



hosting.de

Über uns

Stefan

Als Backend-Entwickler arbeitet Stefan am Code unserer öffentlichen API. Zudem ist er beim Applikations-Scanner für die Backend-Services verantwortlich und setzt dabei auch die Brille eines System-Administrators auf.

Michael

Als einer der Gründer und CSO designet und entwickelt Michael seit mehr als 15 Jahren Software. Bei hosting.de ist er verantwortlich für den Software-Stack mit Fokus auf Software- / Systemarchitektur und die Verbesserung der Sicherheit der Kundenwebsites.

Wer wir sind

- Domains / DNS
- Webhosting / SSL
- E-Mail
- Virtuelle Server / Managed LAEMP Server

Wer wir sind

Public API

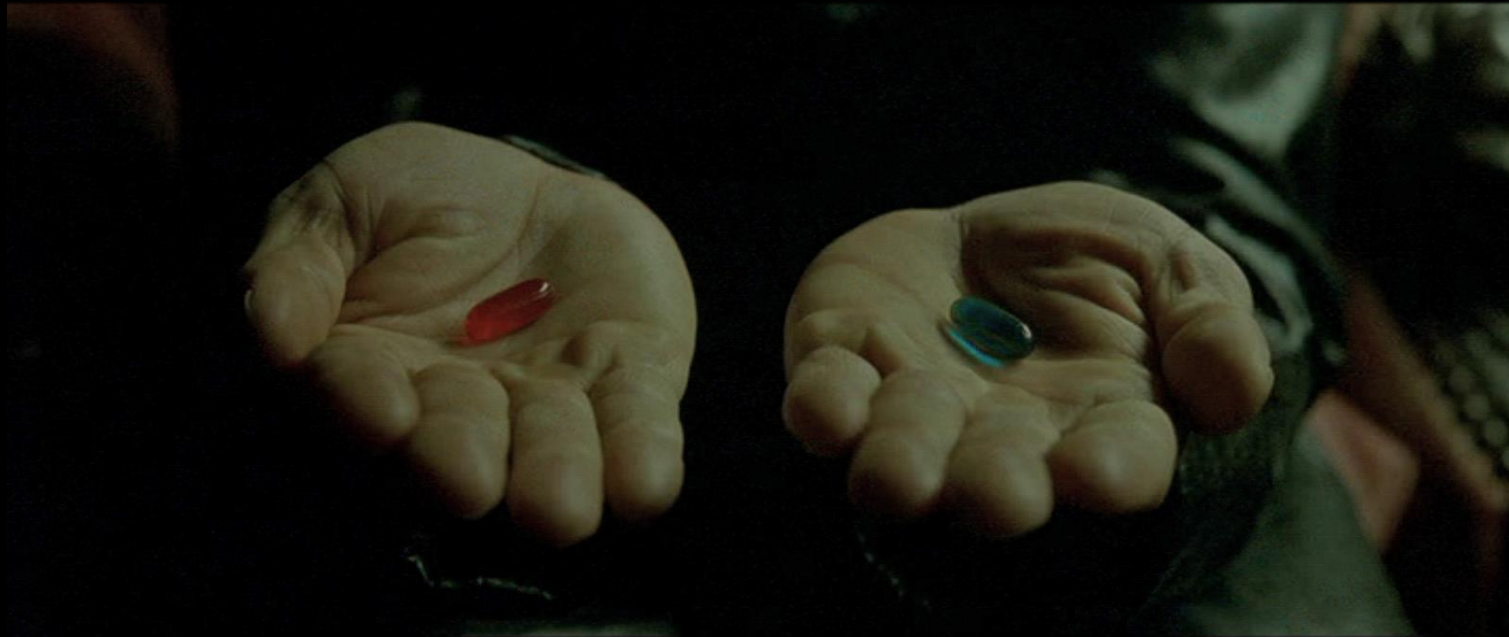
API-Dokumentation: <https://www.hosting.de/api>

Wer wir sind

Ein paar Zahlen:

- ca. 30 Kollegen
- > 35.000 Kunden
- > 250.000 aktive vHosts
- > 5.000 virtuelle Server

Blaue Pille = Ponyhof...



