Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)

DDoS-Angriffe: Gefahren und Verteidigungsstrategien

ECSM

Tobias Scheible, M.Eng.

Tobias Scheible, M.Eng.

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- 1999 GeoCities Website, 2000 eigene Domain, 2001 Kundenprojekte
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter
  - Aktuelle & ehemalige Lehrmodule (Auswahl):
    - Netzsicherheit I: IT-Sicherheit von Netzwerken Hochschulzertifikatsprogramm
    - Grundlagen der digitalen Forensik Masterstudiengang IT GRC Management
    - Internettechnologien Hochschulzertifikatsprogramm
    - Cloud Technologies and Cloud Security Architectures Masterstudiengang IT GRC Management
    - Digitale Forensik Bachelorstudiengang IT Security
    - Internet Grundlagen Masterstudiengang Digitale Forensik
    - Informationssicherheit Bachelorstudiengang Wirtschaftsinformatik
- Buch- & Zeitschriftenautor, Blogger, Referent, …

DDoS-Angriffe: Gefahren und Verteidigungsstrategien

Hochschule Albstadt-Sigmaringen

- 1971 Gründung der Fachhochschule Sigmaringen
- 1988/89 Campus Albstadt
- 2004 Fachhochschule wird in Hochschule umbenannt
- 32 Bachelor- und Masterstudiengänge

Fakultät Engineering

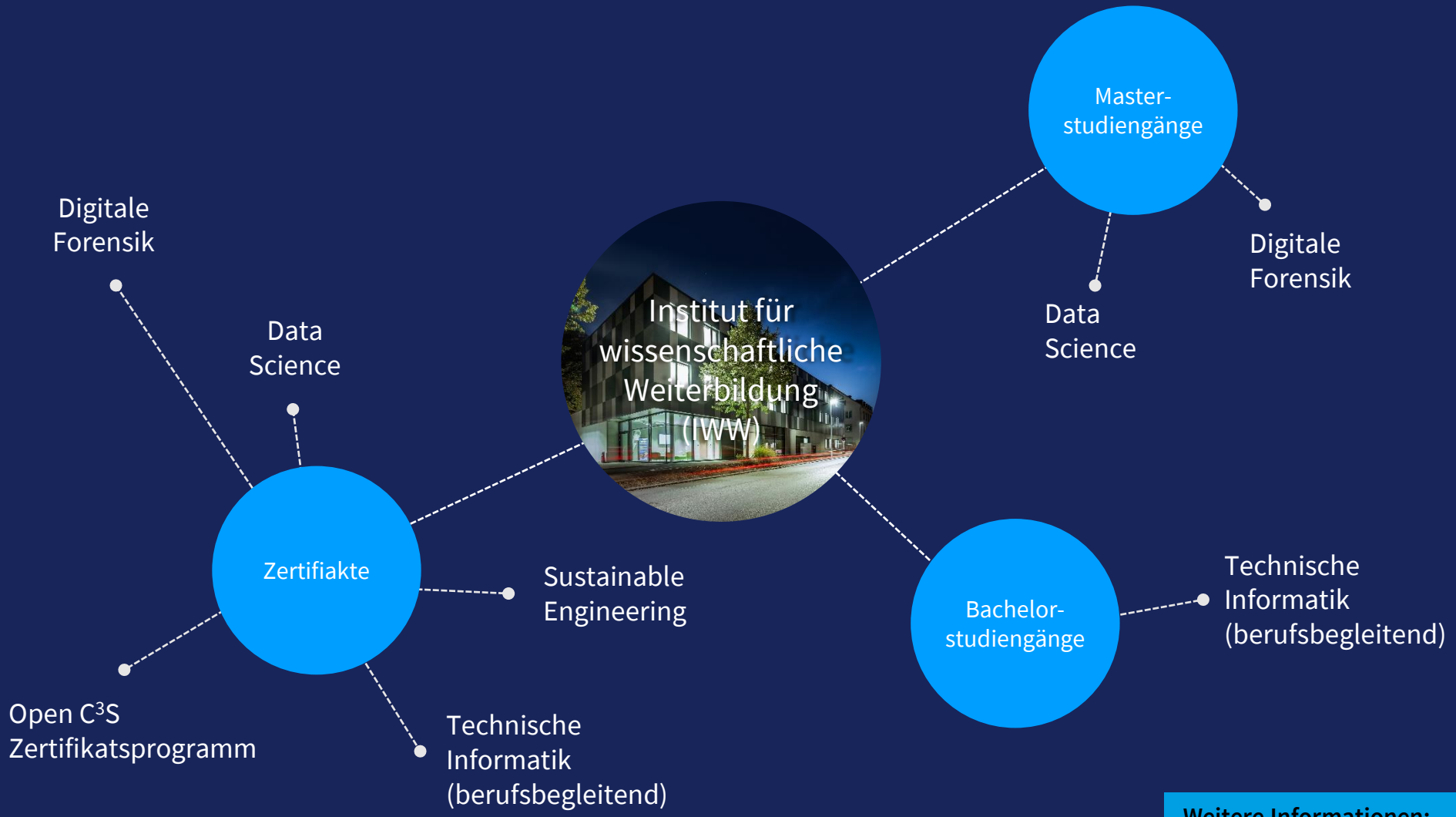
Fakultät Business Science and Management

Fakultät Life Sciences

Fakultät Informatik

DDoS-Angriffe: Gefahren und Verteidigungsstrategien

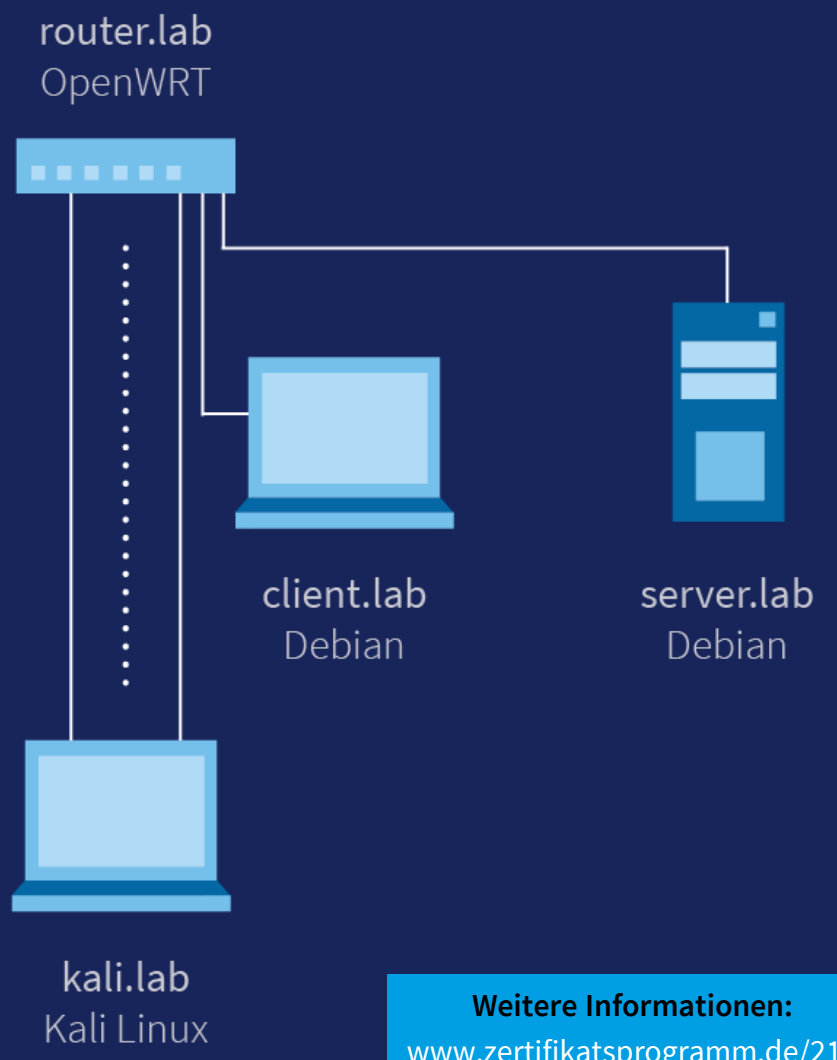
Institut für wissenschaftliche Weiterbildung



Weitere Informationen:
www.hs-albsig.de/iww

DDoS-Angriffe: Gefahren und Verteidigungsstrategien

Netzsicherheit I: IT-Sicherheit von Netzwerken



Weitere Informationen:
www.zertifikatsprogramm.de/214

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)

DDoS-Angriffe: Gefahren und Verteidigungsstrategien

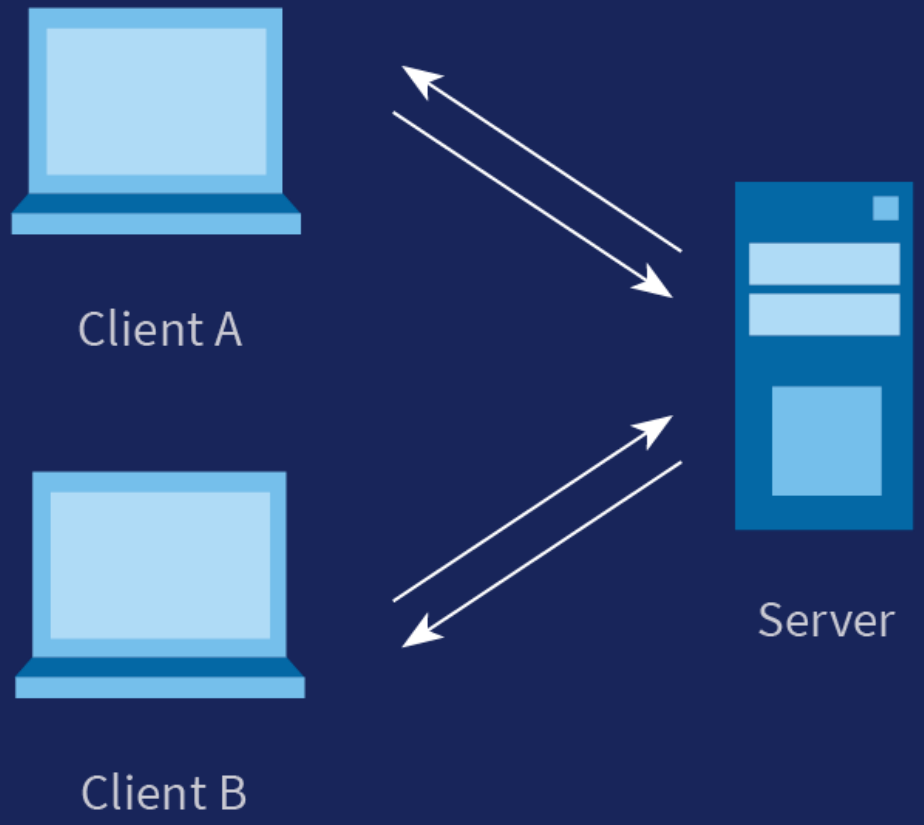
Agenda

- (D)DoS Angriffsmethode
  - Denial of Service (DDoS)
  - Distributed Denial of Service (DDoS)
  - Motivation hinter DDoS-Angriffen
  - Cybercrime-as-a-Service
- Quantitative Angriffe
  - ICMP Flood
  - SYN Flood (TCP/SYN)
  - Verstärkende Angriffe
- Qualitative Angriffe
  - HTTP Flood
  - TLS Handshake
  - Slowloris
- (D)DoS Abwehrstrategien
  - Präventive Maßnahmen
  - Aktive Gegenmaßnahmen
  - DDoS-Mitigation
  - Weitere Ressourcen

