08.12.2023, Version 0.3

Security & Privacy Report

Schwachstellen im KUNO-Sperrsystem

Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationen (KUNO)

kuno-sperrdienst.de

Empfänger: EHI Retail Institute GmbH
Zustellung via E-Mail (datenschutz@ehi.org)

Absender

Tim Philipp Schäfers

Dokumentenversion

Version	Autor	Datum	Kommentar
0.1	Tim Philipp Schäfers	Ende Oktober	Initiale Version
0.2	Tim Philipp Schäfers	November	Funde hinzugefügt
0.3	Tim Philipp Schäfers	08.12.2023	Status zu Lücken ergänzt

Inhaltsverzeichnis

1. Einleitung / Zusammenfassung

Das EHI Retail Institute stellt in Kooperation mit der deutschen Polizei und dem Hauptverband des Deutschen Einzelhandels die Webapplikation KUNO[1] unter kuno-sperrdienst.de bereit. Die Applikation wird von Polizeibehörden verwendet, um bei Diebstahl oder Verlust einer Debitkarte Kontodaten in einer zentrale Sperrdatei einzupflegen. Diese Datei wird wiederum im Einzelhandel berücksichtigt und innerhalb von Abrechnungssystemen eingepflegt, sodass eine Abbuchung per Lastschrift nicht mehr möglich ist (wenn eine IBAN in der Datei als „gesperrt“ vorliegt). Dadurch wird ein Betrug mit geklauten Debitkarten eingedämmt[2].

In der Vergangenheit hat dies dazu geführt, dass der Betrug im unbaren Zahlungsverkehr abgenommen hat, teilweise war ein Rückgang von -28,8% pro Jahr zu verzeichnen[3]. Das entsprechende Sperrsystem wurde zunächst in Dresden 2001 eingeführt[4] und findet mittlerweile in ganz Deutschland Anwendung. Pro Jahr werden über 120.000 Sperrungen über KUNO abgewickelt (2016: 166.000 / laut Webseite: „über 10.000 Meldungen pro Monat“)[5] [6]. Die KUNO-Sperrdatei wird von 96% aller Händler in Deutschland direkt oder indirekt (durch Zahlungsabwickler) genutzt[7]. Neben der Nutzung durch Polizeibehörden und der Nutzung der Sperrdatei durch Unternehmen im Zahlungsbereich bzw. Einzelhandel gibt es auch einen Self-Service für Nutzende (Personen deren Karte gestohlen wurde) auf der Webseite. Unter den häufig gestellten Fragen auf der KUNO-Seite wird die Wirkung von KUNO äußerst positiv beschrieben, darüber hinaus gibt es positive Rückmeldungen aus der Politik und Presse:

„KUNO stellt ein simples, aber wirkungsvolles Sperrsystem dar […]“
Quelle: KUNO-Webseite https://www.kuno-sperrdienst.de/Home/displayAboutKuno (Abruf 22.10.2023)

„So können Sie geklaute EC-Karten effektiv sperren lassen“
Quelle: Handwerksblatt (2016) https://www.handwerksblatt.de/betriebsfuehrung/so-koennen-sie-geklaute-ec-karte-effektiv-sperren-lassen (Abruf 22.10.2023)

„[…] Es ist ein Beitrag zu mehr Sicherheit in unserem Land. Die erweiterte Kartensperre schützt Bürger und Handel vor Scheckkarten-Betrügern […]“
Quelle: Innenminister Jörg Schönbohm (Ministerium des Innern Brandenburg, 2003) https://www.brandenburg.de/cms/detail.php?id=66220 (Abruf 22.10.2023)

Im Rahmen einer Untersuchung konnte der IT-Sicherheitsexperte Tim Philipp Schäfers im Oktober 2023 feststellen, dass das KUNO-Sperrsystem kritische Sicherheitslücken und mögliche Datenschutzverstöße aufweist. **Eine der gefundenen Schwachstellen ermöglicht eine Freischaltung von gesperrten Karten in der KUNO-Sperrdatei, wodurch ein Zahlungsbetrug im unbaren Zahlungsverkehr – trotz vorheriger Sperre – erneut möglich wird.** Der folgende Bericht führt die Erkenntnisse und Schwachstellen weiter aus.

---

[1] Kriminalitätsbekämpfung im unbaren Zahlungsverkehr durch Nutzung nichtpolizeilicher Organisationen
[2] Über KUNO - https://kuno-sperrdienst.de/Home/displayAboutKuno
[3] Polizeiliche Kriminalstatistik 2006, S. 192 https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/pksJahrbuecherBis2011/pks2006.pdf?__blob=publicationFile&v=1
[4] https://www.berliner-zeitung.de/elektroniksystem-meldet-gestohlene-ec-karten-an-geschaefte-sicherheitsluecke-an-geldautomaten-kuno-laesst-karten-betrueger-abblitzen-li.33624
[5] https://www.rheinpfalz.de/wirtschaft_artikel,-kuno-sch%C3%BCtzt-vor-kartengaunern-_arid,902468.html
[6] https://www.kuno-sperrdienst.de/Home/displayFAQ
[7] https://www.rheinpfalz.de/wirtschaft_artikel,-kuno-sch%C3%BCtzt-vor-kartengaunern-_arid,902468.html

2. Übersicht der Funde

Funde im Bereich IT-Sicherheit (Stand: 08.12.2023)

Mängel / Funde	Auswirkung	Status
Webserver gibt detaillierte Informationen im HTTP Response Header aus	Gering	Geschlossen
Fehlende HTTP-Transport-Security-Policy erlaubt MitM-Angriffe	Mittel	Geschlossen
IIS Management Service Default Ports aus dem Internet abrufbar	Mittel	In Prüfung
Ungültiges Zertifikat bei Zugriff auf IIS Management Port im Einsatz	Mittel	In Prüfung
Veraltete JavaScript Bibliothek: jquery-validation 1.11.0 im Einsatz	Hoch	In Prüfung
Veraltete JavaScript Bibliothek: jquery 3.2.1 im Einsatz	Mittel	In Prüfung
Veraltete JavaScript Bibliothek: bootstrap 4.0.0	Mittel	In Prüfung
Übermittlung der Sperrbestätigungsnummer im Kontaktformular erwünscht	Mittel	In Prüfung
Sperrbestätigungsnummer kann durch Brute-Force ermittelt werden & ermöglicht Freischaltung gesperrter Karten (fehlendes Rate-Limiting auf Serverseite)	Hoch	Geschlossen
IBANs und Sperrbestätigungsnummern können durch Brute-Force ermittelt werden und ermöglicht Freischaltung aller gesperrter Karten (fehlendes Rate-Limiting)	Hoch	Geschlossen

Funde im Bereich Datenschutz

Mängel / Funde	Auswirkung	
Nutzung von Google Fonts unmittelbar nach Aufruf der Webseite	Hoch	Geschlossen
Cookie Banner fehlerhaft implementiert: Keine Einwilligung vor Laden der Google Fonts & fehlende Möglichkeit des Widerrufs	Hoch	Geschlossen
Keine Erwähnung der Google Fonts in den Datenschutzbestimmungen	Hoch	Geschlossen (indirekt)
Datenschutzerklärung laut Webseite von 2018 und teilweise veraltet	Mittel	Geschlossen

3. Umgebung / Testparameter

Das KUNO-Sperrsystem verfügt mindestens über 3 Nutzgruppen bzw. Zugangsmöglichkeiten, die im Folgenden näher beschrieben werden. Fokus der vorliegenden Untersuchung war insbesondere der Zugang für Privatpersonen.

3.1 Nutzergruppen

1.) Polizeibehörden und KUNO-Mitarbeiter

Polizeibehörden und KUNO-Mitarbeiter haben die Möglichkeit in einem „Adminbereich" Zugriff auf KUNO zu nehmen, der Login erfolgt mutmaßlich über die Webseite (Anmeldeformular im Footer):

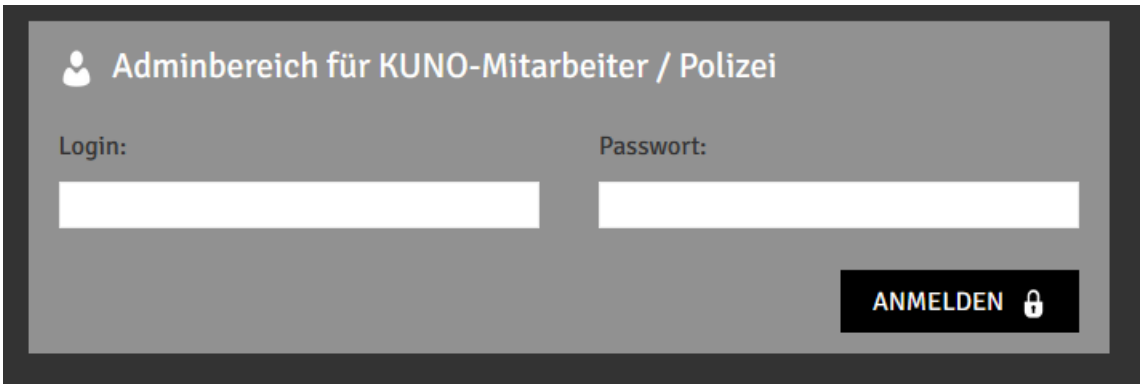


Abbildung 1: Screenshot von kuno-sperrdienst.de (Footer)

Dieser Zugriff ermöglicht einen Vermerk der zu sperrenden Kontodetails (Kontonummer, BLZ, IBAN). Offenbar ist ein Login mittels Nutzernamen und Passwort notwendig.

2.) Netzbetreiber/Finanzdienstleister und größere Händler

Dem FAQ der Webseite[8] ist zu entnehmen, dass Netzbetreiber/Finanzdienstleister und größere Händler Zugriff auf die Sperrdatei nehmen können, um diese bei Transaktionen abzugleichen. Liegt ein Eintrag in der Sperrliste vor, so sind Transaktionen mittels Lastschrift auf diese Karten abzulehnen. Mindestens folgende 14 Anbieter beziehen die KUNO-Sperrliste (Stand Ende Oktober 2023): 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, montrada GmbH, Telecash GmbH & Co. KG, TL1 GmbH, Transact Elektronische Zahlungssysteme GmbH.

Die entsprechenden Daten werden laut Aussagen der Webseite signiert und verschlüsselt übertragen.

