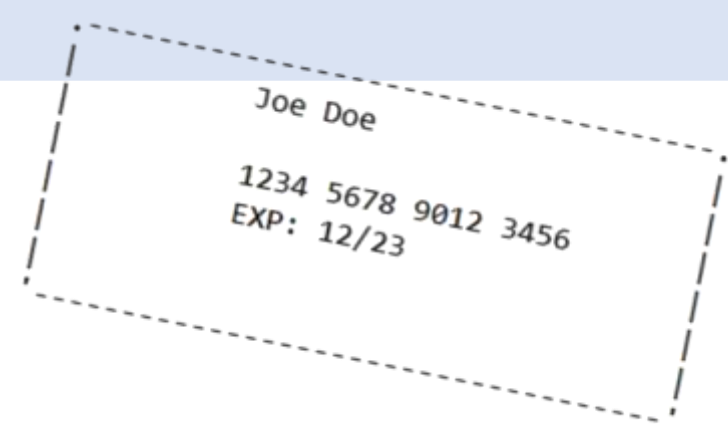


# Oh no: KUNO

## Gesperrte Girocards entsperren



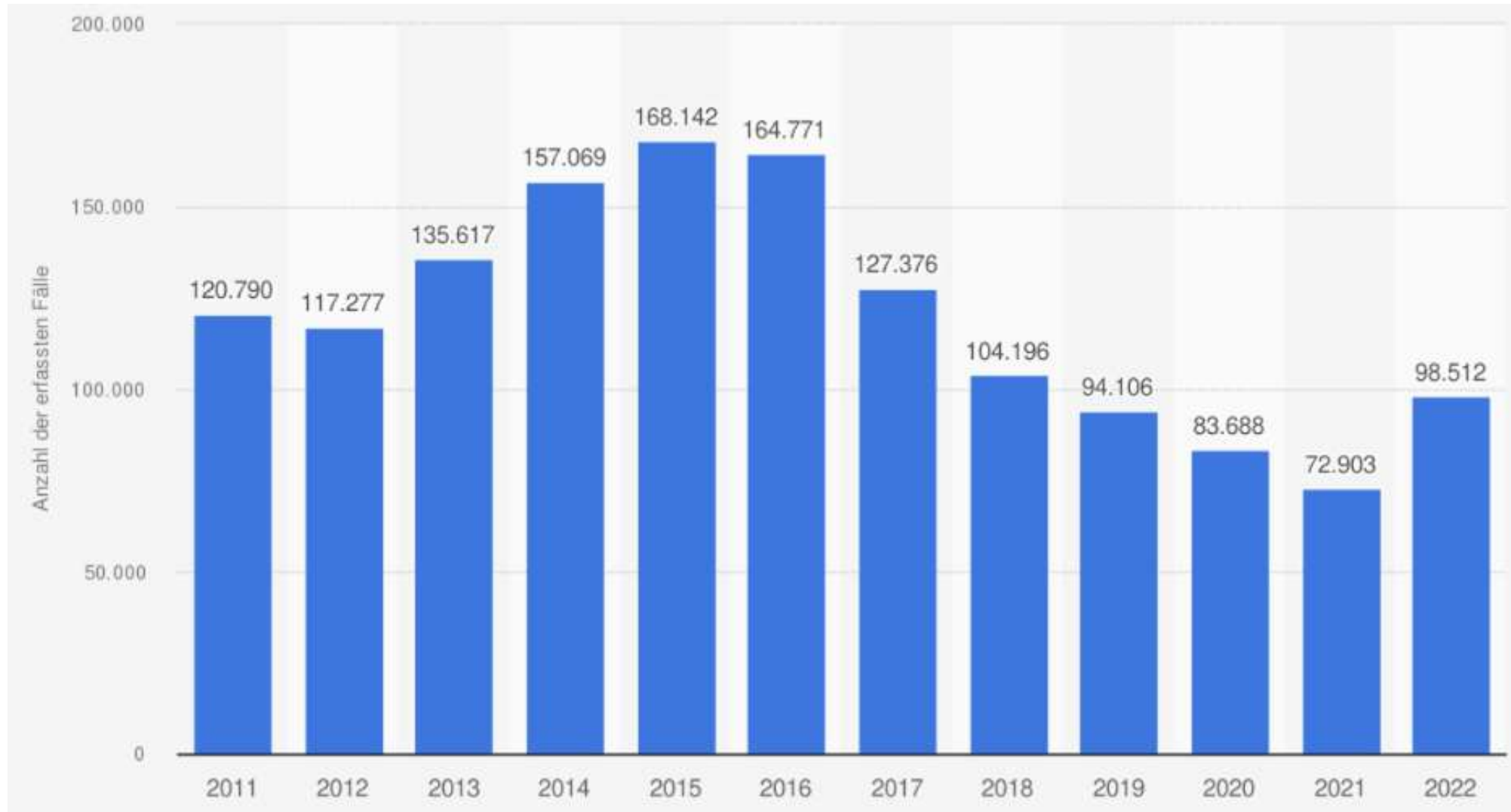
**Tim Philipp Schäfers (TPS)**

37. Chaos Communication Congress (37c3)

30. Dezember 2023, Hamburg



# Statistik zu Taschendiebstahl in Deutschland

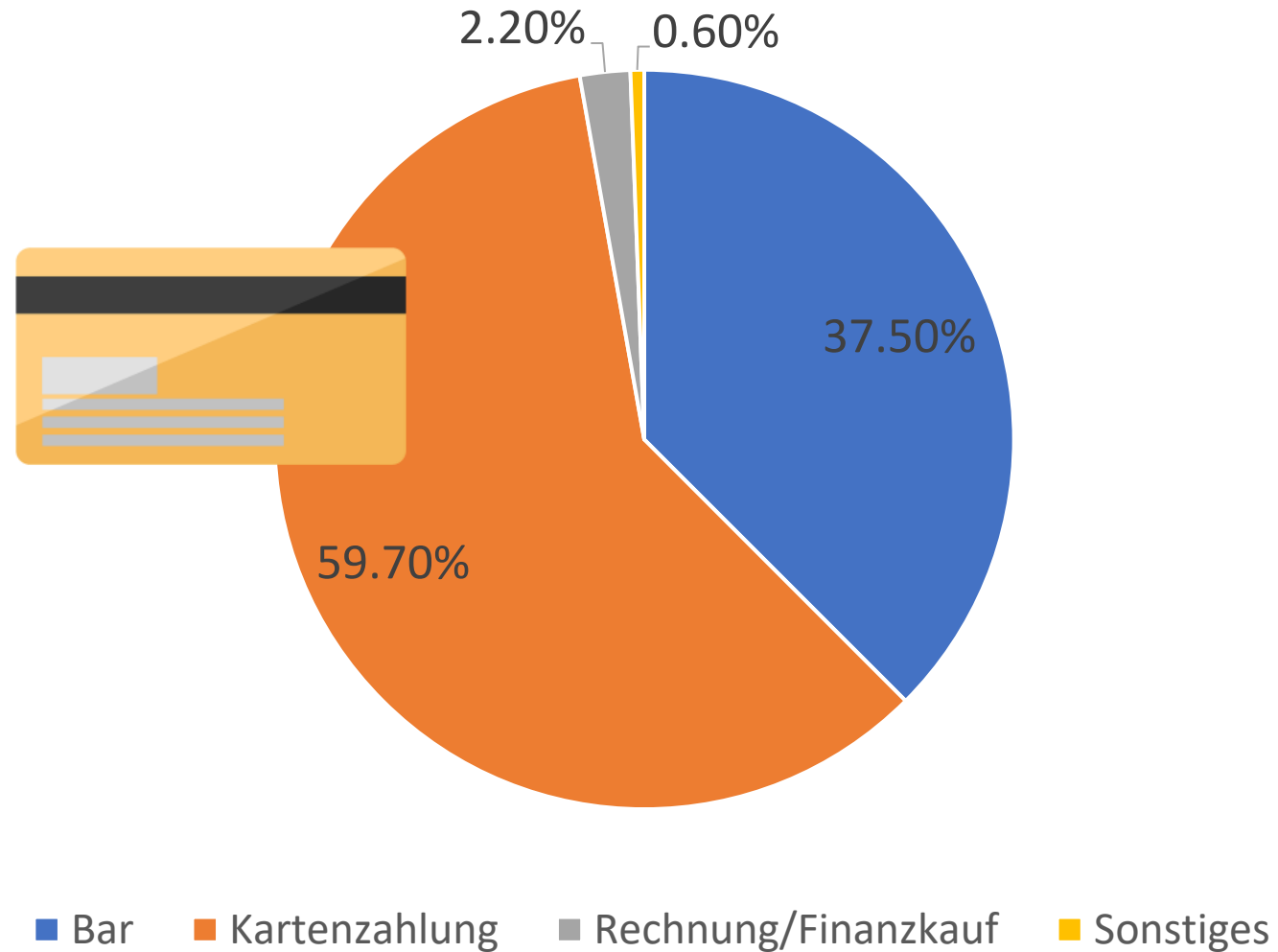


Quelle: BKA - Polizeiliche Kriminalstatistik (PKS)

# (Bargeldlose) Zahlungsmittel



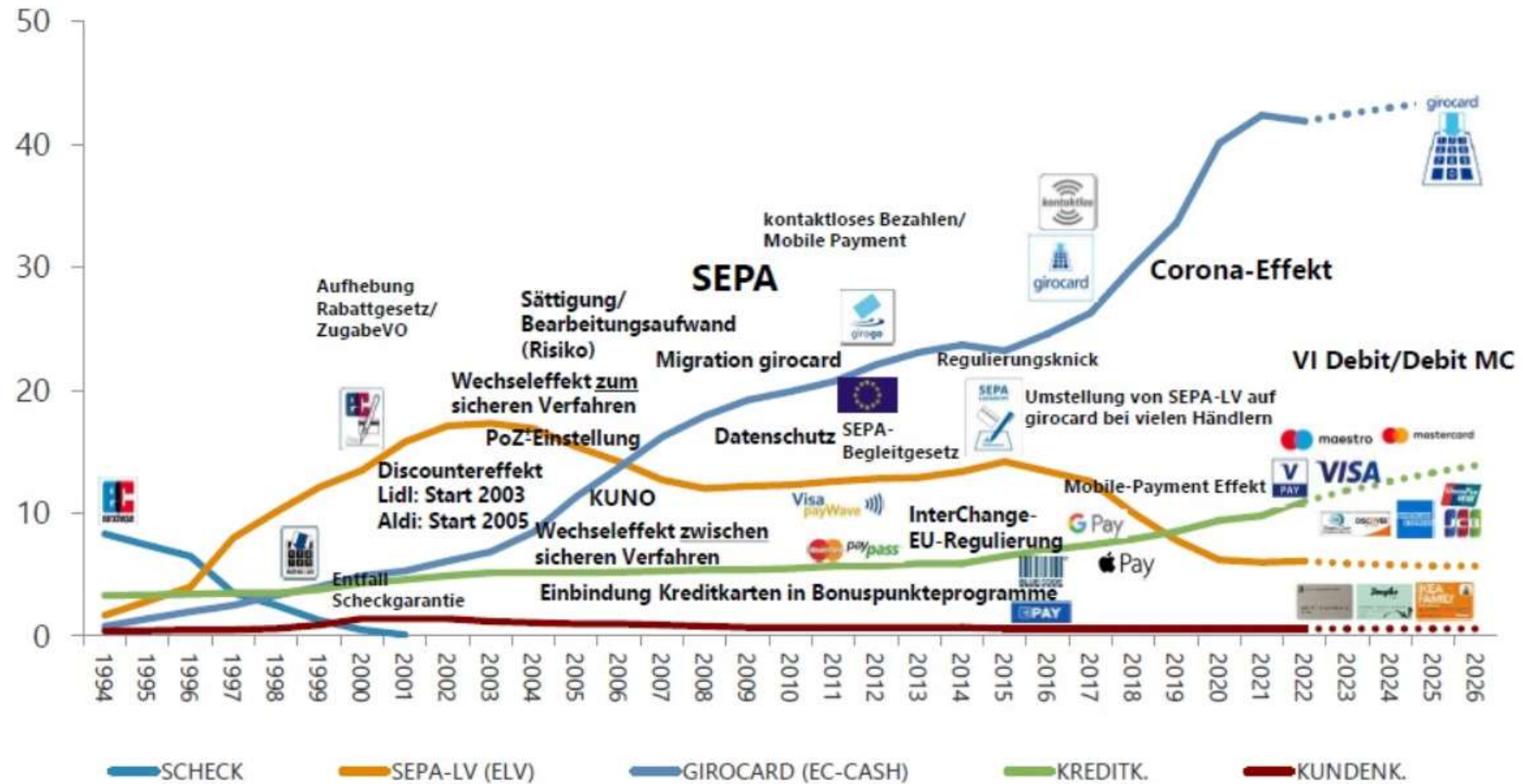
# Verteilung Zahlungsmittel 2022



Quelle: EHI-Studie „Zahlungssysteme im Einzelhandel 2023“ (im stationären Handel)

# Entwicklung von unbaren Zahlungsarten

Anteile der Zahlungsarten in % vom Umsatz 1994-2026



Quelle: EHI-Erhebungen 1995 bis 2021 und EHI-Prognose bis 2026 (Debitkarten von Visa und MasterCard sind Kreditkarten zugerechnet)

Quelle: Hanno Bender & Horst Rüter (EHI), <https://www.bargeldlosblog.de/die-lange-geschichte-der-lastschrift/>

# Zahlungsarten bei Kartenzahlung 2022

| Zahlungsart  | Beginn / Ende   | Marktanteil*                |
|--|---|-----------------------------|
| Elektronisches Lastschriftverfahren (ELV) / SEPA-Lastschrift | Seit 1984   | 6,1 %<br>28,365,000,000 €   |
| Girocard (Maestro)   | 1990er (EC & ECD)<br>ab 2007 (Umbenennung der EC-Karte)<br>2007-2027 (geplantes Ende der Maestro-Karte) | 41,9 %<br>194,835,000,000 € |
| Kreditkarte  | -   | 8,2 % (38,130,000,000 €)    |
| Debit International  | -   | 2,9 % (13,485,000,000 €)    |
| Handelskarte   | -   | 0,6 % (2,790,000,000 €)     |

\* Quelle: EHI-Studie „Zahlungssysteme im Einzelhandel 2023“

\* Marktanteil im Stationären Handel 2022 nach (exkl. Kfz, Mineralöl, Apotheken, E-Commerce/Versandhandel, inkl. Tankstellen-Shopumsätze)

# Zahlungsarten bei Kartenzahlung 2022

| Zahlungsart  | Beginn / Ende   | Marktanteil*                |
|--|---|-----------------------------|
| Elektronisches Lastschriftverfahren (ELV) / SEPA-Lastschrift | <b><u>Seit 1984</u></b>   | 6,1 %<br>28,365,000,000 €   |
| Girocard (Maestro)   | 1990er (EC & ECD)<br>ab 2007 (Umbenennung der EC-Karte)<br>2007-2027 (geplantes Ende der Maestro-Karte) | 41,9 %<br>194,835,000,000 € |
| Kreditkarte  | -   | 8,2 % (38,130,000,000 €)    |
| Debit International  | -   | 2,9 % (13,485,000,000 €)    |
| Handelskarte   | -   | 0,6 % (2,790,000,000 €)     |

\* Quelle: EHI-Studie „Zahlungssysteme im Einzelhandel 2023“

\* Marktanteil im Stationären Handel 2022 nach (exkl. Kfz, Mineralöl, Apotheken, E-Commerce/Versandhandel, inkl. Tankstellen-Shopumsätze)



# Tagesschau vom 28.12.1984 (erster Congress)

Quelle: Auszug Tagesschau vom 28.12.1984 (ARD)





*„[...] Möglichkeiten und Mängel des Computers selbst beurteilen können.“*

➔ Sperrsysteme für Bankkarten ...\*



\* Fokus auf Girocards

Entsprechende Sicherheitslücken wurden im Rahmen von Responsible Disclosure Meldungen den Betreibern gemeldet.