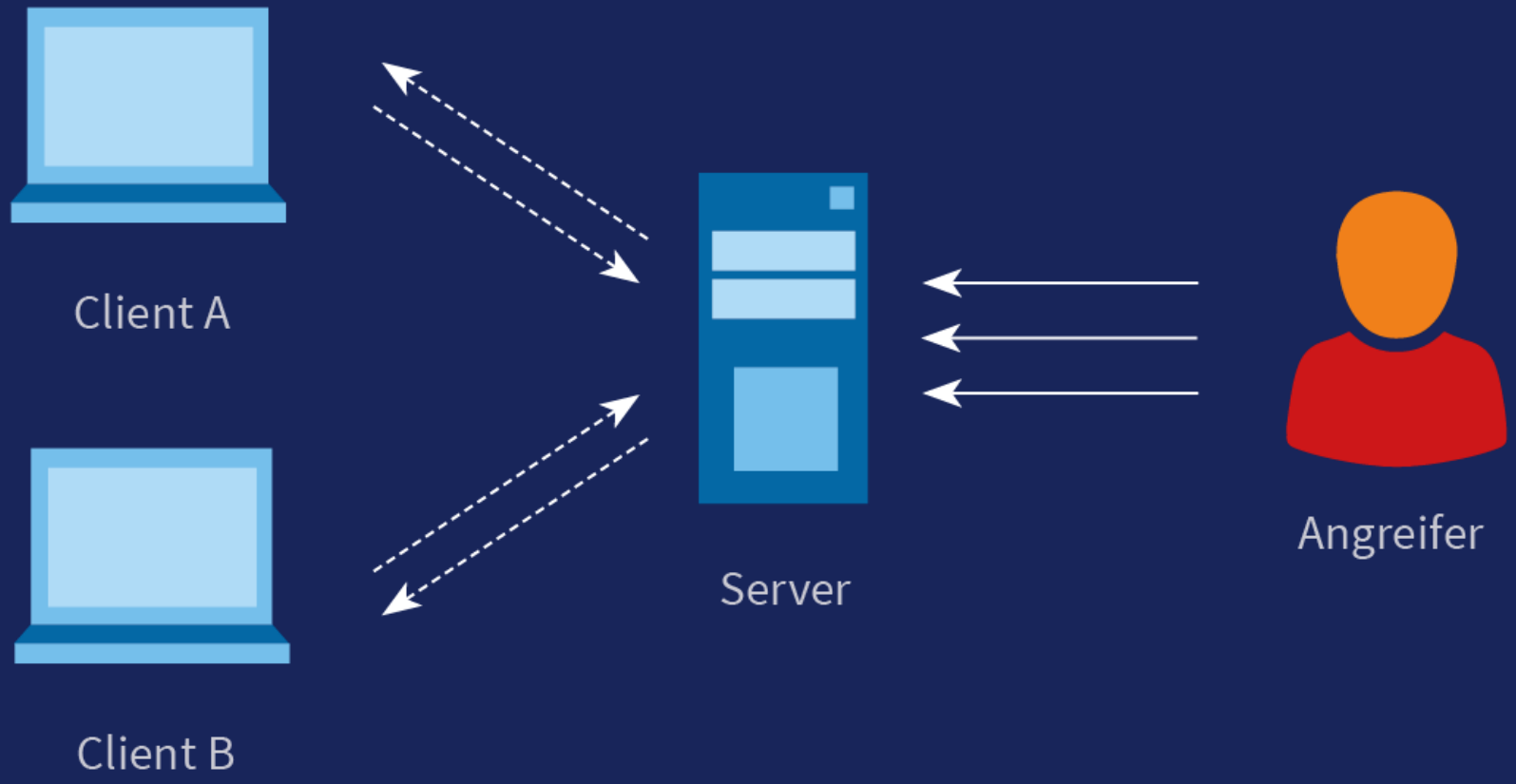
Hinweis
Die komplette Präsentation wird im Anschluss unter *www.scheible.it* bereitgestellt.

(D)DoS Angriffsmethode

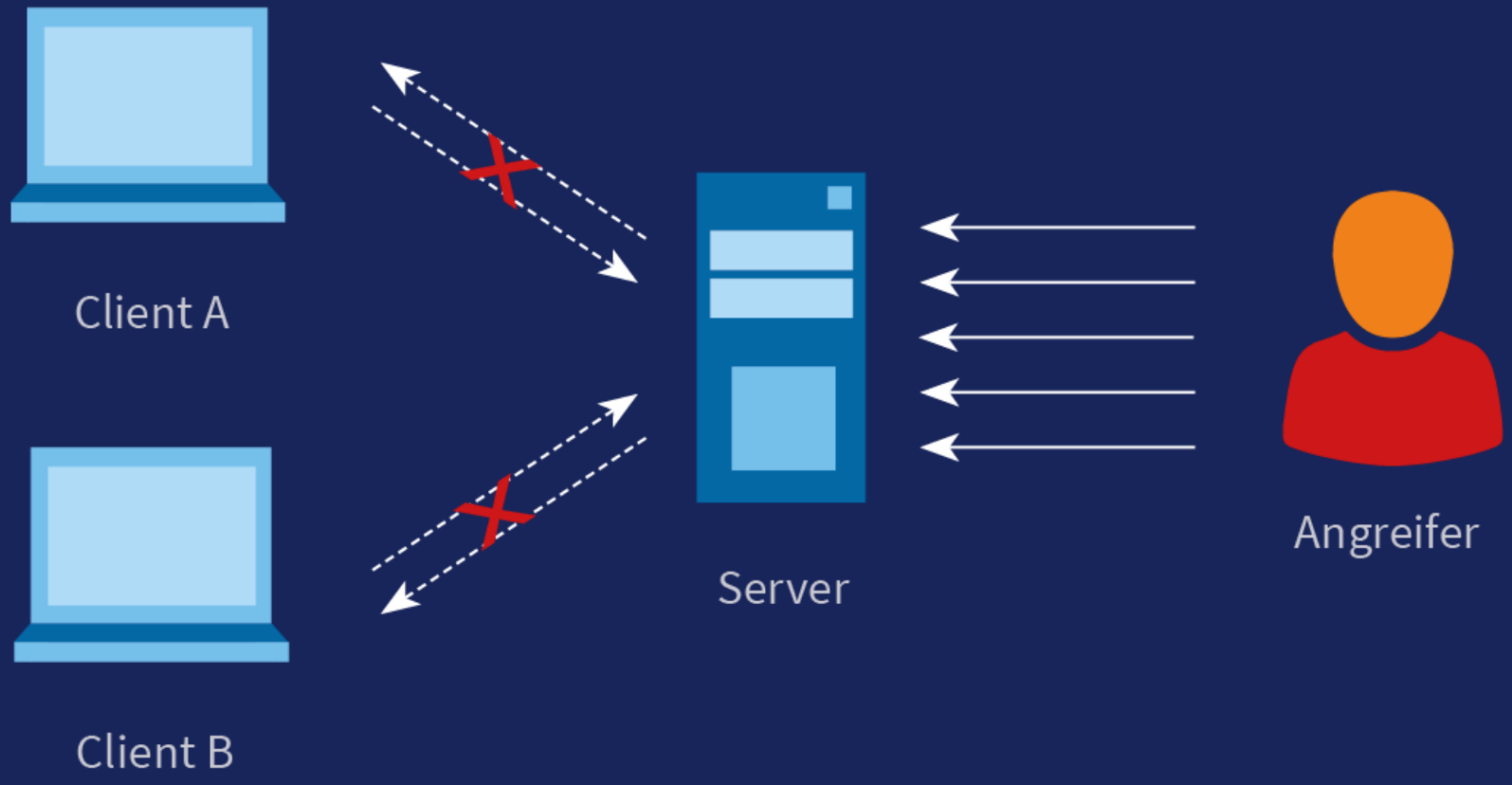
Denial of Service (DoS)



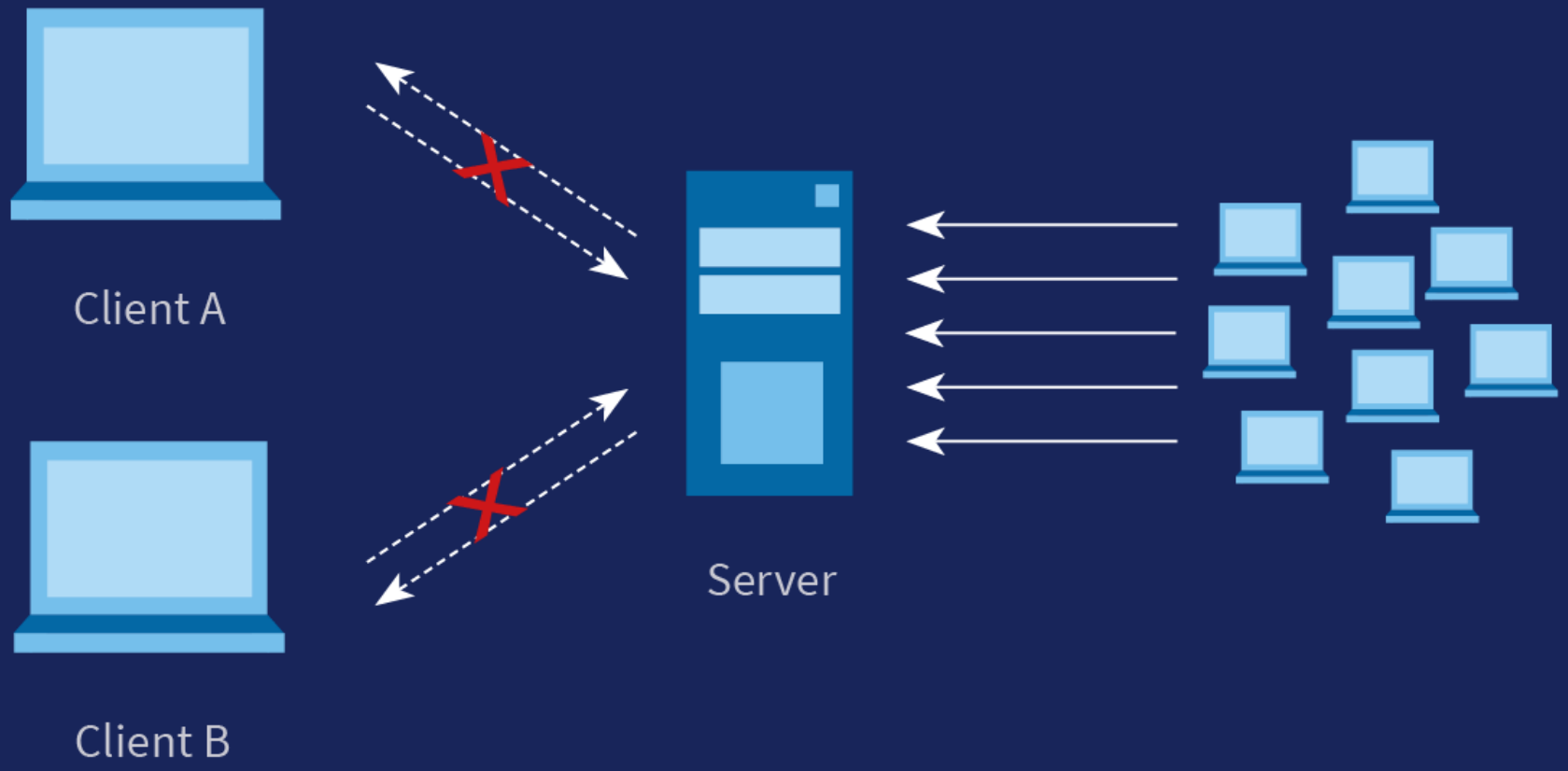
Denial of Service (DoS)



