MYRA SECURITY GMBH
Made in Germany

eco

Technische Gefahren für Netz- und E-Commerce-Betreiber und ihre Abwehr

Sascha Schumann | Geschäftsführer

19.Februar.2014

Wer ist die Myra Security GmbH

Management

Sascha Schumann (Gründer & CEO), PHP Kernentwickler seit 1998,
Buchautor, Gründer der Soprado GmbH 2006

IT-Struktur

Weltweites High-Performance-DNS mit Custom-Policy
CDN basierend auf Anycast und GeoIP-DNS
Hochverfügbares Netzwerk mit Serverstandorten weltweit

Unternehmen

Ausgründung 2012 als eigene GmbH in München
DDoS-Schutz und Optimierung von Inhalten für Web-Applikationen
High Quality Provider “Made in Germany” mit 24/7 Service

Renommierte Unternehmen vertrauen myracloud

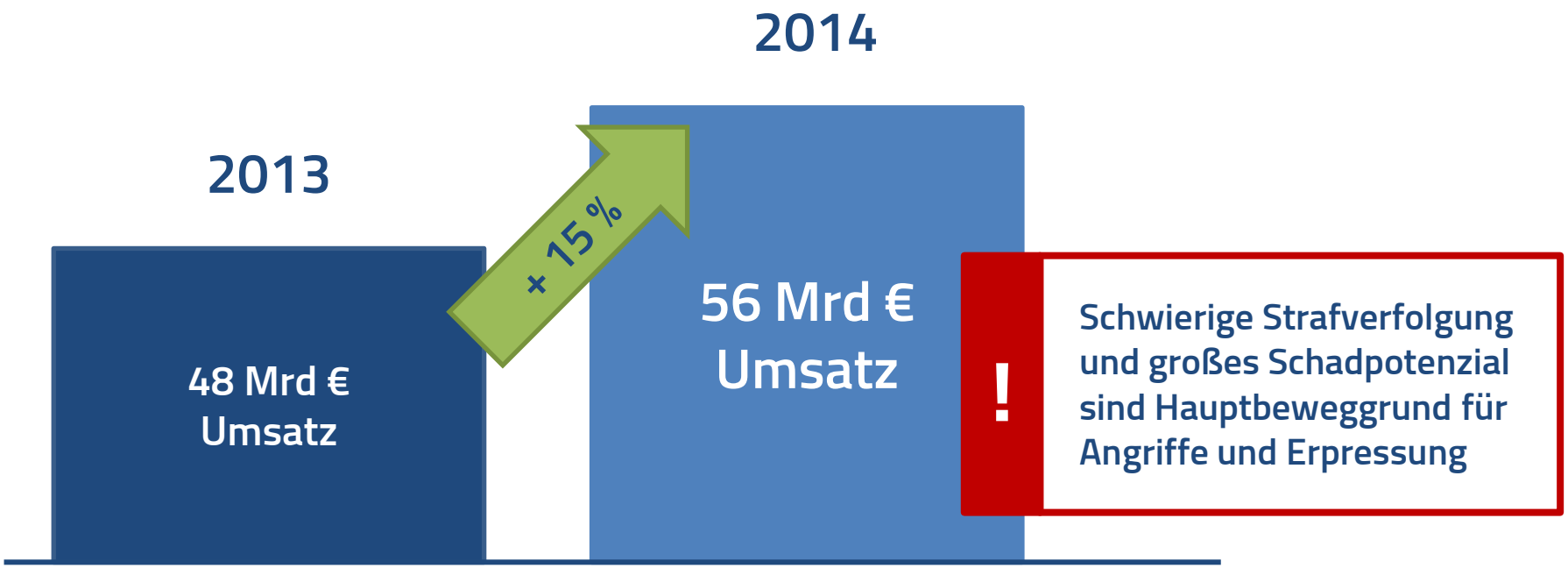
! myracloud sichert aktuell ca. 2,5 Mrd Euro Online-Transaktionsvolumen jährlich.