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

Quelle: KUNO-Webseite https://www.kuno-sperrdienst.de/Home/displayDataProtection (Abruf 23.10.2023)

3.) Privatpersonen und Betroffene

Die Dritte Nutzergruppe stellt Privatpersonen dar, welche durch die Polizei ein KUNO-Merkblatt erhalten. Das KUNO-Merkblatt weist Informationen zur Sperrung zusammenfassend auf, darunter die Kontodetails (Kontonummer, Bankleitzahl, IBAN und Kartennummer) und eine Sperrbestätigungsnummer. Durch Kenntnis dieser Informationen ist es möglich sich in der Webapplikation anzumelden und Aktionen durchzuführen[9].

[8] https://kuno-sperrdienst.de/Home/displayFAQ
[9] https://www.kuno-sperrdienst.de/Home/displayLogin

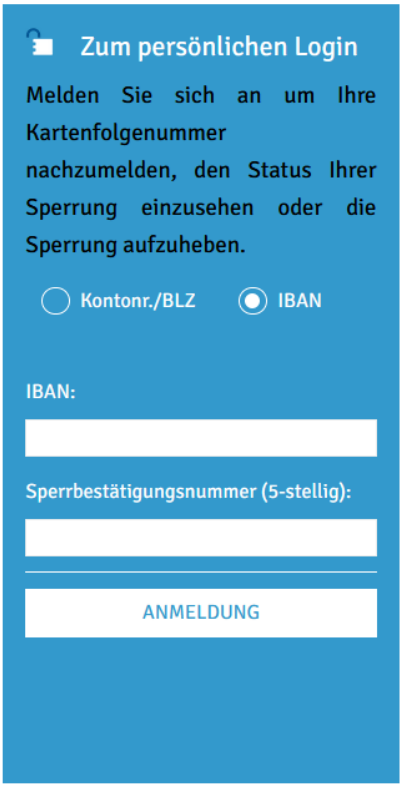


Abbildung 2: Screenshot des KUNO-Login auf kuno-sperrdienst.de

Nach dem Login stehen den betroffenen Personen verschiedene Optionen zur Verfügung, beispielsweise die Aufhebung der entsprechenden Sperre (etwa bei fehlerhafter Meldung oder Wiedererlangung der Karte) oder das Nachmelden einer Kartenfolgenummer.

Abbildung 3: Screenshot der Optionen nach dem Login auf kuno-sperrdienst.de

Folgende Grafik stellt die beschriebenen KUNO-Zugriffe einmal schematisch dar:

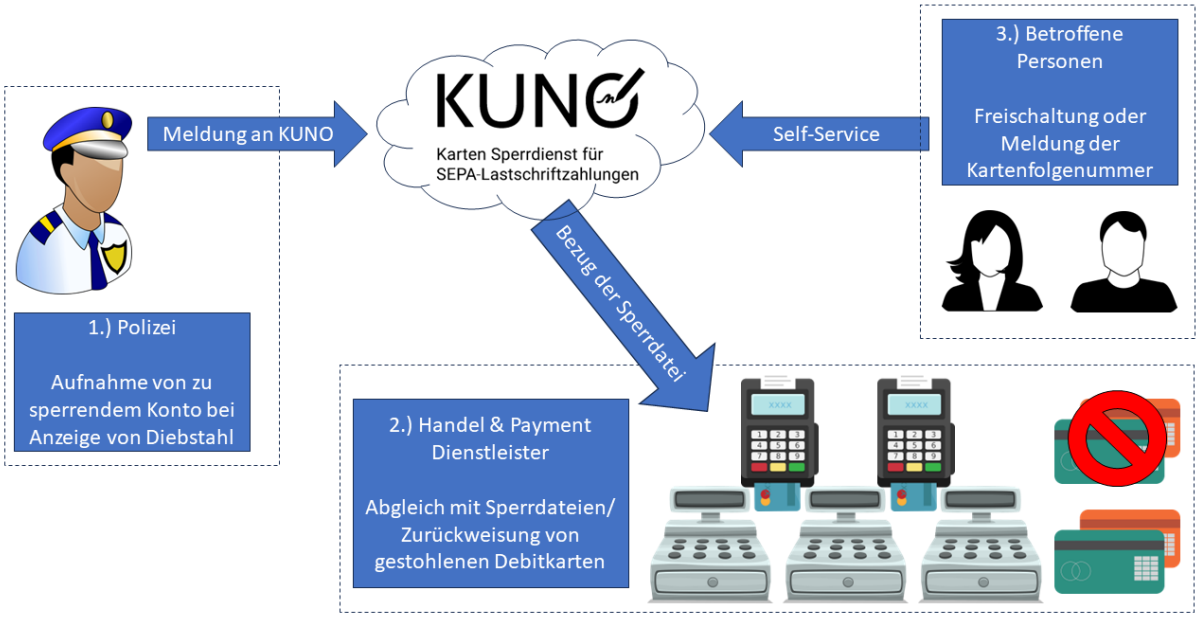


Abbildung 4: Schematische Darstellung des KUNO-Systems

Die Darstellung zeigt die 3 zuvor vorgestellten Rollen und die Kernfunktionen bzw. Interaktionen mit dem KUNO-System.

3.2 Testparameter

Das KUNO-Sperrsystem ist zum Zeitpunkt der Tests (Oktober 2023) über folgende Domain und IPv4-Adresse erreichbar gewesen: kuno-sperrdienst.de (13.69.68.13)

Bei dem System handelt es sich mutmaßlich um einen Microsoft-IIS/10.0 Webserver, welcher auf Microsoft Azure betrieben wird (weitere Details zu dem System in den Schwachstellen).

Der vorliegende Test ist als Blackbox-Test zu betrachten, da kein Zugriff auf den Quellcode oder weitere Informationen des Systems vorlagen[10]. Während des Tests konnte ausschließlich auf Accounts des Self-Service zurückgegriffen werden, es wurden keine Admin- oder Polizeiaccounts genutzt. Trotzdem waren bereits Datenschutzmängel und Sicherheitslücken feststellbar.

Untersuchungen sind nach dem aktuellen Testing-Guide des Open Webapplication Security Projects (OWASP)[11] erfolgt.

Insoweit stellt der vorliegende Bericht möglicherweise nur einen Auszug der Schwachstellen dar. Es ist möglich, dass weitere Schwachstellen in Prozessen oder bei administrativen Funktionen vorliegen.

10 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=3

11 https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf

4. Funde

Im Folgenden werden alle Befunde aufgeführt, welche im Rahmen der Betrachtung des KUNO-Sperrsystems aufgefallen sind (siehe unter anderem Limitierungen in: 3. Umgebung / Testparameter).

4.1 Funde im Bereich IT-Sicherheit

Nachfolgend werden Funde im Bereich der IT-Sicherheit detailliert beschrieben.

4.1.1 Webserver gibt detaillierte Informationen im HTTP Response Header aus

Klasse	IT-Sicherheit
Auswirkung	Gering

Der Webserver gibt durch HTTP-Requests in der HTTP-Response detaillierte Auskunft über die verwendete Webserver Version (inkl. Aspnet-Version).

4.1.1.1 Technische Details / Nachweise

Durch Abruf aller Ressourcen erhält man folgende HTTP-Response:

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
[…]
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Request-Context
Cache-Control: public, no-store, max-age=0
[…]
Vary: *
Content-Length: 21606
X-Aspnetmvc-Version: 5.2
X-Frame-Options: SAMEORIGIN
X-Aspnet-Version: 4.0.30319
Request-Context: appId=cid-v1:b1642552-7b16-48b7-b40f-63266306efc4
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
[…]
```

Durch die Angaben im HTTP Response Header lässt sich entnehmen, dass .NET im Framework 4.0 (4.0.30319) vom 12. April 2010 (Veröffentlichungsdatum) zum Einsatz kommt. Die IIS-Version lässt vermuten, dass eines der folgenden Serverbetriebssysteme zum Einsatz kommt: Windows Server 2016 oder Windows Server 2019.

4.1.1.2 Empfehlung

Das Exponieren der Versionsnummern selbst stellt keine schwerwiegende Sicherheitslücke dar, es kann Angreifern allerdings Aufschluss über die verwendeten Technologien und den Patchstand geben. Im Rahmen von Härtungsmaßnahmen bietet sich an die exakten Versionsnummer nicht an den Endnutzer auszugeben.

Referenzen

OWASP: OTG-INFO-002

MITRE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

4.1.2 Fehlende HTTP-Transport-Security-Policy erlaubt MitM-Angriffe

Klasse	IT-Sicherheit
Auswirkung	Mittel

Die Webapplikation sendet keinen HTTP-Strict-Transport-Security-Header (HSTS). Netzwerktechnisch günstig positionierte Angreifer können mittels Man-in-the-Middle (MitM) daher Datenverkehr zwischen Benutzern und der Webanwendung mitlesen und manipulieren. Durch das Mitsenden eines HSTS-Response-Headers weist eine Webanwendung (HSTS-Host) den Browser an, fortan bis zu einem deklarierten Zeitpunkt ausnahmslos verschlüsselt über eine sichere Verbindung zu kommunizieren.

Nach RFC 6797[12] überschreibt eine HSTS-Policy explizit die Art und Weise, wie der Browser URI-Referenzen, Benutzereingaben (z.B. über die Adressleiste des Browsers) und sonstige Befehle verarbeitet. Ohne HSTS kann ein Man-in-the-Middle-Angreifer (MitM) den Datenverkehr einer vermeintlich sicher über HTTPS kommunizierende Webanwendung in folgenden Szenarien mitlesen und manipulieren:

- Der Benutzer gibt im Browser den Host der Webanwendung ohne Schema ein, also beispielsweise kuno-sperrdienst.de statt HTTPS://kuno-sperrdienst.de. Der Browser sendet dann einen unverschlüsselten HTTP-Request.
- Der Benutzer folgt einem unsicheren HTTP-Link, beispielsweise aus einer E-Mail oder von einer fremden Webseite.
- Die Webanwendung selbst bettet versehentlich unverschlüsselte HTTP-Inhalte ein (Mixed-Content).
- Ein aktiver MitM-Angreifer ersetzt HTTPS-URLs in beispielsweise der initialen HTTP-Response der Webanwendung durch unsichere HTTP-URLs (HTTP-Downgrading durch SSL-Stripping).
- Ein aktiver MitM-Angreifer gibt sich dem Benutzer gegenüber als Host der Webanwendung aus und präsentiert hierzu ein nicht vertrauenswürdiges Zertifikat (MitM-Proxy).

Hätte die Webanwendung dagegen zuvor einen HSTS-Header gesendet, würde der Browser in allen obigen Szenarien sicher verschlüsselt per HTTPS kommunizieren und dem Benutzer keine Möglichkeit bieten, nicht vertrauenswürdige Zertifikate zu akzeptieren.

4.1.2.1 Technische Details / Nachweise

Beispiel: Bei der Eingabe von „kuno-sperrdienst.de/Home/displayLogin“ durch den Nutzenden sendet der Browser folgenden unverschlüsselten HTTP-Request:

```
GET /Home/displayLogin HTTP/1.1
Host: kuno-sperrdienst.de
[…]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.88 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
[…]
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
```

Die Webapplikation antwortet mit folgender unverschlüsselter HTTP-Response:

```
HTTP/1.1 301 Moved Permanently
Content-Length: 0
Connection: close
[…]
Location: https://kuno-sperrdienst.de/Home/displayLogin
```

[12] https://tools.ietf.org/html/rfc6797

Ein Man-in-the-Middle-Angreifer kann diese initiale unverschlüsselte Kommunikation mithören und manipulieren. Hätte die Webapplikation dem Browser dagegen zu einem früheren Zeitpunkt per HSTS-Header mitgeteilt, dass die gesamte Kommunikation stets verschlüsselt zu erfolgen habe, hätte der Browser direkt einen verschlüsselten HTTPS-Request gesendet.

4.1.2.2 Empfehlung

Es wird empfohlen HSTS für die Webapplikation zu aktivieren, dies ist durch Setzen eines HTTP-Response Headers möglich[13].

```
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
```

Durch Setzen des Wertes wird die Gültigkeitsdauer auf 2 Jahre (63072000 Sekunden) festgelegt. Ab mindestens einem Jahr ist es auch denkbar in die sogenannte HSTS-Preload-Liste aufgenommen zu werden[14]. Durch das Setzen dieses Headers wird sichergestellt, dass MitM-Angriffe erheblich erschwer werden.

Referenzen

OWASP: OTG-CONFIG-007
MITRE: CWE-523: Unprotected Transport of Credentials

4.1.3 IIS Management Service Default Ports aus dem Internet abrufbar

Klasse	IT-Sicherheit
Auswirkung	Mittel

Durch einen Portscan auf das System konnte ermittelt werden, dass Management Ports des Webservers aus dem Internet abrufbar sind. Der Zugang zum IIS Management Service auf Port 8172 ist mutmaßlich mittels Nutzername und Passwort und damit mit einem Faktor möglich. Der Zugriff ermöglicht die Konfiguration des Webservers und erlaubt damit einen tiefgreifenden administrativen Zugriff. Üblicherweise werden solche Ports unter anderem auch für das Deployment von neuem Programmcode genutzt.

4.1.3.1 Technische Details / Nachweise

Durch einen Portscan auf das System (mittels nmap) konnte ermittelt werden, dass neben den HTTP Port 80 und Port 443 und einigen weiteren Ports auch Port 8172 zugänglich ist. Bei dem Port handelt es sich um einen IIS Management Service Port[15], welcher tiefgreifenderen Zugriff ermöglicht. Zudem sind die Ports 4022 und 4024 geöffnet, welche laut Herstellerseite zum „Remotedebuggen in Visual Studio“ genutzt werden können[16]. Das öffnen der Ports lässt darauf schließen, dass die Produkte Visual Studio 2019 & Visual Studio 2017 eingesetzt werden[17].

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

PORT    STATE  SERVICE    VERSION
80/tcp  open   http
[…]
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://kuno-sperrdienst.de/
[…]
```

[13] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
[14] https://hstspreload.org/
[15] https://blog.codeinside.eu/2013/04/20/webdeploy-port-ndern-oder-wofr-ist-port-8172-da/
[16] https://learn.microsoft.com/de-de/azure/app-service/environment/network-info
[17] https://learn.microsoft.com/de-de/visualstudio/debugger/remote-debugger-port-assignments?view=vs-2022

```
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
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=waws-prod-am2-275.publish.azurewebsites.windows.net/organizationName=Microsoft
Corporation/stateOrProvinceName=Washington/countryName=US
| Subject Alternative Name: DNS:waws-prod-am2-275.publish.azurewebsites.windows.net, DNS:waws-prod-am2-
275.ftp.azurewebsites.windows.net
| Issuer: commonName=DigiCert SHA2 Secure Server CA/organizationName=DigiCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-09-07T00:00:00
| Not valid after:  2024-09-07T23:59:59
[…]
```

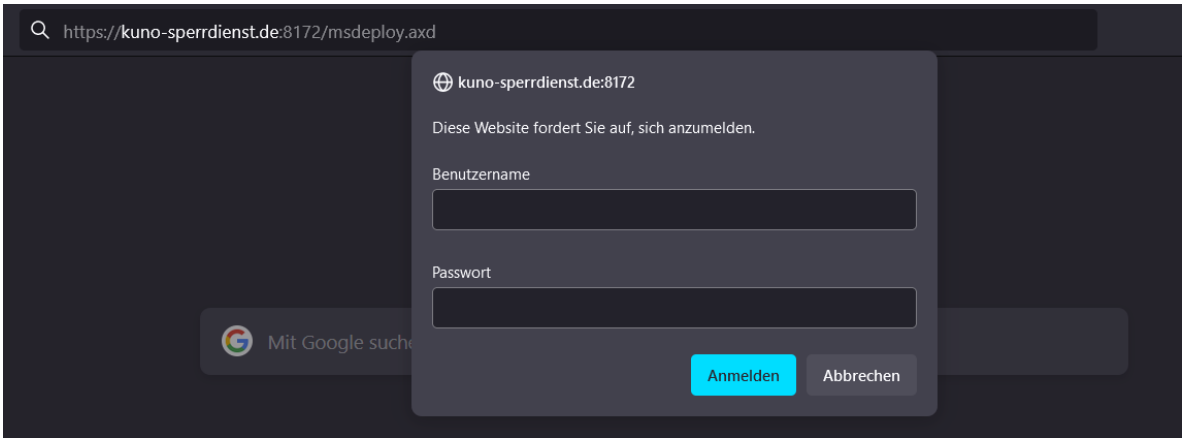


Abbildung 5: msdeploy.axd fordert zur Passworteingabe auf – ein Management-Zugriff ist mit Username/Passwort möglich

4.1.3.2 Empfehlung

Administrative Zugänge sollten ausschließlich von intern zugänglich oder von extern mittels Multi-Faktor abgesichert sein. Im konkreten Fall sollte mindestens Port 8172 geschlossen werden, um einen Bruteforce-Angriff oder ähnliches aus dem Internet zu vermeiden. Darüber hinaus ist es möglich IP-Restrictions einzustellen, um gewollte Zugriffe dediziert von einzelnen IP-Adressen zu ermöglichen[18].

Darüber hinaus sollte geprüft werden, wie sicher Code deployt werden kann. Zudem sind die sonstigen offenen Ports auf Verwendung zu prüfen. Falls diese nicht benötigt werden, sollten sie geschlossen werden, um die Angriffsoberfläche bestmöglich zu reduzieren.

Referenzen

OWASP: OTG-CONFIG-005

CWE-284: Improper Access Control

[18] https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions?tabs=azurecli

4.1.4 Ungültiges Zertifikat bei Zugriff auf IIS Management Port im Einsatz

Klasse	IT-Sicherheit
Auswirkung	Mittel

Bei Zugriff auf den IIS Management Port wird eine Fehlermeldung im Webbrowser angezeigt, da das eingesetzte Zertifikat nicht mit dem Hostnamen der Webseite übereinstimmt.

4.1.4.1 Technische Details / Nachweise

Die abgerufene URL ist:

kuno-sperrdienst.de

Innerhalb des Zertifikats lässt sich folgende URL entnehmen:

waws-prod-am2-275.publish.azurewebsites.windows.net

Weitere Details zum Zertifikat:

ssl-cert: Subject: commonName=waws-prod-am2-275.publish.azurewebsites.windows.net/organizationName=Microsoft Corporation/stateOrProvinceName=Washington/countryName=US
Subject Alternative Name: DNS:waws-prod-am2-275.publish.azurewebsites.windows.net, DNS:waws-prod-am2-275.ftp.azurewebsites.windows.net
Issuer: commonName=DigiCert SHA2 Secure Server CA/organizationName=DigiCert Inc/countryName=US
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2023-09-07T00:00:00
Not valid after: 2024-09-07T23:59:59
MD5: fcf7 87fc b209 b81c 3379 13e6 e718 19e2
SHA-1: d3cd b997 3a0d e884 271f 515d 846e 90d5 ce13 da13

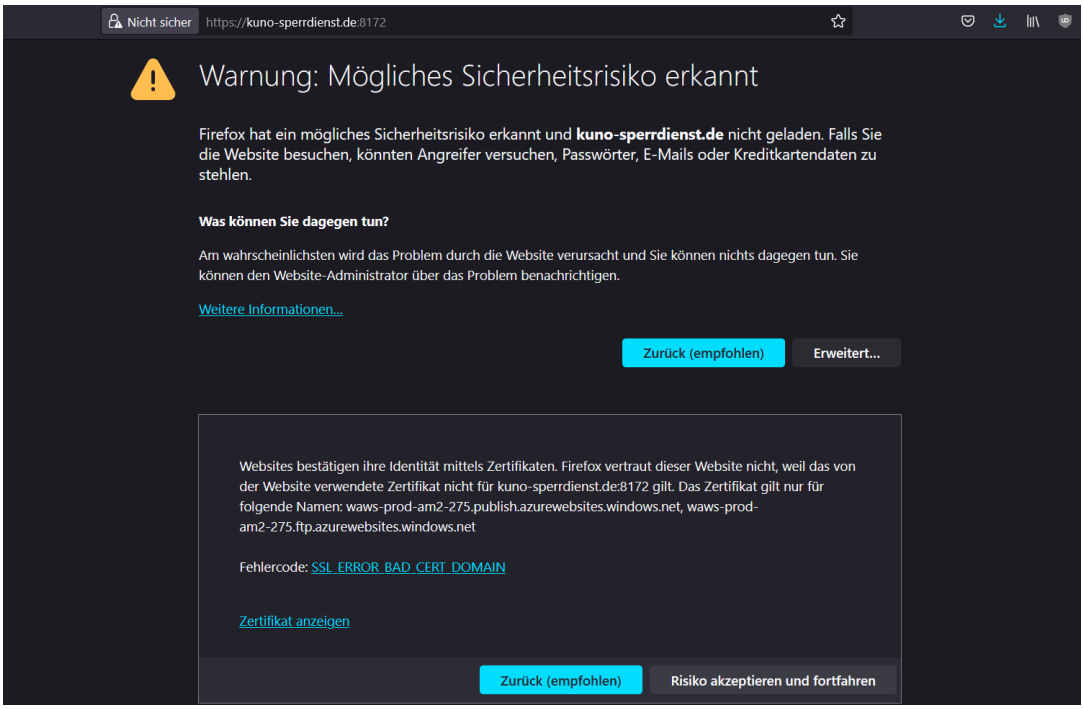


Abbildung 6: Fehlermeldung bei Abruf der administrativen Schnittstelle

4.1.4.2 Empfehlung

Das Zertifikat sollte erneuert werden und mit dem Hostnamen des Systems übereinstimmen. Zudem ist zu hinterfragen, ob dieser Port extern erreichbar sein sollte (siehe letzten Fund).