# Sperr-Notruf

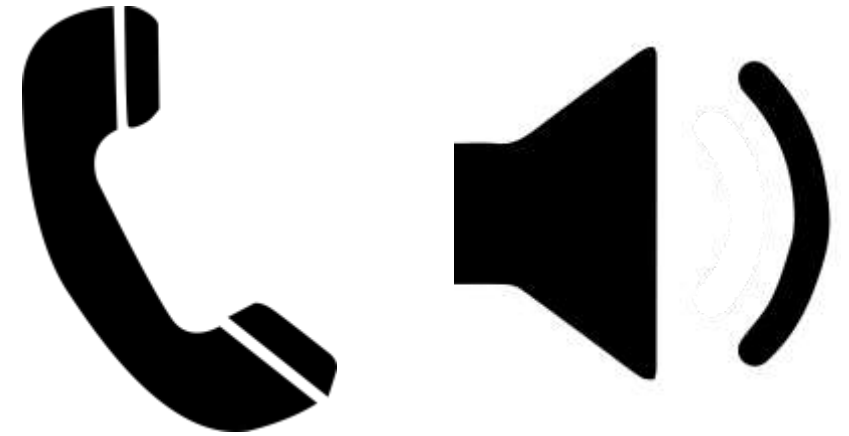
- Sperr-Notruf 116 116 e.V.
- 2002 gegründeter Verein
- 1,5 Millionen Sperrungen und Sperrvermittlungen im Jahr
- > 1.200 angeschlossene Banken + weitere Organisationen
- Sperrung weiterer Karten möglich: Personalausweis, Mitarbeiterausweise, etc.
- technische Realisierung: SERVODATA GmbH



# Sperr-Notruf



- Automatisierter Ablauf für Sperrungen
- Verbindung von einem „Sprachcomputer“ zum anderen
- Anschließende Weiterleitung der Sperre an zuständige Bank



# SperrApp



## SperrApp

SERVODATA GmbH

3.7★

452 reviews ⓘ

50K+

Downloads



USK: All ages ⓘ

Install



<https://play.google.com/store/apps/details?id=de.servodata.sperrapp>



Store

Mac

iPad

iPhone

Watch

AirPods

## App Store Vorschau

Öffne den Mac App Store, um A



### SperrApp <sup>4+</sup>

SERVODATA GMBH

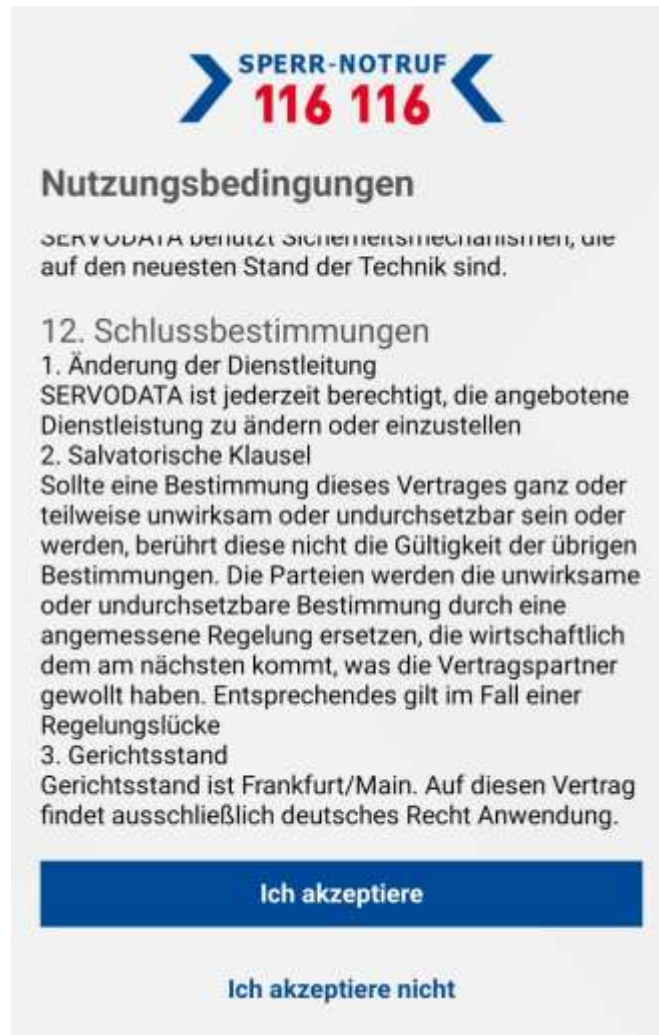
Entwickelt für iPhone

★★★★★ 4,1 • 109 Bewertungen

Gratis

<https://apps.apple.com/de/app/sperrapp/id765585858>

# SperrApp



**SPERR-NOTRUF 116 116**

## Nutzungsbedingungen

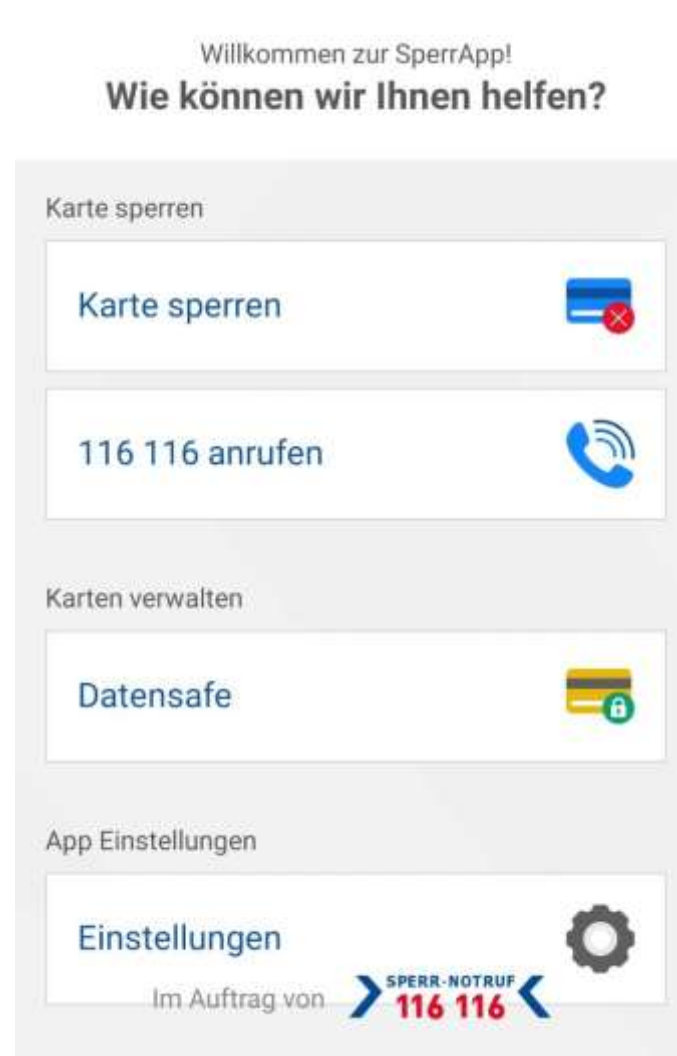
SERVODATA benutzt Sicherheitsmechanismen, die auf den neuesten Stand der Technik sind.

### 12. Schlussbestimmungen

1. Änderung der Dienstleitung  
SERVODATA ist jederzeit berechtigt, die angebotene Dienstleistung zu ändern oder einzustellen
2. Salvatorische Klausel  
Sollte eine Bestimmung dieses Vertrages ganz oder teilweise unwirksam oder undurchsetzbar sein oder werden, berührt diese nicht die Gültigkeit der übrigen Bestimmungen. Die Parteien werden die unwirksame oder undurchsetzbare Bestimmung durch eine angemessene Regelung ersetzen, die wirtschaftlich dem am nächsten kommt, was die Vertragspartner gewollt haben. Entsprechendes gilt im Fall einer Regelungslücke
3. Gerichtsstand  
Gerichtsstand ist Frankfurt/Main. Auf diesen Vertrag findet ausschließlich deutsches Recht Anwendung.


**Ich akzeptiere**


Ich akzeptiere nicht




Willkommen zur SperrApp!  
**Wie können wir Ihnen helfen?**

Karte sperren


Karte sperren 

116 116 anrufen 


Karten verwalten

Datensafe 

App Einstellungen

Einstellungen 

Im Auftrag von **SPERR-NOTRUF 116 116**



☰ Menü ⊕ Karte hinzufügen

## Datensafe

Debitkarte wurde erfolgreich hinzugefügt

## Debitkarte

|                             |                      |                   |
|-----------------------------|----------------------|-------------------|
| IBAN                        | <input type="text"/> | Details           |
| Kartenfolgenummer           | 1                    | Gültigkeit ' 2026 |
| Karteninhaber: Tim Schäfers |                      |                   |

Eigene Screenshots

# SperrApp

[← Zurück](#)

## Sperrungen 1 — 2

Geben Sie die Bankdaten ein, die Sie sperren möchten. Sie können zwischen IBAN oder BLZ & Kontonummer wählen:

Mit IBAN sperren

IBAN  
DE [redacted]

**oder**

Mit BLZ & Kontonummer sperren

|              |             |
|--------------|-------------|
| Bankleitzahl | Kontonummer |
| [redacted]   | [redacted]  |

**Weiter**

[← Zurück](#)

## Sperrung bestätigen 1 — 2

Sind Sie sicher, dass Sie diese Karte sperren möchten?

Bankleitzahl  
[redacted] 1

Name der Bank  
[redacted] Bank

**Weiter**

[Ich habe meine Meinung geändert](#)

Eigene Screenshots

# Sperrren 2023 – aber wie?

Quelle: <https://www.sperr-notruf.de/sperr-fax-sperr-app.html>



## Sperr-Fax

Du kannst schriftlich Deine Sperrungen veranlassen. Einfach das zutreffende Formular auswählen, downloaden, ausfüllen, faxen.

[https://www.sperr-notruf.de/download/Sperr-Notruf\\_116\\_116-Sperrfax-Girocard.pdf](https://www.sperr-notruf.de/download/Sperr-Notruf_116_116-Sperrfax-Girocard.pdf)

100 %

### WAS SOLL GESPERRT WERDEN?

**GIROCARD** (ehemals ec-Karte), Maestro-, Bankkunden- oder Sparkarte

IBAN:

Konto-Nr. (max. 10-stellig):

BLZ (8-stellig):

Name, Ort des Kreditinstituts:

Grundsätzlich werden immer alle auf das Konto ausgestellten Karten gesperrt, **außer Kreditkarten**. Informieren Sie bitte Ihr zuständiges Kreditinstitut schnellstmöglich über den Verlust Ihrer Karte. Zur Entsperrung der Karten wenden Sie sich bitte an Ihr zuständiges Kreditinstitut.

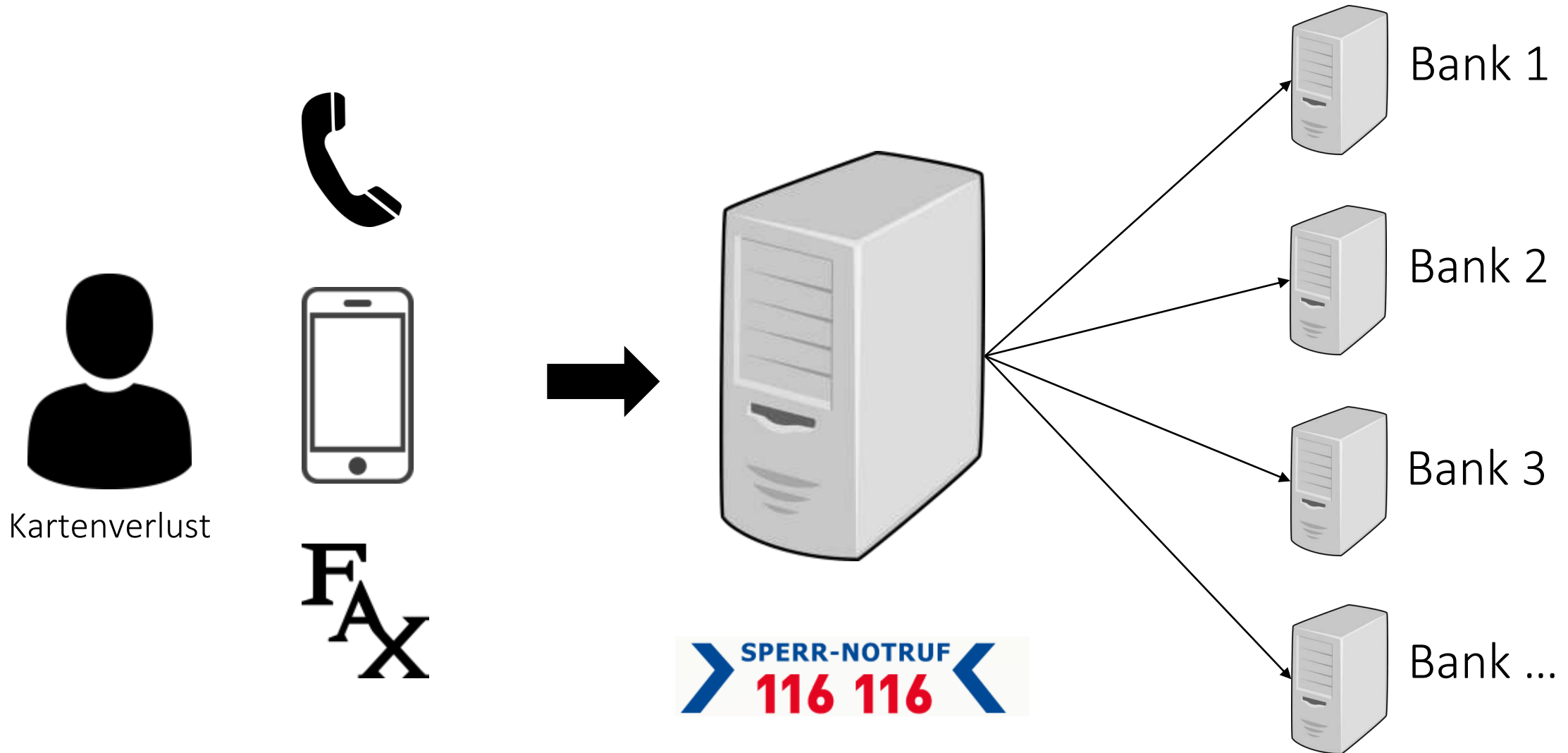
### RECHTLICHER HINWEIS

Der Sperr-Notruf 116 116 gilt für Kunden mit Karten und Medien, deren Herausgeber sich dem Sperr-Notruf angeschlossen haben. Kunden können den Herausgeber ihrer Medien fragen, ob sich diese dem Sperr-Notruf bereits angeschlossen haben. Des Weiteren besteht die Möglichkeit, sich auf der Homepage des Sperr-Notrufs unter [www.sperr-notruf.de](https://www.sperr-notruf.de) über die beteiligten Herausgeber zu informieren. Ihr Sperr-Fax wird von der SERVODATA GmbH an Ihren jeweiligen Vertragspartner zur Sperrung weitergeleitet. Ihre GIROCARD (ehemals EC-KARTE), MAESTRO-, BANKKUNDEN- ODER SPARKARTE ist erst bei Eingang der Anzeige bei Ihrem jeweiligen Vertragspartner gesperrt. Dazu muss dieses Formular vollständig, korrekt und leserlich ausgefüllt sein. Mit Eingang des Faxes bzw. Anrufes ist der Versicherungsschutz gegeben, sofern die gemachten Angaben richtig waren. Sollte die Faxnummer 116 116 nicht erreichbar sein, kann alternativ die Rufnummer +49 30 40 50 40 50 verwendet werden.