Bekannte Partner setzen auf myracloud

*in Vorbereitung, Stand Q1 2014

Sicherheitslage

Online-Handel: Lukratives Ziel für Angreifer

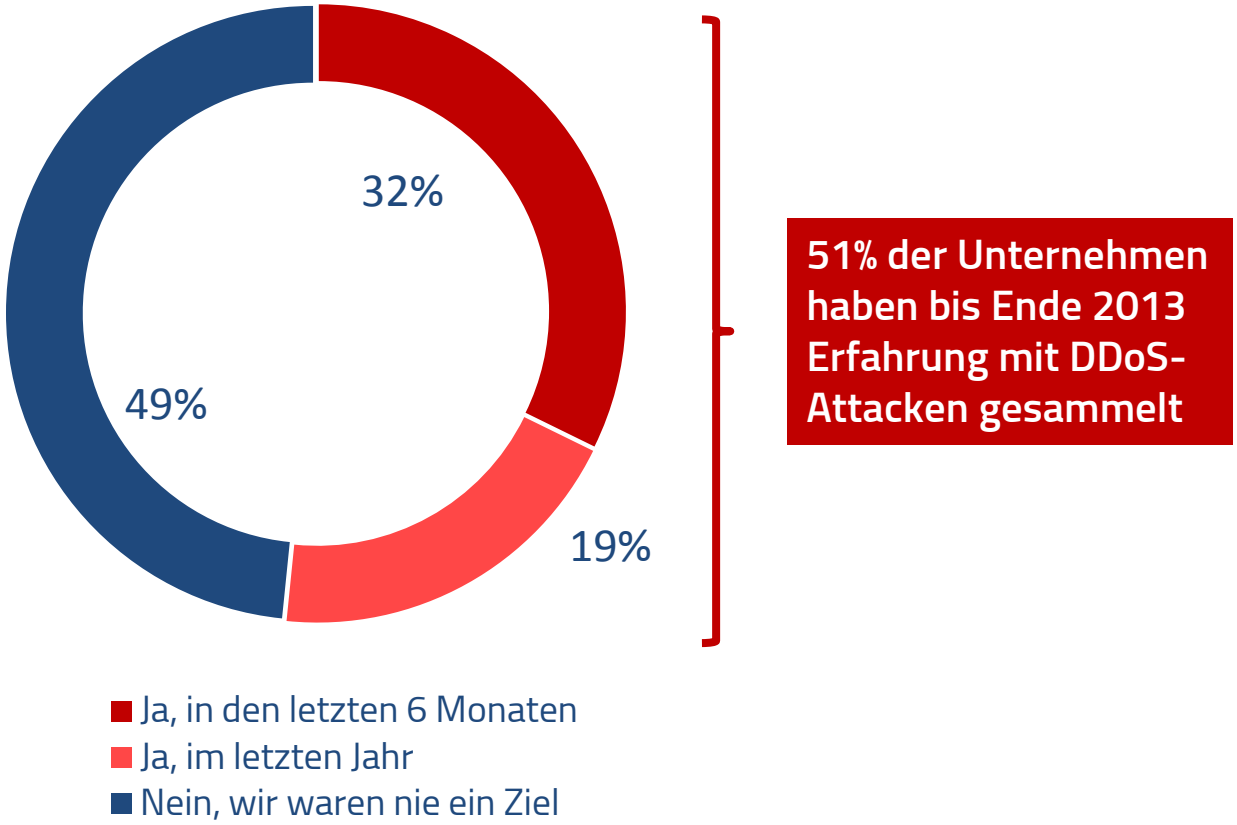


Umsatzausfälle für einen Tag können Online-Händler oft mehrere zehntausend Euro kosten

(1) Quelle: BVH 2014

Erfahrungen der Unternehmen mit DDoS-Attacken

War Ihre Unternehmens-Website bereits Ziel einer DDoS-Attacke?(1)