Referenz

OWASP: OTG-CRYPST-001

4.1.5 Veraltete JavaScript Bibliothek: jquery-validation 1.11.0 im Einsatz

Klasse	IT-Sicherheit
Auswirkung	Hoch (gemäß CVSS-Score)

Beim Laden der Webseiten konnte die veraltete JavaScript Bibliothek „jquery-validation“ identifiziert werden, welche verschiedene Schwachstellen aufweist. Die Auswirkung der Schwachstelle wird an dieser Stelle gemäß dem CVSS-Score der bekannten Schwachstellen in der Bibliothek vorgenommen.

4.1.5.1 Technische Details / Nachweise

Folgende HTTP-Response zeigt die Bibliothek (sie wird bereits bei Abruf der Startseite geladen):

```
HTTP Request
GET /requirements/js/custom.js HTTP/2
Host: www.kuno-sperrdienst.de
[…]

HTTP Response
HTTP/2 200 OK
Content-Type: application/x-javascript
[…]
Server: Microsoft-IIS/10.0
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Etag: "06654c891b5d91:0"
Last-Modified: Thu, 13 Jul 2023 13:56:12 GMT
Vary: Accept-Encoding
Content-Length: 26465
X-Powered-By: ASP.NET

/*! jQuery Validation Plugin - v1.11.0 - 2/4/2013
 https://github.com/jzaefferer/jquery-validation
 Copyright (c) 2013 Jörn Zaefferer; Licensed MIT */
(function($){$.extend($.fn,{validate:function(options){if(!this.length){
[…]
```

Es handelt sich um **“jquery-validation”** in der Version **1.11.0**, welche mindestens folgende, bekannte Schwachstellen aufweist:
CVE-2021-21252 (CVSS: High, 7.5): Regular Expression Denial of Service vulnerability
CVE-2021-43306 (CVSS: High, 7.5): ReDoS vulnerability in URL2 validation
CVE-2022-31147 (CVSS: High, 7.5): ReDoS vulnerability in url and URL2 validation

Details zu den Schwachstellen (entnommen aus gemäß National Vulnerability Database (NVD)):

CVE-2021-21252: The jQuery Validation Plugin provides drop-in validation for your existing forms. It is published as an npm package "jquery-validation". jquery-validation before version 1.19.3 contains one or more regular expressions that are vulnerable to ReDoS (Regular Expression Denial of Service). This is fixed in 1.19.3.

CVE-2021-43306: An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the jquery-validation npm package, when an attacker is able to supply arbitrary input to the url2 method.

CVE-2022-31147: The jQuery Validation Plugin (jquery-validation) provides drop-in validation for forms. Versions of jquery-validation prior to 1.19.5 are vulnerable to regular expression denial of service (ReDoS) when an attacker is able to supply arbitrary input to the url2 method. This is due to an incomplete fix for CVE-2021-43306. Users should upgrade to version 1.19.5 to receive a patch.

Gängige JavaScript-Bibliotheken genießen in der Regel den Vorteil, dass sie intensiv geprüft werden. Dies kann bedeuten, dass Fehler schnell erkannt und im Vorfeld behoben werden, was zu einem stetigen Strom an Sicherheitsupdates führt, die angewendet werden müssen. Obwohl es verlockend sein mag, Aktualisierungen zu ignorieren, kann die Verwendung einer Bibliothek mit fehlenden

Sicherheitspatches dazu führen, dass Ihre Website besonders leicht auszunutzen ist. Daher ist es wichtig sicherzustellen, dass alle verfügbaren Sicherheitsupdates zeitnah angewendet werden. Einige Bibliotheksschwachstellen machen jede Anwendung offen, die die Bibliothek importiert, andere betreffen jedoch nur Anwendungen, die bestimmte Bibliotheksfunktionen verwenden. Es kann schwierig sein, genau zu ermitteln, welche Bibliotheksschwachstellen Ihre Website betreffen. Wir empfehlen daher, trotzdem alle verfügbaren Sicherheitsupdates zu installieren.

4.1.5.2 Empfehlung

Entwickele Sie eine Patch-Management-Strategie, um sicherzustellen, dass Sicherheitsupdates umgehend auf alle Drittanbieter-Bibliotheken in Ihrer Anwendung angewendet werden. Erwägen Sie außerdem, Ihre Angriffsfläche zu verringern, indem Sie alle Bibliotheken entfernen, die nicht mehr verwendet werden.

Referenz

MITRE: CWE-1104: Use of Unmaintained Third Party Component

4.1.6 Veraltete JavaScript Bibliothek: jquery 3.2.1 im Einsatz

Klasse	IT-Sicherheit
Auswirkung	Mittel

Beim Laden der Webseiten konnte eine veraltete JavaScript Bibliothek „jquery“ identifiziert werden, welche verschiedene Schwachstellen aufweist. Die Auswirkung der Schwachstelle wird an dieser Stelle gemäß dem CVSS-Score der bekannten Schwachstellen in der Bibliothek vorgenommen.

4.1.6.1 Technische Details / Nachweise

Folgende HTTP-Response zeigt die Bibliothek (sie wird bereits bei Abruf der Startseite geladen):

```
HTTP Request
GET /requirements/js/jquery/jquery.min.js HTTP/2
Host: www.kuno-sperrdienst.de
[…]

HTTP Response
HTTP/2 200 OK
Content-Type: application/x-javascript
[…]
Server: Microsoft-IIS/10.0
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Etag: "06654c891b5d91:0"
Last-Modified: Thu, 13 Jul 2023 13:56:12 GMT
Vary: Accept-Encoding
Content-Length: 86663
X-Powered-By: ASP.NET

/*! jQuery v3.2.1 | (c) JS Foundation and other contributors | jquery.org/license */
!function(a,b){
[…]
```

Es handelt sich um **“jquery”** in der Version **3.2.1**, welche mindestens folgende, bekannte Sicherheitslücken aufweist:
CVE-2019-11358 (CVSS: Medium, 6.1): jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution
CVE-2020-11022 (CVSS: Medium, 6.1): Regex in its jQuery.htmlPrefilter sometimes may introduce XSS
CVE-2020-11023, CVE-2020-23064: (CVSS: Medium, 6.1): passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.

Gängige JavaScript-Bibliotheken genießen in der Regel den Vorteil, dass sie intensiv geprüft werden. Dies kann bedeuten, dass Fehler schnell erkannt und im Vorfeld behoben werden, was zu einem stetigen Strom an Sicherheitsupdates führt, die angewendet werden müssen. Obwohl es verlockend sein mag, Aktualisierungen zu ignorieren, kann die Verwendung einer Bibliothek mit fehlenden Sicherheitspatches dazu führen, dass Ihre Website besonders leicht auszunutzen ist. Daher ist es wichtig sicherzustellen, dass alle verfügbaren Sicherheitsupdates zeitnah angewendet werden. Einige Bibliotheksschwachstellen machen jede Anwendung offen, die die Bibliothek importiert, andere betreffen jedoch nur Anwendungen, die bestimmte Bibliotheksfunktionen verwenden. Es kann schwierig sein, genau zu ermitteln, welche Bibliotheksschwachstellen Ihre Website betreffen. Wir empfehlen daher, trotzdem alle verfügbaren Sicherheitsupdates zu installieren.

4.1.6.2 Empfehlung

Entwickele Sie eine Patch-Management-Strategie, um sicherzustellen, dass Sicherheitsupdates umgehend auf alle Drittanbieter-Bibliotheken in Ihrer Anwendung angewendet werden. Erwägen Sie außerdem, Ihre Angriffsfläche zu verringern, indem Sie alle Bibliotheken entfernen, die nicht mehr verwendet werden.

Referenz

MITRE: CWE-1104: Use of Unmaintained Third Party Component

4.1.7 Veraltete JavaScript Bibliothek: bootstrap 4.0.0

Klasse	IT-Sicherheit
Auswirkung	Mittel

Beim Laden der Webseiten konnte eine veraltete JavaScript Bibliothek „bootstrap“ identifiziert werden, welche verschiedene Schwachstellen aufweist. Die Auswirkung der Schwachstelle wird an dieser Stelle gemäß dem CVSS-Score der bekannten Schwachstellen in der Bibliothek vorgenommen.

4.1.7.1 Technische Details / Nachweise

Folgende HTTP-Response zeigt die Bibliothek (sie wird bereits bei Abruf der Startseite geladen):

```
HTTP Request
GET /requirements/js/bootstrap/bootstrap.min.js HTTP/2
Host: www.kuno-sperrdienst.de
[…]

HTTP Response
HTTP/2 200 OK
Content-Type: application/x-javascript
[…]
Server: Microsoft-IIS/10.0
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Etag: "06654c891b5d91:0"
Last-Modified: Thu, 13 Jul 2023 13:56:12 GMT
Vary: Accept-Encoding
Content-Length: 48950
X-Powered-By: ASP.NET

/*!
 * Bootstrap v4.0.0 (https://getbootstrap.com)
 * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors)
 * Licensed under MIT ( […]
```

Es handelt sich um **“bootstrap”** in der Version **4.0.0**, welche mindestens folgende, bekannte Sicherheitslücken aufweist:

CVE-2019-8331 (CVSS: Medium, 6.1): XSS in data-template, data-content and data-title properties of tooltip/popover
CVE-2018-14041 (CVSS: Medium, 6.1): XSS in data-target property of scrollspy
CVE-2018-14040 (CVSS: Medium, 6.1): XSS in collapse data-parent attribute
CVE-2018-14042 (CVSS: Medium, 6.1): XSS in data-container property of tooltip
CVE-2016-10735 (CVSS: Medium, 6.1): XSS is possible in the data-target attribute.