Was macht IHR eigentlich genau..?

- Wie benutzen Kunden unsere Services?
- Wie können wir unsere Kunden weitergehend unterstützen?
- Wie können wir unsere Infrastruktur optimieren?

Wie benutzen Kunden unsere Services?

Was passiert auf einem Webserver eigentlich...?

- Dateien / Webspaces manuell prüfen
- Automatisierbare Skripte (grep, find)
- Bestehende Tools, z.B. CMS Garden Scanner
(<https://github.com/CMS-Garden/cmsscanner>)

Wie benutzen Kunden unsere Services?

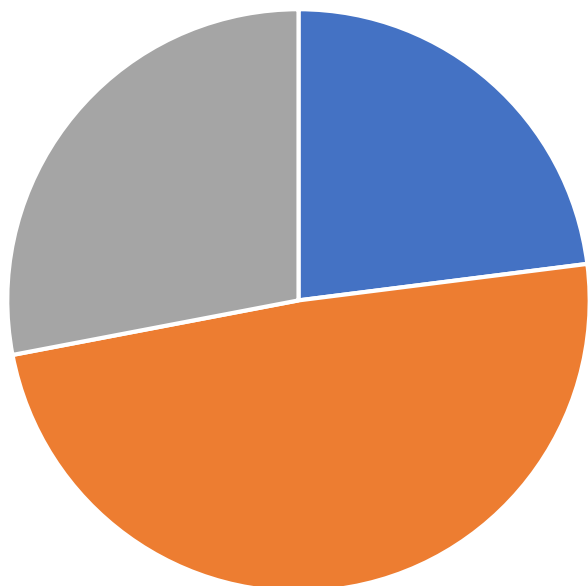
Probleme

- Wtf... Dinge per Hand prüfen?
- Applikationsspezifische Anpassungen
- Syntax könnte sich zwischen Versionen ändern
- Versionsdatei kann leer sein oder nicht vorhanden sein
- Versionsdatei lügt