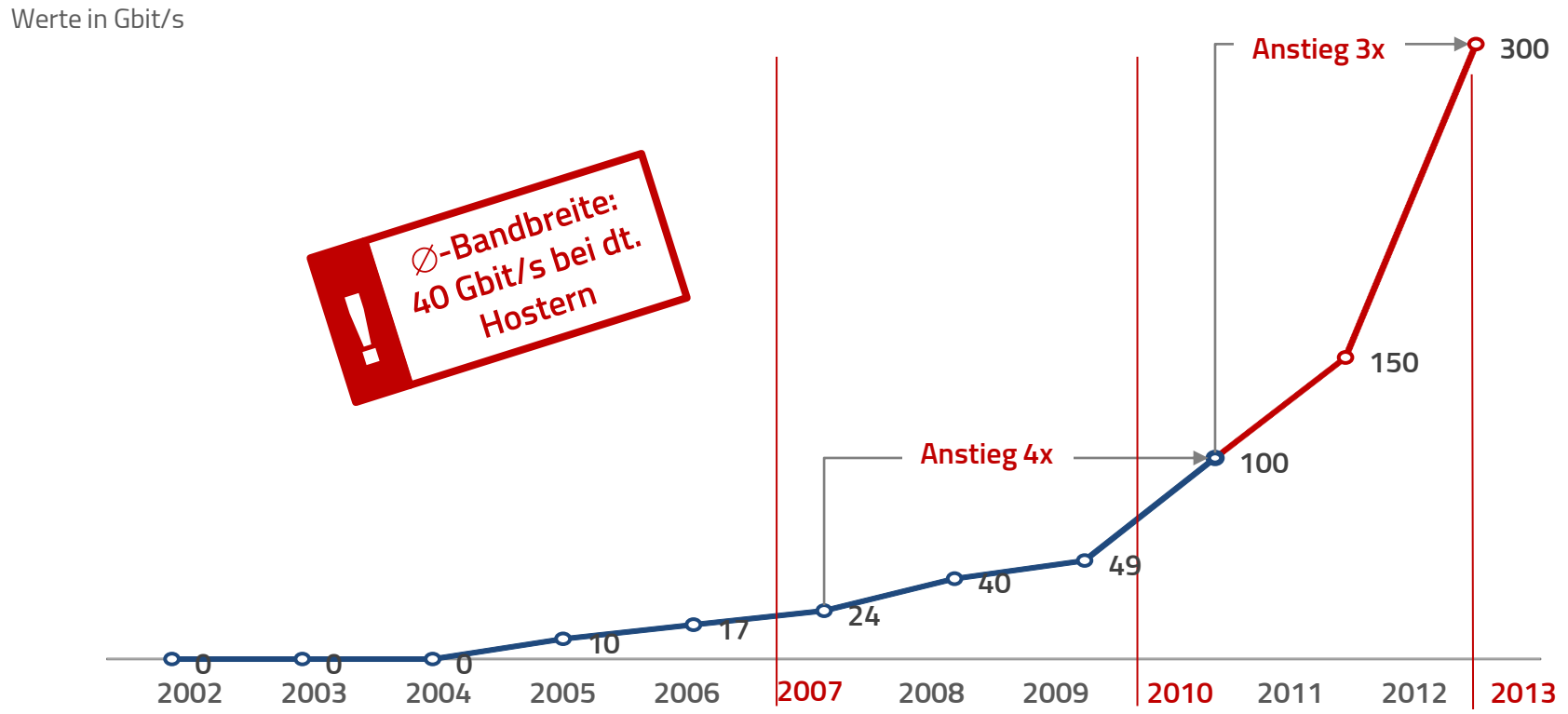


51% der Unternehmen haben bis Ende 2013 Erfahrung mit DDoS-Attacken gesammelt

(1) Quelle: Umfrage SC Magazine, http://www.scmagazine.com/ddos-attack-targets/slideshow/1001/#1

Erfahrungen dt. Unternehmen mit DDoS-Attacken

Anstieg der Peak-Bandbreite von DDoS-Attacken in 2007 – 2013(1)



DDoS-Angriffe treffen mit immer mehr Bandbreite auf die Infrastrukturen

(1) Quelle: Prolexic 2014

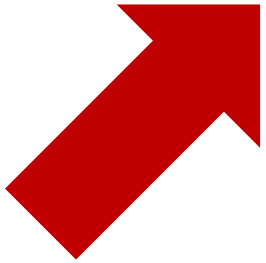
Entwicklung der Angriffe seit 2012

Anzahl der Attacken

+ 26%

Mehr Interesse an Angriffen auf E-Commerce und News-Portale durch sinkende Einstiegshürden

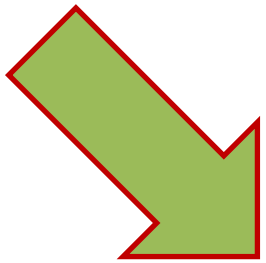
Angriffe auf Layer 7



+ 17%

Schwerer abzuwehrende Angriffe richten sich gezielt auf Applikationen für ein Höchstmaß an Schaden

Dauer der Attacken



- 29%

Von 32 Stunden auf 22 Stunden

Kurze gezielte Angriffe in mehreren Wellen statt langanhaltende Einzelangriffe schützen Botnetze

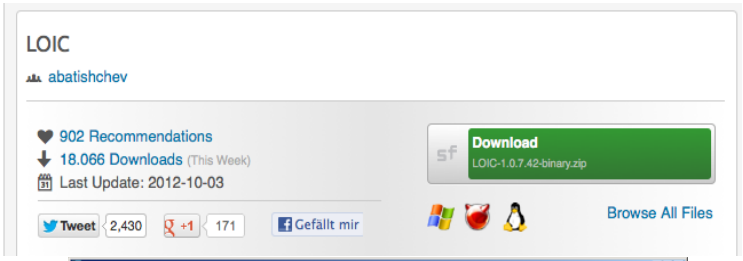
Immer mehr spezialisierte Angriffe auf Schwachstellen in Schutz und Infrastruktur

(1) Quelle: Prolexic 2014

Angriffsarten

DDoS-Angriffe: Eintrittshürden

Do-It-Yourself-Tools



Low-Orbit-Ion-Cannon (LOIC)
High-Orbit-Ion-Cannon (HOIC)

Einfacher Zugang

- Tools herunterladbar
- Einfach zu verwenden
- Proxy-Integration zu Verschleierung

Bedrohung für Websites

- Viele verschiedene und spezialisierte Tools auf dem Markt
- Angreifer sind einfach rekrutierbar (Anonymous)

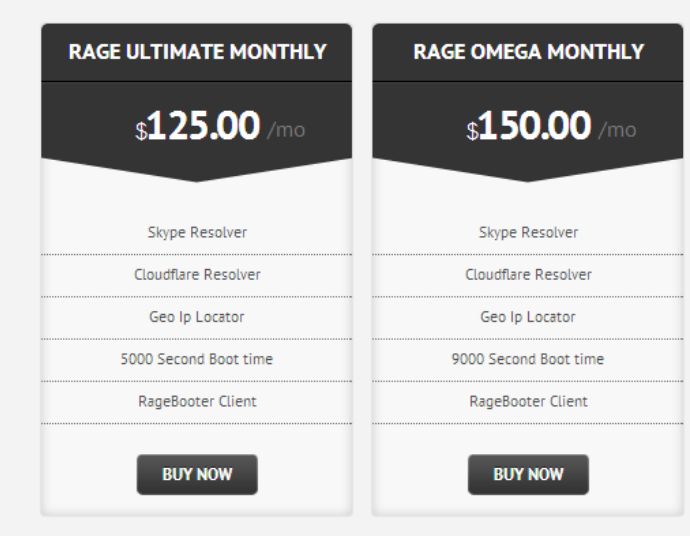
Konsequenzen

- Viele Angreifer erreichen große Bandbreiten
- Strafrechtliche Verfolgung ist extrem schwierig