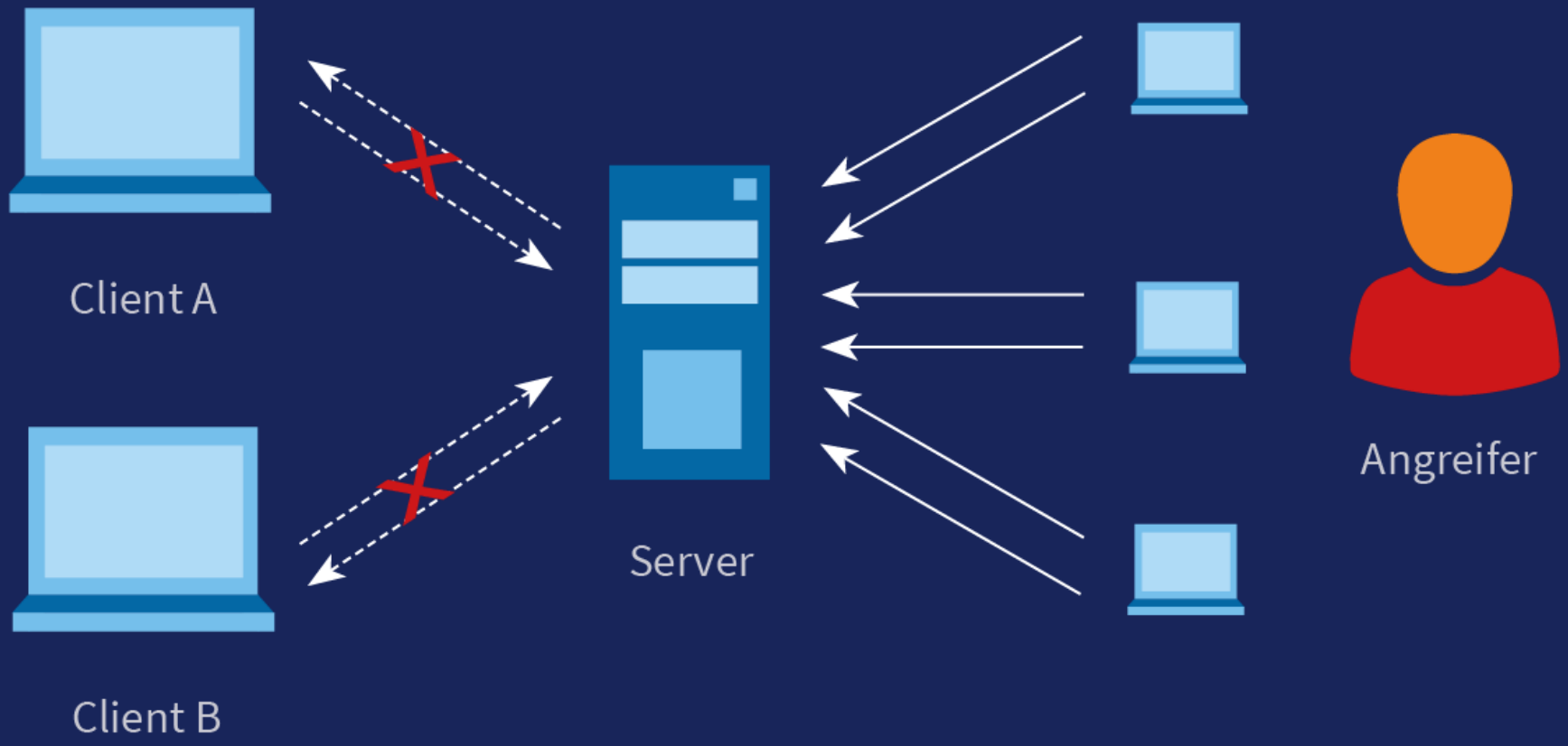
Denial of Service (DoS)



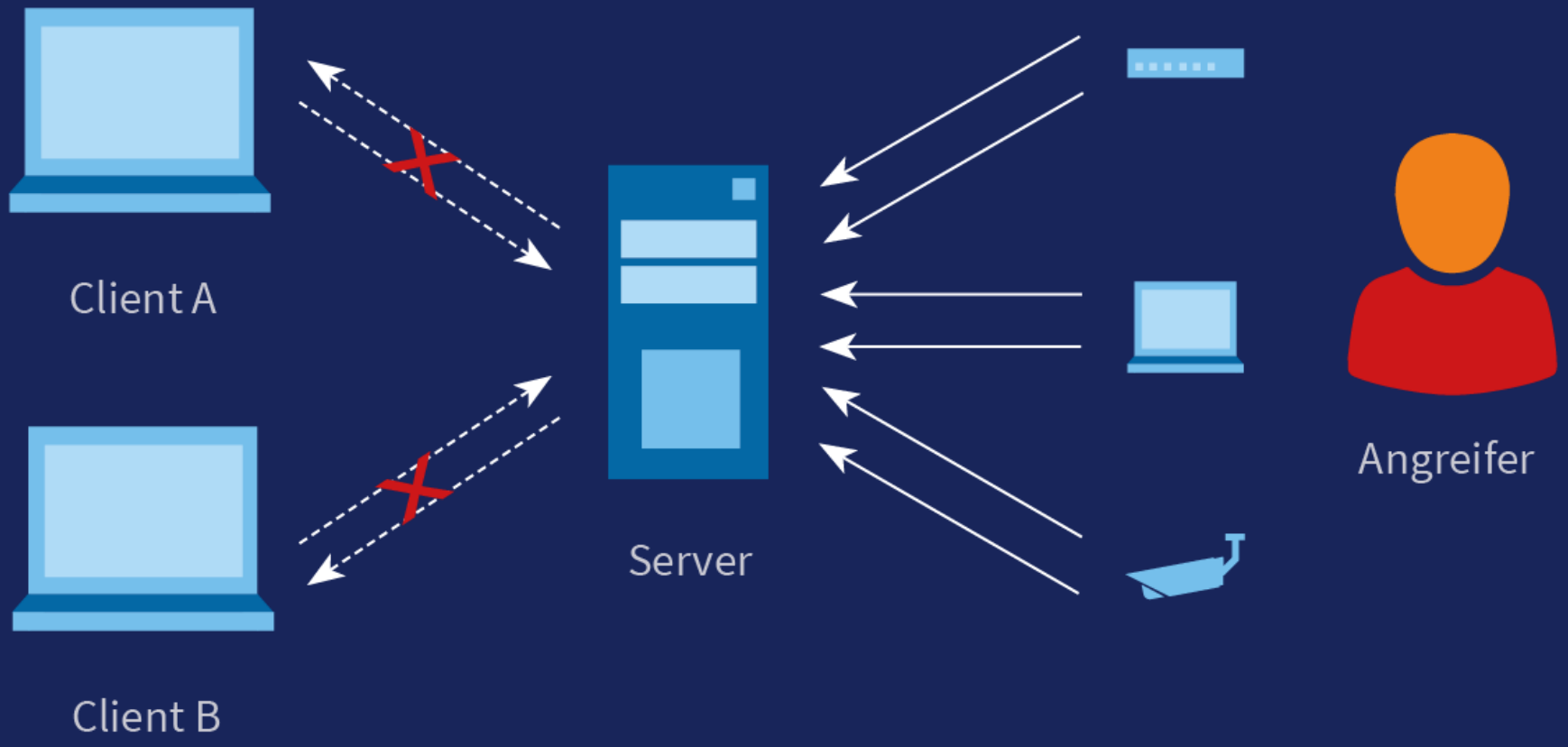
Denial of Service (DoS) - Überlastung



Distributed Denial of Service (DDoS)



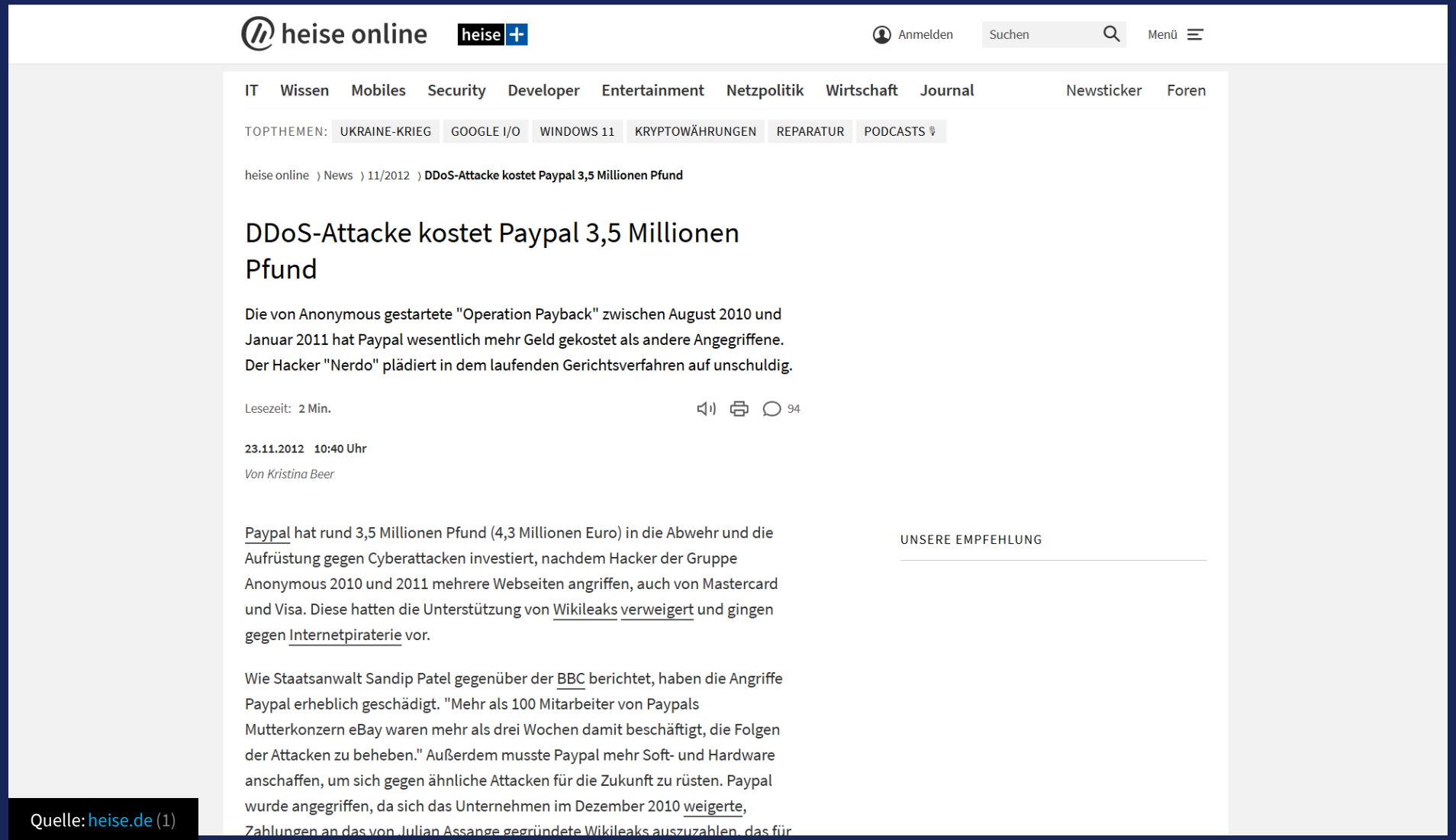
Distributed Denial of Service (DDoS)



Motivation hinter DDoS-Angriffen

Protestaktionen
Hacktivismus
Cyber-Vandalismus

Motivation hinter DDoS-Angriffen



heise online heise+ Anmelden Suchen Menü

IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN: UKRAINE-KRIEG GOOGLE I/O WINDOWS 11 KRYPTOWÄHRUNGEN REPARATUR PODCASTS

heise online › News › 11/2012 › DDoS-Attacke kostet Paypal 3,5 Millionen Pfund

DDoS-Attacke kostet Paypal 3,5 Millionen Pfund

Die von Anonymous gestartete "Operation Payback" zwischen August 2010 und Januar 2011 hat Paypal wesentlich mehr Geld gekostet als andere Angegriffene. Der Hacker "Nerdo" plädiert in dem laufenden Gerichtsverfahren auf unschuldig.

Lesezeit: 2 Min. 94

23.11.2012 10:40 Uhr

Von Kristina Beer

Paypal hat rund 3,5 Millionen Pfund (4,3 Millionen Euro) in die Abwehr und die Aufrüstung gegen Cyberattacken investiert, nachdem Hacker der Gruppe Anonymous 2010 und 2011 mehrere Webseiten angriffen, auch von Mastercard und Visa. Diese hatten die Unterstützung von Wikileaks verweigert und gingen gegen Internetpiraterie vor.