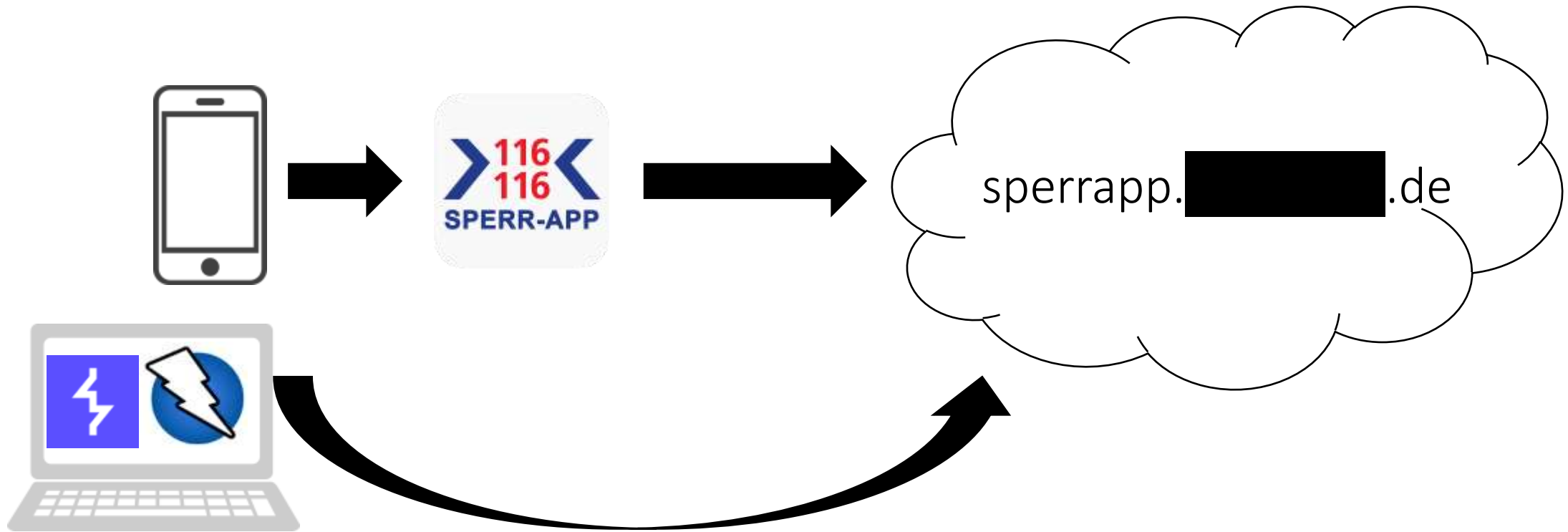
Datum:  Unterschrift des Karteninhabers: X



# 116 116 Sperr-Notruf - Funktionalität

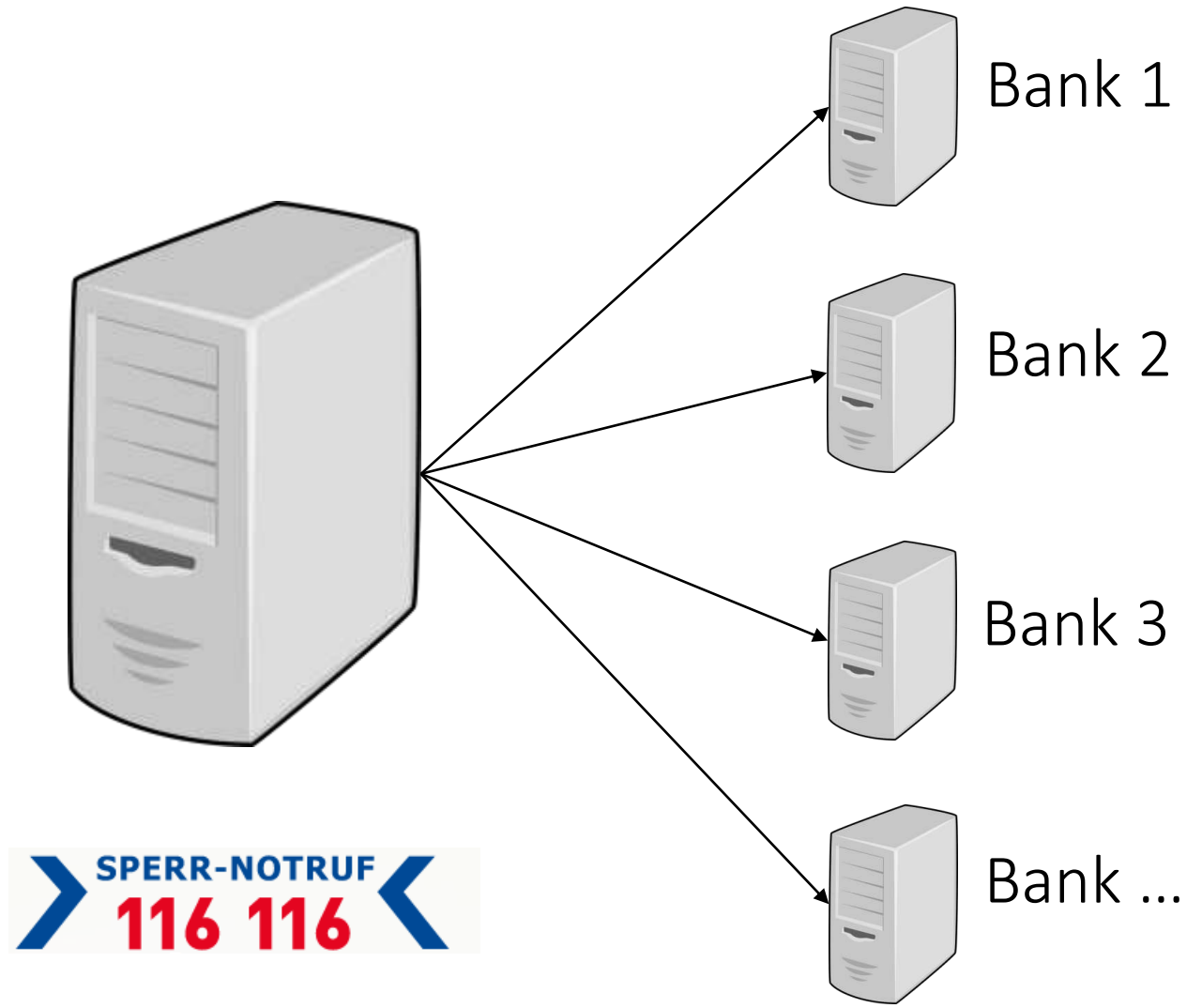


# Sperr-App

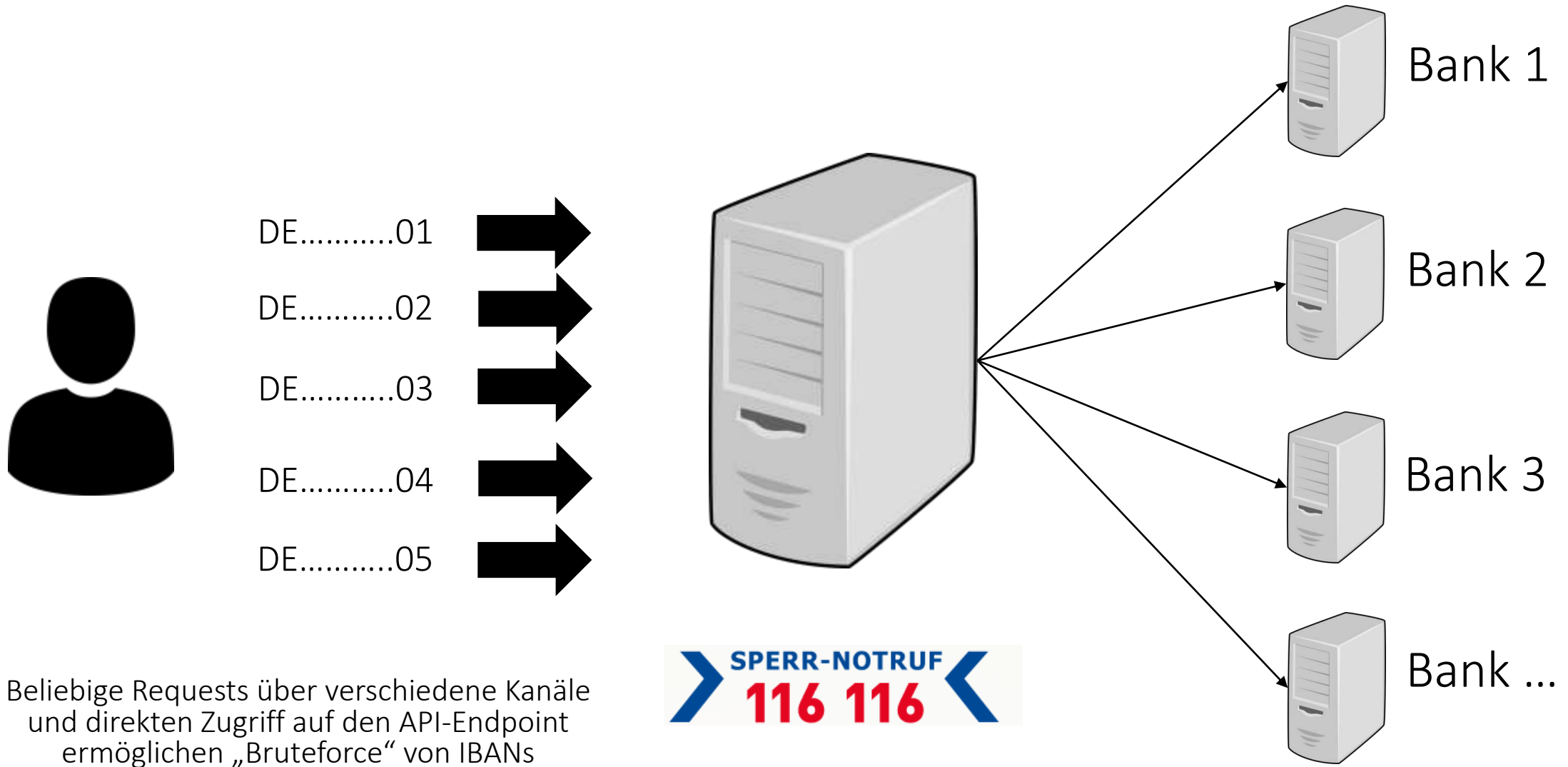


Ratelimiting Bypass via  
Intercepting Proxy auf lokalem Rechner

# Sperr-Notruf - Funktionalität



# Sperr-Notruf - Massensperrung





Beliebige Requests über verschiedene Kanäle und direkten Zugriff auf den API-Endpoint ermöglichen „Bruteforce“ von IBANs

Karte gesperrt, alles gut? 😊  
Leider nicht ganz ...

# Nicht alles wurde gesperrt 😱?

Quelle: <https://www.sperr-notruf.de/anzeige-erstatten-bei-diebstahl.html>

  <https://www.sperr-notruf.de/anzeige-erstatten-bei-diebstahl.html>

## Auch das **elektronische Lastschriftverfahren** **per Unterschrift sperren!**

Kriminelle könnten versuchen, mit Deiner gestohlenen girocard einzukaufen und die Zahlung an der Kasse per falscher Unterschrift zu bestätigen. Bei der örtlichen Polizei kannst Du Dich dagegen absichern. Wenn Du den Kartendiebstahl zur Anzeige bringst, erfasst die Polizei auf Wunsch auch eine **KUNO-Meldung**. Halte dazu Deine IBAN bereit (oder Deine BLZ und Kontonummer) sowie die Kartenfolgenummer (wenn bekannt).



# KUNO? 😊



Quelle: privat | Kuni



KUNO? 😊



Quelle: Pixabay | maminounou

# KUNO-Sperrsystem

Quelle: Auszug ZDF WISO vom 09.05.2016 (ZDF)



# KUNO-Sperrsystem

**KUNO**  
Karten Sperrdienst für  
SEPA-Lastschriftzahlungen

Eine Initiative von:

**EHI** Retail Institute®

**HDE**  
Handelsverband  
Deutschland

Wir wollen  
dass Sie  
sicher leben.  
**Ihre Polizei**

[HOME](#)

[ÜBER KUNO](#)

[FAQ](#)

[KONTAKT](#)

[LOGIN](#)

**KUNO**

**Karten-Sperrdienst**

**für SEPA-Lastschriftzahlungen**

**Wozu KUNO?**

Banken sperren ausschließlich für PIN-basierte Kartenzahlungen. Mit Hilfe von KUNO sperren Sie Ihre Karte zusätzlich für Zahlungen mit Unterschrift.



## girocard gestohlen oder verloren?

Ihnen wurde die girocard gestohlen oder Sie haben ihr Portemonnaie samt allen wichtigen Karten verloren? Handeln Sie nun schnell und lassen Sie Ihre girocard für das elektronische Lastschriftverfahren bei der Polizei sperren. **Mit dem Einrichten einer KUNO-Sperre sind Sie auf der sicheren Seite.**



**KARTENFOLGENUMMER  
NACHMELDEN**

Wofür steht KUNO? 😊

K  
U  
N  
O

Wofür steht KUNO? 😊

**K**riminalitätsbekämpfung im  
**U**nbaren Zahlungsverkehr durch  
**N**utzung nichtpolizeilicher  
**O**rganisationen

# KUNO-Sperrsystem

## Betreiber:

- EHI Retail Institute GmbH
  - Handelsverband Deutschland
  - Deutsche Polizei - ProPK (Polizeiliche Kriminalprävention der Länder und des Bundes)
- 
- Sperrung der SEPA-Lastschrift (ELV) pro IBAN durch Eintrag in Sperrdatei
  - Testsystem 2001, Ausweitung ab 2005 nach Beschluss der Innenministerkonferenz
  - > 120.000 Sperrungen im Jahr
  - technische Realisierung: EHI Retail Institute GmbH (mit Dienstleistern)

**KUNO** 

Karten Sperrdienst für  
SEPA-Lastschriftzahlungen





# KUNO-Sperrsystem - Versprechen

„Mit dem Einrichten einer KUNO-Sperre sind Sie auf der sicheren Seite.“  
KUNO – Startseite

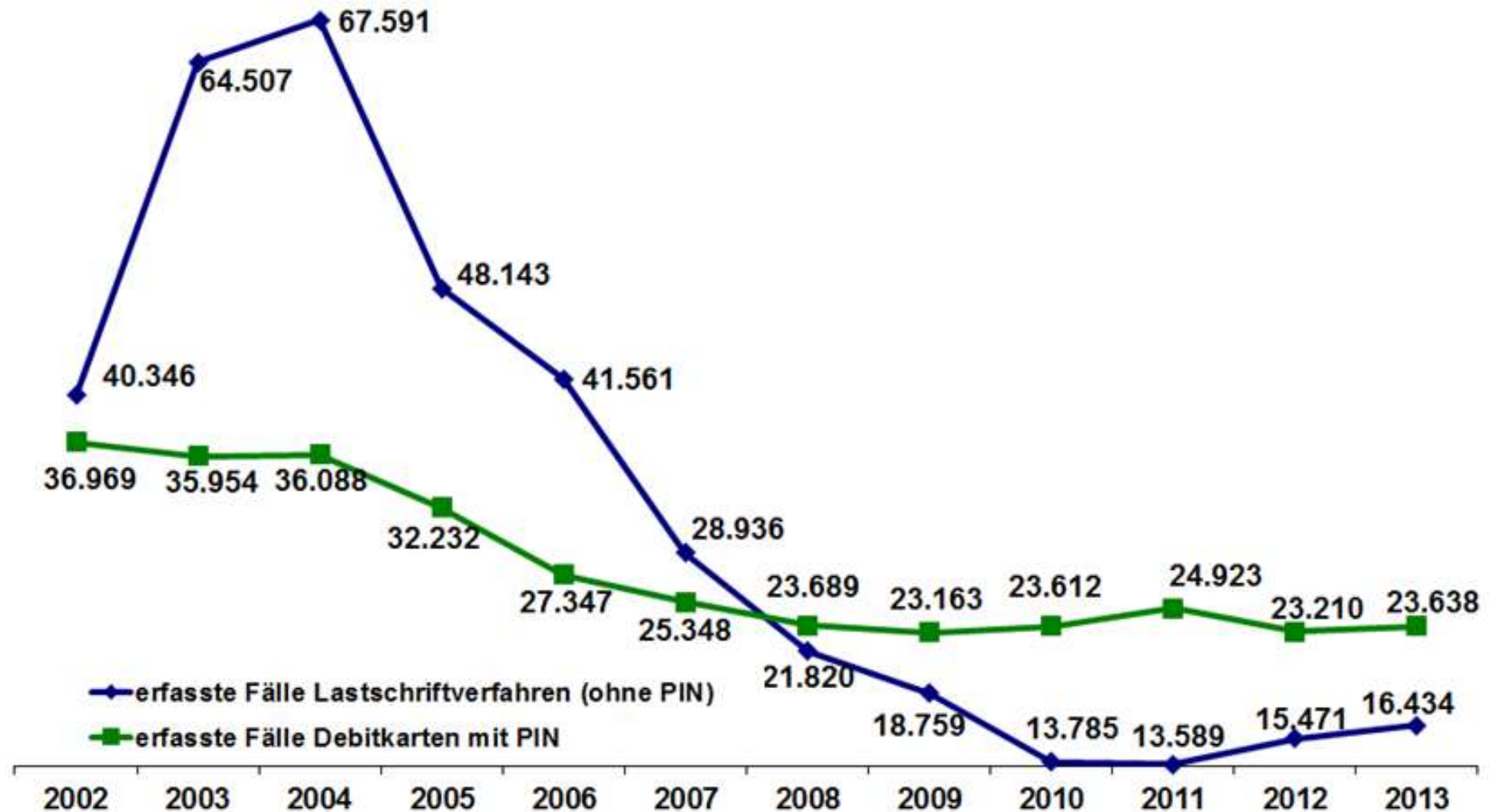
„[...] Es ist ein Beitrag zu mehr Sicherheit in unserem Land. Die erweiterte Kartensperre schützt Bürger und Handel vor Scheckkarten-Betrügern [...]“  
Innenminister Jörg Schönbohm  
(Ministerium des Innern Brandenburg, 2003)