Gängige JavaScript-Bibliotheken genießen in der Regel den Vorteil, dass sie intensiv geprüft werden. Dies kann bedeuten, dass Fehler schnell erkannt und im Vorfeld behoben werden, was zu einem stetigen Strom an Sicherheitsupdates führt, die angewendet werden müssen. Obwohl es verlockend sein mag, Aktualisierungen zu ignorieren, kann die Verwendung einer Bibliothek mit fehlenden Sicherheitspatches dazu führen, dass Ihre Website besonders leicht auszunutzen ist. Daher ist es wichtig sicherzustellen, dass alle verfügbaren Sicherheitsupdates zeitnah angewendet werden. Einige Bibliotheksschwachstellen machen jede Anwendung offen, die die Bibliothek importiert, andere betreffen jedoch nur Anwendungen, die bestimmte Bibliotheksfunktionen verwenden. Es kann schwierig sein, genau zu ermitteln, welche Bibliotheksschwachstellen Ihre Website betreffen. Wir empfehlen daher, trotzdem alle verfügbaren Sicherheitsupdates zu installieren.

4.1.7.2 Empfehlung

Entwickele Sie eine Patch-Management-Strategie, um sicherzustellen, dass Sicherheitsupdates umgehend auf alle Drittanbieter-Bibliotheken in Ihrer Anwendung angewendet werden. Erwägen Sie außerdem, Ihre Angriffsfläche zu verringern, indem Sie alle Bibliotheken entfernen, die nicht mehr verwendet werden.

Referenz

MITRE: CWE-1104: Use of Unmaintained Third Party Component

4.1.8 Übermittlung der Sperrbestätigungsnummer im Kontaktformular erwünscht

Klasse	IT-Sicherheit
Auswirkung	Mittel

Im Rahmen des Kontaktformulars (erreichbar unter: https://kuno-sperrdienst.de/Home/Contact) wird darum gebeten die Kontodaten und die Sperrbestätigungsnummer mitzuteilen. Dies ist als ungewöhnlich zu betrachten, da durch die angegebenen Informationen ein vollständiger Login in den Account möglich ist. Es ist nicht Best Practise, dass eine Übermittlung von Logindaten an den Support vorgenommen werden. Darüber hinaus ist davon auszugehen, dass das Schutzziel der Nachvollziehbarkeit (wer hat die Logindaten wann verwendet) nicht mehr ermöglicht werden kann, wenn mehrere Entitäten über das Passwort (in diesem Fall die Sperrbestätigungsnummer) verfügen.

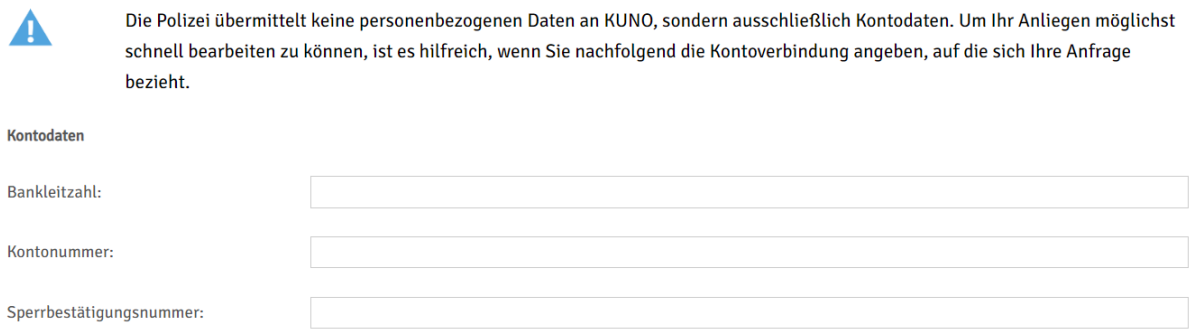


Abbildung 7: Bildschirmfoto des Kontaktformulars

4.1.8.1 Technische Details / Nachweise

Folgender HTTP-Request zeigt die Übermittlung der Parameter, die einen Login ermöglichen:

HTTP Request
POST /Home/Contact HTTP/2
Host: www.kuno-sperrdienst.de
[…]
Referer: https://www.kuno-sperrdienst.de/Home/Contact
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

CustomerEmail=&
__RequestVerificationToken=gecl7oAHYTyFxyNp8s7sWZVPZmnVS3_gOauh8BZBcpSP7UwiomWOrnpOgo4LKbtDhj6uZ-dBV4UsNNbGCdhkslnwXnaRJikoukZacB3ih7c1&
UserLastName=Testnachname&
UserFirstName=Testvorname&
UserEmail=test%40tim-philipp-schaefers.de&
FlagMeldungVeranlasst=1&
StateID=5&
BanLeiZah=Bankleitzahl&
KonNum=Kontonummer&
SpeBesNum=Sperrbest%C3%A4tigungsnummer&
Comments=Testkommentar

Wie aus dem Mitschnitt des Netzwerksverkehrs zu entnehmen ist findet im Kontaktformular die vollständige Übermittlung der Daten, welche für den Login benötigt werden, statt. Damit ist es Supportmitarbeitende möglich diese Daten zu verwenden

4.1.8.2 Empfehlung

Es wird empfohlen keine Übermittlung der Sperrbestätigungsnummer im Kontaktformular vorzunehmen, da dies nicht der gängigen Best Practise entspricht. Supportmitarbeitende sollten nicht die Logindaten von Nutzeraccounts erhalten. Darüber hinaus besteht die Gefahr, dass diese Daten an Dritte gelangen, da sie zumindest zweitweise gespeichert werden (bspw. in E-Mail-Postfächern). Um trotzdem eine Art Authentifizierung zu ermöglichen ist es denkbar einen Teil des Sperrcodes zu verwenden, bspw. ausschließlich die ersten 2-Stellen (zur Qualität des Sperrcodes gibt es in den folgenden Funden allerdings weitere Anmerkungen) – alternativ sollte auf eine Art Telefonpin, welcher sich von der Sperrbestätigungsnummer unterscheidet, zurückgegriffen werden (dieser Pin könnte zusätzlich auf dem KUNO-Merkblatt platziert werden oder postalisch zugestellt werden).

4.1.9 Sperrbestätigungsnummer kann durch Brute-Force ermittelt werden & ermöglicht Freischaltung gesperrter Karten (fehlendes Rate-Limiting auf Serverseite)

Klasse	IT-Sicherheit
Auswirkung	Hoch

Bei Kenntnis einer „gesperrten“ IBAN kann man eine Anmeldung gemäß KUNO-Sperrsystem mittels IBAN und Sperrbestätigungsnummer nach einem erfolgreichen Login vornehmen.

Die Sperrbestätigungsnummer ist auf dem KUNO-Merkblatt der Polizei vermerkt und ist eine 5-stellige Nummer. Insgesamt lässt sich durch die Schwäche der Sperrbestätigungsnummer ein Brute-Force Angriff (online) vornehmen, womit man Zugriff auf Accounts mit der dazugehörigen IBAN nehmen kann. Nach einem Login ist die „Freischaltung“ der gesperrten Karte direkt möglich.

Das Loginformular für Endnutzende ist folgend dargestellt:

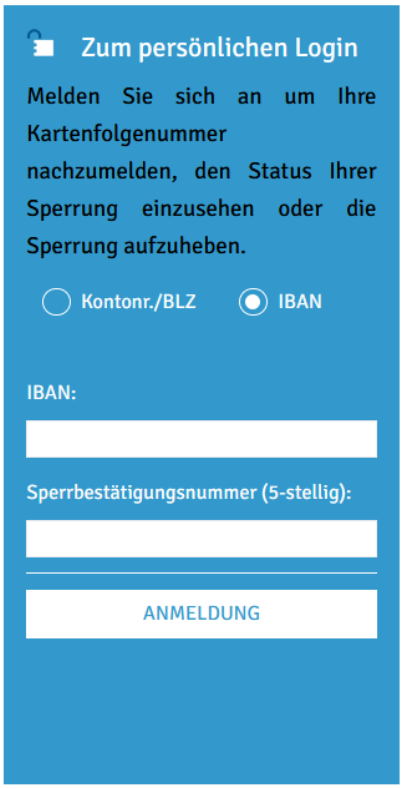


Abbildung 8: Screenshot des KUNO-Login auf kuno-sperrdienst.de

4.1.9.1 Technische Details / Nachweise

Da in diesem Szenario die IBAN als bekannt angenommen wird[19] ist ausschließlich die Sperrbestätigungsnummer zu erraten (durch Bruteforce zu ermitteln). Insgesamt befinden sich die möglichen Kombinationen in diesem Zahlenraum: 00000 bis 99999. Somit kommen 100.000-1 Möglichkeiten in Frage.

Die Übermittlung erfolgt bei der Anmeldung mittels folgendem HTTP-Request:

HTTP Request

```
POST /Home/displayLogin HTTP/2
Host: www.kuno-sperrdienst.de
[…]
```

[19] Bei Taschendiebstahl ist diese für Täter leicht zu erlangen, da sie auf der Karte angebracht ist.