Wie Staatsanwalt Sandip Patel gegenüber der BBC berichtet, haben die Angriffe Paypal erheblich geschädigt. "Mehr als 100 Mitarbeiter von Paypals Mutterkonzern eBay waren mehr als drei Wochen damit beschäftigt, die Folgen der Attacken zu beheben." Außerdem musste Paypal mehr Soft- und Hardware anschaffen, um sich gegen ähnliche Attacken für die Zukunft zu rüsten. Paypal wurde angegriffen, da sich das Unternehmen im Dezember 2010 weigerte, Zahlungen an das von Julian Assange gegründete Wikileaks auszuzahlen, das für

UNSERE EMPFEHLUNG

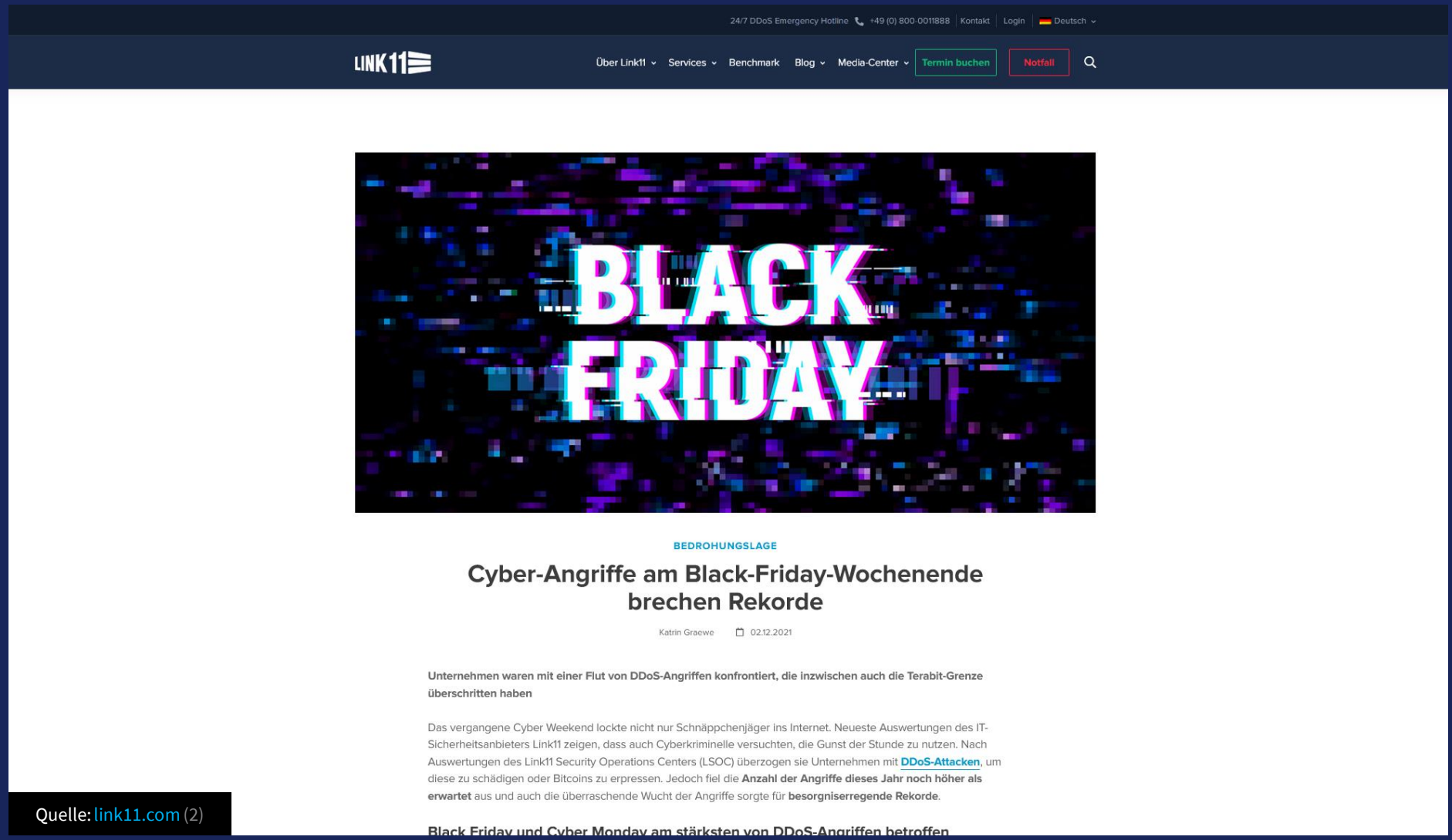
Quelle: heise.de (1)

Motivation hinter DDoS-Angriffen

Protestaktionen
Hacktivismus
Cyber-Vandalismus

Gezielte Schädigungen
Konkurrenz ausschalten
Produktvorstellung verhindern

Motivation hinter DDoS-Angriffen



24/7 DDoS Emergency Hotline +49 (0) 800-0011888 | Kontakt | Login | Deutsch

LINK11 | Über Link11 | Services | Benchmark | Blog | Media-Center | Termin buchen | Notfall

BEDROHUNGSLAGE

Cyber-Angriffe am Black-Friday-Wochenende brechen Rekorde

Katrin Graewe 02.12.2021

Unternehmen waren mit einer Flut von DDoS-Angriffen konfrontiert, die inzwischen auch die Terabit-Grenze überschritten haben

Das vergangene Cyber Weekend lockte nicht nur Schnäppchenjäger ins Internet. Neueste Auswertungen des IT-Sicherheitsanbieters Link11 zeigen, dass auch Cyberkriminelle versuchten, die Gunst der Stunde zu nutzen. Nach Auswertungen des Link11 Security Operations Centers (LSOC) überzogen sie Unternehmen mit **DDoS-Attacken**, um diese zu schädigen oder Bitcoins zu erpressen. Jedoch fiel die **Anzahl der Angriffe dieses Jahr noch höher als erwartet** aus und auch die überraschende Wucht der Angriffe sorgte für **besorgniserregende Rekorde**.

Black Friday und Cyber Monday am stärksten von DDoS-Angriffen betroffen

Quelle: link11.com (2)

Motivation hinter DDoS-Angriffen

Protestaktionen
Hacktivismus
Cyber-Vandalismus

Gezielte Schädigungen
Konkurrenz ausschalten
Produktvorstellung verhindern

Lösegeldforderungen
DDoS-Erpressungen
Ransom DDoS-Angriffe

Motivation hinter DDoS-Angriffen

Quelle: onlinehaendler-news.de (3)

Motivation hinter DDoS-Angriffen

Protestaktionen
Hacktivismus
Cyber-Vandalismus

Gezielte Schädigungen
Konkurrenz ausschalten
Produktvorstellung verhindern

Lösegeldforderungen
DDoS-Erpressungen
Ransom DDoS-Angriffe

Politische Motivation
Systematische Störungen
Staatliche Akteure

Motivation hinter DDoS-Angriffen

LOGIN REGISTRIEREN

DER TAGESSPIEGEL

POLITIK BERLIN WIRTSCHAFT GESELLSCHAFT KULTUR MEINUNG SPORT WISSEN VERBRAUCHER INTERAKTIV Suchbegriff eingeben

Agenda Brexit Digitalisierung & KI Energie & Klima Gesundheit & E-Health Mobilität & Transport

Politik › Vergeltung für Waffenlieferungen: Prorussische Hacker attackieren offenbar Websites deutscher Behörden

Vergeltung für Waffenlieferungen

06.05.2022, 21:30 Uhr

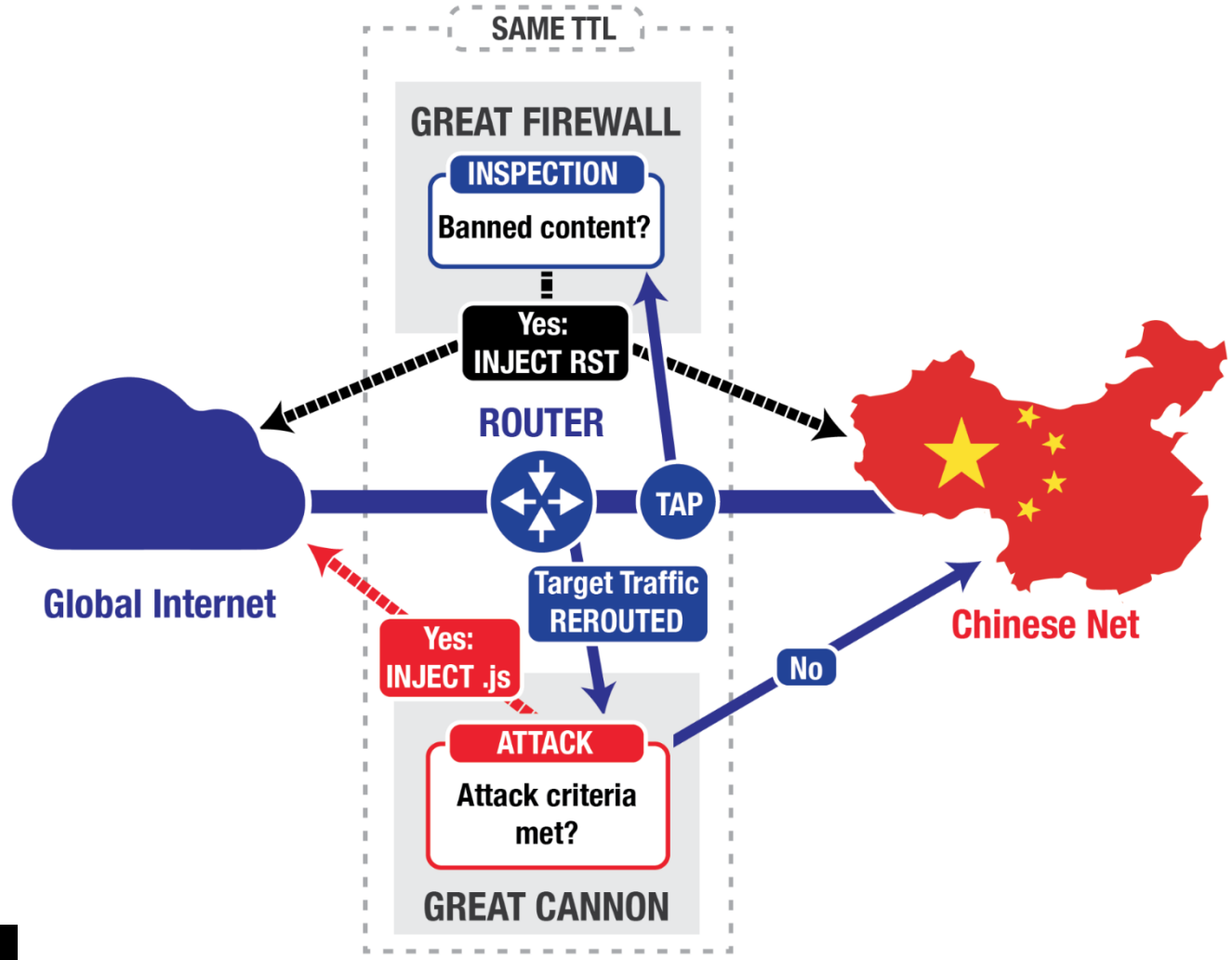
Prorussische Hacker attackieren offenbar Websites deutscher Behörden

Deutsche Ministerien, Politiker und Behörden sind einem Bericht zufolge Ziel von Cyberangriffen geworden. Auch die SPD-Website von Kanzler Scholz sei betroffen.