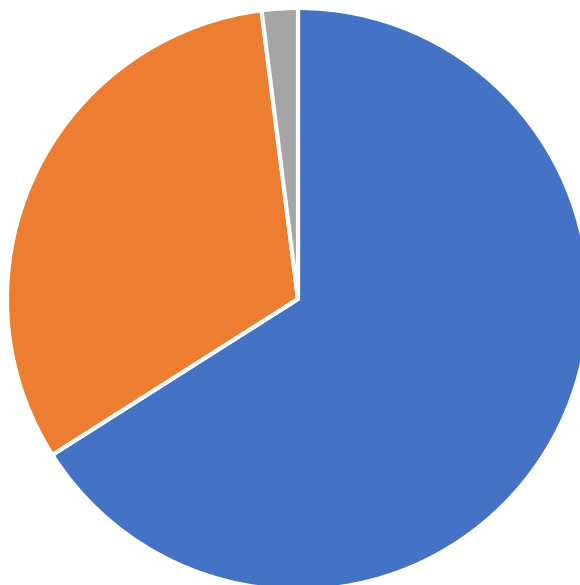


Ergebnisse einer internen Analyse

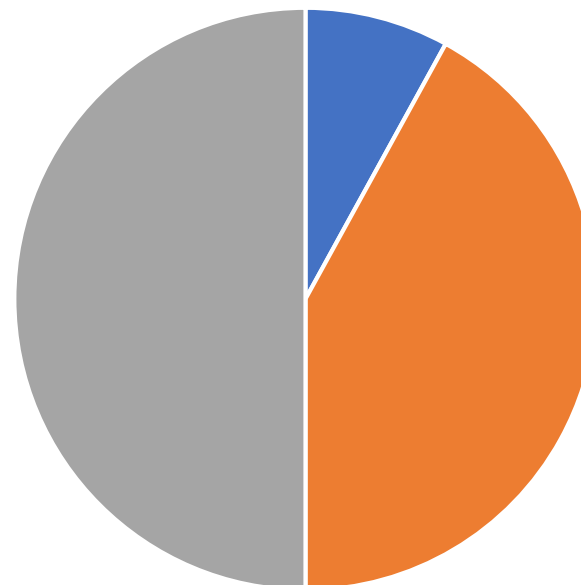
Graph A



Graph B



Graph C



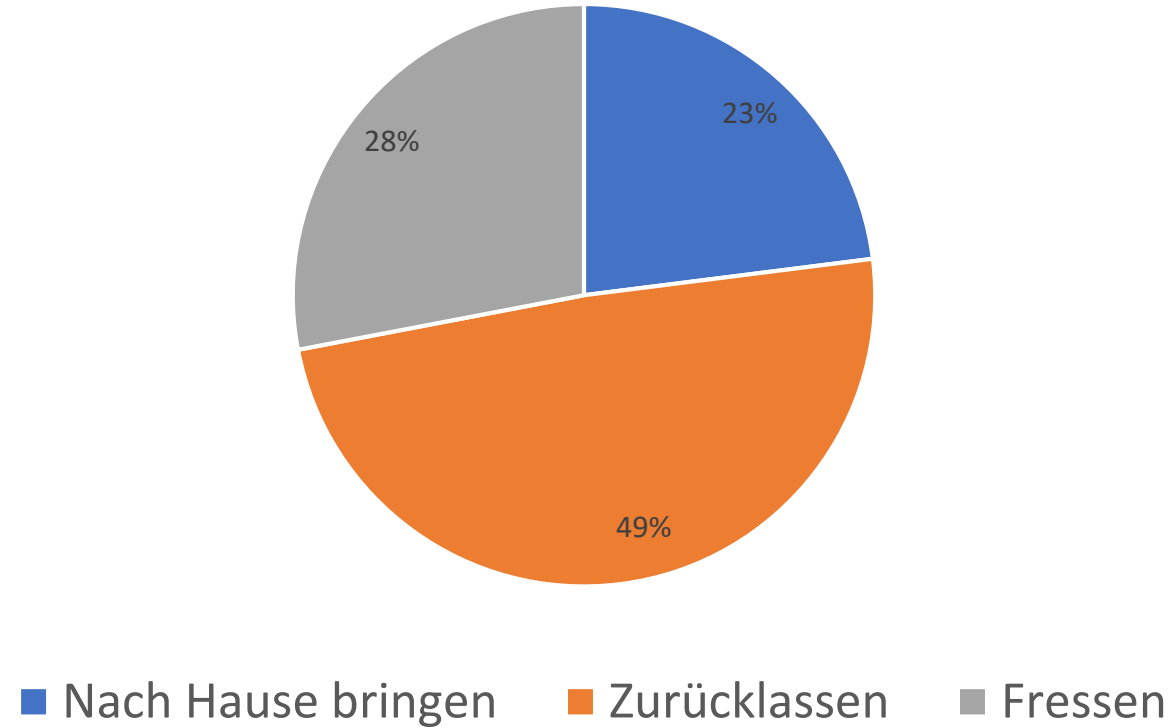
 Aktuell

 Letzte minor Version

 Outdated

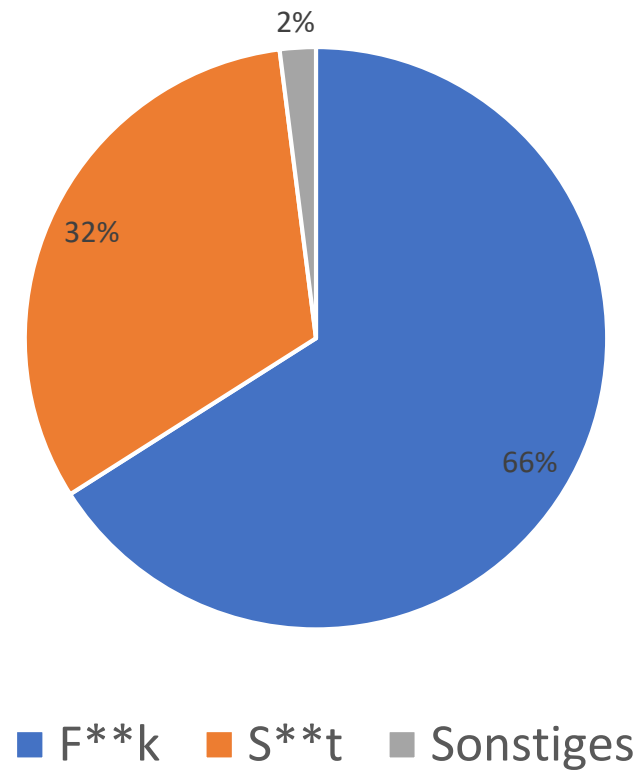
Graph A

Was Katzen mit ihrer erlegten Beute machen



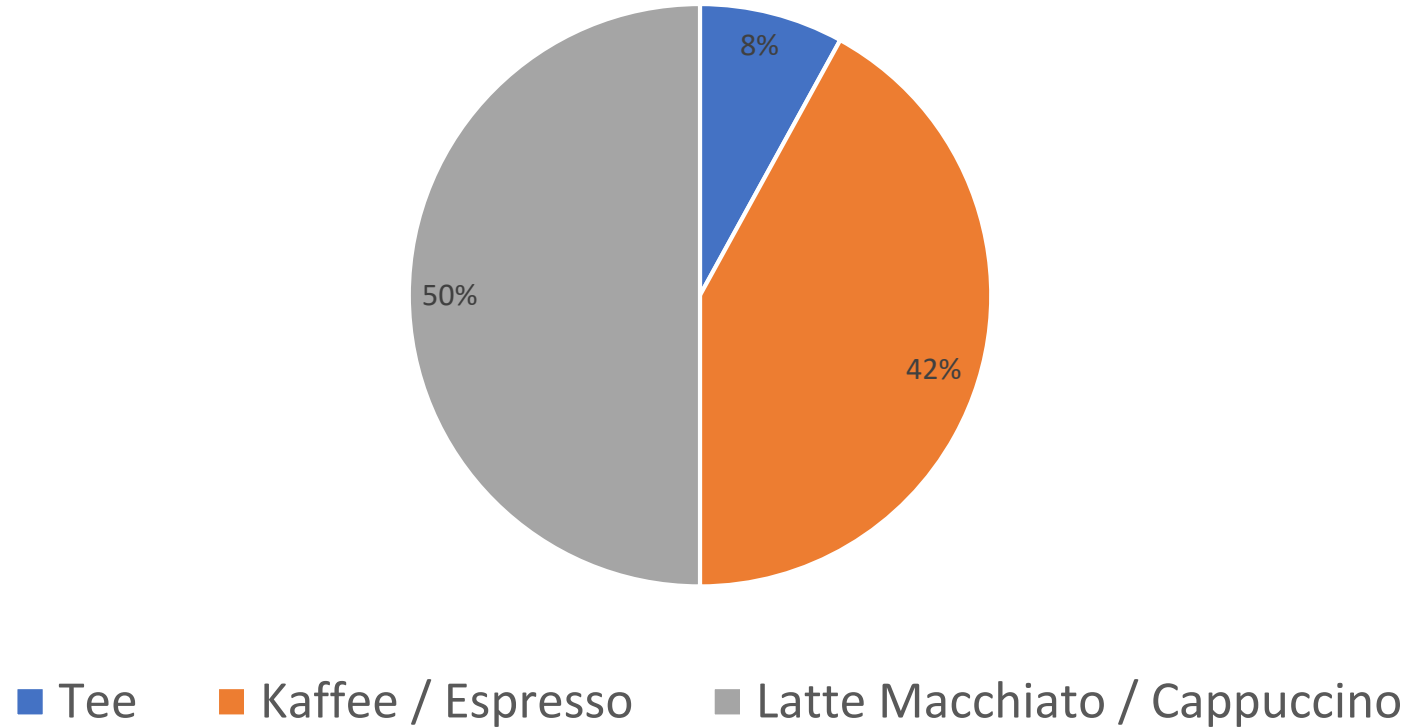
