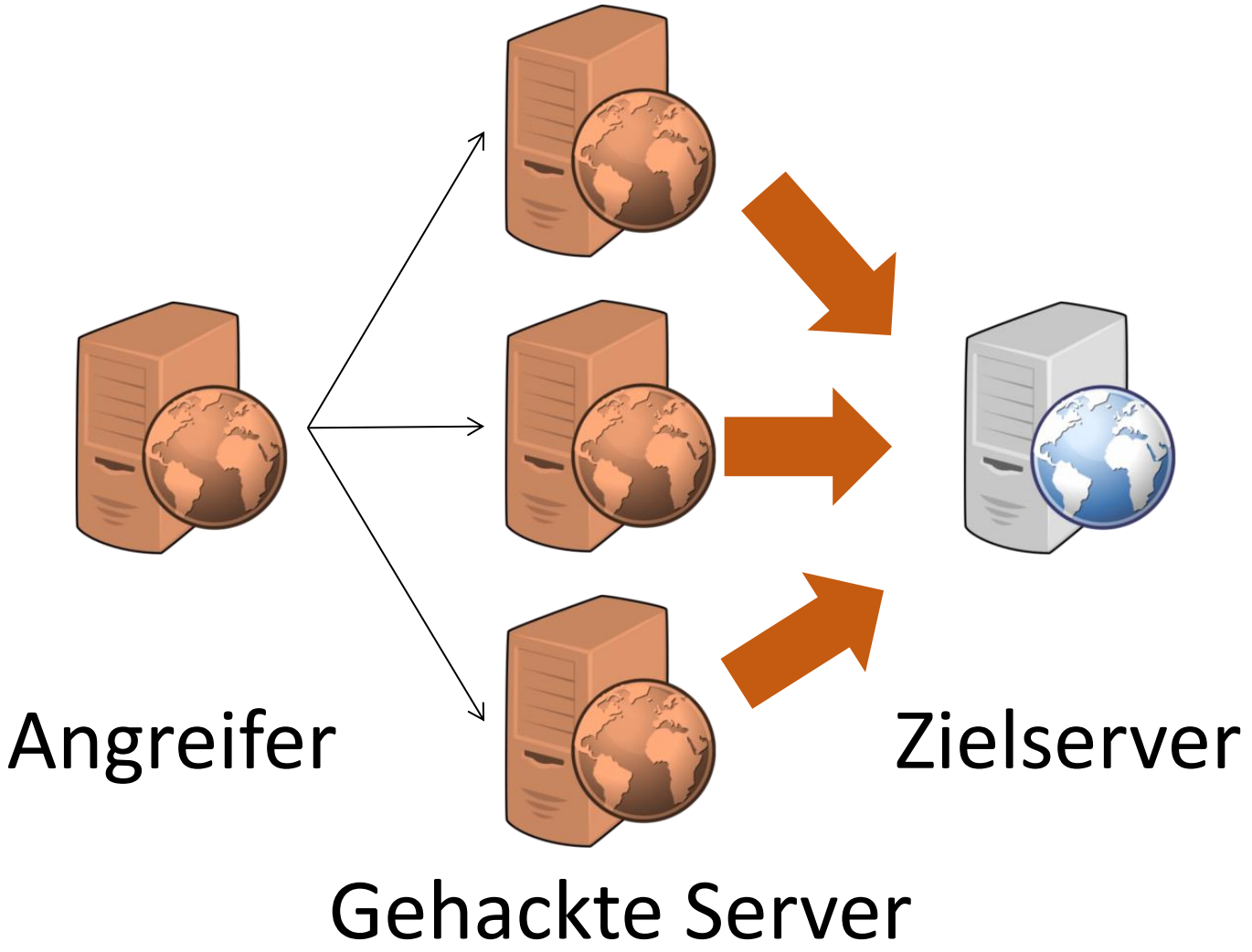


http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html

Die Geschäftsmodelle der Hacker

DDOS-Attacken

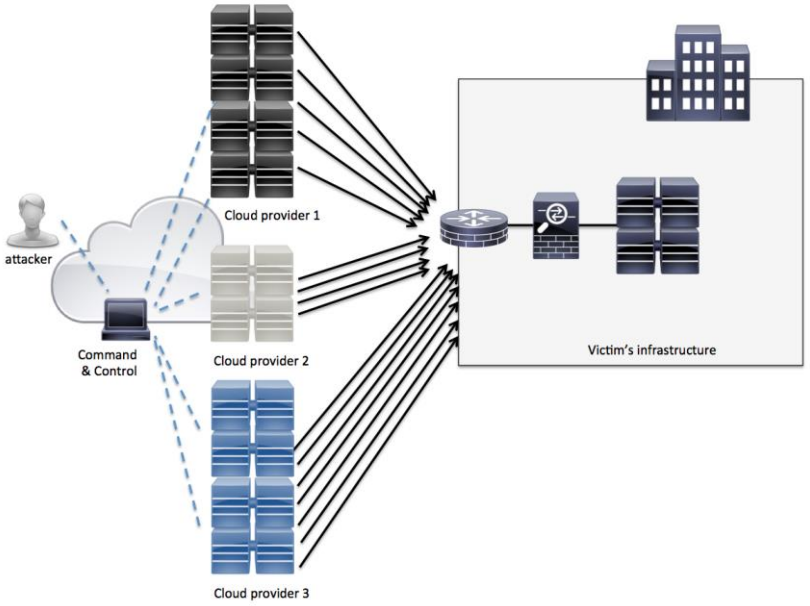


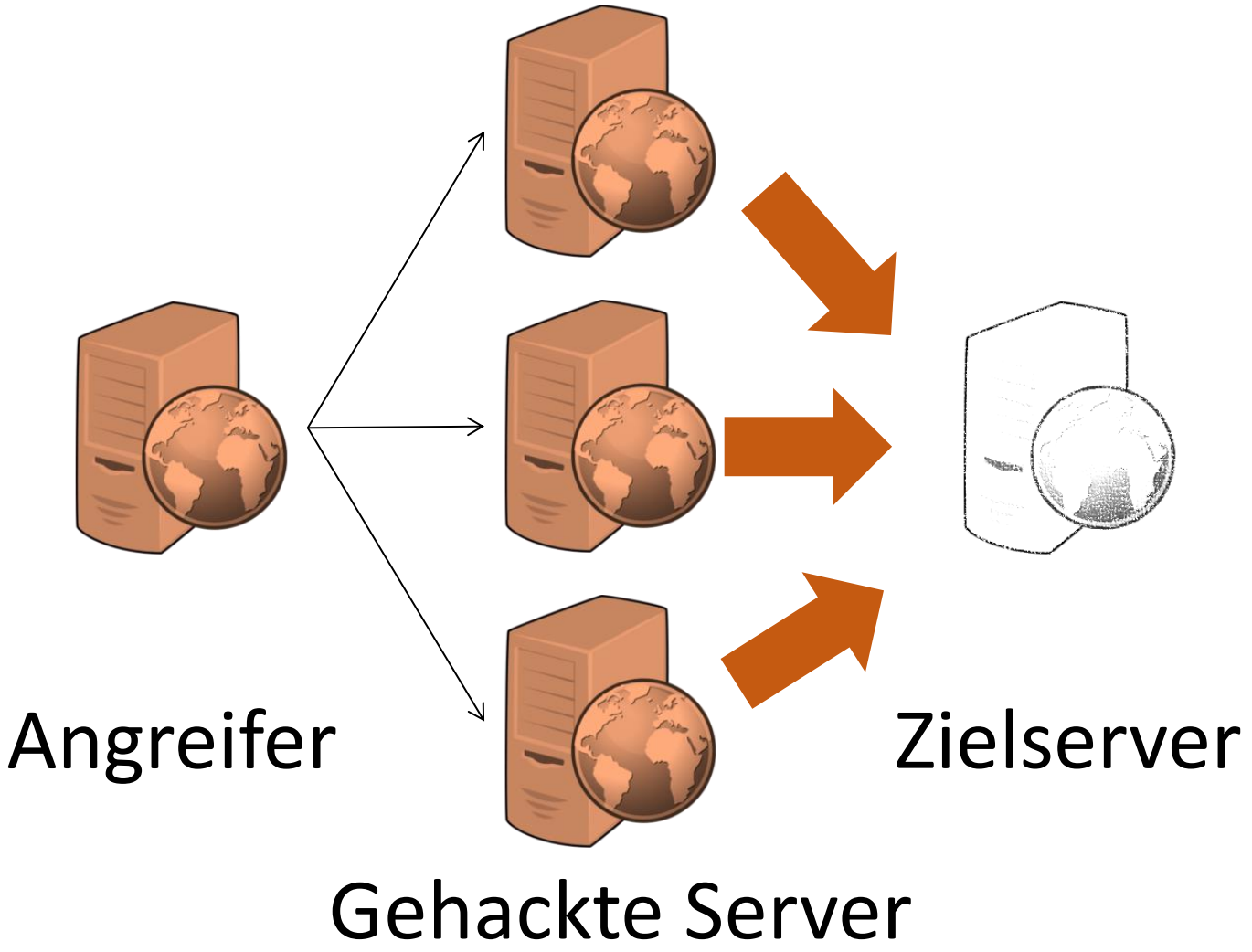


http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html