(1) Source: webroot.com / sourceforge.net

DDoS-Angriffe: Eintrittshürden

DDoS als Dienstleistung



1 Stunde Downtime oft schon für unter 100$

Einfacher Zugang

- Zugang über Website oder Foren
- Anonyme Zahlung möglich (Bitcoins)
- Zugriff auf große Botnetze ohne Aufwand

Bedrohung für Websites

- IP-Resolver umgehen Schutzmechanismen (Cloudflare)
- DDoS-Spezialisten variieren Angriffe

Konsequenzen

- Websites sind einfach abzuschießen
- Nahezu keine rechtliche Handhabe

(1) Source: webroot.com / sourceforge.net

DNS – Beispiel für Verwundbarkeit

DNS Amplification: Verstärkung um Faktor 30 - 50

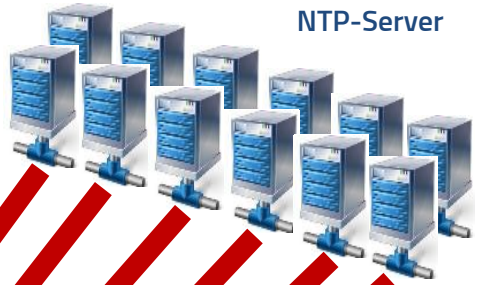
Beispiel:
dig ripe.net. any +edns=0 +bufsize=8000

```
;; Query time: 1 msec
;; SERVER: 213.133.100.100#53(213.133.100.100)
;; WHEN: Mon Dec  9 18:22:26 2013
;; MSG SIZE  rcvd: 2622
```

```
dig ripe.net. any +edns=0 +bufsize=3000

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> ripe.net. any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56608
;; flags: qr rd ra; QUERY: 1, ANSWER: 23, AUTHORITY: 0, ADDITIONAL: 6

;; QUESTION SECTION:
;ripe.net.                      IN      ANY

;; ANSWER SECTION:
ripe.net.               3509    IN      SOA     pri.authdns.ripe.net. dns.ripe
ripe.net.               3509    IN      RRSIG   SOA 5 2 3600 20140108141509 20
ZtoaDoSADeKT9PV5TRMpvjzsA1q7IZ OYiwd9LGfzr99//PfBo+FufReOwsMMjlF9oifj8CFqRx+tI
ripe.net.               12177   IN      A       193.0.6.139
ripe.net.               12177   IN      RRSIG   A 5 2 21600 20140108141509 201
x+5HGZXMnP38IH9+i8IXA25HpQ+OR 9r56g7A/y6CrO9Uqm/ivUs5E/nQhbr2c3RCmoRcZyuTsU895
ripe.net.               209     IN      AAAA    2001:67c:2e8:22::c100:68b
ripe.net.               209     IN      RRSIG   AAAA 5 2 300 20140108141509 20
3rgswzQRZzvwG879jTEUAQygWtoKt+ wlMt2jtTekKRFKXkwOlydr4E92Z4Pk2kHMVSg8svJxiPC7F
ripe.net.               505     IN      NS      sec3.apnic.net.
ripe.net.               505     IN      NS      sec1.apnic.net.
ripe.net.               505     IN      NS      pri.authdns.ripe.net.
ripe.net.               505     IN      NS      sns-pb.isc.org.
ripe.net.               505     IN      NS      tinnie.arin.net.
ripe.net.               505     IN      NS      ns3.nic.fr.
ripe.net.               505     IN      RRSIG   NS 5 2 3600 20140108141509 201
tpm1R7TIpO6zJB7zNfWxhoYzpxD/k 9y7n+qeKMdGSMvBOJdvOYxucCBNnYCOF/I79Pww5G8H7IMfx
ripe.net.               23      IN      MX      250 kaka.ripe.net.
ripe.net.               23      IN      MX      200 koko.ripe.net.
ripe.net.               23      IN      RRSIG   MX 5 2 300 20140108141509 2013
6AMiNWN6/hzQnRO5k/iUIe3yxZAY UVfDM4w5sOSmq4feFVu+ga9tz99vpbaM4KuGA8S+dsZ9odMR4
ripe.net.               3509    IN      DNSKEY  256 3 5 AwEAAX5niIktGAUdDijpgi
GMRD26xPVeEz/6PmdZJ5KwEGGguSiWvLOoJQ LC5hCWKl
ripe.net.               3509    IN      DNSKEY  257 3 5 AwEAAalnxwsXNVENfxBjx5
cG+Ys7XtJScqL7T9jnUfHUgLSS7VbNRLdODx 4Oelfn9WgaRZkq7Oj6wUeadwDn6zaBPw4Vc3yH6VO
gFOzZ1MuNxfmuF7QK 5SSjPoDRdDE=
ripe.net.               3509    IN      DNSKEY  257 3 5 AwEAAYSPd7+AJXOT1k1d6e
F8XiuPsemLLNbhosGofv5vO3i2TKxJI/sgf1 n9WtkMY1bCTTaSUn5GmjKDvOXRPKkzA4RCQv8s18p
1EuMzsZU21iGhRO1N Z4HFSr9jb3U=
ripe.net.               3509    IN      DNSKEY  256 3 5 AwEAAZx4OS5w7+F2hh4IYW
jm9sNP2S9uokTfBYzgIoTObFwpBLK3yd3o6N 8zLdDzh5
ripe.net.               3509    IN      RRSIG   DNSKEY 5 2 3600 20140108141509
l+4OOmlrjdwY2nf3Th/iQyqAaCXoMJOro bZEu9/8uS8x6UbDUCPEejHYVKkU5pufNuDTIRDtxtA6U
pDqrCiwZ8kU+AO AVJPJ9dLJ9QpclGGXUQ+YfZaLezO4nsjASIA72SlMlYWkVo8FbHXkik2 xXDR8C
ripe.net.               209     IN      NSEC    256cns.ripe.net. A NS SOA MX A
ripe.net.               209     IN      RRSIG   NSEC 5 2 300 20140108141509 20
KOPtx8GYd+y2DvcTrSw87LmbEuzTmg 1rtSPcx/d4QlupBbVyjxy7Pm333YSQtdIRxOGWtG6yo4FKO

;; ADDITIONAL SECTION:
pri.authdns.ripe.net.   3434    IN      A       193.0.9.5
pri.authdns.ripe.net.   3434    IN      AAAA    2001:67c:e0::5
koko.ripe.net.          13288   IN      A       193.0.19.72
koko.ripe.net.          19164   IN      AAAA    2001:67c:2e8:11::c100:1348
kaka.ripe.net.          13289   IN      A       193.0.19.71
kaka.ripe.net.          19164   IN      AAAA    2001:67c:2e8:11::c100:1347

;; Query time: 1 msec
;; SERVER: 213.133.100.100#53(213.133.100.100)
;; WHEN: Mon Dec  9 18:22:26 2013
;; MSG SIZE  rcvd: 2622
```