Graph B

Benutzte Schimpfwörter in GitHub Commit-Messages

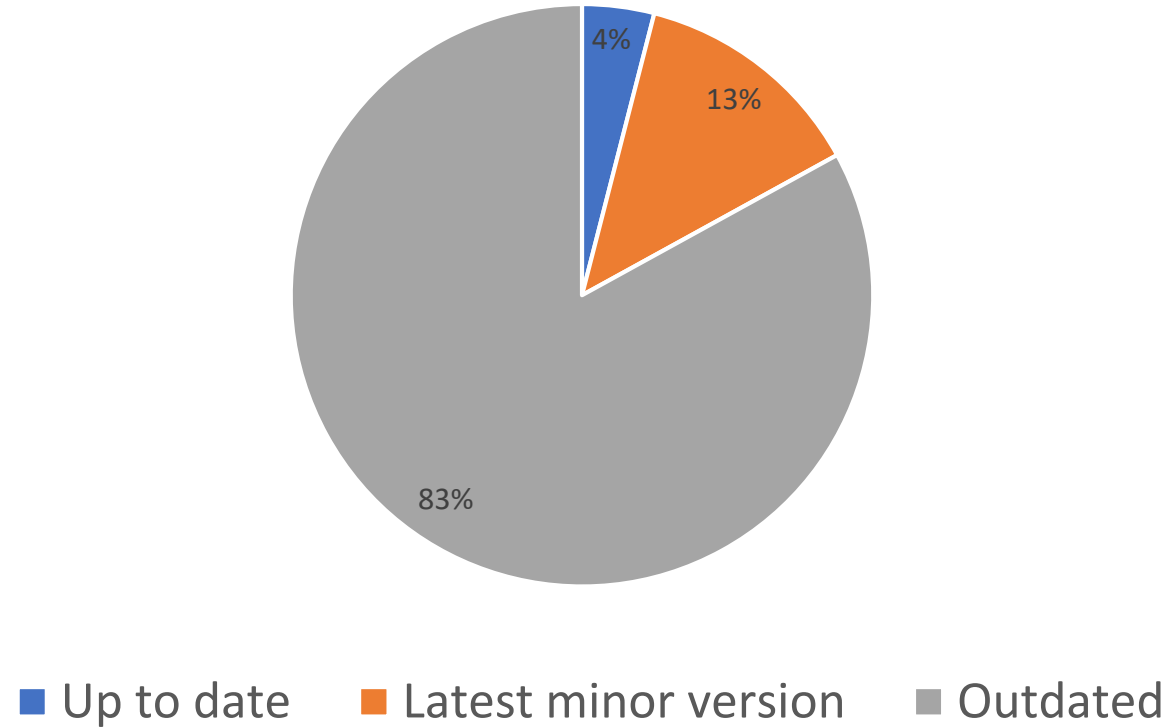


Graph C

Verzehrte Getränke der hosting.de Kollegen



Tatsächliches Ergebnis



Ergebnis in Zahlen

- Letzte Version zum jetzigen Zeitpunkt – 3.9.0 (4%)
- Letztes Minor-Release – 3.8 (13%)
- Zwischen 3.0 und 3.7 (30%)
- Unter 3.0 (53%)

Verteilung der Outdated-Versions

- Ab 3.0 (37%)
- Unter 3.0 (63%)



Konsequenzen für...

- Den Kunden
 - Verlust von Reputation
 - Einschränkung der Verfügbarkeit
 - Wiederherstellen eines nicht kompromittierten Zustandes – jeder hat Backups!
- Den Hoster
 - Blacklisting
 - Performance, andere Kunden werden beeinflusst
 - DDoS

Okay... was jetzt..?