__RequestVerificationToken=zEEY0_okO0jV_OGAVmookW7INGdon8e-ZuX03i0J7S7kWDXglH0gX6jdpEPe0TrxNrwXI-_pxGchznb5blUywDP_uzp1n3XXQE28V-eBZok1
&I_B_A_N=DEXXX
&SpeBesNum=11111
&btnSubmit_IBAN=Anmeldung

Der gezeigte Parameter kann bei Anfragen mittels MitM-Proxy[20] manipuliert werden, dies ermöglicht das Ausprobieren beliebiger Kombinationen (mit anschließendem Versand an den Server). Das Vorgehen kann beispielsweise folgendermaßen aussehen:

1. Versuch: **00000**
2. Versuch: **00001**
3. Versuch: **00002**
[…]
99999. Versuch: **99998**
10000. Versuch: **99999**

Das gleiche Vorgehen kann auch für die Anmeldung mittels Kontonummer und Bankleitzahl (BLZ) vorgenommen werden[21]:

HTTP Request
POST /Home/displayLogin HTTP/2
Host: www.kuno-sperrdienst.de
[...]
__RequestVerificationToken=xNDJnsnbdLCH0CVdjQwsGo3PkltCnkVmCu-snZ-2Mb7tBHdWwufF8wM6eqI0Bn4D39NKI6zRyjhOiBTu7RtMubrh9uGRl_nppFQhCQQQywQ1
&BanLeiZah=XXXXXX
&KonNum=XXXXXXX
&SpeBesNum=11111
&btnSubmit_KB=Anmeldung

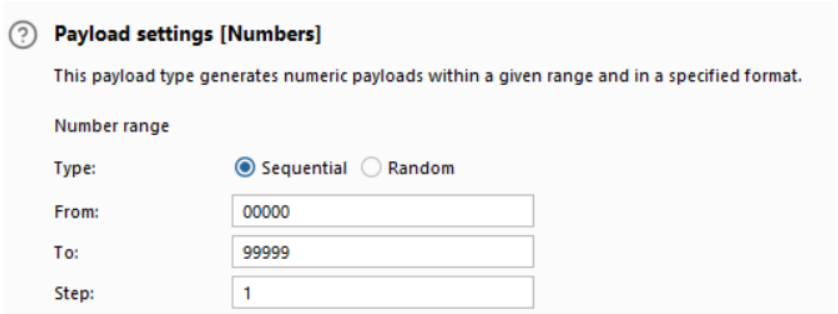


Abbildung 9: Payload-Anpassung in Burp Suite Intruder

Die entsprechende Stelle in dem HTTP-Request wird durch eine Payload ersetzt. Das geschilderte Vorgehen konnte bei KUNO exemplarisch durchgeführt werden, insgesamt war es möglich 100.000 HTTP-Anfragen in 2,5 Stunden (ca. 150 Minuten) durchzuführen (entspricht ca. 11 HTTP-Requests pro Sekunde). Bei parallelisierten Abfragen von verschiedenen Systemen oder der Optimierung der Anfragen (beispielsweise über 100 Anfragen pro Sekunde) sind noch deutlich schnellere Abfragen denkbar.

Abbildung 10: Laufende Abfrage der Sperrbestätigungsnummern innerhalb von Burp Suite Intruder

[20] Denkbar sind Programme wie ZAP Attack Proxy oder Burp Suite.
[21] Offensichtlich liegt diese Art der Anmeldung für Kompatibilitätszwecke (Nutzung vor SEPA) vor.

Im Rahmen des Tests konnte ermittelt werden, dass offenbar keinerlei Ratelimiting (Begrenzung der Anfragen) vorliegt, weder IP-Adressen noch User-Agents oder IBANs (Accounts) werden nach einer Vielzahl von Versuchen gesperrt[22]. Dies ermöglicht es beliebig viele Anfragen zu stellen (einzig limitierender Faktor ist die Internetleitung und das Backend des KUNO-Sperrsystem).

Durch die Auswertung der HTTP-Responses ist es möglich zu ermitteln, ob die verwendete Sperrbestätigungsnummer zu der IBAN zuordenbar und damit korrekt ist – oder nicht.

HTTP-Response bei fehlerhafter Sperrbestätigungsnummer

HTTP Response

```
HTTP/2 302 Found
Content-Type: text/html; charset=utf-8
[…]
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Request-Context
Cache-Control: public, no-store, max-age=0
[…]
Location: https://www.kuno-sperrdienst.de/
Set-Cookie: ASP.NET_SessionId=cdop5c2zpsdiloslnsxxh3hx; path=/; secure; HttpOnly; SameSite=Lax
Vary: *
Content-Length: 149
X-Aspnetmvc-Version: 5.2
X-Aspnet-Version: 4.0.30319
Request-Context: appId=cid-v1:b1642552-7b16-48b7-b40f-63266306efc4
X-Powered-By: ASP.NET

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="https://www.kuno-sperrdienst.de/">here</a>.</h2>
</body></html>
```

HTTP-Response bei korrekter Sperrbestätigungsnummer

HTTP Response

```
HTTP/2 302 Found
Content-Type: text/html; charset=utf-8
[…]
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Request-Context
Cache-Control: public, no-store, max-age=0
[…]
Location: /Private/StatusSummary
Set-Cookie: ASP.NET_SessionId=bpbji20u2wzxxnohgo3r4lxx; path=/; secure; HttpOnly; SameSite=Lax
Vary: *
Content-Length: 139
X-Aspnetmvc-Version: 5.2
X-Aspnet-Version: 4.0.30319
Request-Context: appId=cid-v1:b1642552-7b16-48b7-b40f-63266306efc4
X-Powered-By: ASP.NET

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Private/StatusSummary">here</a>.</h2>
</body></html>
```

[22] Im Test wurden jedoch maximal 25 gleichzeitige Anfragen verwendet, um eine Überlastung der abgefragten Systeme auszuschließen. Zudem wurde die Seite gemonitort, um mögliche Störungen durch das Testing auszuschließen und unmittelbar zu reagieren.

Neben der eigentlichen Meldung in der HTTP-Response kann beispielsweise auch die Länge der HTTP-Response herangezogenen werden, um auszuwerten welcher Sperrbestätigungsnummer der korrekte ist.

Die Länge bei fehlerhafter Sperrbestätigungsnummer beträgt: 800

Die Länge bei korrekter Sperrbestätigungsnummer beträgt: 780

In Programmen wie Burp Suite werden die HTTP-Requests anschließend folgendermaßen dargestellt und können ausgewertet werden (in diesem Fall ist die Sperrbestätigungsnummer 94032):

Request	Payload	Status code	Error	Timeout	Length	Comment
94024	94023	302			800	
94025	94024	302			800	
94026	94025	302			800	
94027	94026	302			800	
94028	94027	302			800	
94029	94028	302			800	
94030	94029	302			800	
94031	94030	302			800	
94032	94031	302			800	
94033	94032	302			780	
94034	94033	302			800	
94035	94034	302			800	
94036	94035	302			800	

Abbildung 11: Anfragen eines Bruteforce-Angriffs im Burp Suite Modul Intruder

Nachdem die korrekte Sperrbestätigungsnummer zu der IBAN ermittelt werden konnte, kann ein Login damit erfolgen. Anschließend wird eine Übersicht über bestehende Sperrungen angezeigt:

Abbildung 12: Anzeige nach dem erfolgreichen Login

In diesem Portal können Nutzende KUNO-Sperrungen aufheben, dazu stehen folgende Gründe der Entsperrung zur Auswahl:

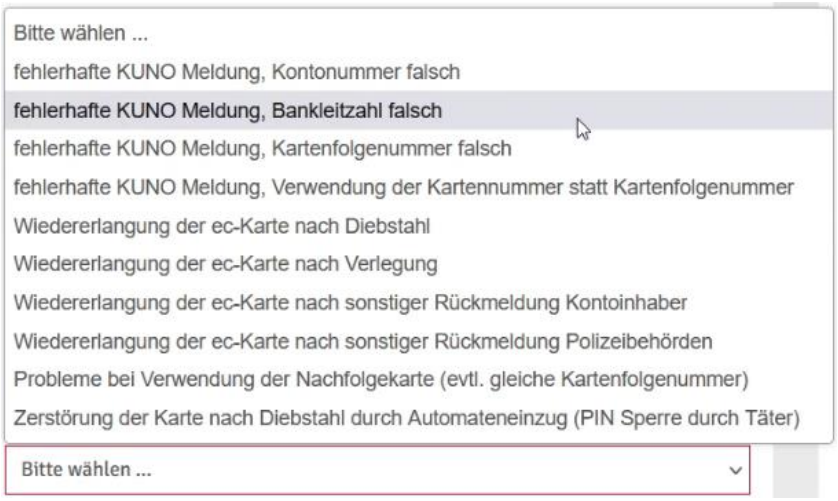


Abbildung 13: Auswahl zu "Grund der Entsperrung"

Nach der Auswahl eines Grundes muss der Nutzende bestätigen, dass es sich um die eigenen Kontodaten handelt und die Sperrmeldung gelöscht werden soll.

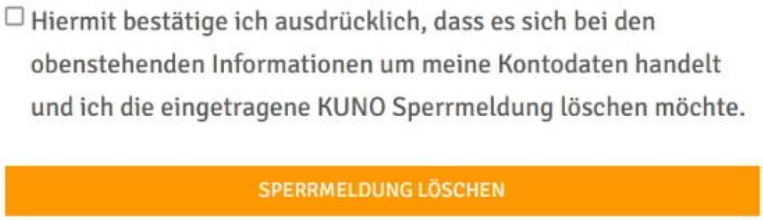


Abbildung 14: Notwendigkeit zur Bestätigung vor der Löschung der KUNO-Sperrmeldung

Durch Klick auf den Button „Sperrmeldung löschen“ wird die Karte wieder freigeschaltet.

4.1.9.2 Empfehlung

Anfragen an Server und Backendsysteme sollten grundsätzlich stark limitiert werden (Einsatz von sogenanntem Rate Limiting), um Bruteforce so zeitaufwändig wie möglich zu machen. Darüber hinaus empfiehlt sich ein Security Monitoring, um auf Auffälligkeiten reagieren zu können.

Rate Limiting ist eine Technik, die in der Informatik verwendet wird, um die Anzahl der Anfragen oder Aktionen, die von einem Benutzer oder einer Anwendung in einem bestimmten Zeitraum durchgeführt werden können, zu begrenzen. Dies wird oft eingesetzt, um die Serverinfrastruktur vor Überlastung und Missbrauch zu schützen. Es gibt verschiedene Arten von Rate Limiting, die je nach Anwendungsfall unterschiedlich konfiguriert werden können. Dies sind einige gängige Arten:

- Anfragerate-Limiting: Begrenzt die Anzahl der Anfragen, die ein Benutzer oder eine Anwendung pro Zeiteinheit stellen kann. Dies hilft, vor zu vielen gleichzeitigen Anfragen zu schützen.
- IP-basiertes Rate Limiting: Begrenzt die Anzahl der Anfragen, die von einer bestimmten IP-Adresse in einem bestimmten Zeitraum durchgeführt werden können. Dies kann dazu beitragen, DDoS-Angriffe (Distributed Denial of Service) abzuschwächen.
- Token-Bucket Rate Limiting: Basierend auf dem Token-Bucket-Algorithmus, bei dem Tokens in einem "Eimer" gesammelt werden. Jede Anfrage benötigt eine bestimmte Anzahl von Tokens.