NTP-Amplification

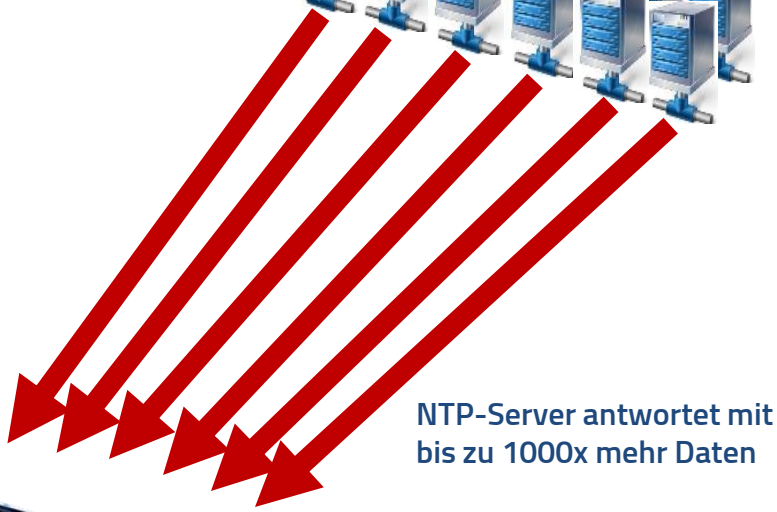
Angreifer frägt NTP-Server mit gespoofter IP-Adresse des Opfers an



NTP-Server

Die Angriffs-Bandbreite

- DNS-Amplification:
  Faktor 30-50
- NTP-Amplification:
  Faktor 10-1.000
- Angriffe mit mehreren
  100 Gbit/s möglich



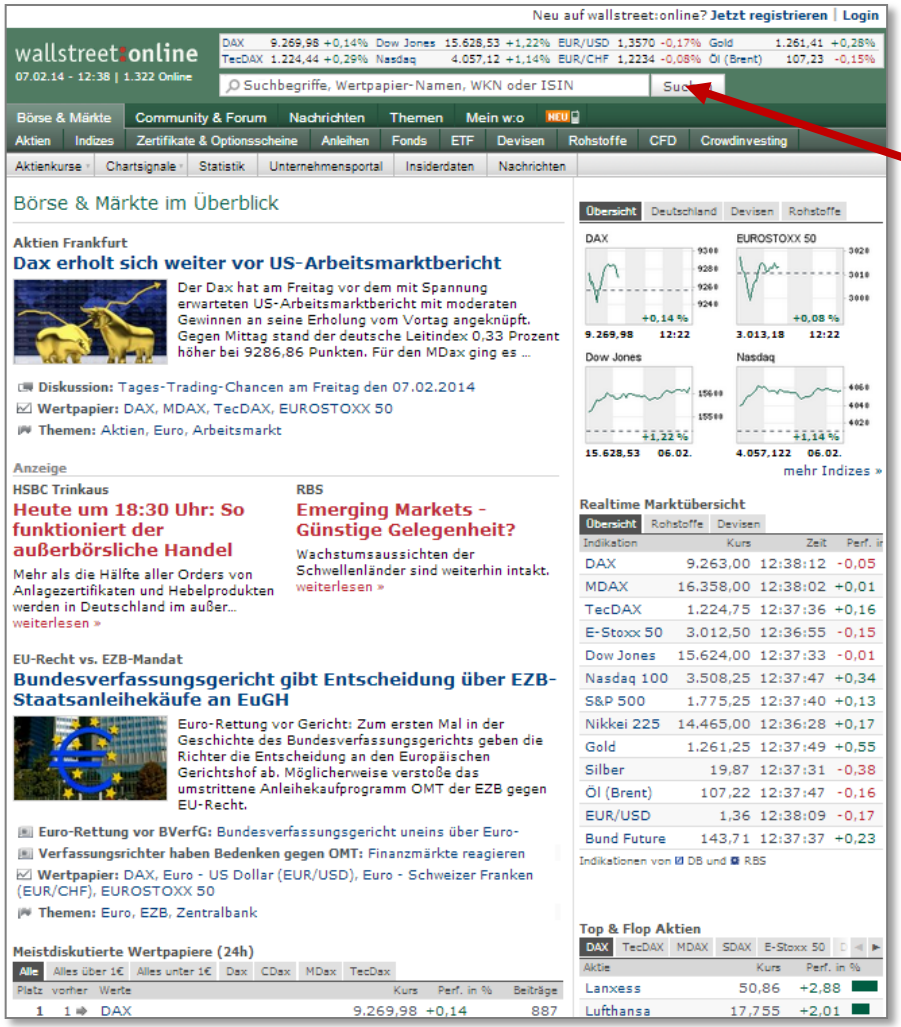
NTP-Server antwortet mit bis zu 1000x mehr Daten