Die Geschäftsmodelle der Hacker

DDOS-Attacken





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

Die Geschäftsmodelle der Hacker

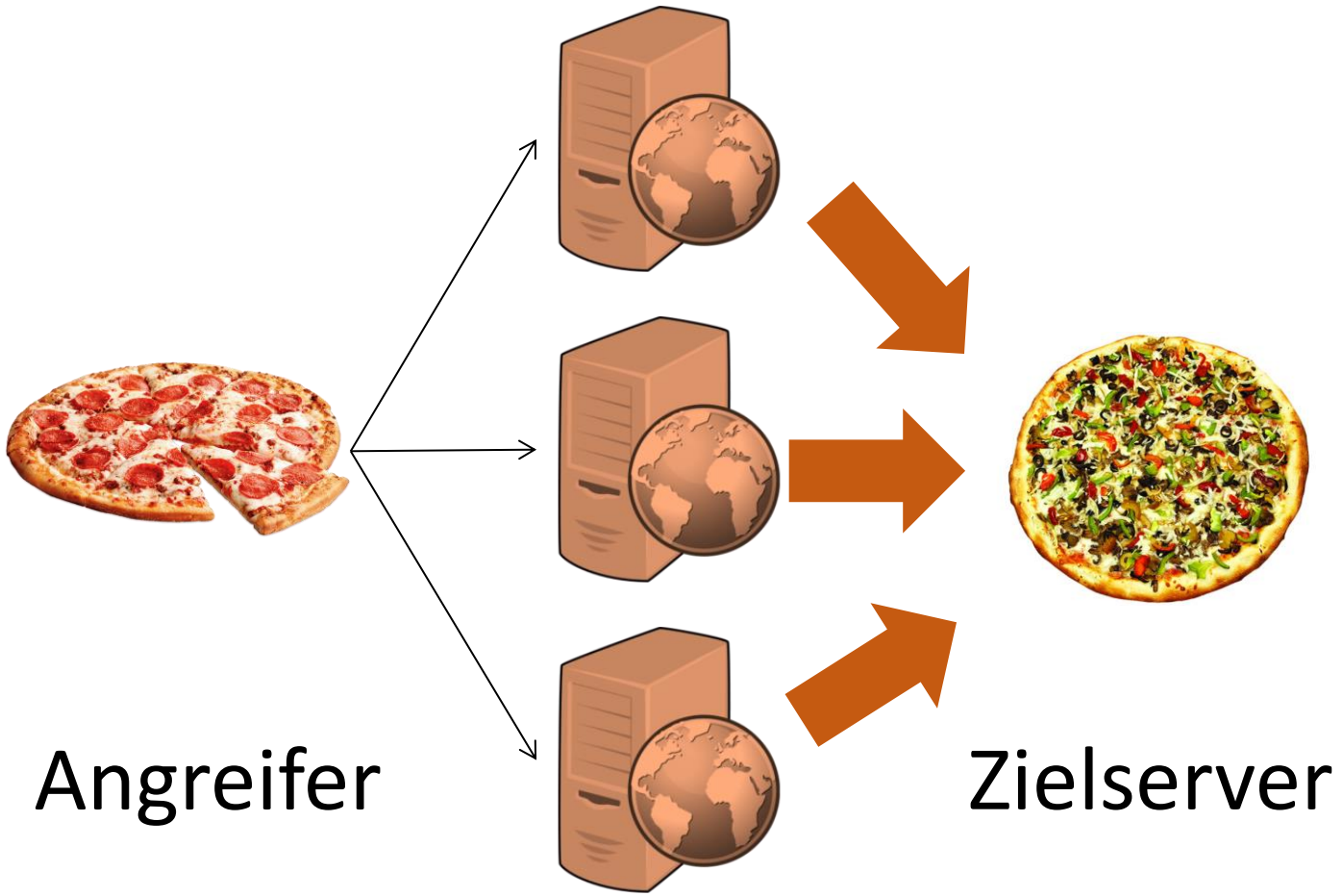
DDOS-Attacken

DER SPIEGEL

22. April 2012, 08:33 Uhr

Razzia bei Berliner Bestellplattform Lieferheld