„So können Sie geklaute EC-Karten effektiv sperren lassen.“  
Handwerksblatt 2016

„KUNO stellt ein simples, aber wirkungsvolles Sperrsystem dar [...]“  
KUNO – Über uns



# KUNO-Sperrsystem zeigt Wirkung



Quelle: <https://einzelhandel.de/themeninhalte/zahlungssysteme/281-nachrichten/6502-polizeiliche-kriminalstatistik-betrug-implv-verfahren-weiter-auf-niedrigem-niveau> / Polizeiliche Kriminalstatistik 2002-2013

# KUNO-Sperrsystem - Funktionalität



Meldung an KUNO

1.) Polizei

Aufnahme von zu sperrendem Konto bei Anzeige von Diebstahl



Self-Service\*

3.) Betroffene Personen

Freischaltung oder Meldung der Kartenfolgenummer



Bezug der Sperddatei

2.) Handel & Payment Dienstleister

Abgleich mit Sperrdateien/  
Zurückweisung von gestohlenen Debitkarten



\* 3 Bundesländer (Mecklenburg-Vorpommern, Rheinland-Pfalz, Sachsen) erlauben kein Self-Service.

Karte gesperrt, alles gut? 😊  
Leider nicht ganz ...

# Auszug: Sicherheits- & Datenschutzprobleme aus der Responsible Disclosure Meldung



32-seitiger Report

# Port Scan ...

```
nmap -p 1-65535 -T4 -A -v kuno-sperrdienst.de
```

```
PORT STATE SERVICE VERSION
```

```
80/tcp open http
```

```
[...]
```

```
443/tcp open ssl/https Microsoft-IIS/10.0
```

```
[...]
```

```
| http-methods:
```

```
| Supported Methods: OPTIONS TRACE GET HEAD POST
```

```
|_ Potentially risky methods: TRACE
```

```
|_ http-server-header: Microsoft-IIS/10.0
```

```
|_ http-title: Willkommen bei KUNO Sperrdienst - Eine Initiative von EHI, HDE...
```

```
[...]
```

```
1221/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
[...]
```

```
3544/tcp closed teredo
```

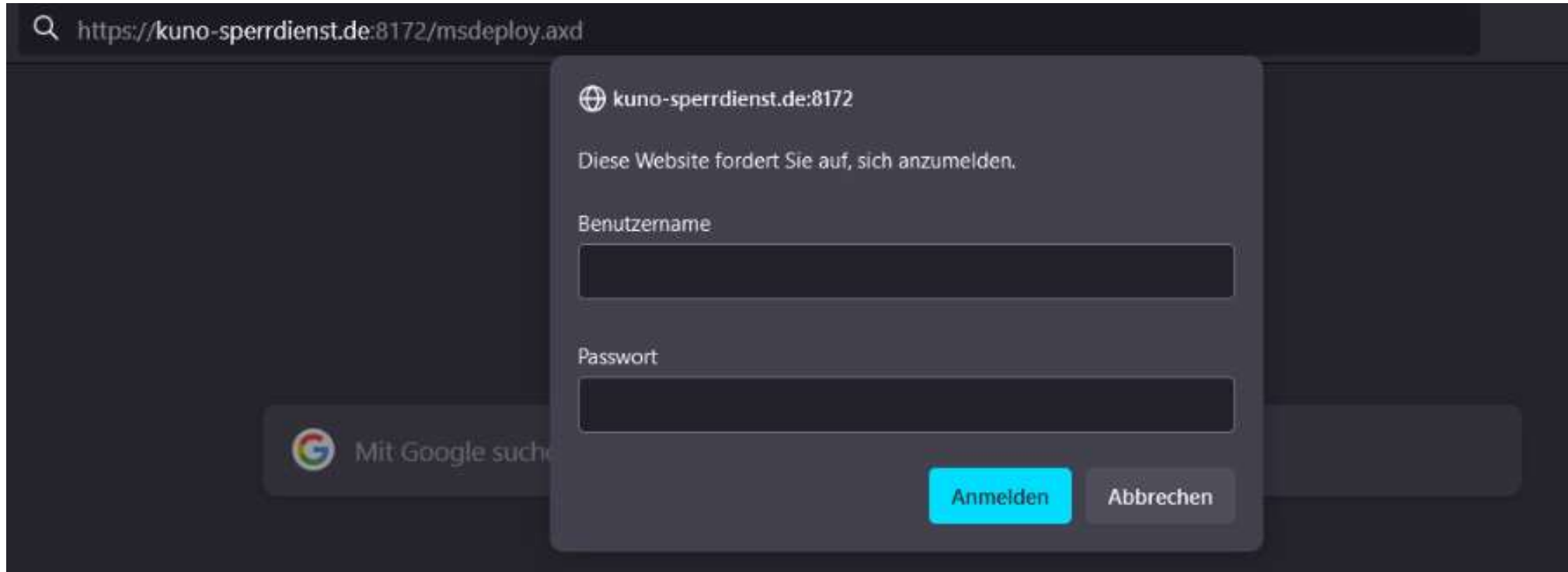
```
4022/tcp open dnox?
```

```
4024/tcp open tnp1-port?
```

```
8172/tcp open ssl/http Microsoft IIS httpd 10.0
```



# IIS Management Port im Internet



**Port 8172 - Standard-Port des IIS Management Services**

**Webserver auf Microsoft Azure ...**

**Bereitstellung von Webpaketen mittels MSDeploy (Username/Passwort)**

# IIS Management Port im Internet

## Azure App Service - How to block MsDeploy.axd on port 8172

Ask Question

Asked 3 years, 7 months ago Modified 3 years, 7 months ago Viewed 968 times

 Part of Microsoft Azure Collective



We have an App Service running in Azure that hosts a website. We've recently had a security review on the web site and one of the items found was that the end point below was exposed.

4



```
https://<appName>.azurewebsites.net:8172/msdeploy.axd
```



The recommendation is that this end point should be blocked and using a whitelist to allow limited access (e.g. the build machine that deploys to Azure). How do I block this end point?

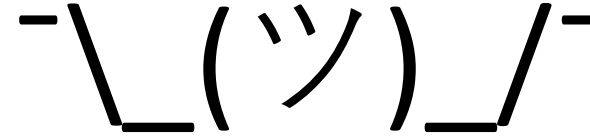
Quelle: <https://stackoverflow.com/questions/61905095/azure-app-service-how-to-block-msdeploy-axd-on-port-8172>



# IIS Management Port im Internet

## Azure App Service - How to block MsDeploy.axd on port 8172

Ask Question



Asked 3 years, 7 months ago Modified 3 years, 7 months ago Viewed 968 times

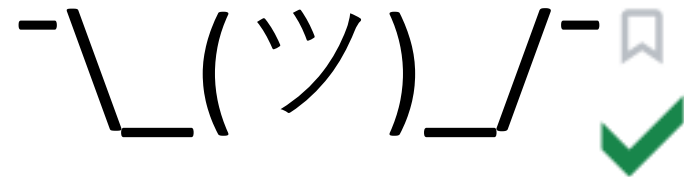
Part of Microsoft Azure Collective

2 Answers

Sorted by: Highest score (default)

4  
We have an App Service run recently had a security review found was that the end point  
`https://<appName>.azurewebsites.net`  
The recommendation is that a whitelist to allow limited access (to the App Service). How do I block this endpoint?

2  
After discussions with Microsoft support it appears that port 8172 is enabled for backwards compatibility with old versions of MsDeploy. This port is being phased out and will be open sometimes and not other times.



The fix was for us to create a new resource group, app service plan and app services multiple times until we ended up a server that had the port closed. This was frustrating but ultimately it did resolve the issue.

Quelle: <https://stackoverflow.com/questions/61905095/azure-app-service-how-to-block-msdeploy-axd-on-port-8172>

# Datenschutz: Google Fonts ☹️ ⚡

```
← → ↻ 🏠 view-source:https://kuno-sperrdienst.de/
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <!-- Title -->
5   <title>Willkommen bei KUNO Sperrdienst - Eine Initiative von EHI, HDE und ProPK</title>
6
7   <!-- Required Meta Tags Always Come First -->
8   <meta charset="utf-8">
9   <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
10  <meta http-equiv="x-ua-compatible" content="ie=edge">
11  <link href="https://fonts.googleapis.com/css?family=Signika+Negative&display=swap" rel="stylesheet">
12  <!-- Favicon -->
13  <link rel="shortcut icon" href="/favicon_512x512.png">
14
15  <!-- Google Fonts -->
16  <link rel="stylesheet" href="//fonts.googleapis.com/css?family=Open+Sans%3A400%2C300%2C500%2C600%2C700">
17
18  <!-- CSS Global Compulsory -->
19  <link rel="stylesheet" href="/requirements/css/bootstrap/bootstrap.min.css">
20
21  <link re
22  <link re
23
24  <!-- CSS
25  <link re
26  <link re
27  <link re
28
29  <!-- CSS
30  <link re
31 </head>
```

Keine Erwähnung in den Datenschutzbestimmungen

Keine Verbindung mit Cookie Banner

https://www.golem.de/news/landgericht-muenchen-einbindung-von-google-fonts-ist-rechtswidrig-2202-162826.html

**golem.de** IT-NEWS FÜR PROFIS

HOME TICKER PODCAST NEWSLETTER **GOLEM PLUS** FORUM **ANMELDEN**

Artikel, News, ... **Suchen** **Mehr lesen mit Golem Plus**

KARRIEREWELT JOBS IT-FACHTRAININGS COACHINGS SPRACHKURSE GEHALTSHECK | GOLEM-PC TECHNIK-RATGEBER DEALS

LANDGERICHT MÜNCHEN

## Einbindung von Google Fonts ist rechtswidrig

Wer Schriftarten von [Google](#)-Servern ohne Zustimmung einbindet, verstößt gegen die [DSGVO](#). Die Gerichtsentscheidung betrifft aber auch andere [CDNs](#).



1. Februar 2022, 11:26 Uhr, Moritz Tremmel

# Fix: Entwickler tun genau was sie sollen 😊 😊

```
view-source:https://kuno-sperrdienst.de/

1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <!-- Title -->
5   <title>Willkommen bei KUNO Sperrdienst - Eine Initiative von EHI, HDE und PropK</title>
6
7   <!-- Required Meta Tags Always Come First -->
8   <meta charset="utf-8">
9   <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
10  <meta http-equiv="x-ua-compatible" content="ie=edge">
11  <!-- Favicon -->
12  <link rel="shortcut icon" href="/favicon_512x512.png">
13
14  <!-- Google Fonts -->
15  <link rel="stylesheet" href="/requirements/css/fonts.css">
16
17  <!-- CSS Global Compulsory -->
18  <link rel="stylesheet" href="/requirements/css/bootstrap/bootstrap.min.css">
19
20  <link rel="stylesheet" href="/requirements/css/icon-awesome/css/font-awesome.min.css">
21  <link rel="stylesheet" href="/requirements/css/hamburgers/hamburgers.min.css">
22
23  <!-- CSS Unify -->
24  <link rel="stylesheet" href="/requirements/css/unify-core.css">
25  <link rel="stylesheet" href="/requirements/css/unify-components.css">
26  <link rel="stylesheet" href="/requirements/css/unify-globals.css">
27
28  <!-- CSS Customization -->
29  <link rel="stylesheet" href="/requirements/css/custom.css">
30 </head>
```

# Datenschutz: Fragwürdiges Cookie Banner

**KUNO**  
Karten Sperrdienst für  
SEPA-Lastschriftzahlungen

Eine Initiative von:

**EHI** Retail Institute®

**HDE**  
Handelsverband  
Deutschland

Wir wollen  
dass Sie  
sicher leben  
Ihre Polizei

HOME

ÜBER KUNO

FAQ

KONTAKT

LOGIN



girocard gestohlen oder verloren?

Ihnen wurde die girocard gestohlen oder Sie haben ihr Portemonnaie samt allen wichtigen



Diese Website verwendet Cookies

Cookies erleichtern die Bereitstellung unserer Dienste. Mit der Nutzung unserer Dienste erklären Sie sich damit einverstanden, dass wir Cookies verwenden.

[Weitere Informationen](#)