IT-Infrastruktur des Website-Betreibers

Fallbeispiel DDoS-Attacke

MYRA SECURITY GMBH
Made in Germany

wallstreet:online – Anatomie des Angriffs



Varianten der Angriffe

- GET-Flood auf das Suchfeld
- Sehr teure Anfrage für Webserver und Datenbank

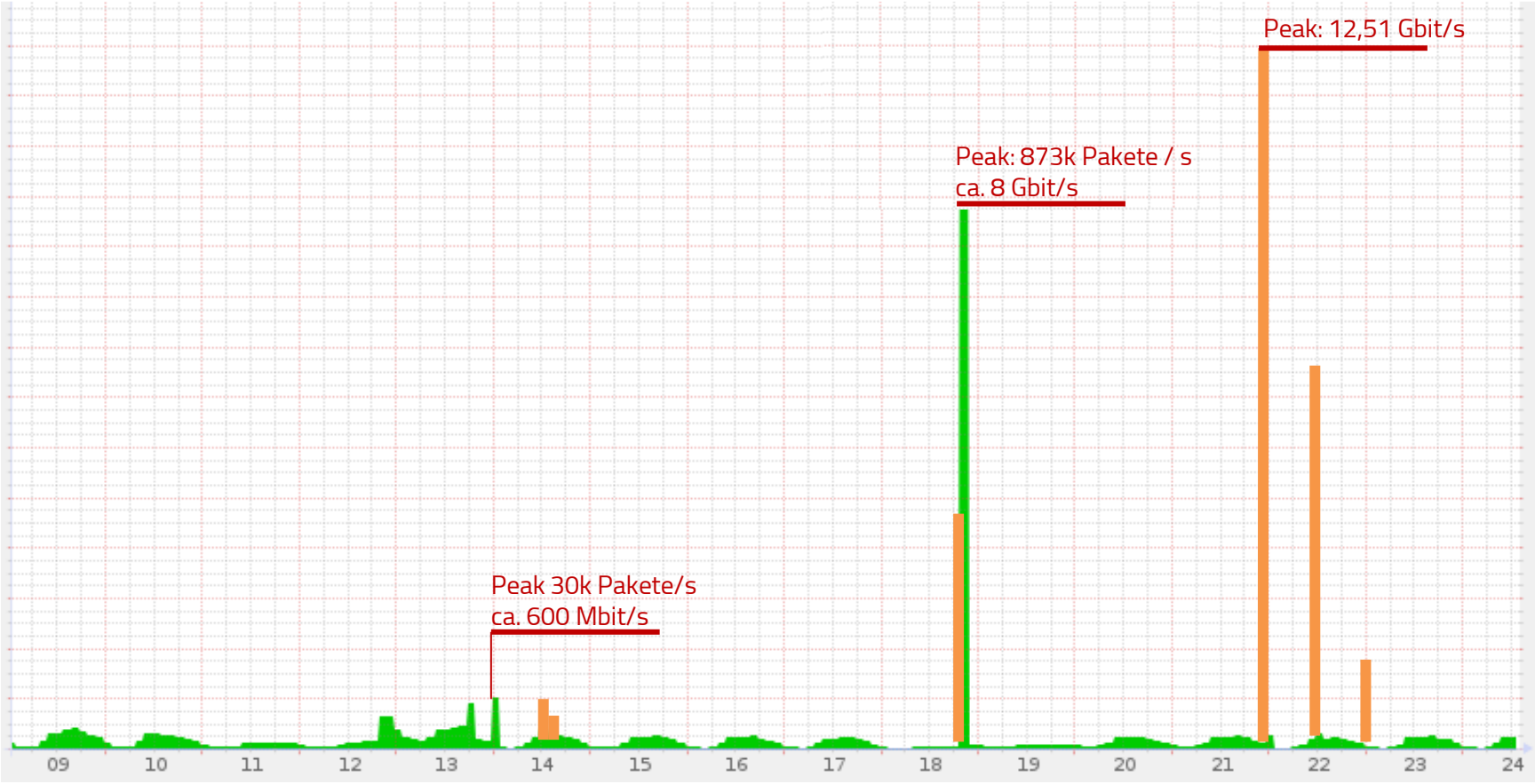
- GET-Flood auf Teile des Forums
- Gezielter Angriff auf spezielle Ressourcen