Internetseiten deutscher Behörden wurden Ziel von Hackerangriffen. FOTO: PICTURE ALLIANCE/DPA

Quelle: tagesspiegel.de (4)

Motivation hinter DDoS-Angriffen



Quelle: citizenlab.ca (5)

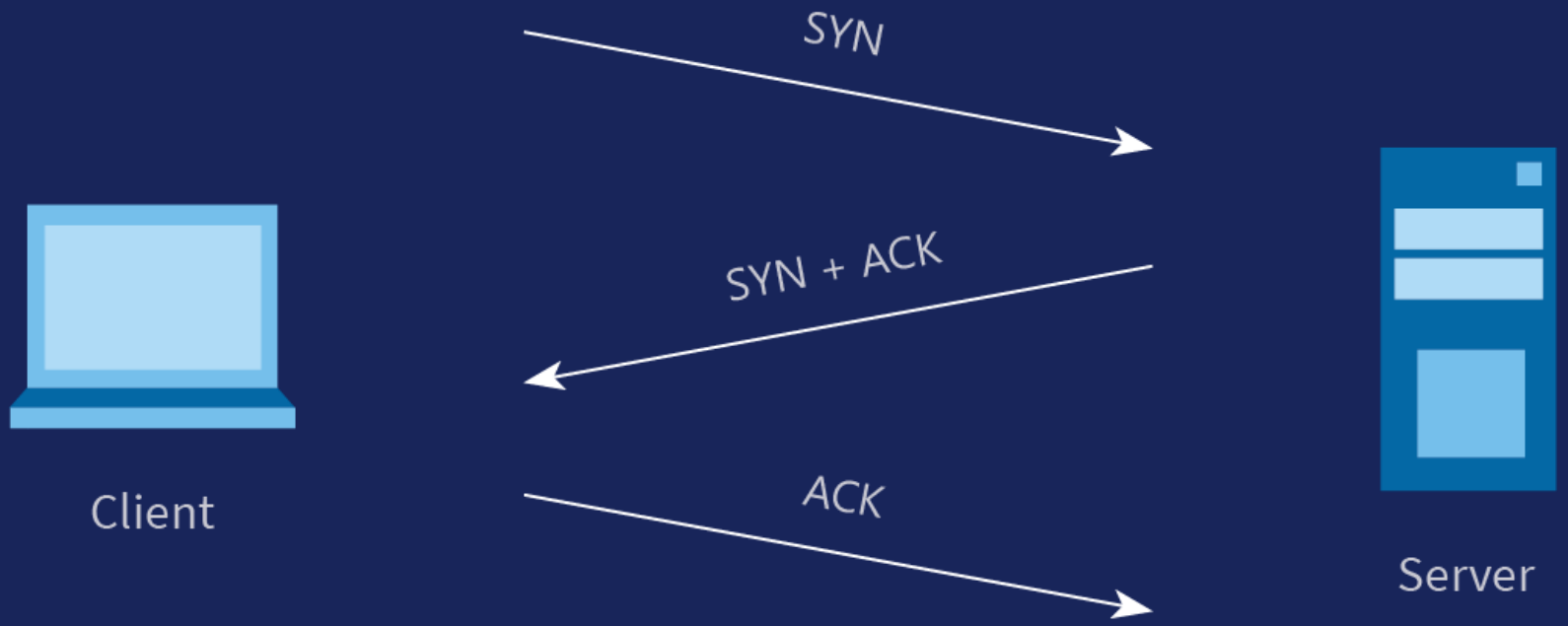
Cybercrime-as-a-Service

Quelle: youtube.com (6)

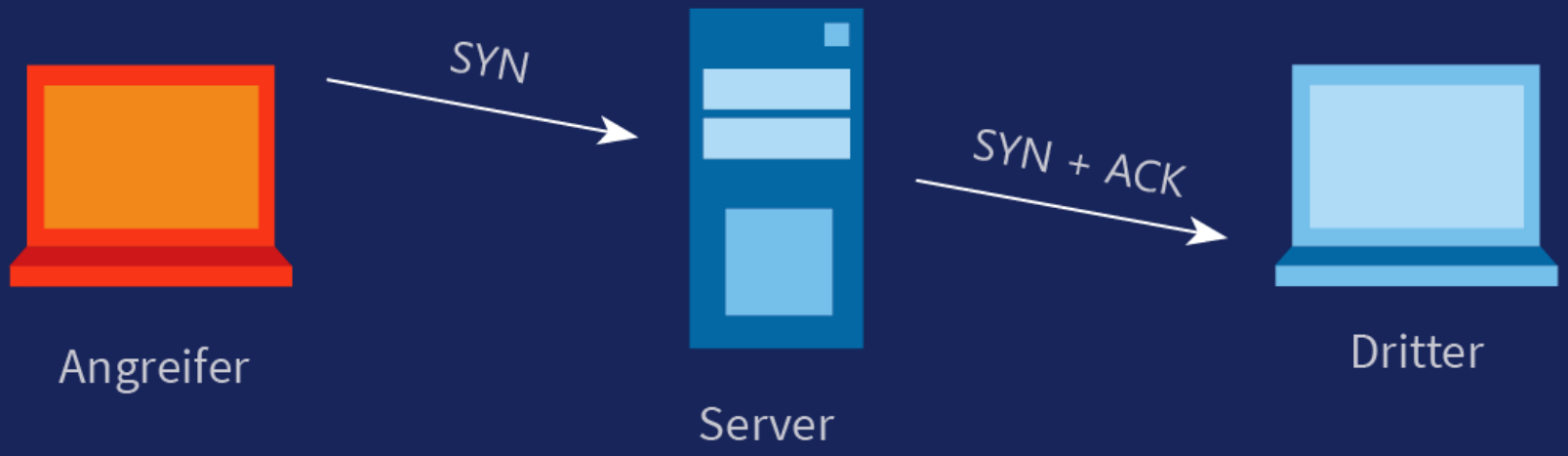
Quantitative Angriffe

PRAXIS ICMP Flood

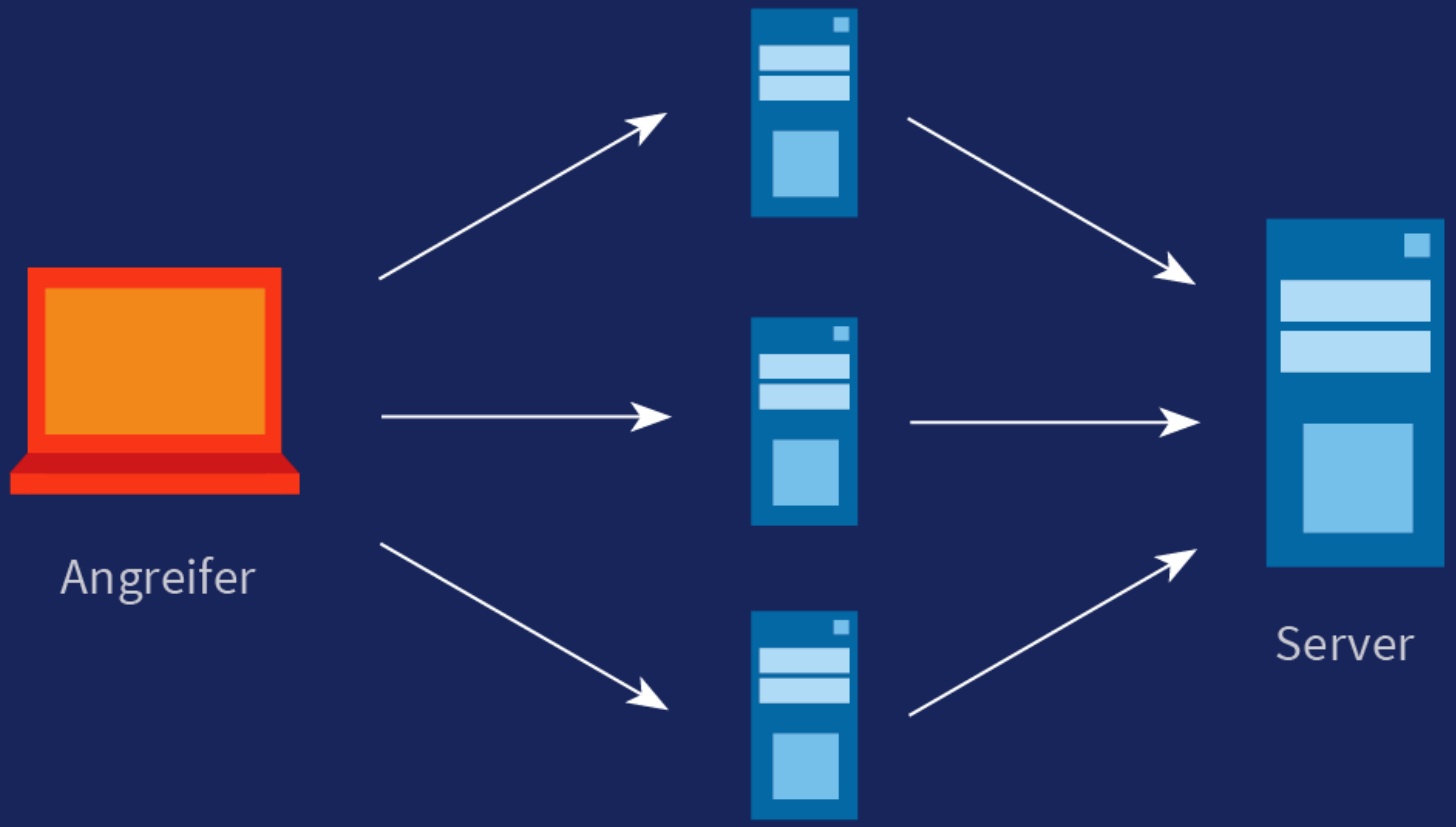
SYN Flood (TCP/SYN)



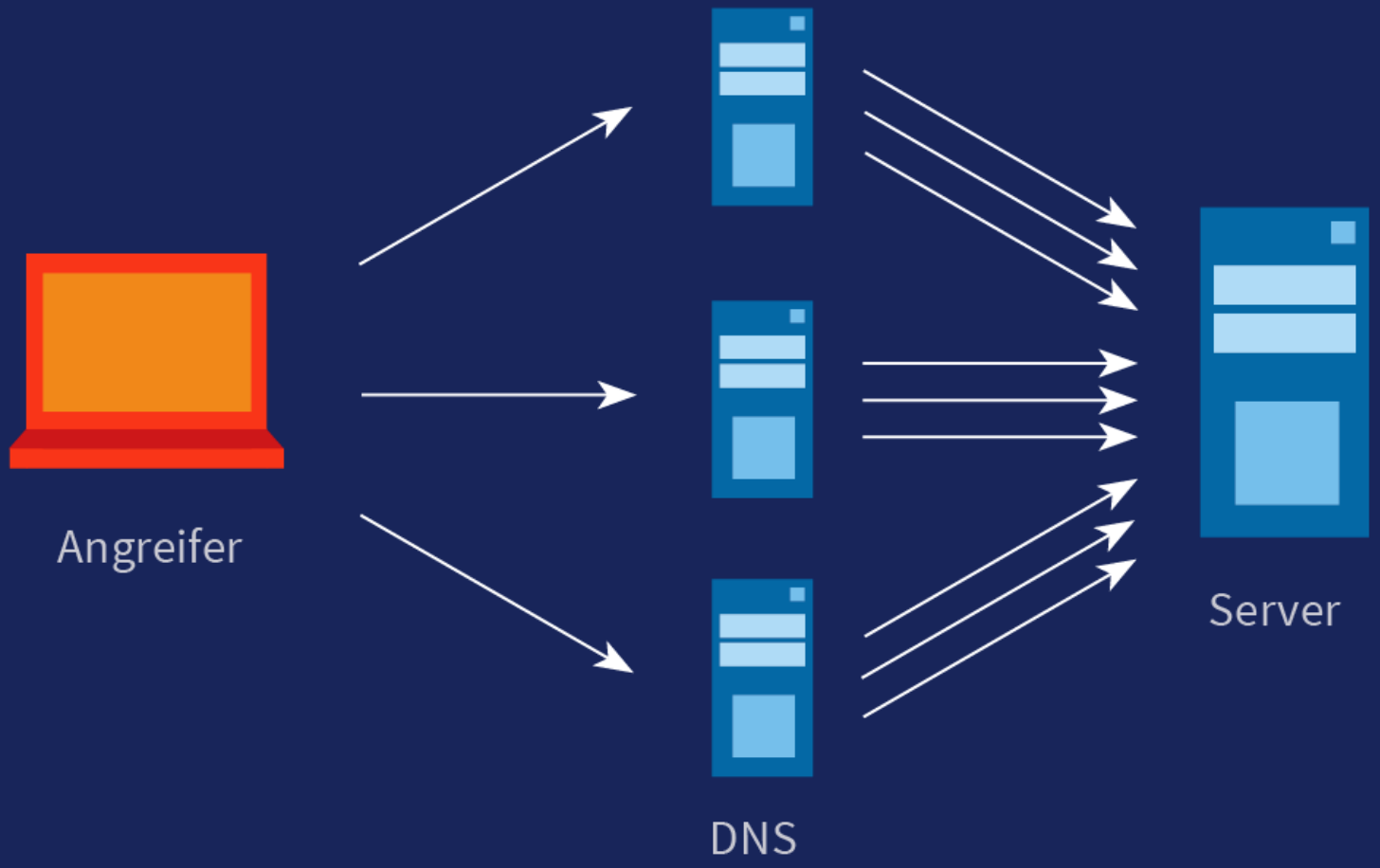
PRAXIS SYN Flood (TCP/SYN)