OK



# Datenschutz: Fragwürdiges Cookie Banner

🕸 <https://www.kuno-sperrdienst.de/requirements/js/eu-cookie-banner.js>

```
// Create's 'Implied Consent' EU Cookie Law Banner v:2.4
// Conceived by Robert Kent, James Bavington & Tom Foyster
// Put into a namespace and by Björn Rosell
// Also changed behaviour so you have to click accept to make the banner stay away.
// To make it behave like the original, set "createCookieWhenBannerIsShown" to true.

var CookieBanner = (function () {
  return {
    'createCookieWhenBannerIsShown': false,
    'createCookieWhenAcceptIsClicked': true,
    'cookieDuration': 14, // Number of days before the cookie expires, and the banner reappears
    'cookieName': 'cookieConsent', // Name of our cookie
    'cookieValue': 'accepted', // Value of cookie

    '_createDiv': function (html) {
      var bodytag = document.getElementsByTagName('body')[0];
      var div = document.createElement('div');
      div.setAttribute('id', 'cookie-law');
      div.innerHTML = html;

      // bodytag.appendChild(div); // Adds the Cookie Law Banner just before the closing </body> tag
      // or
      bodytag.insertBefore(div, bodytag.firstChild); // Adds the Cookie Law Banner just after the opening <body> tag

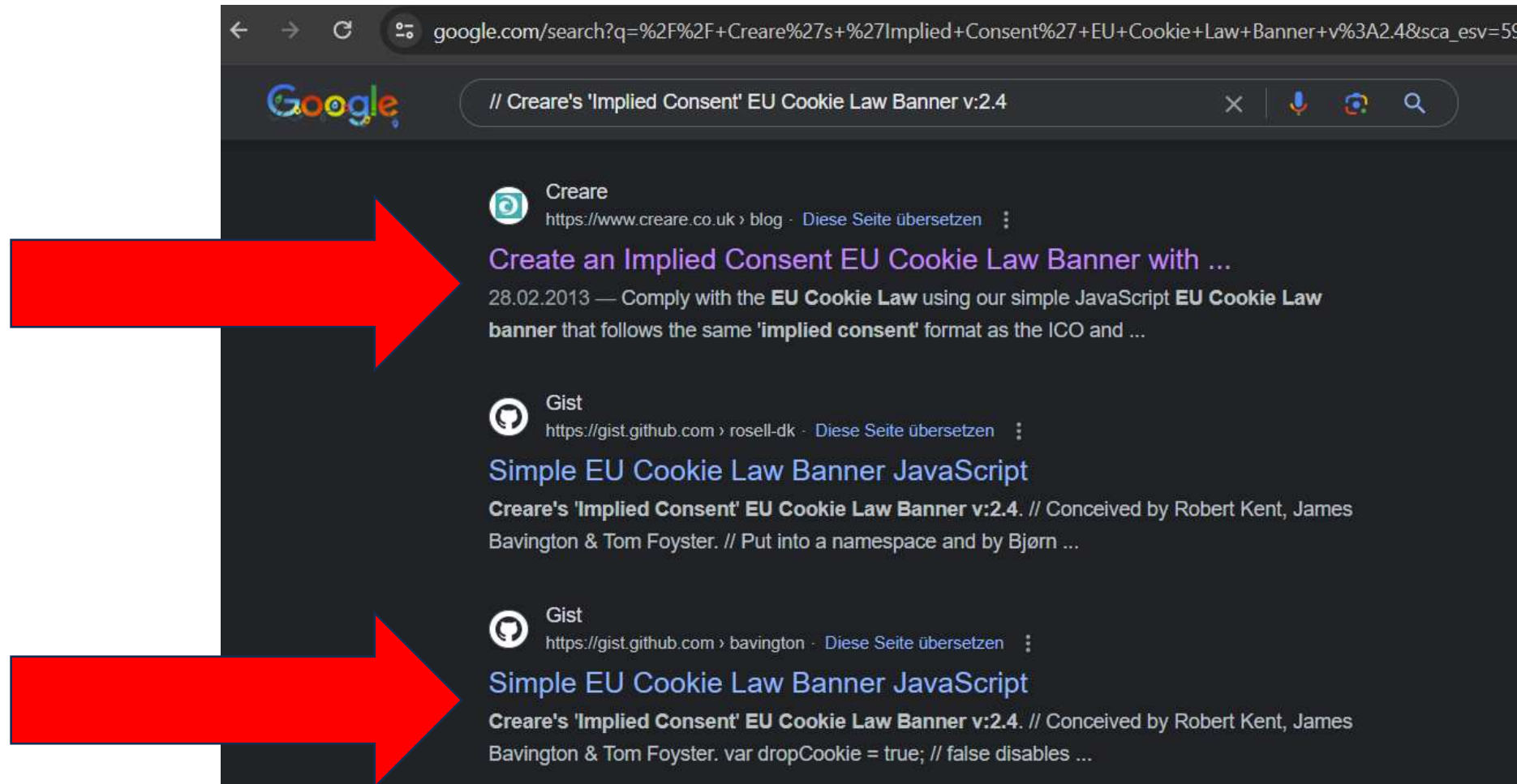
      document.getElementsByTagName('body')[0].className += ' cookiebanner'; //Adds a class to the <body> tag when the banner is visible

      if (CookieBanner.createCookieWhenBannerIsShown) {
        CookieBanner.createAcceptCookie();
      }
    },
  },
},
```



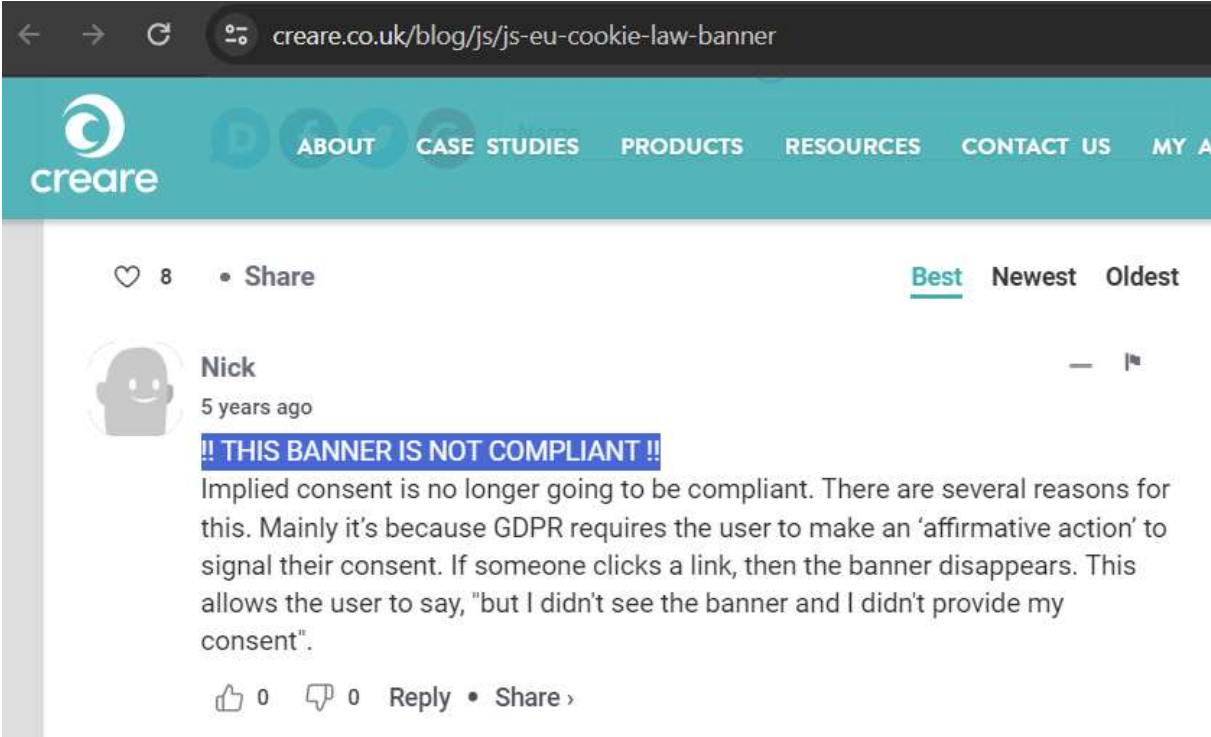
# Datenschutz: Fragwürdiges Cookie Banner

☹️ Suche nach der JavaScript-Datei – **zahlreiche Hinweise auf „Non-Compliance“**

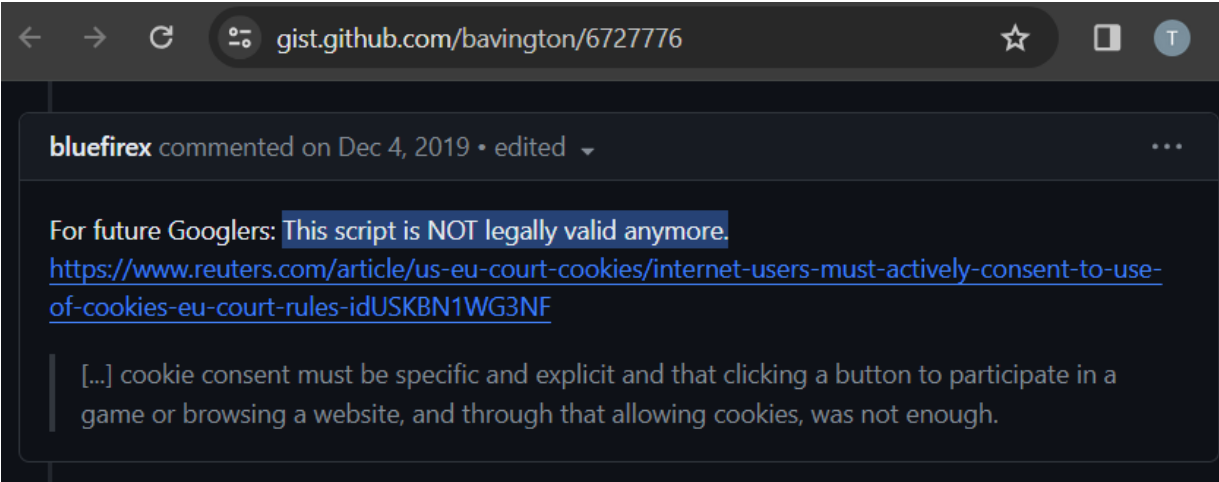


# Datenschutz: Fragwürdiges Cookie Banner

🕒 Suche nach der JavaScript-Datei – **zahlreiche Hinweise auf „Non-Compliance“**



The screenshot shows a browser window with the URL `create.co.uk/blog/js/js-eu-cookie-law-banner`. The page header includes the 'create' logo and navigation links for 'ABOUT', 'CASE STUDIES', 'PRODUCTS', 'RESOURCES', 'CONTACT US', and 'MY ACCOUNT'. The main content area shows a post with 8 likes and a 'Share' button. The post is by 'Nick', dated '5 years ago'. The title of the post is **!! THIS BANNER IS NOT COMPLIANT !!**. The text of the post reads: 'Impliant. Is no longer going to be compliant. There are several reasons for this. Mainly it's because GDPR requires the user to make an 'affirmative action' to signal their consent. If someone clicks a link, then the banner disappears. This allows the user to say, "but I didn't see the banner and I didn't provide my consent".' At the bottom of the post, there are icons for 'Like' (0), 'Comment' (0), 'Reply', and 'Share'.



The screenshot shows a browser window with the URL `gist.github.com/bavington/6727776`. It displays a comment by 'bluefirex' from December 4, 2019. The comment text is: 'For future Googlers: This script is NOT legally valid anymore. <https://www.reuters.com/article/us-eu-court-cookies/internet-users-must-actively-consent-to-use-of-cookies-eu-court-rules-idUSKBN1WG3NF> [...] cookie consent must be specific and explicit and that clicking a button to participate in a game or browsing a website, and through that allowing cookies, was not enough.'

# Security: Kontaktformular fragt nach „Sperrnummer“

https://kuno-sperrdienst.de/Home/Contact

**KUNO** Eine Initiative von:  
Karten Sperrdienst für  
SEPA-Lastschriftzahlungen

**EHI** Retail Institute®

HDE  
Handelsverband  
Deutschland

Wir wollen  
Eins  
Sicher leben.  
Ihre Polizei

HOME ÜBER KUNO FAQ **KONTAKT** LOGIN

**Kontodaten**

Bankleitzahl:

Kontonummer:

Sperrbestätigungsnummer:

**Ihre Fragen, Kommentare, Anregungen \***

*Alle von Ihnen gemachten Angaben werden selbstverständlich vertraulich behandelt. Aus Sicherheitsgründen wird beim Absenden der Daten Ihre IP-Kennung protokolliert und für 3 Monate gespeichert.*

**ANFRAGE ABSENDEN**

# Sperrbestätigungsnummer? 🤔

Quelle: <https://www.hna.de/lokales/witzenhausen/ec-karte-weg-neues-sperrsystem-polizei-hessen-hilft-9554676.html>



The screenshot shows a news article from HNA. The browser address bar displays the URL: <https://www.hna.de/lokales/witzenhausen/ec-karte-weg-neues-sperrsystem-polizei-hessen-hilft-9554676.html>. The HNA logo is in the top left, and navigation links for 'UKRAINE-KRIEG', 'KASSEL', 'LOKALES', 'WELT', and 'VERBRAUCHER' are in the top right. The main image shows a police officer in a blue uniform with a name tag 'HENNEMUTH' pointing at a computer monitor. The monitor displays a web form with a green header. Another person is visible in the background.

Das ist „Kuno“: Ulrich Hennemuth zeigt die Sperrmeldung, die ausgefüllt werden muss, um dann die gestohlene oder verlorene Girokarte per Computer schnell sperren zu können. Hinten schaut Ermittlungsgruppenleiter Jürgen Heldmann zu. © Forbert

# Sperrbestätigungsnummer? 🤔

A screenshot of a blue login form titled "Zum persönlichen Login". The text reads: "Melden Sie sich an um Ihre Kartenfolgenummer nachzumelden, den Status Ihrer Sperrung einzusehen oder die Sperrung aufzuheben." The phrase "Sperrung aufzuheben." is highlighted with a red box. Below this, there are two radio buttons: "Kontonr./BLZ" (unselected) and "IBAN" (selected). Under "IBAN:", there is a white input field. Below that, the text "Sperrbestätigungsnummer (5-stellig):" is followed by another white input field. At the bottom, there is a white button labeled "ANMELDUNG".

Self-Service / Login bei KUNO:

- 1.) IBAN (steht auf nahezu jeder Girocard)
- 2.) Sperrbestätigungsnummer (5-stellig)



Die haben doch bestimmt Rate-Limits, oder? 😐

POST /Home/displayLogin HTTP/2

Host: www.kuno-sperrdienst.de

[...]

\_\_RequestVerificationToken=zEEY0\_okO0jV[...]mookW7INGdon8e-

ZuX03i0J7S7kWDXglH0gX6jdpEPe0TrxNrwxI-

\_pxGchznb5blUywDP\_uzp1n3XXQE28V-eBZok1

&I\_B\_A\_N=DEXXXXXXXXXXX

&SpeBesNum=11111

&btnSubmit\_IBAN=Anmeldung

# Die haben doch bestimmt Rate-Limits, oder? 🤔

**ⓘ Payload positions**  
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:   Update Host header to match target

```
1 POST /Home/DisplayLogin HTTP/2
2 Host: kuno-spendienst.de
3 Cookie: __RequestVerificationToken= v3jIq_huIfEAP2oiHEEALYtScv...1GadcljyEun0R173hKehou811370cpms8T1027eKy04ii ARBAffinity=
4e280882c12ad112bb0c43944c5907841ba6dd5719cc5ah1d00b88a26c4e1i ARBAffinitySameSite=Hs2908697c12ad112bb0c...add5719cc5ah1d00b88a26c4e1i
4 Content-Length: 207
5 Cache-Control: max-age=0
6 Sec-Ch-Ua:
7 Sec-Ch-Ua-Mobile: ?
8 Sec-Ch-Ua-Platform: ""
9 Upgrade-Insecure-Requests: 1
10 Origin: https://kuno-spendienst.de
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5948.141 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referrer: https://kuno-spendienst.de/
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 __RequestVerificationToken=SCWCEK9R177Wu0RnTcJ0f_bSeG1.../TqW_qYhSEv0880DAGu1E3:So11E8hg-yfy-y_w7L091Thic2Dq1A1_B_A_H=DE1...14SpDea3hu=8...A
    btnSubmit_IBAN=Anax10uvy
```



# Die haben doch bestimmt Rate-Limits, oder? 😐

**Payload positions**  
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:   Update Host header to match target

```
1 POST /Home/DisplayLogin HTTP/2
2 Host: kuno-sperddienst.de
3 Cookie: __RequestVerificationToken=vs3Iq_huJ
4   0e250882c12ed112bb0c43044c5902841ba6dd5719cc
5 Content-Length: 207
6 Cache-Control: max-age=0
7 Sec-Ch-Ua:
8 Sec-Ch-Ua-Mobile: ?0
9 Sec-Ch-Ua-Platform: ""
10 Upgrade-Insecure-Requests: 1
11 Origin: https://kuno-sperddienst.de
12 Content-Type: application/x-www-form-urlencoded
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win
14   10; rv:109.0) Gecko/20100101 Firefox/109.0
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Referer: https://kuno-sperddienst.de/
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 __RequestVerificationToken=SCWCEjyRl17xWu0TR
   dt0Subst_IDAN=Amx1d0uyg
```

Attack Save Columns 3. Intruder attack of https://kuno-sperddienst.de

Results Positions Payloads Resource pool Settings

Filter: Showing all items

| Request | Payload | Status code | Error                    | Timeout                  | Length | Comment |
|---------|---------|-------------|--------------------------|--------------------------|--------|---------|
| 526     | 90525   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 527     | 90526   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 528     | 90527   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 529     | 90528   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 530     | 90529   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 531     | 90530   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 532     | 90531   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 533     | 90532   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 534     | 90533   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 535     | 90534   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 536     | 90535   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 537     | 90536   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 538     | 90537   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 539     | 90538   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 540     | 90539   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 541     | 90540   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 542     | 90541   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 543     | 90542   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |
| 544     | 90543   | 302         | <input type="checkbox"/> | <input type="checkbox"/> | 792    |         |

3. Intruder attack of https://www.kuno-sperddienst.de

Sniper attack, numbers. 1 payload position

26790 requests (0 errors)