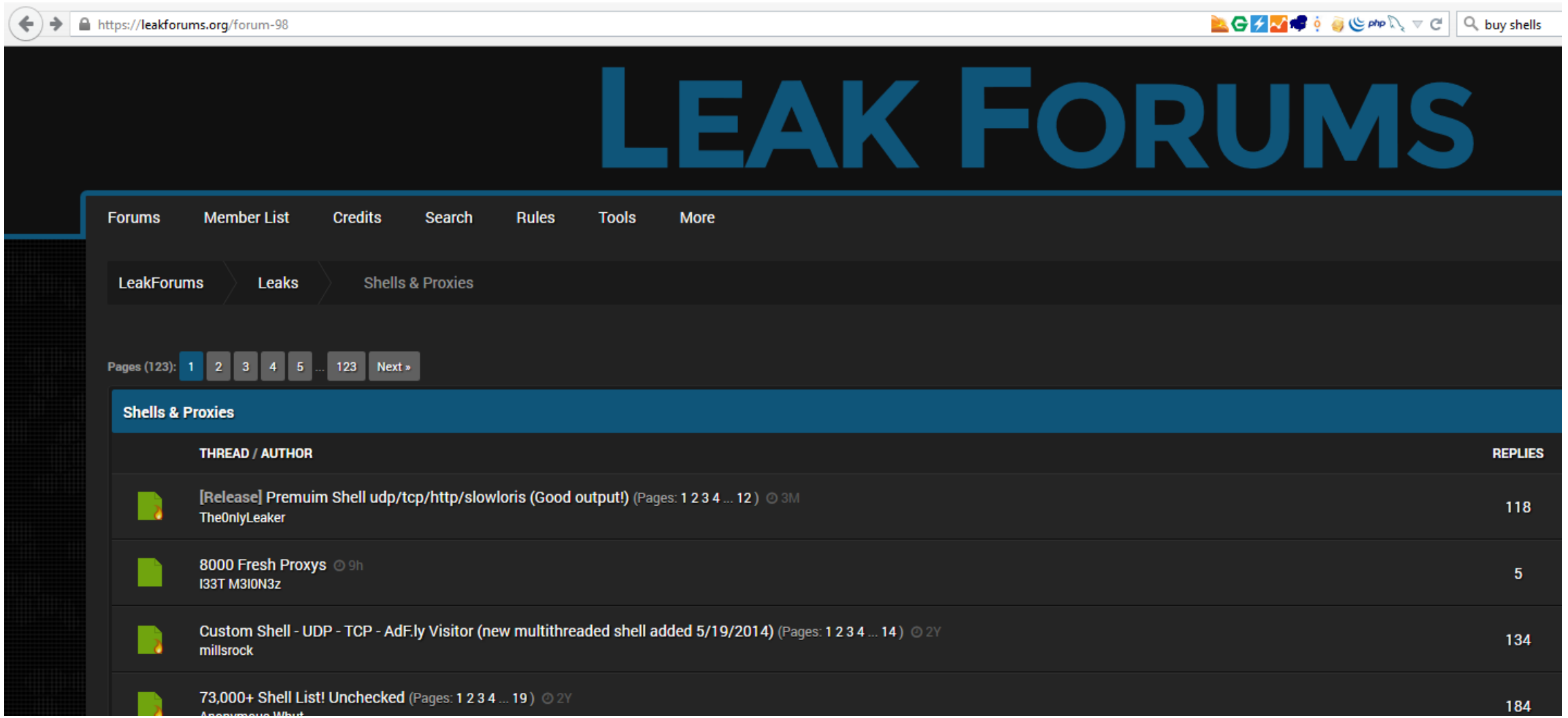
Die Berliner Staatsanwaltschaft ermittelt gegen die vier Geschäftsführer der Online-Bestellplattform Lieferheld wegen des Verdachts auf Computersabotage. Am Mittwoch durchsuchten Beamte des Landeskriminalamts Berlin die Geschäftsräume des 2010 gegründeten Unternehmens, das nach eigenen Angaben bereits 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 unerreichbar 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



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

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.