Verstärkende Angriffe (reflection)

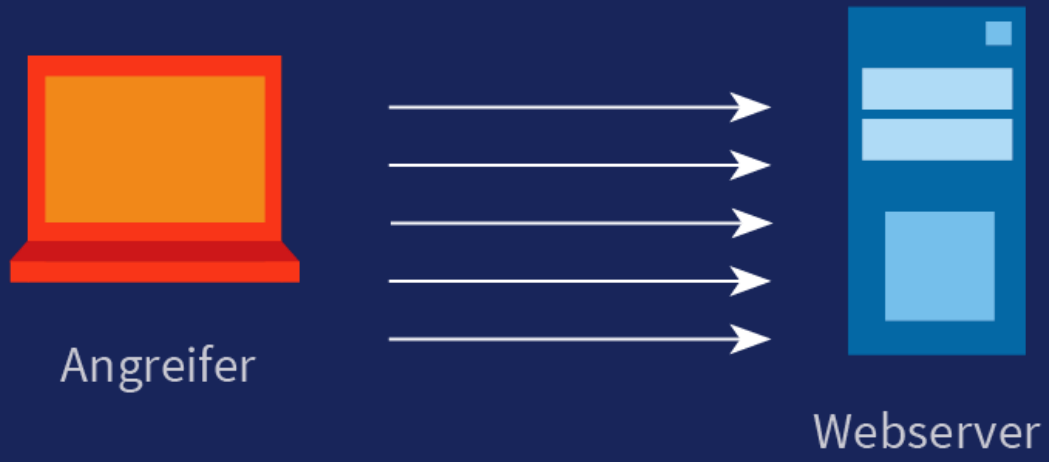


Verstärkende Angriffe (amplification)

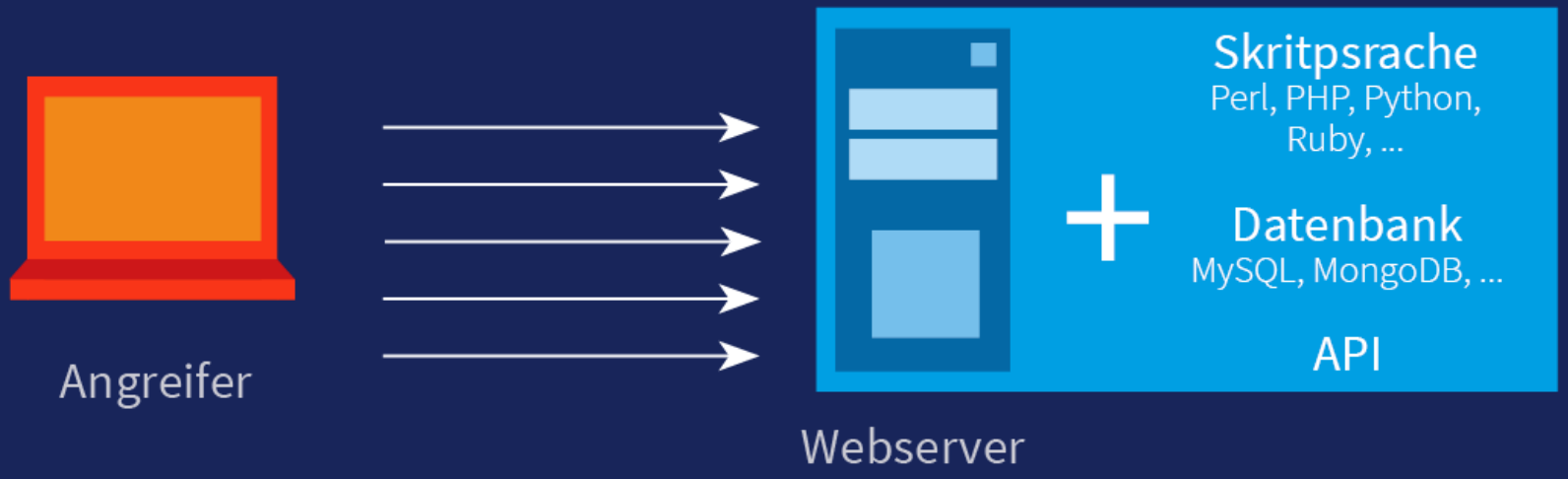


Qualitative Angriffe

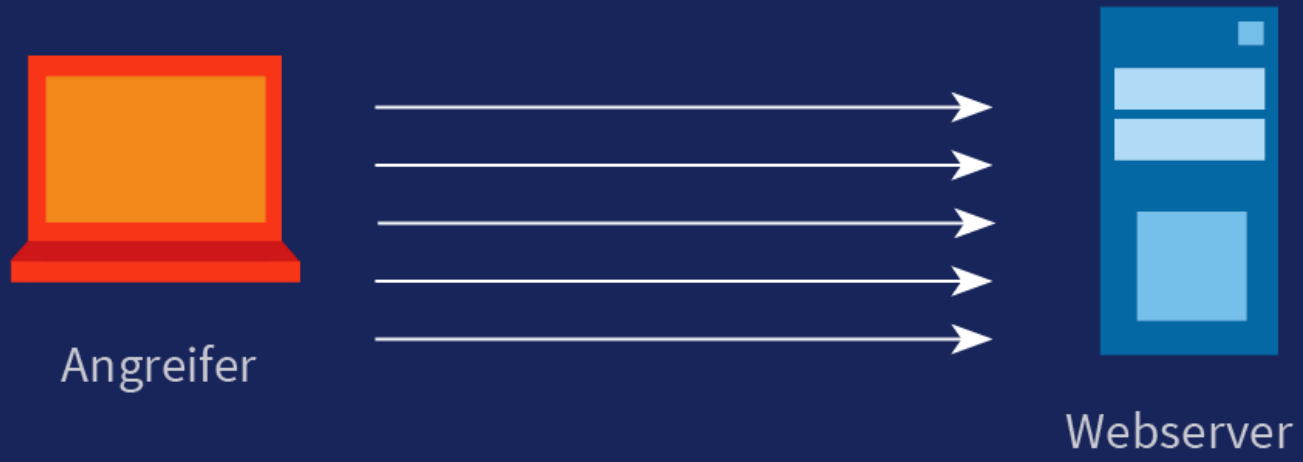
HTTP Flood



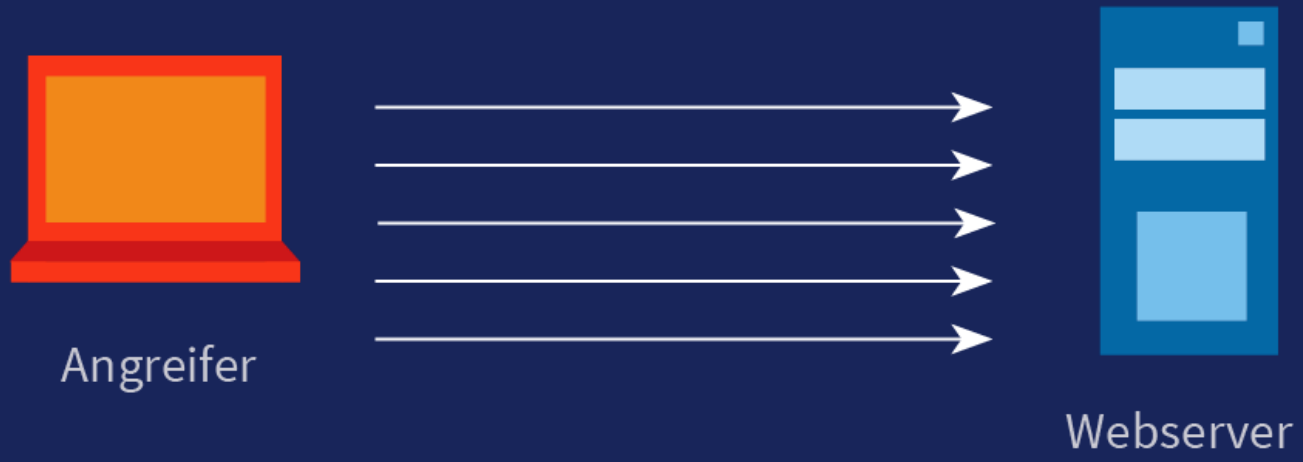
PRAXIS HTTP Flood



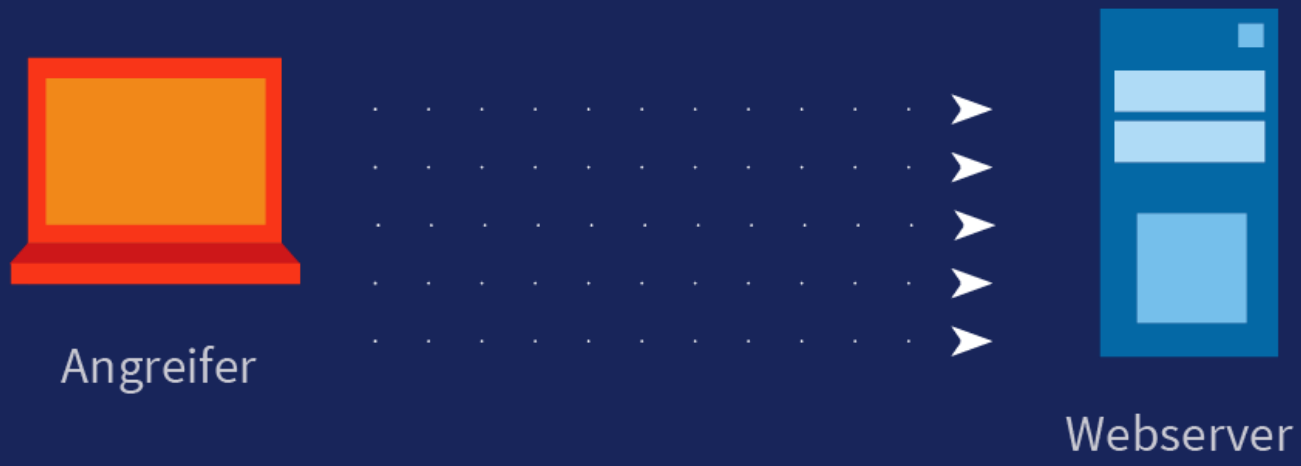
PRAXIS TLS Handshake (HTTPS)



Slowloris



PRAXIS Slowloris



(D)DoS Abwehrstrategien

Präventive Maßnahmen

- **Monitoring**
  Um einen Überblick über die anfallenden Lasten zu bekommen und auffälligen Datenverkehr analysieren zu können, müssen entsprechende Maßnahmen umgesetzt werden, um den Netzwerkverkehr überwachen zu können.
- **Struktur**
  Als Nächstes müssen entsprechende Komponenten vor den potenziell gefährdeten Systemen platziert werden, die eine Filterung ermöglichen. Dazu gehören Firewalls, Proxys und Loadbalancer.
- **Segmentierung**
  Da häufig nicht nur das angegriffene System unter der starken Last zu leiden hat, sondern auch vorgelagerte Netzwerkkomponenten und zum Teil auch das gesamte Netzwerksegment, sollten gefährdete Systeme in eigene Netze separiert werden.
- **Konfiguration**
  Über entsprechende Konfigurationen können Systeme gegen DDoS-Angriffe gehärtet werden. Sie müssen diese Maßnahmen vorab erheben und umsetzen.