Wenn der Eimer leer ist, werden keine weiteren Anfragen akzeptiert, bis neue Tokens hinzugefügt werden.

- Concurrency Rate Limiting: Begrenzt die gleichzeitige Anzahl von Verbindungen oder Operationen, die eine Anwendung durchführen kann.

Rate Limiting ist wichtig, um sicherzustellen, dass Ressourcen effizient genutzt werden, die Systemleistung stabil bleibt und um vor bösartigen Aktivitäten oder unbeabsichtigtem Missbrauch zu schützen. Es wird häufig in Webanwendungen, APIs (Application Programming Interfaces) und anderen verteilten Systemen eingesetzt.

Beispielsweise könnten bzw. sollten bei KUNO bereits 5 falsche Eingaben einer Sperrbestätigungsnummer dazu führen, dass die anfragende IP-Adresse für gewisse Zeit blockiert wird oder ein Login in das Konto der zugeordneten IBAN zunächst einmal nicht mehr möglich ist. Neben der Implementierung innerhalb der Applikation ist auch ein Einsatz einer sogenannten Webapplication Firewall (WAF) denkbar, da ein solches System ungewöhnliche Anfragen ebenfalls unterbinden kann.

4.1.10 IBANs und Sperrbestätigungsnummern können durch Brute-Force ermittelt werden und ermöglicht Freischaltung aller gesperrter Karten (fehlendes Rate-Limiting)

Klasse	IT-Sicherheit
Auswirkung	Hoch

Wie im Fund zuvor geschildert können Sperrbestätigungsnummern mittels Brute-Force ermittelt werden. Eine ähnliche Vorgehensweise ist auch für IBANs (mit Sperrbestätigungsnummern) denkbar, da diese ebenfalls streng nach Zahlen aufgebaut sind.

Abbildung 15: Aufbau einer IBAN

Die notwendigen Abfragen sind allerdings deutlich umfangreicher (u.a. auf Grund der Länge und Prüfziffern), da eine Vielzahl an Kombinationen getestet werden muss. Auf Grund des fehlenden Rate-Limitings konnte allerdings ebenfalls ermittelt werden, dass dieses Vorgehen möglich ist[23]. **Mit diesem Vorgehen lassen sich sämtliche IBANs und Sperrbestätigungscodes aus der Datenbank auslesen und freischalten[24].**

4.1.10.1 Technische Details / Nachweise

Statt Abfragen ausschließlich auf die Sperrbestätigungsnummer auszurichten ist es bei diesem Vorgehen notwendig, dass neben der Sperrbestätigungsnummer auch die IBAN enumeriert wird.

Die International Bank Account Number (IBAN) in Deutschland besteht aus 22 Zeichen, darunter eine Länderkennung (DE für Deutschland) und eine Prüfziffer[25]. Die restlichen Zeichen repräsentieren die Bankleitzahl und die Kontonummer. Jedes Zeichen kann 10 mögliche Werte (0-9) haben, und es gibt auch Buchstaben (A-Z) für einige Positionen. Da jede Stelle in der IBAN unterschiedliche Werte haben kann, müssten alle möglichen Kombinationen für jede Stelle multiplizieren.

In Deutschland gibt es rund 8.000 Bankleitzahlen, und die Kontonummern können eine variable Länge haben, normalerweise bis zu 10 Ziffern (der Rest wird meist mit Nullen versehen).

Die IBAN DE94100500006600046463 hat die folgende Struktur:

DE: Länderkennung für Deutschland.

94: Zwei Prüfziffern.

100500006600046463: Die Kombination aus der Bankleitzahl und der Kontonummer.

Die Bankleitzahl (BLZ) "10050000" identifiziert eine bestimmte Bank, und die Kontonummer "6600046463" identifiziert ein bestimmtes Konto bei dieser Bank. Wie erkennbar ist führt diese Bank

[23] Im Rahmen der Tests wurde kein unbefugter Zugriff auf Daten Dritter genommen.
[24] In der Praxis würde eine solche Vorgehensweise mehrere Wochen dauern und könnte bei sehr vielen Anfragen auffallen.
[25] Nach ISO 13616-1:2020 wären auch maximale 34-Stellen möglich, in Deutschland liegen allerdings 22 Stellen vor.

führende Sechsen und Nullen (66000) bei Ihren Kontonummern, womit der mögliche Zahlenraum sich eingrenzen lässt. Es ergibt sich ein möglicher Zahlenraum von 66000 bis 66999. Je nach Bank können so spezifische Bereiche in den KUNO-Daten abgescannt werden, um Einträge zu identifizieren.

Abfragen würden so durchgeführt werden, dass pro IBAN die Sperrbestätigungsnummer enumeriert wird. Das Vorgehen sieht etwa folgendermaßen aus:

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
[…]	[…]	[…]

Pro einzigartige IBAN müssen maximal 100.000 HTTP-Requests durchgeführt werden. Die Abfrage dazu ist grundsätzlich die gleiche wie beim Fund zuvor:

HTTP Request
POST /Home/displayLogin HTTP/2
Host: www.kuno-sperrdienst.de
[…]
__RequestVerificationToken=zEEY0_okO0jV_OGAVmookW7INGdon8e-ZuX03i0J7S7kWDXglH0gX6jdpEPe0TrxNrwXI-_pxGchznb5blUywDP_uzp1n3XXQE28V-eBZok1
&I_B_A_N=DEXXX
&SpeBesNum=11111
&btnSubmit_IBAN=Anmeldung

Eine positive Rückmeldung des Servers erfolgt ausschließlich, wenn sowohl eine Richtige IBAN als auch eine korrekte Sperrbestätigungsnummer eingegeben wird.

Die Länge bei fehlerhafter IBAN & Sperrbestätigungsnummer beträgt: 800

Die Länge bei korrekter IBAN & Sperrbestätigungsnummer beträgt: 780

Abschließend gleichen die Schritte zur Entsperrung den Schritten aus dem Fund zuvor.

4.1.10.2 Empfehlung

Neben der Sperrbestätigungsnummer sollten auch Anfragen bzgl. der IBAN, Kontonummer oder BLZ zu einer Begrenzung mittels Rate-Limiting führen. Anfragen an Server und Backendsysteme sollten grundsätzlich stark limitiert werden (Einsatz von sogenanntem Rate Limiting), um Bruteforcing zu erschweren.

Rate Limiting ist eine Technik, die in der Informatik verwendet wird, um die Anzahl der Anfragen oder Aktionen, die von einem Benutzer oder einer Anwendung in einem bestimmten Zeitraum durchgeführt werden können, zu begrenzen. Dies wird oft eingesetzt, um die Serverinfrastruktur vor Überlastung und Missbrauch zu schützen. Es gibt verschiedene Arten von Rate Limiting, die je nach Anwendungsfall unterschiedlich konfiguriert werden können. Dies sind einige gängige Arten:

- Anfragerate-Limiting: Begrenzt die Anzahl der Anfragen, die ein Benutzer oder eine Anwendung pro Zeiteinheit stellen kann. Dies hilft, vor zu vielen gleichzeitigen Anfragen zu schützen.
- IP-basiertes Rate Limiting: Begrenzt die Anzahl der Anfragen, die von einer bestimmten IP-Adresse in einem bestimmten Zeitraum durchgeführt werden können. Dies kann dazu beitragen, DDoS-Angriffe (Distributed Denial of Service) abzuschwächen.
- Token-Bucket Rate Limiting: Basierend auf dem Token-Bucket-Algorithmus, bei dem Tokens in einem "Eimer" gesammelt werden. Jede Anfrage benötigt eine bestimmte Anzahl von Tokens. Wenn der Eimer leer ist, werden keine weiteren Anfragen akzeptiert, bis neue Tokens hinzugefügt werden.
- Concurrency Rate Limiting: Begrenzt die gleichzeitige Anzahl von Verbindungen oder Operationen, die eine Anwendung durchführen kann.

Rate Limiting ist wichtig, um sicherzustellen, dass Ressourcen effizient genutzt werden, die Systemleistung stabil bleibt und um vor bösartigen Aktivitäten oder unbeabsichtigtem Missbrauch zu schützen. Es wird häufig in Webanwendungen, APIs (Application Programming Interfaces) und anderen verteilten Systemen eingesetzt.

In diesem Szenario wäre zwar bereits das Ausprobieren des Sperrbestätigungscodes ausreichend, um den Angriff zu verhindern – es sollte jedoch ein umfassendes Threat Modell und limitierendes Rate-Limiting eingeführt werden (für alle Parameter und Felder).

4.2 Funde im Bereich Datenschutz

Nachfolgend werden Funde im Bereich des Datenschutzes beschrieben.

4.2.1 Nutzung von Google Fonts unmittelbar nach Aufruf der Webseite

Klasse	Datenschutz
Auswirkung	Hoch

Die Webseite „kuno-sperrdienst.de“ hat sogenannte Google Fonts eingebunden[26]. Dabei handelt es sich um Schriftart-Dateien, welche von einem Server des Unternehmen Google (Alphabet Inc.) geladen werden. Bei Abruf dieser Schriftarten werden Nutzerdaten, darunter auch die IP-Adresse, an Google übertragen. Nach dem Urteil des Landgericht München I, Urteil vom 20.01.2022, Az. 3 O 17493/20 stellt dies (ohne Einwilligung) einen Verstoß gegen die Datenschutzgrundverordnung (DSGVO) dar[27]. Es liegt keine Rechtmäßigkeit der Verarbeitung vor (vgl. Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung).

4.2.1.1 Technische Details / Nachweise

Bei Abruf der Startseite kuno-sperrdienst.de lässt sich im Netzwerkverkehr und dem Quellcode der geladenen Seite die Einbettung von Schriftarten der URL googleapis.com vernehmen. Diese Beobachtung kann auch über entsprechende Analyse-Tools gemacht werden: https://webbkoll.dataskydd.net/en/results?url=http%3A%2F%2Fkuno-sperrdienst.de%2F

Auf der Webseite werden folgende Ressourcen eingebunden und bei Abruf geladen:
https://fonts.googleapis.com/css?family=Signika+Negative&display=swap
https://fonts.googleapis.com/css?family=Open+Sans:400,300,500,600,700

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
[...]