26% complete View details >>

# Die haben doch bestimmt Rate-Limits, oder? 😐

**Payload positions**  
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:   Update Host header to match target

1 POST /Home/displayLogin HTTP/2  
2 Host: kuno-sperddienst.de  
3 Cookie: \_\_RequestVerificationToken=vs3Iq\_hub  
4 Content-Length: 207  
5 Cache-Control: max-age=0  
6 Sec-Ch-Ua:  
7 Sec-Ch-Ua-Mobile: ?0  
8 Sec-Ch-Ua-Platform: ""  
9 Upgrade-Insecure-Requests: 1  
10 Origin: https://kuno-sperddienst.de  
11 Content-Type: application/x-www-form-urlencoded  
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win  
13 Accept: text/html,application/xhtml+xml,  
14 Sec-Fetch-Site: same-origin  
15 Sec-Fetch-Mode: navigate  
16 Sec-Fetch-User: ?1  
17 Sec-Fetch-Dest: document  
18 Referrer: https://kuno-sperddienst.de/  
19 Accept-Encoding: gzip, deflate  
20 Accept-Language: en-US,en;q=0.9  
21  
22 \_\_RequestVerificationToken=SCWCEKqR17xWuDR  
btnSubmit\_IBAH=Amx10uy

Attack Save Columns 3. intruder attack of https://kuno-sperddienst.de

Results Positions Payloads Resource pool Settings

Filter: Showing all items

| Request | Request | Payload | Status code | Error | Timeout | Length | Comment |
|---------|---------|---------|-------------|-------|---------|--------|---------|
| 526     | 90525   |         |             |       |         |        |         |
| 527     | 90526   |         |             |       |         |        |         |
| 528     | 90527   | 94024   | 94025       | 302   |         | 800    |         |
| 529     | 90528   | 94025   | 94024       | 302   |         | 800    |         |
| 530     | 90529   | 94026   | 94025       | 302   |         | 800    |         |
| 531     | 90530   | 94027   | 94026       | 302   |         | 800    |         |
| 532     | 90531   | 94028   | 94027       | 302   |         | 800    |         |
| 533     | 90532   | 94029   | 94028       | 302   |         | 800    |         |
| 534     | 90533   | 94030   | 94029       | 302   |         | 800    |         |
| 535     | 90534   | 94031   | 94030       | 302   |         | 800    |         |
| 536     | 90535   | 94032   | 94031       | 302   |         | 800    |         |
| 537     | 90536   | 94033   | 94032       | 302   |         | 780    |         |
| 538     | 90537   | 94034   | 94033       | 302   |         | 800    |         |
| 539     | 90538   | 94035   | 94034       | 302   |         | 800    |         |
| 540     | 90539   | 94036   | 94035       | 302   |         | 800    |         |
| 541     | 90540   |         |             |       |         |        |         |
| 542     | 90541   |         |             |       |         |        |         |
| 543     | 90542   |         |             |       |         |        |         |
| 544     | 90543   |         |             |       |         |        |         |



# Bereit für den Login ... 😊

## Self-Service / Login bei KUNO:



1.) IBAN (steht auf nahezu jeder Girocard)



2.) Sperrbestätigungsnummer (5-stellig)

A screenshot of a mobile login form for KUNO. The form has a blue header with a lock icon and the text 'Zum persönlichen Login'. Below the header, there is a paragraph of text: 'Melden Sie sich an um Ihre Kartenfolgenummer nachzumelden, den Status Ihrer Sperrung einzusehen oder die Sperrung aufzuheben.' There are two radio buttons: 'Kontnr./BLZ' (unselected) and 'IBAN' (selected). Below the radio buttons, there are two input fields: 'IBAN:' and 'Sperrbestätigungsnummer (5-stellig):'. At the bottom of the form is a button labeled 'ANMELDUNG'.

# Hinter dem Login ...



Eine Initiative von:



## Meine Übersicht (1 aktive Sperrmeldung)



### KUNO-Sperrung anzeigen / aufheben

Meldeart: Sperrmeldung (Kontensperre)  
Empfangszeitpunkt: 2023 4 Uhr

Sie können hier Ihre KUNO-Sperrung aufheben, so dass Sie Konto (exklusive separater Kartensperren) wieder in vollem Umfang nutzen können.

Grund der Entsperrung:

Bitte wählen ...

Hiermit bestätige ich ausdrücklich, dass es sich bei den obenstehenden Informationen um meine Kontodaten handelt und ich die eingetragene KUNO Sperrmeldung löschen möchte.

SPERRMELDUNG LÖSCHEN



### Kartenfolgenummer nachmelden

Damit Ihre Karte dauerhaft gesperrt werden kann, und Sie auch vor unbefugter Nutzung Ihrer Karte per Unterschrift geschützt sind, ist es erforderlich, dass Sie uns die Kartenfolgenummer Ihrer zu sperrenden Karte übermitteln. Bitte geben Sie diese daher nachfolgend an:

Kartenfolgenummer (1-stellig):

Hiermit bestätige ich ausdrücklich, dass es sich bei den obenstehenden Informationen um meine Kontodaten handelt und ich die eingetragene Kartenfolgenummer nachmelden möchte.

BESTÄTIGEN




# Hinter dem Login ...

https://www.kuno-sperredienst.de/Private/StatusSummary

**KUNO** Eine Initiative von:


LOGOUT


Bitte wählen ...

- fehlerhafte KUNO Meldung, Kontonummer falsch
- fehlerhafte KUNO Meldung, Bankleitzahl falsch
- fehlerhafte KUNO Meldung, Kartenfolgenummer falsch
- fehlerhafte KUNO Meldung, Verwendung der Kartennummer statt Kartenfolgenummer
- Wiedererlangung der ec-Karte nach Diebstahl** 
- Wiedererlangung der ec-Karte nach Verlegung
- Wiedererlangung der ec-Karte nach sonstiger Rückmeldung Kontoinhaber
- Wiedererlangung der ec-Karte nach sonstiger Rückmeldung Polizeibehörden
- Probleme bei Verwendung der Nachfolgekarte (evtl. gleiche Kartenfolgenummer)
- Zerstörung der Karte nach Diebstahl durch Automateinzug (PIN Sperre durch Täter)

uch vor  
sind,  
er zu

idelt  
:n

Bitte wählen ... 

SPERMELDUNG LÖSCHEN 

BESTÄTIGEN





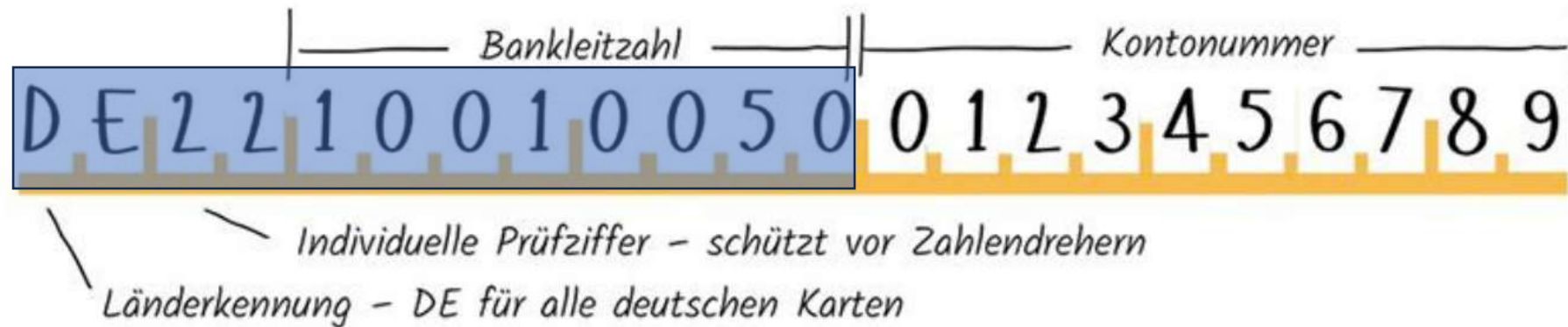
Damit wäre SEPA-Lastschrift für dieses  
Konto/Karte **unlocked\***



\* Rollout der Sperr-Datei in der Regel nach 24 Stunden oder früher ...

# Ausweitung denkbar ...

Statt „nur“ Brute force auf Sperrbestätigungsnummer ...  
auch Brute force der IBAN (maximal 100.000 Requests notwendig)



ISO 13616-1:2020 sieht u.a. 34-stellige IBANs vor  
Deutschland: 22-stellige IBANs



# Vorgehen zur Entsperrung aller Karten ...

| Versuchsnummer | IBAN (abgetrennte BLZ und Kontonummer) | Sperrbestätigungsnummer |
|----------------|--|-------------------------|
| 1              | DE94   10050000   6600046463           | 00000                   |
| 2              | DE94   10050000   6600046463           | 00001                   |
| 3              | DE94   10050000   6600046463           | 00002                   |
| [...]          | DE94   10050000   6600046463           | [...]                   |
| 100.000        | DE94   10050000   6600046463           | 99999                   |
| 100.001        | DE94   10050000   6600046464           | 00000                   |
| 100.002        | DE94   10050000   6600046464           | 00001                   |
| 100.003        | DE94   10050000   6600046464           | 00002                   |
| [...]          | DE94   10050000   6600046464           | [...]                   |
| 200.000        | DE94   10050000   6600046464           | 99999                   |
| 200.001        | DE94   10050000   6600046465           | 00000                   |
| 200.002        | DE94   10050000   6600046465           | 00001                   |
| [...]          | [...]                                  | [...]                   |

Das Vorgehen ist eher theoretisch und würde für alle IBANs in Deutschland mehrere Wochen dauern.

# Kosten für einen „KUNO-Check“

| D: ERWEITERUNGSMÖGLICHKEITEN   |                            |                    |
|--|----------------------------|--------------------|
| Risikomanagement   | Abrechnung                 | Preis              |
| Risikomanagement zur Zahlungsausfall-Minimierung   | Einrichtung:<br>Monatlich: | 99,00 €<br>19,00 € |
| Bankaccount Check – Plausibilitätsprüfung der Kontoverbindung (separater Aufruf)               | Je Vorgang:                | 0,05 €             |
| NCA Check (Non Consumer Account) – Prüfung gegen öffentliche Bankverbindungen inkl. KUNO-Liste | Je Vorgang:                | 0,05 €             |
| POS Sperrdatei – Abgleich mit Sperrliste aus dem stationären Handel inkl. KUNO-Liste           | Je Vorgang:                | 0,09 €             |
| Address Check Basic – Adressprüfung auf Existenz in 20 Ländern                                 | Je Vorgang:                | 0,15 €             |
| Address Check Person – Namens- und Adressprüfung auf Postzustellbarkeit (nur DE)               | Je Vorgang:                | 0,19 €             |
| infoscore Bonitätsprüfung Basic nur harte Merkmale (Schuldnerverzeichnis, Insolvenzen etc.)    | Je Vorgang:                | 0,45 €             |
| infoscore Bonitätsprüfung Professional alle Merkmale (harte Merkmale + Merkmale aus Inkasso)   | Je Vorgang:                | 0,85 €             |

| Rechnungsstellung  | Abrechnung                 | Preis               |
|--|----------------------------|---------------------|
| Automatisierte Rechnungsstellung per E-Mail oder Post  | Einrichtung:<br>Monatlich: | 199,00 €<br>29,00 € |
| Generieren von Rechnungs- und/oder Gutschriftsbelegen**  | Je Vorgang:                | 0,19 €              |
| Versand von Rechnungs- und/oder Gutschriftsbelegen per E-Mail  |                            | kostenlos           |
| Versand von Rechnungs- und/oder Gutschriftsbelegen per Post (einseitig, s/w, Deutschland, zzgl. Porto)   | Je Vorgang:                | 0,44 €              |
| Versand von Rechnungs- und/oder Gutschriftsbelegen per Post (einseitig, Farbe, Deutschland, zzgl. Porto)   | Je Vorgang:                | 1,40 €              |
| Versand von Rechnungs- und/oder Gutschriftsbelegen über kundeneigenen Mailserver via SMTP  | Einrichtung:<br>Monatlich: | 99,00 €<br>19,00 €  |
| Standard Rechnungs- und/oder Gutschriftstemplate   |                            | kostenlos           |
| Zusätzliches Standard Rechnungs- und/oder Gutschriftstemplate; Auf Händler-Briefpapier basierendes und für einen weiteren Vertriebskanal nutzbares Standard-Template | Einrichtung:<br>Monatlich: | 49,00 €<br>10,00 €  |
| Forderungsmanagement   | Abrechnung                 | Preis               |

Quelle: Payone Preis-/Leistungsverzeichnis (Zugriff: 20.12.2023)

[https://media3.payone.com/f/64176/x/5c33c0e5ba/preis-leistungsverzeichnis-e-com\\_de.pdf](https://media3.payone.com/f/64176/x/5c33c0e5ba/preis-leistungsverzeichnis-e-com_de.pdf)

# Kosten für einen „KUNO-Check“

| D: ERWEITERUNGSMÖGLICHKEITEN  |                            |                    | Rechnungsstellung  | Abrechnung                 | Preis               |
|---|----------------------------|--------------------|--|----------------------------|---------------------|
| Risikomanagement  | Abrechnung                 | Preis              | Automatisierte Rechnungsstellung per E-Mail oder Post  | Einrichtung:<br>Monatlich: | 199,00 €<br>29,00 € |
| Risikomanagement zur Zahlungsausfall-Minimierung  | Einrichtung:<br>Monatlich: | 99,00 €<br>19,00 € | Generieren von Rechnungs- und/oder Gutschriftsbelegen**  | Je Vorgang:                | 0,19 €              |
| Bankaccount Check – Plausibilitätsprüfung der   | Je Vorgang:                | 0,05 €             |  |                            |                     |
| <b>NCA Check (Non Consumer Account) – Prüfung gegen öffentliche Bankverbindungen inkl. KUNO-Liste</b> |                            |                    | Je Vorgang:  |                            | <b>0,05 €</b>       |
| <b>POS Sperrdatei – Abgleich mit Sperrliste aus dem stationären Handel inkl. KUNO-Liste</b>           |                            |                    | Je Vorgang:  |                            | <b>0,09 €</b>       |
| mit harten Merkmalen (Schuldnerverzeichnis, Insolvenzen etc.)   |                            |                    | Zusätzliches Standard Rechnungs- und/oder Gutschriftstemplate; Auf Händler-Briefpapier basierendes und für einen weiteren Vertriebskanal nutzbares Standard-Template | Einrichtung:<br>Monatlich: | 49,00 €<br>10,00 €  |
| infoscore Bonitätsprüfung Professional alle Merkmale (harte Merkmale + Merkmale aus Inkasso)          | Je Vorgang:                | 0,85 €             |  |                            |                     |
|   |                            |                    | Forderungsmanagement   | Abrechnung                 | Preis               |

Quelle: Payone Preis-/Leistungsverzeichnis (Zugriff: 20.12.2023)

[https://media3.payone.com/f/64176/x/5c33c0e5ba/preis-leistungsverzeichnis-e-com\\_de.pdf](https://media3.payone.com/f/64176/x/5c33c0e5ba/preis-leistungsverzeichnis-e-com_de.pdf)



# Datenschutzbestimmungen KUNO-Sperrsystem

alt (< November 2023)

## Informationen zum Datenschutz

Das EHI möchte Ihre personenbezogenen Daten schützen. Personenbezogene Daten sind alle Daten, die in Zusammenhang mit Ihrem Namen gespeichert sind. Mit der Anzeige bei der Polizei und der Meldung an die KUNO-Plattform erhalten wir lediglich die Informationen zu Ihrer Kontoverbindung inkl. Kartenfolgenummer. Weitere personenbezogene Daten, wie Name oder Adresse, werden nicht gespeichert.

Das EHI nutzt Ihre Daten ausschließlich, um diese an die an KUNO angeschlossenen (Handels-) Unternehmen weiterzuleiten. In diesem Zusammenhang werden auch Ihre Zugriffe auf die KUNO-Plattform protokolliert und Ihre Kontodaten in einer Datenbank über einen klar definierten Zeitraum abgespeichert. Die Kommunikation zwischen der Polizei und der KUNO-Plattform sowie zwischen der KUNO-Plattform und den angeschlossenen Händlern verläuft dabei signiert und verschlüsselt.