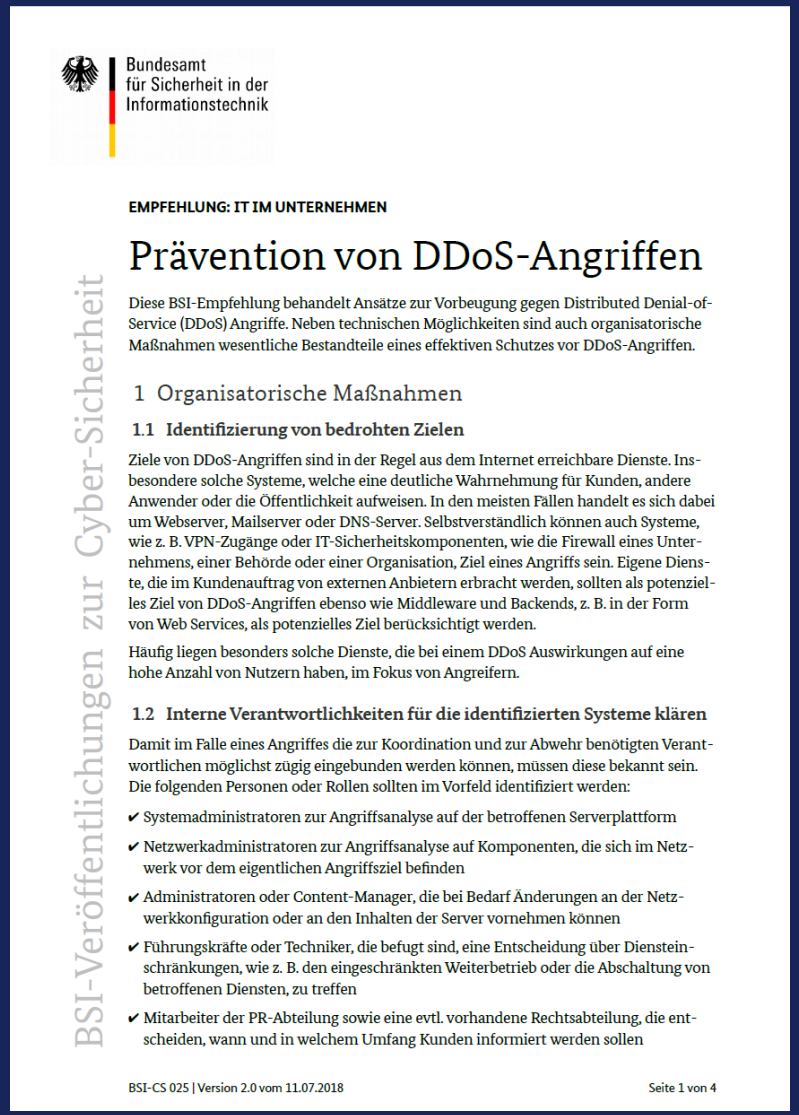
Aktive Gegenmaßnahmen

- **Blackholing**
  Beim Blackholing werden alle Netzwerkpakete verworfen, die einer spezifischen IP-Adresse zugeordnet werden können. Alternativ können auch ganze Blöcke von IP-Adressen oder ganze GEO-IP-Regionen blockiert werden.
- **Sinkholing**
  Ist die eigene Netzwerkinfrastruktur überlastet, wird häufig der Ansatz gewählt, dass alle Anfragen zu einer IP-Adresse oder URL blockiert werden, die angegriffen werden. Damit kann ein Angriff möglichst früh blockiert werden. Der angegriffene Dienst ist zwar nicht mehr erreichbar, dafür alle anderen Dienste.
- **Filterung**
  Gerade bei Angriffen auf der Anwendungsebene können Profile von Anfragen erstellt werden und alle weiteren Anfragen mit dem gleichen Profil verworfen werden. Zum Beispiel können bei HTTP-Flood-Angriffen die Header Felder ausgewertet werden, um diese zu erkennen und zu blockieren.

DDoS-Mitigation

- Ein weiterer Ansatz ist, dass nicht selbst ein DDoS-Angriff abgewehrt wird, sondern ein vorgelagerter Anbieter dies übernimmt.
- Dies kann bei einer Website ein Proxy-Dienst sein, der alle Anfragen entgegennimmt und nur korrekte an den Webserver weiterleitet. Dadurch kann keine Anfrage mehr direkt an den Webserver gesendet werden und der Proxy-Dienst verfügt über genügend Bandbreite und Fähigkeiten, um auch große Angriffe abzuwehren.
  - Myra Security GmbH (Deutschland > München)
  - ArvanCloud (Deutschland > Düsseldorf)
  - Link11 GmbH (Deutschland > Frankfurt)
  - Leaseweb (Niederlande > Amsterdam)
  - KeyCDN (Schweiz > Ermatingen)
- Solche Dienste werden zum Beispiel auch ISPs angeboten, um Firmenanschlüsse zu schützen. Hier werden mit entsprechenden Routings Angriffe gewährt.

Weitere Ressourcen



Bundesamt für Sicherheit in der Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Prävention von DDoS-Angriffen

BSI-Veröffentlichungen zur Cyber-Sicherheit

Diese BSI-Empfehlung behandelt Ansätze zur Vorbeugung gegen Distributed Denial-of-Service (DDoS) Angriffe. Neben technischen Möglichkeiten sind auch organisatorische Maßnahmen wesentliche Bestandteile eines effektiven Schutzes vor DDoS-Angriffen.

1 Organisatorische Maßnahmen

1.1 Identifizierung von bedrohten Zielen

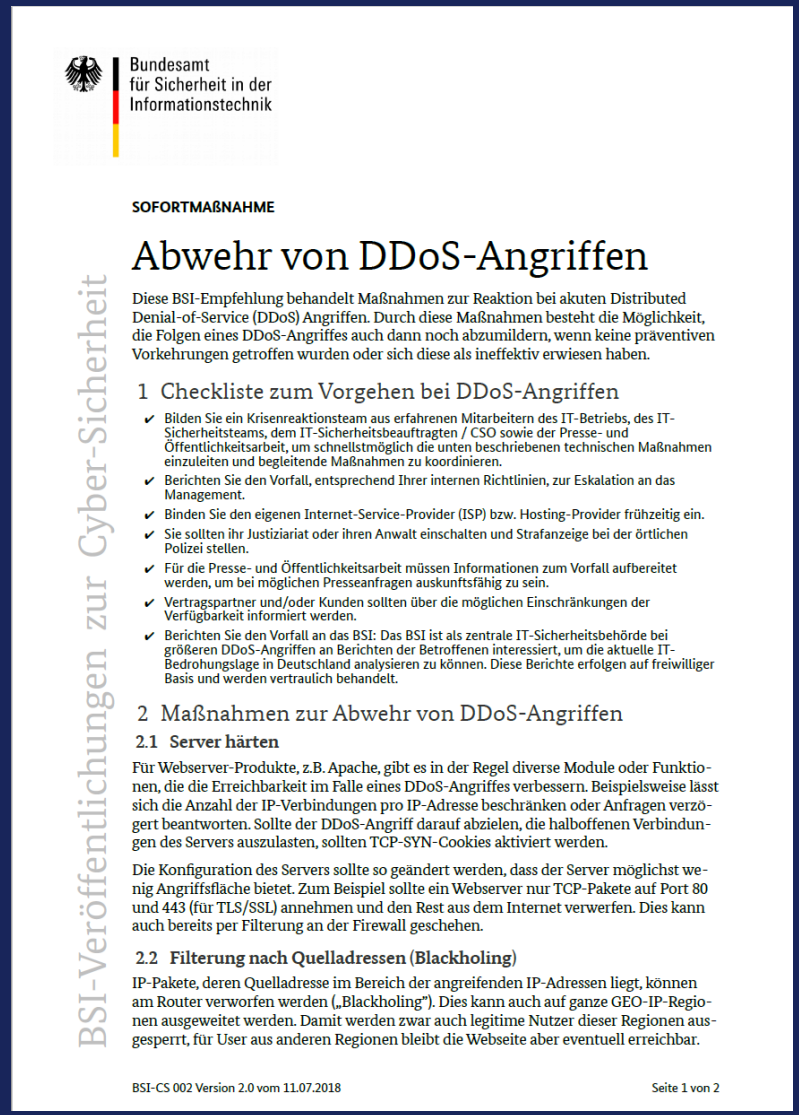
Ziele von DDoS-Angriffen sind in der Regel aus dem Internet erreichbare Dienste. Insbesondere solche Systeme, welche eine deutliche Wahrnehmung für Kunden, andere Anwender oder die Öffentlichkeit aufweisen. In den meisten Fällen handelt es sich dabei um Webserver, Mailserver oder DNS-Server. Selbstverständlich können auch Systeme, wie z. B. VPN-Zugänge oder IT-Sicherheitskomponenten, wie die Firewall eines Unternehmens, einer Behörde oder einer Organisation, Ziel eines Angriffs sein. Eigene Dienste, die im Kundenauftrag von externen Anbietern erbracht werden, sollten als potenzielles Ziel von DDoS-Angriffen ebenso wie Middleware und Backends, z. B. in der Form von Web Services, als potenzielles Ziel berücksichtigt werden.

Häufig liegen besonders solche Dienste, die bei einem DDoS Auswirkungen auf eine hohe Anzahl von Nutzern haben, im Fokus von Angreifern.

1.2 Interne Verantwortlichkeiten für die identifizierten Systeme klären

Damit im Falle eines Angriffes die zur Koordination und zur Abwehr benötigten Verantwortlichen möglichst zügig eingebunden werden können, müssen diese bekannt sein. Die folgenden Personen oder Rollen sollten im Vorfeld identifiziert werden:

- ✔ Systemadministratoren zur Angriffsanalyse auf der betroffenen Serverplattform
- ✔ Netzwerkadministratoren zur Angriffsanalyse auf Komponenten, die sich im Netzwerk vor dem eigentlichen Angriffsziel befinden
- ✔ Administratoren oder Content-Manager, die bei Bedarf Änderungen an der Netzwerkkonfiguration oder an den Inhalten der Server vornehmen können
- ✔ Führungskräfte oder Techniker, die befugt sind, eine Entscheidung über Dienstein-schränkungen, wie z. B. den eingeschränkten Weiterbetrieb oder die Abschaltung von betroffenen Diensten, zu treffen
- ✔ Mitarbeiter der PR-Abteilung sowie eine evtl. vorhandene Rechtsabteilung, die entscheiden, wann und in welchem Umfang Kunden informiert werden sollen



Bundesamt für Sicherheit in der Informationstechnik

SOFORTMAßNAHME

Abwehr von DDoS-Angriffen

BSI-Veröffentlichungen zur Cyber-Sicherheit

Diese BSI-Empfehlung behandelt Maßnahmen zur Reaktion bei akuten Distributed Denial-of-Service (DDoS) Angriffen. Durch diese Maßnahmen besteht die Möglichkeit, die Folgen eines DDoS-Angriffes auch dann noch abzumildern, wenn keine präventiven Vorkehrungen getroffen wurden oder sich diese als ineffektiv erwiesen haben.