- DNS-Amplification
- Angriffe auf die Filter-Server

- Slow-Loris-Attacke
- Im Peak über 120.000 Verbindungen

- Angriff dauerte fast 3 Wochen an
- Attacke wurde auf assoziierte Websites ausgedehnt
- Muster wurden ständig variiert

Übersicht Angriff wallstreet-online.de



Pakete / Sekunde auf wallstreet-online.de (Layer 7)

Traffic auf Filterschicht 1 (Layer 3/4)

Kundenmeinung– wallstreet:online

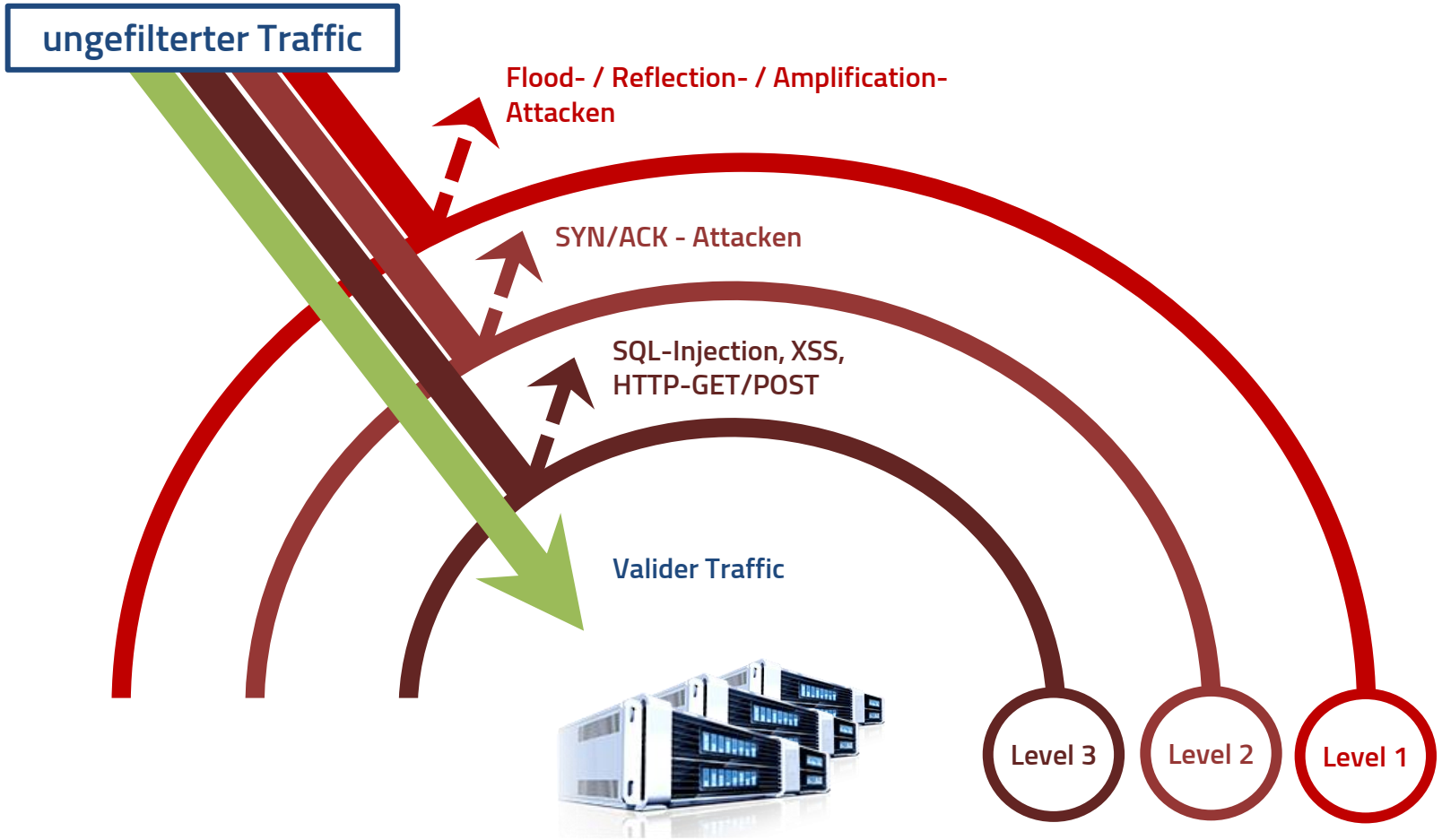
„Wir sind froh darüber, uns frühzeitig für eine umfassende IT-Sicherheitslösung entschieden zu haben, sodass durch den Angriff auftretende Störungen sofort eingedämmt wurden und Schäden somit erst gar nicht entstanden."