Das EHI verkauft Ihre personenbezogenen Daten nicht an Dritte.

## Datenschutzerklärung

neu (> Dezember 2023)

## Informationen zum Datenschutz

Das EHI möchte Ihre personenbezogenen Daten schützen. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen (Art. 4 Nr. 1 DSGVO). Mit der Anzeige bei der Polizei und der Meldung an die KUNO-Plattform erhalten wir die Informationen zu Ihrer Kontoverbindung inkl. Kartenfolgenummer. Weitere personenbezogene Daten, wie Name oder Adresse, werden nicht gespeichert.

Das EHI nutzt Ihre Daten ausschließlich, um diese an die an KUNO angeschlossenen (Handels-) Unternehmen weiterzuleiten. In diesem Zusammenhang werden auch Ihre Zugriffe auf die KUNO-Plattform protokolliert und Ihre Kontodaten in einer Datenbank über einen klar definierten Zeitraum abgespeichert. Die Kommunikation zwischen der Polizei und der KUNO-Plattform sowie zwischen der KUNO-Plattform und den angeschlossenen Händlern verläuft dabei signiert und verschlüsselt.

## Datenschutzhinweise

# Datenschutzbestimmungen KUNO-Sperrsystem

alt (< November 2023)

## Informationen zum Datenschutz

Das EHI möchte Ihre personenbezogenen Daten schützen. Personenbezogene Daten sind alle Daten, die in Zusammenhang mit Ihrem Namen gespeichert sind. Mit der Anzeige bei der Polizei und der Meldung an die KUNO-Plattform erhalten wir lediglich die Informationen zu Ihrer Kontoverbindung inkl. Kartenfolgenummer. Weitere personenbezogene Daten, wie Name oder Adresse, werden nicht gespeichert.

Das EHI nutzt Ihre Daten ausschließlich, um diese an die an KUNO angeschlossenen (Handels-) Unternehmen weiterzuleiten. In diesem Zusammenhang werden auch Ihre Zugriffe auf die KUNO-Plattform protokolliert und Ihre Kontodaten in einer Datenbank über einen klar definierten Zeitraum abgespeichert. Die Kommunikation zwischen der Polizei und der KUNO-Plattform sowie zwischen der KUNO-Plattform und den angeschlossenen Händlern verläuft dabei signiert und verschlüsselt.

Das EHI verkauft Ihre personenbezogenen Daten nicht an Dritte.

## Datenschutzerklärung

neu (> Dezember 2023)

## Informationen zum Datenschutz

Das EHI möchte Ihre personenbezogenen Daten schützen. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen (Art. 4 Nr. 1 DSGVO). Mit der Anzeige bei der Polizei und der Meldung an die KUNO-Plattform erhalten wir die Informationen zu Ihrer Kontoverbindung inkl. Kartenfolgenummer. Weitere personenbezogene Daten, wie Name oder Adresse, werden nicht gespeichert.

Das EHI nutzt Ihre Daten ausschließlich, um diese an die an KUNO angeschlossenen (Handels-) Unternehmen weiterzuleiten. In diesem Zusammenhang werden auch Ihre Zugriffe auf die KUNO-Plattform protokolliert und Ihre Kontodaten in einer Datenbank über einen klar definierten Zeitraum abgespeichert. Die Kommunikation zwischen der Polizei und der KUNO-Plattform sowie zwischen der KUNO-Plattform und den angeschlossenen Händlern verläuft dabei signiert und verschlüsselt.

## Datenschutzhinweise

# Kein Verkauf von Daten? 🤔

## Datenschutzerklärung

Das EHI verkauft Ihre personenbezogenen Daten nicht an Dritte.

Ansonsten erfolgt keine Weitergabe und kein Verkauf Ihrer personenbezogenen Daten an Dritte. Das EHI trifft bestmögliche Vorkehrungen für die Sicherheit Ihrer Daten.

## Händler FAQ

### 4. Was kostet mich die KUNO-Anbindung als Händler? ^

Bei einem jährlichen Außenumsatz von bis zu 75 Mio. Euro berechnen wir für Ihre Teilnahme eine **feste Jahrespauschale von 120,00 Euro netto**. Bei einem höheren Außenumsatz verwenden wir einen Kostenumlageschlüssel, der jährlich neu kalkuliert wird. Genauere Informationen hierzu können Sie über unser Kontaktformular anfordern.

VS.

# Auszug aus dem KUNO FAQ für Händler

## 2. Nutze ich KUNO vielleicht bereits? ^

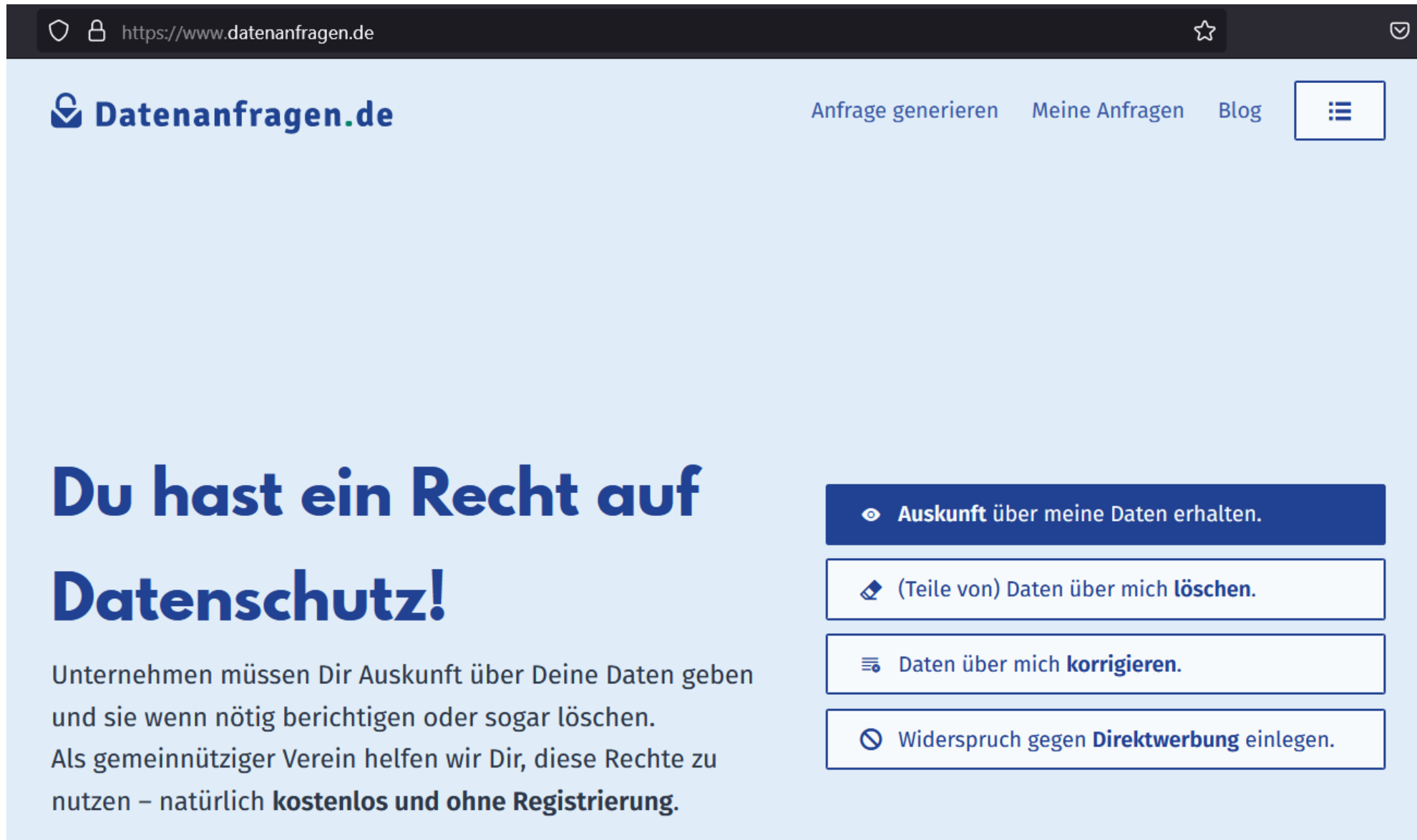
Die unten aufgeführten Netzbetreiber/Finanzdienstleister haben sich bereits der zentralen Meldestelle des EHI angeschlossen und gleichen somit ihre Zahlungstransaktionen mit KUNO-Daten ab. Wenn Sie Kunde der hier aufgeführten Dienstleister sind, brauchen Sie sich nicht mehr separat beim EHI als Empfänger registrieren, dies hat dann bereits der Dienstleister übernommen.

- Real inform GmbH
- AFC Rechenzentrum GmbH
- arvato infoscore Consumer Data GmbH
- Ingenico Payment Services GmbH
- HIT Hanseatische Inkasso-Treuhand GmbH
- Hobex AG
- ICP GmbH
- InterCard AG
- montada GmbH





Viele bieten auch „Bonitätsprüfungen“ an



# Artikel 15 DSGVO: Recht auf Auskunft



The screenshot shows the website <https://www.datenanfragen.de>. The page features a navigation bar with the site logo, a search bar, and links for 'Anfrage generieren', 'Meine Anfragen', and 'Blog'. The main content area is titled 'Du hast ein Recht auf Datenschutz!' and explains that companies must provide access to their data. A list of rights is shown in a sidebar:

-  **Auskunft** über meine Daten erhalten.
-  (Teile von) Daten über mich **löschen**.
-  Daten über mich **korrigieren**.
-  Widerspruch gegen **Direktwerbung** einlegen.

Guten Tag,  
ich bitte hiermit um Auskunft gemäß Art. 15 DSGVO. Bitte bestätigen Sie mir, ob Sie mich betreffende personenbezogene Daten verarbeiten (vgl. Art. 4 Nr. 1 und 2 DSGVO).

Falls dem so sein sollte, stellen Sie mir bitte im Sinne des Art. 15 Abs. 3 DSGVO eine Kopie sämtlicher personenbezogener Daten, die Sie zu meiner Person verarbeiten, einschließlich eventueller mich betreffender pseudonymisierter Daten im Sinne des Art. 4 Nr. 5 DSGVO, zur Verfügung. Weiterhin bitte ich Sie in diesem Fall im Sinne des Art. 15 Abs. 1 DSGVO um Auskunft über:

1. die Verarbeitungszwecke;
2. die Kategorien personenbezogener Daten, die verarbeitet werden;
3. die Empfänger und Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden;
4. falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
5. wenn die personenbezogenen Daten nicht bei mir erhoben wurden, alle verfügbaren Informationen über die Herkunft der Daten;
6. falls zutreffend, das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – sofern gegeben – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für meine Person.

Falls Sie mich betreffende anonymisierte Daten verarbeiten, bitte ich Sie darum, mir das nicht nur mitzuteilen, sondern auch das verwendete Verfahren verständlich zu erläutern.

Sofern Sie meine personenbezogenen Daten an ein Drittland oder an eine internationale Organisation übermitteln, bitte ich über die geeigneten Garantien gemäß Art. 46 DSGVO im Zusammenhang mit der Übermittlung unterrichtet zu werden.

Meine Anfrage schließt explizit auch sämtliche weiteren Angebote und Unternehmen ein, für die Sie Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO sind.

Die Auskunft ist nach Art. 12 Abs. 3 DSGVO unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang der Anfrage zu erteilen. Sie hat nach Art. 15 Abs. 3 DSGVO kostenlos zu erfolgen.

Guten Tag,  
ich bitte hiermit um Auskunft gemäß Art. 15 DSGVO. Bitte bestätigen Sie mir, ob Sie mich betreffende personenbezogene Daten verarbeiten (vgl. Art. 4 Nr. 1 und 2 DSGVO).

Falls dem so sein sollte, stellen Sie mir bitte im Sinne des Art. 15 Abs. 3 DSGVO eine Kopie sämtlicher personenbezogener Daten, die Sie zu meiner Person verarbeiten, einschließlich eventueller mich betreffender pseudonymisierter Daten im Sinne des Art. 4 Nr. 5 DSGVO, zur Verfügung. Weiterhin bitte ich Sie in diesem Fall im Sinne des Art. 15 Abs. 3 DSGVO folgende Informationen zu offenlegen:

1. die Verarbeitungszwecke
2. die Kategorien personenbezogener Daten, die verarbeitet werden
3. die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt werden, wenn eine Offenlegung nicht erforderlich ist
4. falls möglich, die geplante Dauer der Speicherung der Daten, andernfalls die Kriterien für die Dauer der Speicherung
5. wenn die Daten nicht von Ihnen stammen, die Herkunft der Daten, wer die Daten ursprünglich erhebt und wie die Daten von Ihnen in Verbindung mit den Daten anderer Personen gebracht werden
6. falls zutreffend, die Weitergabe der Daten an Dritte

Falls Sie mich kontaktieren, bitte ich Sie, dies nicht zu tun, wenn Sie dies nicht wünschen.

Sofern Sie mich kontaktieren, bitte ich Sie, dies nicht zu tun, wenn Sie dies nicht wünschen. Übermittlung unternehmensspezifischer Informationen ist zulässig.

Meine Anfrage schließt explizit auch sämtliche weiteren Angebote und Unternehmen ein, für die Sie Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO sind.

Die Auskunft ist nach Art. 12 Abs. 3 DSGVO unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang der Anfrage zu erteilen. Sie hat nach Art. 15 Abs. 3 DSGVO kostenlos zu erfolgen.

TL;DR

Welche Daten speichert ihr über mich?  
Wer hat meine Daten erhalten?

(Betroffenenrecht nach Artikel 15 DSGVO)

Daten  
der, falls dies  
tionen über die  
ling gemäß  
lvierte Logik  
e Person.  
ur mitzuteilen,  
sation  
s mit der

Reply Forward Archive Junk Delete More

From Datenschutz <datenschutz@ehi.org>

To Tim Philipp Schäfers (IT) <it@tim-philipp-schaefers.de>

12/15/2023, 12:02 PM

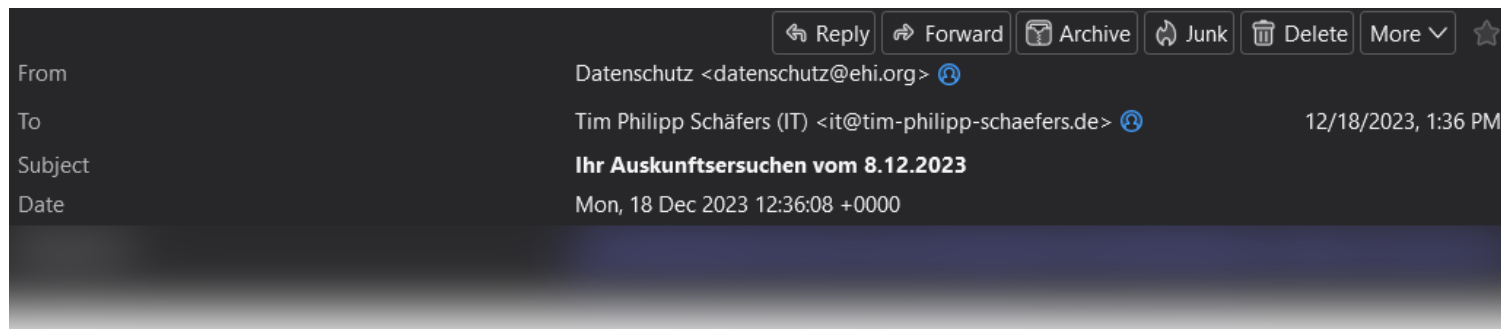
Subject **AW: AW: AW: DSGVO Anfrage gemäß Art. 15 DSGVO**

Date Fri, 15 Dec 2023 11:02:59 +0000

Guten Tag Herr Schäfers,

um sicherzustellen, dass Sie der berechnigte Kontoinhaber der von Ihnen angegebenen Kontodaten sind, müssten Sie uns einmal **zur Identifizierung die letzten zwei Ziffern Ihrer Sperrbestätigungsnummer mitteilen.**





Guten Tag Herr Schäfers,

mit Ihrem Auskunftersuchen vom 8.12.2023 haben Sie uns gebeten, Ihnen Auskunft darüber zu geben, welche personenbezogenen Daten wir von Ihnen zu welchem Zweck verarbeiten. Wie besprochen erhalten Sie die gewünschte Auskunft im Anhang als PDF.