1 Checkliste zum Vorgehen bei DDoS-Angriffen

- ✔ Bilden Sie ein Krisenreaktionsteam aus erfahrenen Mitarbeitern des IT-Betriebs, des IT-Sicherheitsteams, dem IT-Sicherheitsbeauftragten / CSO sowie der Presse- und Öffentlichkeitsarbeit, um schnellstmöglich die unten beschriebenen technischen Maßnahmen einzuleiten und begleitende Maßnahmen zu koordinieren.
- ✔ Berichten Sie den Vorfall, entsprechend Ihrer internen Richtlinien, zur Eskalation an das Management.
- ✔ Binden Sie den eigenen Internet-Service-Provider (ISP) bzw. Hosting-Provider frühzeitig ein.
- ✔ Sie sollten ihr Justiziariat oder ihren Anwalt einschalten und Strafanzeige bei der örtlichen Polizei stellen.
- ✔ Für die Presse- und Öffentlichkeitsarbeit müssen Informationen zum Vorfall aufbereitet werden, um bei möglichen Presseanfragen auskunftsfähig zu sein.
- ✔ Vertragspartner und/oder Kunden sollten über die möglichen Einschränkungen der Verfügbarkeit informiert werden.
- ✔ Berichten Sie den Vorfall an das BSI: Das BSI ist als zentrale IT-Sicherheitsbehörde bei größeren DDoS-Angriffen an Berichten der Betroffenen interessiert, um die aktuelle IT-Bedrohungslage in Deutschland analysieren zu können. Diese Berichte erfolgen auf freiwilliger Basis und werden vertraulich behandelt.

2 Maßnahmen zur Abwehr von DDoS-Angriffen

2.1 Server härten

Für Webserver-Produkte, z.B. Apache, gibt es in der Regel diverse Module oder Funktionen, die die Erreichbarkeit im Falle eines DDoS-Angriffes verbessern. Beispielsweise lässt sich die Anzahl der IP-Verbindungen pro IP-Adresse beschränken oder Anfragen verzögert beantworten. Sollte der DDoS-Angriff darauf abzielen, die halboffenen Verbindungen des Servers auszulasten, sollten TCP-SYN-Cookies aktiviert werden.

Die Konfiguration des Servers sollte so geändert werden, dass der Server möglichst wenig Angriffsfläche bietet. Zum Beispiel sollte ein Webserver nur TCP-Pakete auf Port 80 und 443 (für TLS/SSL) annehmen und den Rest aus dem Internet verwerfen. Dies kann auch bereits per Filterung an der Firewall geschehen.

2.2 Filterung nach Quelladressen (Blackholing)

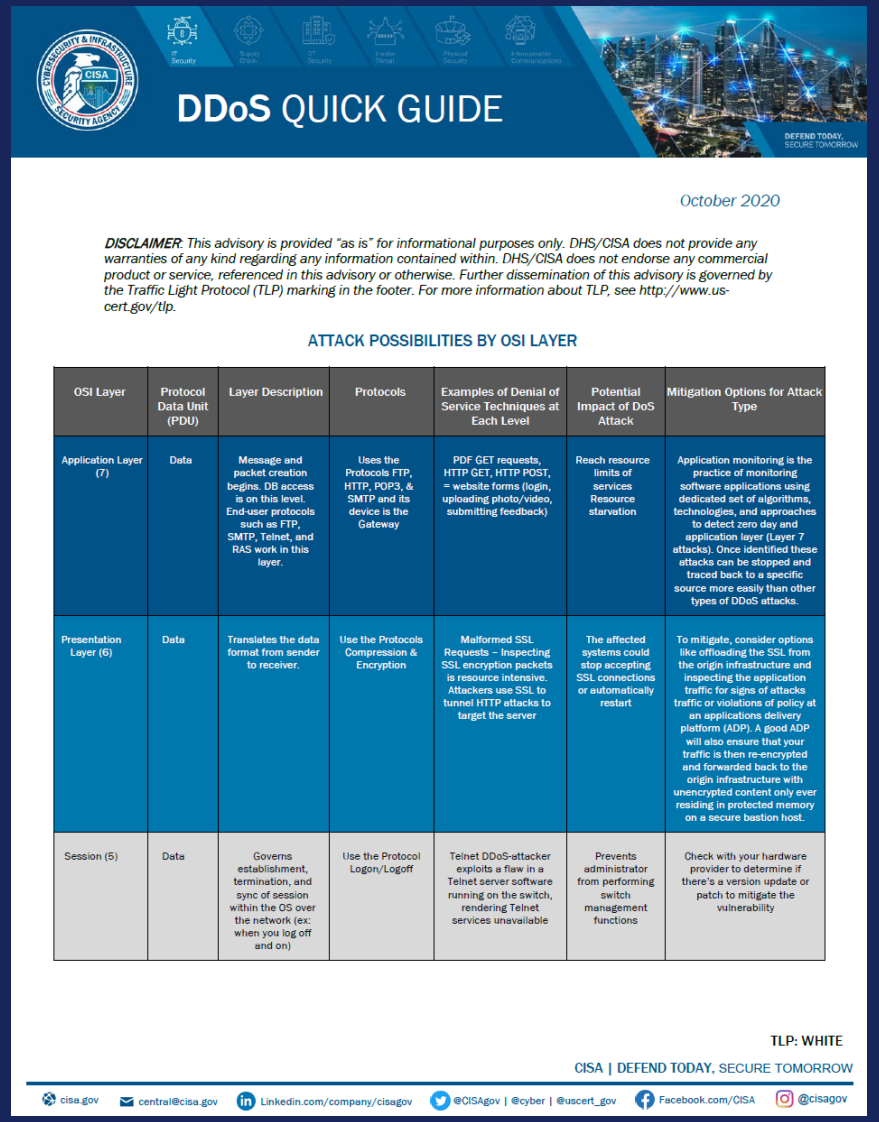
IP-Pakete, deren Quelladresse im Bereich der angreifenden IP-Adressen liegt, können am Router verworfen werden („Blackholing"). Dies kann auch auf ganze GEO-IP-Regionen ausgeweitet werden. Damit werden zwar auch legitime Nutzer dieser Regionen ausgesperrt, für User aus anderen Regionen bleibt die Webseite aber eventuell erreichbar.

Weitere Ressourcen

Bundesministerium
Inneres

Distributed Denial of Service (DDoS)

Hintergründe, präventive Maßnahmen und Mitigationsmaßnahmen



DDoS QUICK GUIDE

DEFEND TODAY, SECURE TOMORROW

October 2020

***DISCLAIMER**: This advisory is provided "as is" for informational purposes only. DHS/CISA does not provide any warranties of any kind regarding any information contained within. DHS/CISA does not endorse any commercial product or service, referenced in this advisory or otherwise. Further dissemination of this advisory is governed by the Traffic Light Protocol (TLP) marking in the footer. For more information about TLP, see http://www.us-cert.gov/tlp.*

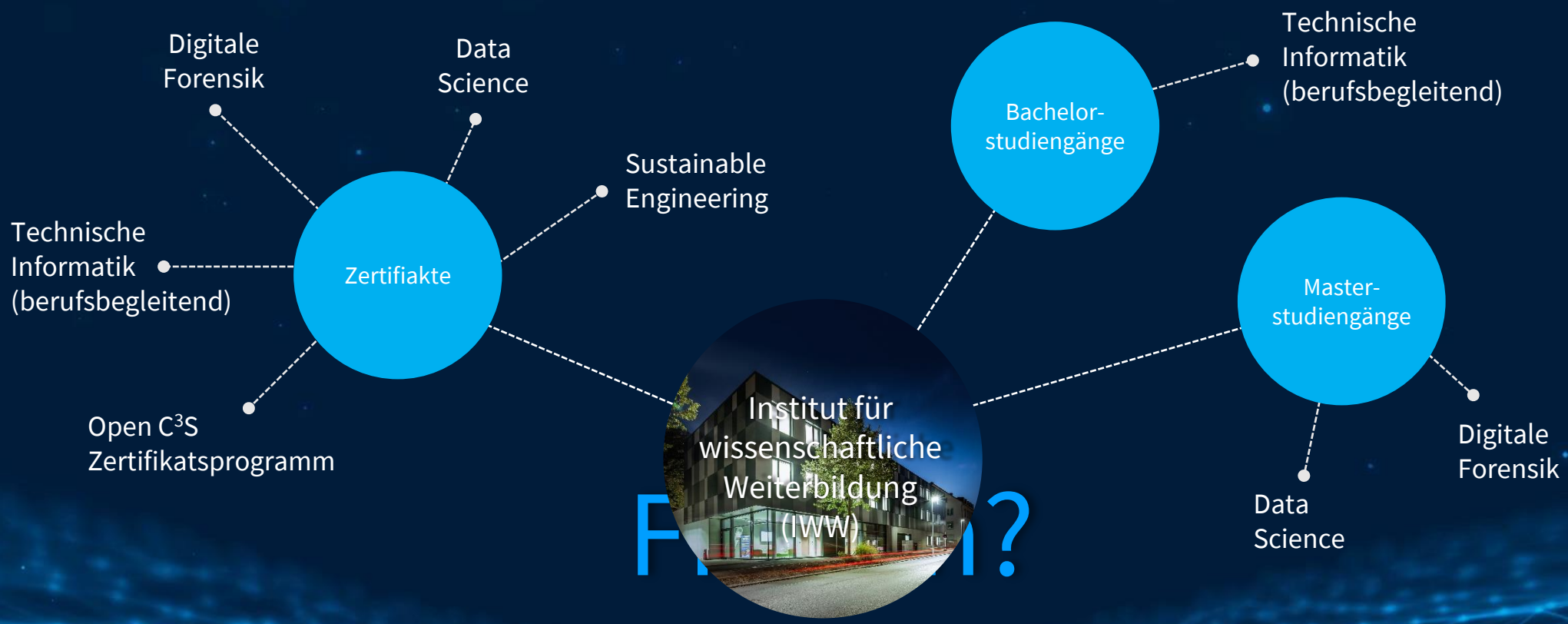
ATTACK POSSIBILITIES BY OSI LAYER

OSI Layer	Protocol Data Unit (PDU)	Layer Description	Protocols	Examples of Denial of Service Techniques at Each Level	Potential Impact of DoS Attack	Mitigation Options for Attack Type
Application Layer (7)	Data	Message and packet creation begins. DB access is on this level. End-user protocols such as FTP, SMTP, Telnet, and RAS work in this layer.	Uses the Protocols FTP, HTTP, POP3, & SMTP and its device is the Gateway	PDF GET requests, HTTP GET, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation	Application monitoring is the practice of monitoring software applications using dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDoS attacks.
Presentation Layer (6)	Data	Translates the data format from sender to receiver.	Use the Protocols Compression & Encryption	Malformed SSL Requests – Inspecting SSL encryption packets is resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server	The affected systems could stop accepting SSL connections or automatically restart	To mitigate, consider options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host.
Session (5)	Data	Governs establishment, termination, and sync of session within the OS over the network (ex: when you log off and on)	Use the Protocol Logon/Logoff	Telnet DDoS-attacker exploits a flaw in a Telnet server software running on the switch, rendering Telnet services unavailable	Prevents administrator from performing switch management functions	Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability

TLP: WHITE

CISA | DEFEND TODAY, SECURE TOMORROW

cisa.gov central@cisa.gov Linkedin.com/company/cisagov @CISAgov | @cyber | @uscert_gov Facebook.com/CISA @cisagov



Vielen Dank für Ihre Aufmerksamkeit

Weitere Vorträge: weiter-bildung.info | Präsentation online unter: scheible.it

Quellen

(1) https://www.heise.de/newsticker/meldung/DDoS-Attacke-kostet-Paypal-3-5-Millionen-Pfund-1755660.html, abgerufen am 22.05.2022

(2) https://www.link11.com/de/blog/bedrohungslage/cyber-angriffe-am-black-friday-wochenende-brechen-rekorde/, abgerufen am 22.05.2022

(3) https://www.onlinehaendler-news.de/digital-tech/cyberkriminalitaet/136332-ransomware-haelfte-opfer-zahlt-loesegeld, abgerufen am 22.05.2022

(4) https://www.tagesspiegel.de/politik/vergeltung-fuer-waffenlieferungen-prorussische-hacker-attackieren-offenbar-websites-deutscher-behoerden/28313970.html, abgerufen am 22.05.2022

(5) https://citizenlab.ca/2015/04/chinas-great-cannon/, abgerufen am 22.05.2022

(6) https://www.youtube.com/watch?v=5M9k7wfiWiI, abgerufen am 22.05.2022

(7) https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/magenta-security-kongress-2016/magenta-security-kongress-2016/lernen-aus-ddos-angriff-auf-dyn-444378, abgerufen am 22.05.2022