→ Applikationen immer Up-To-Date halten und immer ein sauberes Backup vorrätig haben

Und wer kümmert sich darum?!

- Der Benutzer/Kunde!
- Die Agentur, die die Seite betreut
- Webservices (z.B. myJoomla, Watchful.li, Sucuri, Sitelock)
 - Kosten zwischen 1 Euro und 20 Euro pro Monat
 - Checks für Malware in Intervallen zwischen 24h und 30 Minuten – oder sogar manuell

Lösung gefunden, wir können heim..?

Öhm, nope – einige der Probleme dabei...

- Integration (Addon / Weitergabe von Logins)
- Zeit!

Unser Ziel: Echtzeiterkennung!



We need guns... A lot of them!



We need guns... A lot of them!

- Applikationsunabhängiger Ansatz
- Prüfsummen-basiertes Fingerprinting anstatt sich auf den Inhalt von z.B. version.php zu verlassen
- Monitoring von Dateiänderungen in Echtzeit
- Kategorisierung der Dateiänderung
- Auf bösartige Dateiänderungen reagieren

Unser Ansatz: hash-based fingerprinting

- Organisiere alle Softwares in allen Versionen
 - Es gibt keinen Standard zum Releasen von Software
 - GitHub release vs. release auf der Website
 - Packaging is a pain...
- Index erstellen

Echtzeitüberwachung von Dateiänderungen

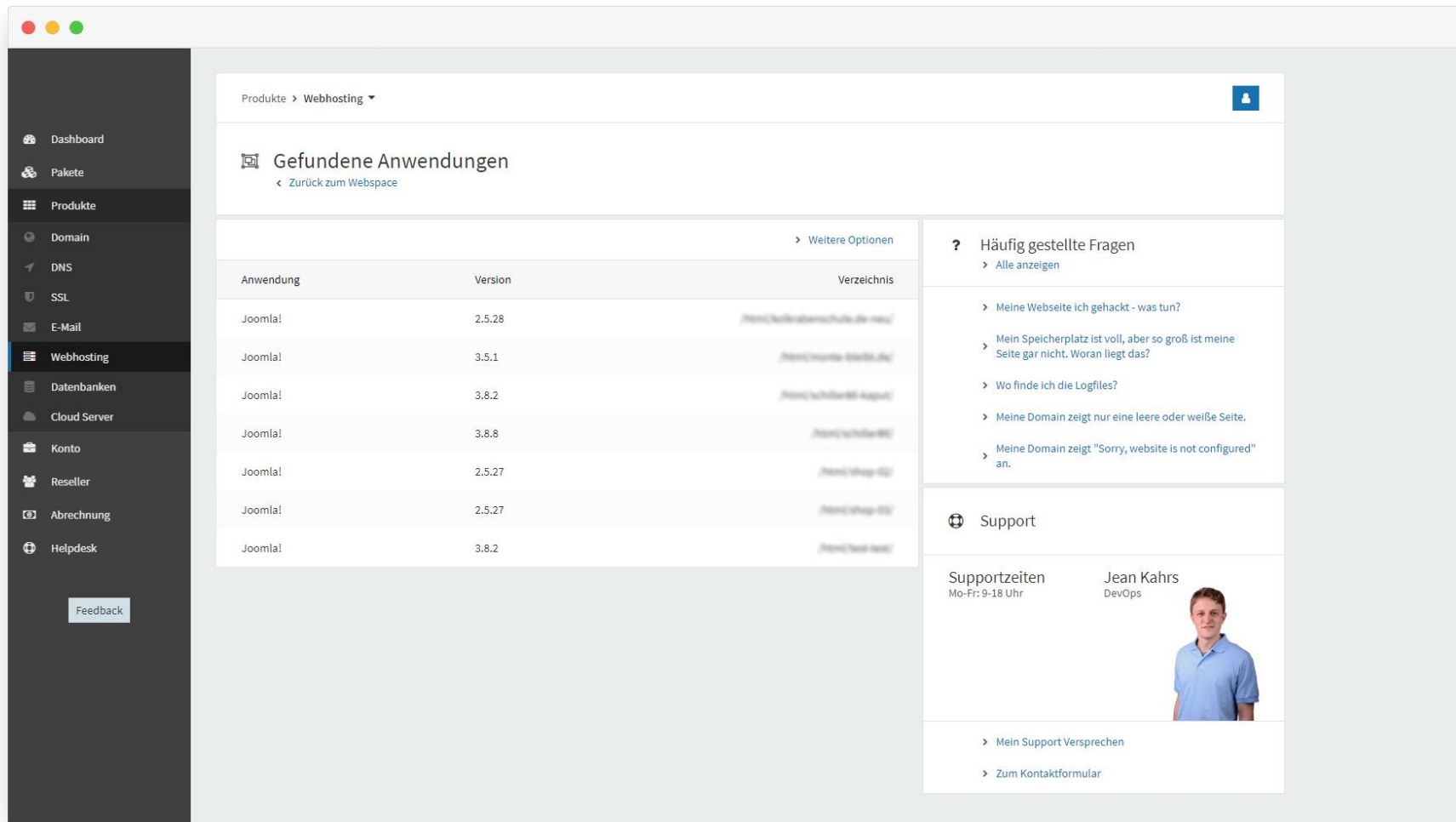
- Keine Tools verfügbar, die einfach benutzt werden können
 - inotify: skaliert nicht, Limit für Anzahl an überwachten Dateien
 - fanotify: keine Events für Anlegen / Umbenennen von Dateien
- Linux, Retter in der Not
 - Wir können einfach den Kernel fragen
 - Überwachen der gewünschten Events