Christoph Kolbinger, CTO, wallstreet:online AG, Januar 2014

Abwehr von Attacken

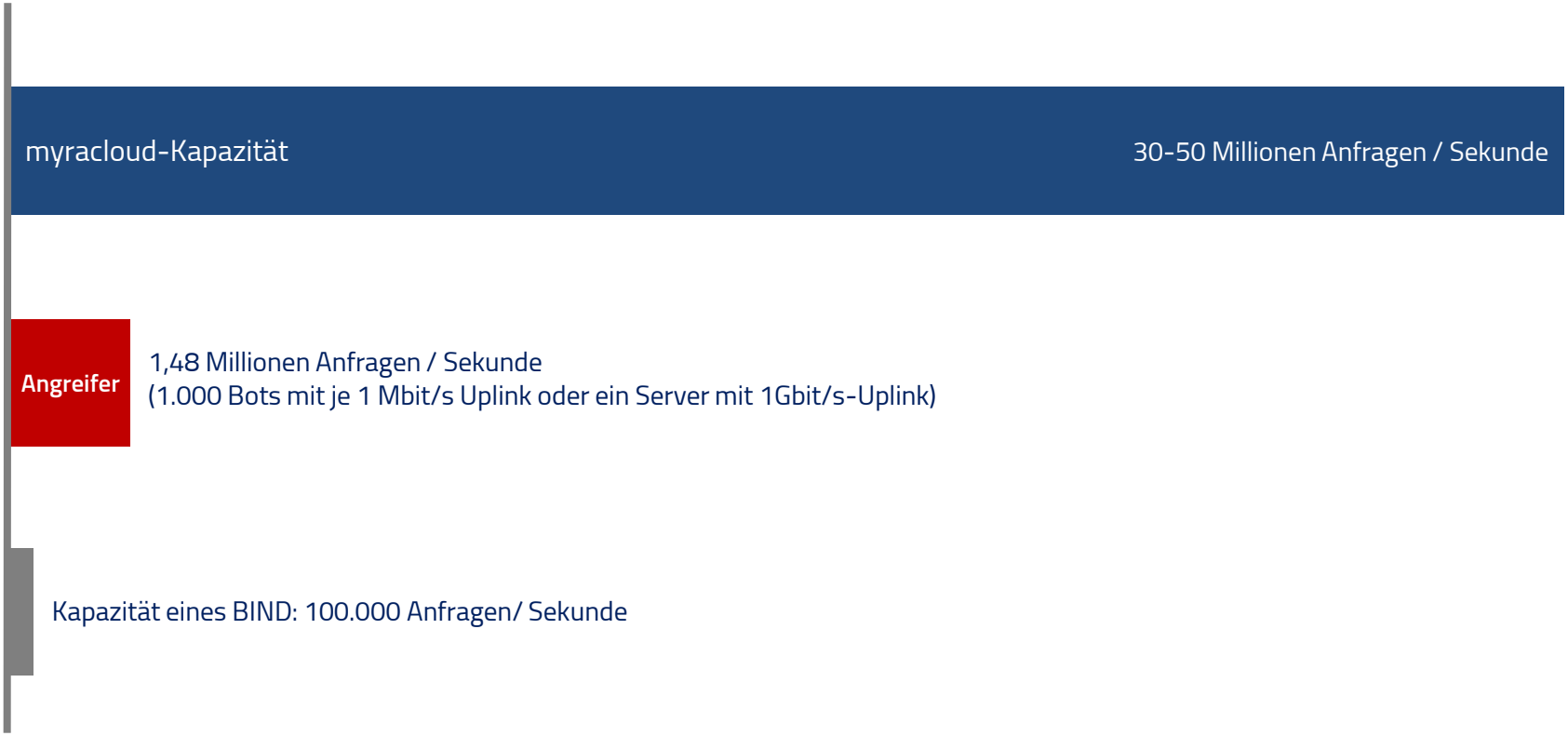
MYRA SECURITY GMBH
Made in Germany

Netzwerk-Schutz durch Multi-Level-Filtering



Effektiver Schutz für Ihre IT-Infrastuktur

myracloud-DNS – Leistungsfähigkeit im Vergleich



myracloud Protection Suite – Cloud und Appliance

! Standard-Szenario

Die myracloud Protection Suite analysiert und filtert den Traffic im RZ des Kunden

Kleine Angriffe können von der Appliance selbst abgewehrt werden

myracloud-Appliance

Abgleich der Filterregeln mit der Cloud

Cloud-basierter DDoS-Schutz

IT-Infrastruktur des Kunden

myracloud Protection Suite – Cloud und Appliance

! Angriffs-Szenario

- Bei großen Volumenangriffen meldet die Appliance das Angriffsmuster an die Cloud
- Traffic wird umgeroutet und gefiltert
- Gerenigter Traffic fließt weiter zum Kunden

myracloud-Appliance

Stetige Kommunikation mit der Cloud

Cloud-basierter DDoS-Schutz

IT-Infrastruktur des Kunden

MYRA
SECURITY GMBH
Made in Germany

Sascha Schumann, Geschäftsführer
+49 89 / 41 41 41 -337
sascha.schumann@myracloud.com

http://myrasecurity.com
Myra Security GmbH | Wredestr. 7 | 80335 München