Zu Ihren weiteren Fragen kann ich Ihnen folgende Antworten geben:

**Unternehmen können sich für eine Gebühr von 120,00€ im Jahr dem KUNO-Projekt anschließen.** Die Gebühr erfolgt aufgrund der technischen Umsetzung und den Kosten, die damit verbunden sind. Die Kontodaten werden ohne Namen an die angeschlossenen Handelsunternehmen bzw. deren Zahlungsdienstleister/ Netzwerkbetreiber weitergegeben, sodass Zahlungen mit den als gestohlen gemeldeten Karten beim Bezahlvorgang abgelehnt werden können. Der Zweck ist klar eingeschränkt und auf die Nutzung zur Kartensperrung begrenzt und vertraglich festgehalten.

Im Zuge Ihres Auskunftersuchens finden Sie die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind im Anhang. **Aus Sicherheitsgründen, um eine betrügerische Verwendung zu verhindern, können wir Privatpersonen nicht über die Namen der angeschlossenen Händler informieren.** Rechtsgrundlage der Datenverarbeitung ist unser berechtigtes Interesse an der Datensicherheit und dem Schutz vor betrügerischen Verwendungen und Missbrauch der Daten gemäß Art. 6 (1)(f) DSGVO.

Das EHI Retail Institute ist keine Behörde. Das EHI ist ein wissenschaftliches Institut des Handels mit rund 800 Mitgliedern und über 70 Jahre Erfahrung. Im Vordergrund steht der Austausch mit der Handelsbranche und eine praxisrelevante Forschung. Das KUNO-Projekt ist in Zusammenarbeit mit Polizeibehörden und Wirtschaft entstanden und soll ein einfaches, aber wirkungsvolles Sperrsystem darstellen, um Zahlungen per Debitkarte im elektronischen Lastschriftverfahren – also mit Unterschrift – sicherer zu gestalten. Der Name KUNO ist die Abkürzung für „Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationsstrukturen“.

> 1 attachment: Auskunft.pdf 55.1 KB

Save

Antwort auf die DSGVO Artikel 15 Anfrage:  
*Ja – wir haben deine Daten gespeichert und geben sie weiter (sinngemäß).*

*„Aus Sicherheitsgründen, um eine betrügerische Verwendung zu verhindern, können wir Privatpersonen nicht über die Namen der angeschlossenen Händler informieren.“*

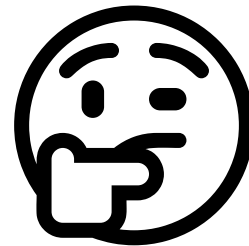
Datenschutz – EHI Retail Institute GmbH  
E-Mail vom 18.12.2023 - \ (ツ) / -



„Sicherheitsgründe“

vs.

Betroffenheitsrechte  
nach Artikel 15 DSGVO





Es gibt ggfs. noch mehr zu „entdecken“ 😊

## - Admin-Portal

The screenshot displays the KUNO website interface. At the top, the URL is <https://kuno-sperrdienst.de>. The header includes the KUNO logo, the text "Eine Initiative von:" followed by logos for EHI Retail Institute, HDE Handelsverband Deutschland, and another logo. Navigation links for HOME, ÜBER KUNO, FAQ, KONTAKT, and LOGIN are visible.

The main content area is divided into several sections:

- Left Section:** "Karte anzuzeigen, wenden Sie sich an Ihre nächstgelegene Polizeidienststelle." Below this, a blue box contains a bullet point: "■ Erbiten Sie dort zudem eine KUNO-Meldung und lassen Sie sich eine Sperrbestätigungsnummer und ein KUNO-Merkblatt aushändigen."
- Middle Section:** "erhalten Sie bei der Aktivierung einer KUNO-Sperre eine Sperrbestätigungsnummer von der Polizei ausgehändigt." Below this, another blue box contains a bullet point: "■ Mit dieser Nummer können Sie online Ihre Kartenfolgenummer nachmelden oder Ihre KUNO-Sperre löschen."
- Right Section:** "nachstehende Formular mit Ihren persönlichen Kontodaten sowie der individuellen Sperrbestätigungsnummer, welche Ihnen im Rahmen Ihrer Kartensperrung von der Polizei übergeben wurde aus."

On the right side, there is a registration form with the following fields:

- Radio buttons for "Kontanz./BLZ" (selected) and "IBAN".
- Text input for "Bankleitzahl:".
- Text input for "Kontonummer:".
- Text input for "Sperrbestätigungsnummer (5-stellig):".
- A button labeled "ANMELDUNG".

At the bottom, there is an "Adminbereich für KUNO-Mitarbeiter / Polizei" section with a login form:

- Fields for "Login:" and "Passwort:".
- A button labeled "ANMELDEN" with a lock icon.

Two large red arrows are overlaid on the image: one pointing down from the middle section to the login form, and another pointing left from the right side towards the login form.

Footer text includes "© EHI Retail Institute 2018 - 2023" and links for "Impressum" and "Datenschutz".

Es gibt ggfs. noch mehr zu „entdecken“ 😊

## - Admin-Portal

The screenshot shows the login page for the KUNO Admin-Portal. The browser address bar displays 'https://kuno-sperrdienst.de'. The page header includes the KUNO logo (Karten Sperrdienst für SEPA-Lastschriftzahlungen), the text 'Eine Initiative von:' followed by logos for EHI Retail Institute and HDE Handelsverband Deutschland, and navigation links for HOME, ÜBER KUNO, FAQ, KONTAKT, and LOGIN. The main content area is a grey box with the title 'Adminbereich für KUNO-Mitarbeiter / Polizei' and a user icon. Below the title are two input fields labeled 'Login:' and 'Passwort:'. A black button with the text 'ANMELDEN' and a lock icon is positioned at the bottom right of the login area. The footer contains the copyright notice '© EHI Retail Institute 2018 - 2023' and links for 'Impressum' and 'Datenschutz'.

- \\_ (ツ) \\_ / -

Es gibt ggfs. noch mehr zu „entdecken“ 😊

## - Übermittlung der Sperrdatei



The screenshot shows the top navigation bar of the KUNO website. The address bar displays the URL: <https://www.kuno-sperrdienst.de/Home/displayDataProtection>. Below the address bar, the KUNO logo is prominently displayed on the left, with the text "Karten Sperrdienst für SEPA-Lastschriftzahlungen" underneath. To the right of the KUNO logo, it says "Eine Initiative von:" followed by the logos of EHI Retail Institute, HDE Handelsverband Deutschland, and Ihre Polizei. On the far right of the navigation bar, there are three menu items: "HOME", "ÜBER KUNO", and "FAQ".

Die Kommunikation zwischen der Polizei und der KUNO-Plattform sowie zwischen der KUNO-Plattform und den angeschlossenen Händlern verläuft dabei **signiert und verschlüsselt**.

# Es gab zahlreiche weitere „Problemchen“

CVE-2016-10735, CVE-2018-14040, CVE-2018-14041, CVE-2018-14042,  
CVE-2019-8331, CVE-2019-11358, CVE-2020-11022, CVE-2020-11023,  
CVE-2020-23064, CVE-2021-21252, CVE-2021-43306, CVE-2022-31147

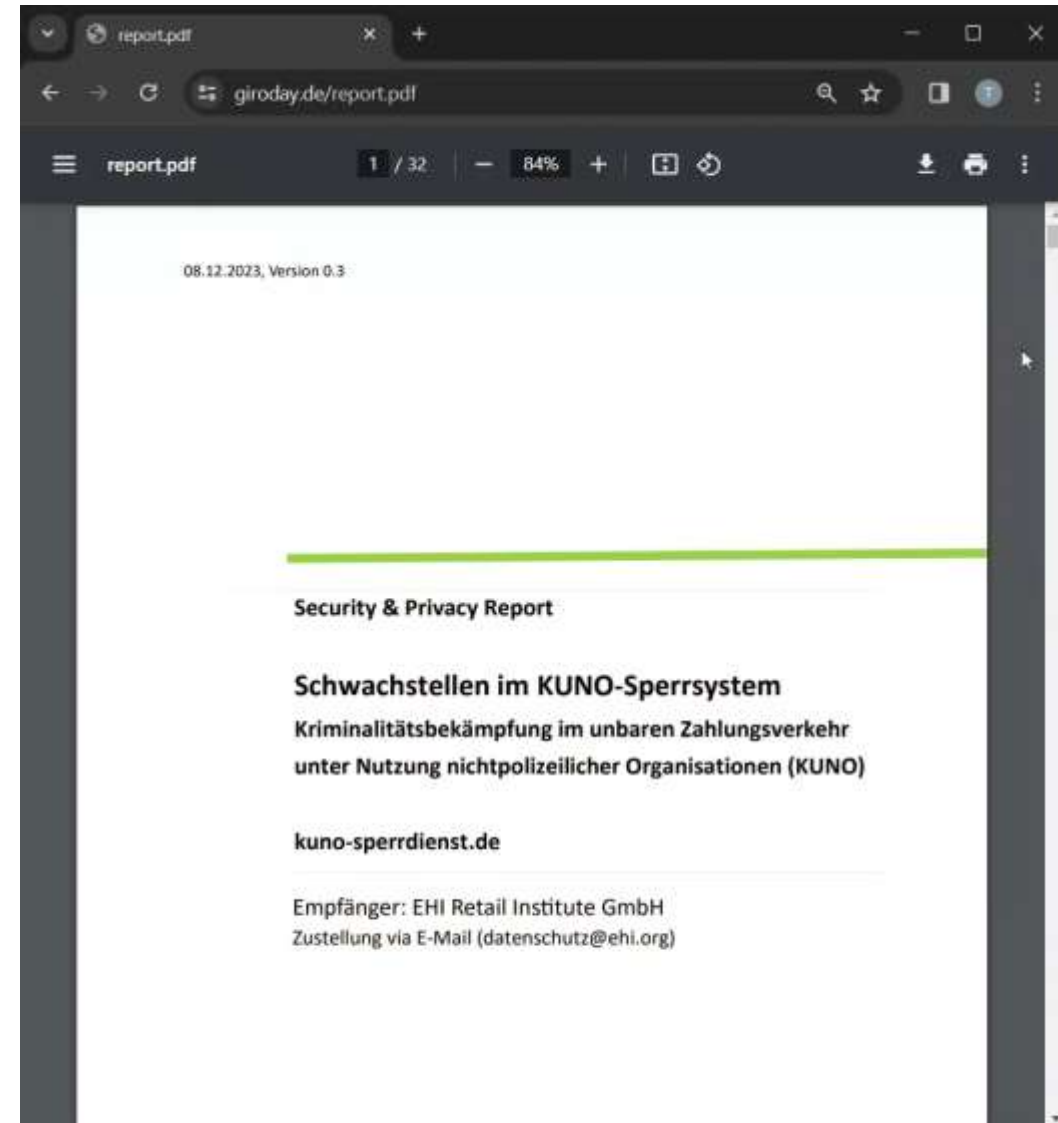
HTTP Server Header (inkl. Versionsnummern) exposed

Weitere Management Ports offen

HSTS-Header nicht in Benutzung

Weitere Herausforderungen im Bereich Datenschutz

...



Giroday != Zeroday

Danke an Rico, Niklas und Tim für den Support und die Idee zum Namen

# Herzlichen Dank ♥



- Professioneller Umgang mit der Meldung
- Schnelle Schließung der (meisten) Lücken
- Grundsätzlich funktionierendes Sperrsystem



# Funfact 😊

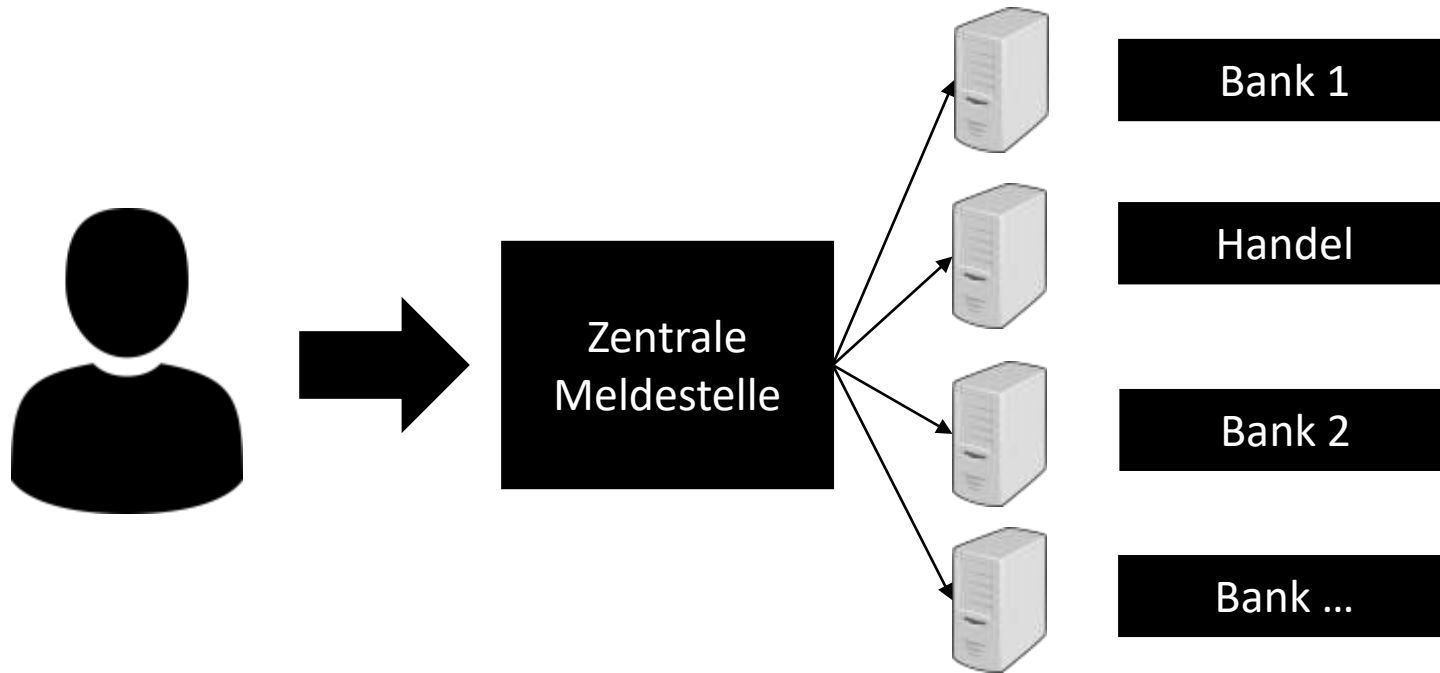
Buchungen werden folgendermaßen vermerkt:

ELV68197325 26.04 18.07 ME0  
EC 68197325 260410180710OC0

Zahlungsart, Terminal-ID, Datum, Uhrzeit, Autorisierung  
Kartenfolgenummer

➔ Wenn man >10x die Karte verliert, dann sind alle Kombinationen gesperrt 😊

# Vision / Forderungen



- Eine zentrale Sperrstelle für alle Zahlarten
- Transparent & nachvollziehbar (Open-Source)
- Finanzierung nachvollziehbar
- „Sicher“ und auditierbar

# Call to Action

- Informiert andere, damit ALLE Methoden gesperrt werden ...
- Lasst uns gemeinsam daran arbeiten, dass Sperrungen mittelfristig besser durchgeführt werden können.
- Ein paar Wikipedia Artikel bräuchten mal ein Update 😊
- Nutzt Zugriffe auf Systeme, um diese zu verbessern ...

# Vielen Dank!



Quelle: Fnord Show 30c3

# Herzlichen Dank!

Falls es Fragen gibt oder jemand meine Karte findet 😊

[it@tim-philipp-schaefers.de](mailto:it@tim-philipp-schaefers.de)

Weitere Infos & Folien:  
[giroday.de](http://giroday.de)