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

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

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.

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

Angreifer setzt auf fallenden Börsenkurs.

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

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.

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

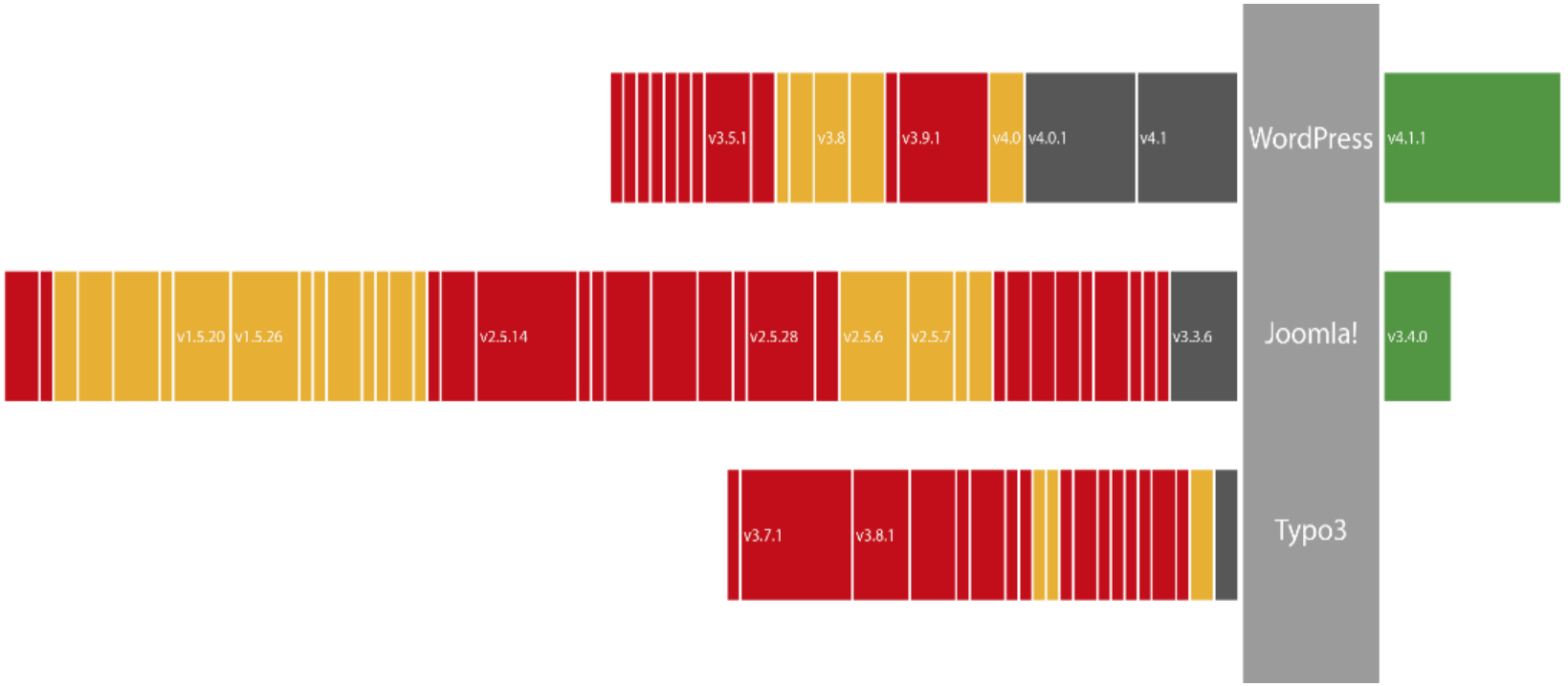
Angreifer setzt auf fallenden Börsenkurs.