Verhalten bei Dateiänderungen

- Neuer Fingerprint ist bekannt (z.B. durch Softwareupdate)
- Fingerprint ist unbekannt
 - Veränderung analysieren
 - Kunden über Veränderung informieren
 - Eintrag in einem Index für bösartige Veränderungen

DEMO

Was heißt das für euch?



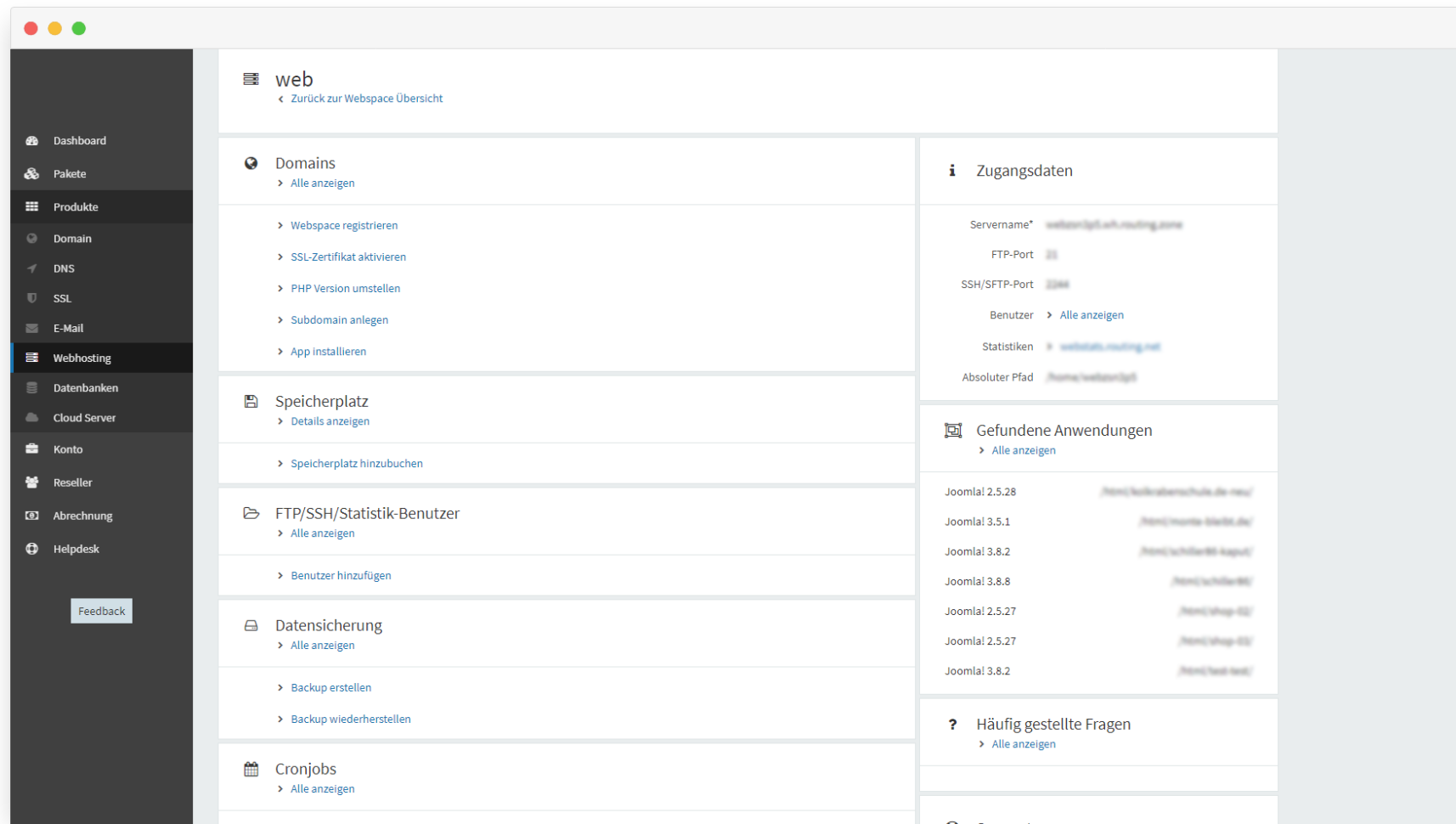
The screenshot displays the hosting.de control panel interface. On the left is a dark sidebar with navigation links: Dashboard, Pakete, Produkte, Domain, DNS, SSL, E-Mail, Webhosting (highlighted), Datenbanken, Cloud Server, Konto, Reseller, Abrechnung, and Helpdesk. A 'Feedback' button is at the bottom of the sidebar.

The main content area is titled 'Produkte > Webhosting' and shows 'Gefundene Anwendungen' (Found Applications) with a link to 'Zurück zum Webspace'. Below this is a table of Joomla! installations:

Anwendung	Version	Verzeichnis
Joomla!	2.5.28	/home/xxxxxx/public_html/
Joomla!	3.5.1	/home/xxxxxx/htdocs/
Joomla!	3.8.2	/home/xxxxxx/htdocs/
Joomla!	3.8.8	/home/xxxxxx/htdocs/
Joomla!	2.5.27	/home/xxxxxx/htdocs/
Joomla!	2.5.27	/home/xxxxxx/htdocs/
Joomla!	3.8.2	/home/xxxxxx/htdocs/

On the right side of the main area, there are two sections: 'Häufig gestellte Fragen' (Frequently Asked Questions) with a link 'Alle anzeigen' and a list of questions, and 'Support' featuring 'Supportzeiten' (Mo-Fr: 9-18 Uhr), the name 'Jean Kahrs' (DevOps), a photo of a man, and links for 'Mein Support Versprechen' and 'Zum Kontaktformular'.

Was heißt das für euch?



Was bringt die Zukunft... für euch?

- „Update verfügbar“ anzeigen
- PHP-Versionupdate vorschlagen
- Versionsmonitoring mit Hinweis auf veraltete Version
- Addons / Extensions anzeigen
- Auto-Update
- Anti-Virus-Maßnahmen

Was bringt die Zukunft... für das Projekt?

- Analyse der HTTP-Request Payload
- Erkennen neuer Exploits
- Projekt wird OpenSource..? Wir alle wollen ein sichereres Internet

Danke fürs zuhören!



Folien verfügbar unter <https://github.com/hosting-de-labs/talks>