Über die angreifbare Webseite werden Fehlinformationen gestreut.

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

Wie wurden Cyberattacken ein Massenproblem?

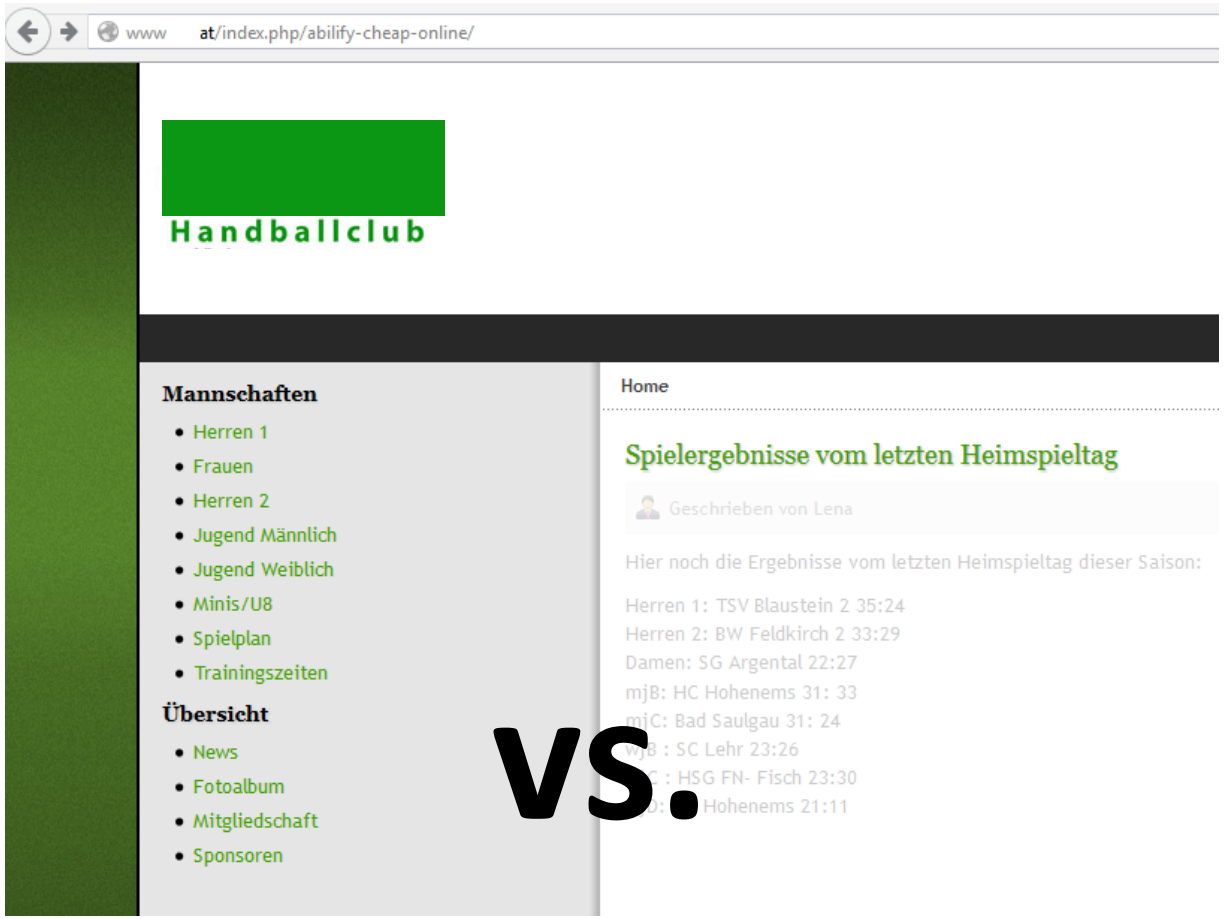
Die Herausforderung



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

Die Geschäftsmodelle der Hacker

„Pharma-Shop“ Angriff



Die Geschäftsmodelle der Hacker

„Pharma-Shop“ Angriff

Die Geschäftsmodelle der Hacker

„Pharma-Shop“ Angriff

Selbstversuch per Google Suche:

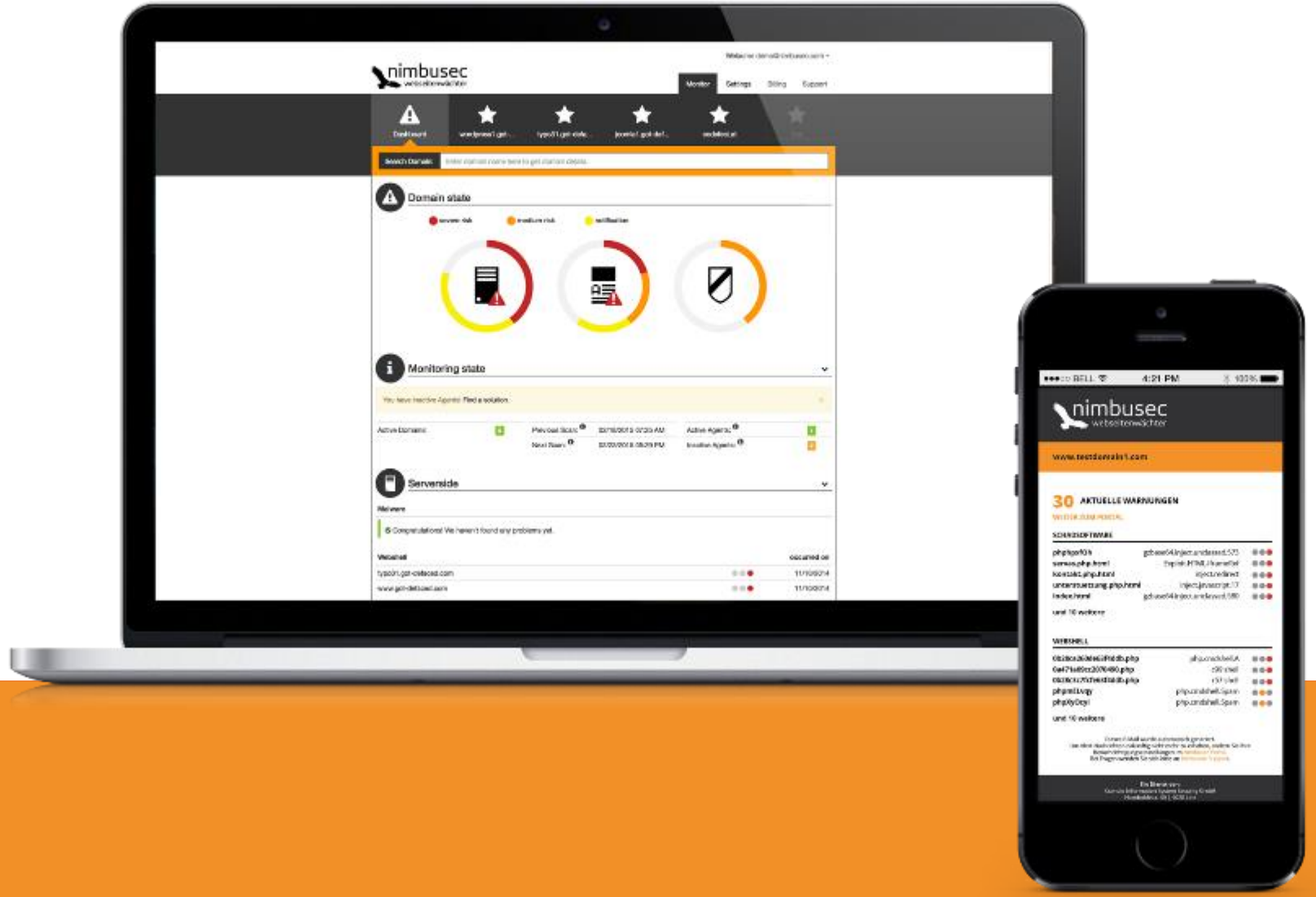
site:at cheap viagra

Ausgezeichnet:

START SECURE 2015
BM.I futurezone.at

CONSTANTINUS
ÖSTERREICHS BERATUNGS- UND IT-PREIS

EDISON
DER PREIS



Im Einsatz:

Red Bull

AMA
AgrarMarkt Austria

TU WIEN
Technische Universität Wien
Department für Raumplanung
Rechtswissenschaften
raum law

Katholische Kirche
in Oberösterreich