<!DOCTYPE html>
<html lang="en">
<head>
  <!-- Title -->
  <title>Willkommen bei KUNO Sperrdienst - Eine Initiative von EHI, HDE und ProPK</title>

  <!-- Required Meta Tags Always Come First -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
  <meta http-equiv="x-ua-compatible" content="ie=edge">
  <link href="https://fonts.googleapis.com/css?family=Signika+Negative&display=swap" rel="stylesheet">
  <!-- Favicon -->
  <link rel="shortcut icon" href="/favicon_512x512.png">

  <!-- Google Fonts -->
  <link rel="stylesheet" href="//fonts.googleapis.com/css?family=Open+Sans%3A400%2C300%2C500%2C600%2C700">

[...]
</head>
<body>
[..]
```

4.2.1.2 Empfehlung

Die Nutzung von Google Fonts sollte unterbunden werden, etwa indem eine lokale Einbettung von Schriftarten auf dem Webserver erfolgt, in diesem Fall fließen keine Daten mehr an Google. Alternativ ist eine Einbettung von Google Fonts denkbar, es sollte vor dem Laden der Schriftarten allerdings eine freiwillige, spezifische und informierte Einwilligung der betroffenen Person vorliegen, da ansonsten Google IP-Adressen übermittelt werden, welche als personenbezogenen bzw. -beziehbaren Daten zu betrachten sind.

---

[26] Das Verhalten liegt mindestes seit 2020 vor, wie dem Quelltext aus dem Internetarchiv entnehmbar ist: https://web.archive.org/web/20200510225351/https://kuno-sperrdienst.de/

[27] https://rewis.io/urteile/urteil/lhm-20-01-2022-3-o-1749320/

4.2.2 Cookie Banner fehlerhaft implementiert: Keine Einwilligung vor Laden der Google Fonts & fehlende Möglichkeit des Widerrufs

Klasse	Datenschutz
Auswirkung	Hoch

Auf der Webseite kuno-sperrdienst.de werden Google Fonts geladen. Auf der Webseite werden folgende Ressourcen eingebunden und bei Abruf unmittelbar geladen (siehe letzten Fund):

https://fonts.googleapis.com/css?family=Signika+Negative&display=swap
https://fonts.googleapis.com/css?family=Open+Sans:400,300,500,600,700

Das Cookie Banner hat keinen Einfluss auf das Laden der Schriftarten (es erfolgt somit ohne Einwilligung). Darüber hinaus ist nach einem Klick auf „OK“ kein Widerruf der Cookie-Einstellung möglich.

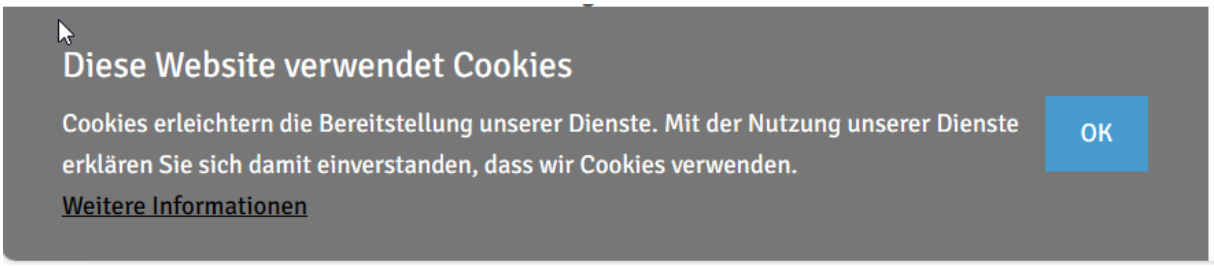


Abbildung 16: Screenshot des eingesetzen Cookie Banners auf kuno-sperrdienst.de

4.2.2.1 Technische Details / Nachweise

Das Laden der Dateien vom Google Server erfolgt unmittelbar nach Abruf der Startseite:

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
[…]

<!DOCTYPE html>
<html lang="en">
<head>
  <!-- Title -->
  <title>Willkommen bei KUNO Sperrdienst - Eine Initiative von EHI, HDE und ProPK</title>

  <!-- Required Meta Tags Always Come First -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
  <meta http-equiv="x-ua-compatible" content="ie=edge">
  <link href="https://fonts.googleapis.com/css?family=Signika+Negative&display=swap" rel="stylesheet">
  <!-- Favicon -->
  <link rel="shortcut icon" href="/favicon_512x512.png">

  <!-- Google Fonts -->
  <link rel="stylesheet" href="//fonts.googleapis.com/css?family=Open+Sans%3A400%2C300%2C500%2C600%2C700">

  <!-- CSS Global Compulsory -->
  <link rel="stylesheet" href="/requirements/css/bootstrap/bootstrap.min.css">
```

Bei dem verwendeten Cookie-Banner handelt es sich um ein Script des Github Nutzers „bavington“[28], welches dieses bereits 2014 (vor dem Inkrafttreten der DSGVO) veröffentlicht hat.

```
HTTP Request
GET / requirements/js/eu-cookie-banner.js
Host: www.kuno-sperrdienst.de
[…]
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

[28] https://gist.github.com/bavington/6727776

```
Priority: u=0, i

HTTP Response
HTTP/2 200 OK
[...]
// Creare's 'Implied Consent' EU Cookie Law Banner v:2.4
// Conceived by Robert Kent, James Bavington & Tom Foyster
// Put into a namespace and by BjÃ¸rn 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;
[...]
```

Ein Nutzer der Plattform Github hat in einem Kommentar zu der JavaScript Bibliothek bereits 2019 angemerkt, dass die Implementierung nicht mit der Datenschutzgrundverordnung vereinbar ist[29].

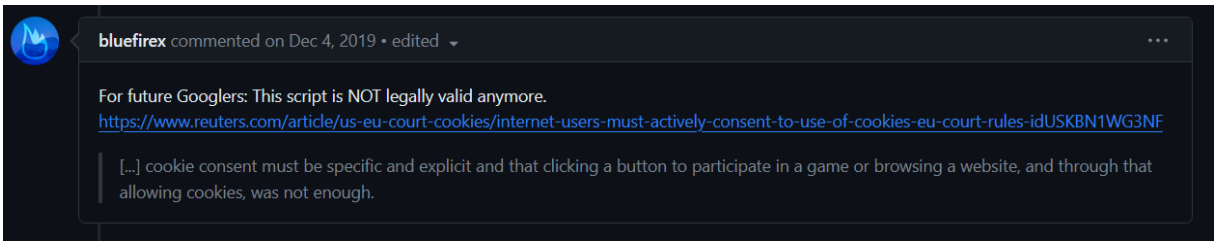


Abbildung 17: Kommentar in Github zu dem JavaScript Code

Der Kommentar verweist unter anderem auf folgenden Reuters Artikel in dem ausführlicher beschrieben wird, was bei dem Setzen von Cookies zu beachten ist: https://www.reuters.com/article/us-eu-court-cookies/internet-users-must-actively-consent-to-use-of-cookies-eu-court-rules-idUSKBN1WG3NF

4.2.2.2 Empfehlung

Das Cookie Banner sollte mit den Funktionen der Webseite verknüpft werden (es darf kein Laden von Drittressourcen ohne Einwilligung der Nutzenden bzw. vor Klick auf „OK“ geben).
Darüber hinaus ist eine Möglichkeit des Wiederrufs zu gewähren (etwa indem die Cookie-Einstellungen in einem Datenschutzbereich angepasst werden können).
Zudem sollte regelmäßig die Ordnungsmäßigkeit der Webseite validiert werden (werden tatsächlich alle Drittressourcen vom Cookie-Banner berücksichtigt und innerhalb der Datenschutzbestimmungen ausgewiesen).
Eine Einwilligung in Bezug auf das Cookie Banner sollte zudem freiwillig, informiert, spezifisch und eindeutig sein, um den Anforderungen der DSGVO Rechnung zu tragen.

[29] https://gist.github.com/bavington/6727776?permalink_comment_id=3100419#gistcomment-3100419

4.2.3 Keine Erwähnung der Google Fonts in den Datenschutzbestimmungen

Klasse	Datenschutz
Auswirkung	Hoch

Die angeführten Google Fonts werden nicht in den Datenschutzbestimmungen erwähnt, womit der Informationspflicht an Nutzende nicht nachgekommen wird (vgl. Art. 13 DSGVO Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person).

Siehe Datenschutzbestimmungen: https://kuno-sperrdienst.de/Home/displayDataProtection

Siehe archivierte Version: https://web.archive.org/web/20231113155108/https://kuno-sperrdienst.de/Home/displayDataProtection

4.2.3.1 Empfehlung

Sofern die entsprechenden Schriftarten von Google (siehe Befunde zuvor) weiterhin extern eingebunden und zum Einsatz kommen sollen, ist es wichtig darüber in den Datenschutzbestimmungen aufzuklären.

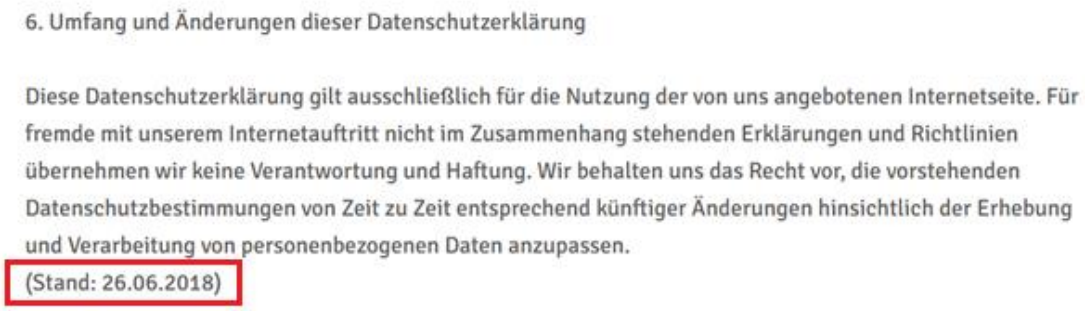
4.2.4 Datenschutzerklärung laut Webseite von 2018 und teilweise veraltet

Klasse	Datenschutz
Auswirkung	Mittel

Die Datenschutzerklärung der Webseite kuno-sperrdienst.de[30] ist vom 26.06.2018. Dies ist 32 Tage nach dem Geltungsbeginn der Datenschutzgrundverordnung (DSGVO). Seit dem 26.06.2018 wurde die Datenschutzbestimmung offenbar nicht mehr angepasst.

Siehe Datenschutzbestimmungen: https://kuno-sperrdienst.de/Home/displayDataProtection

Siehe archivierte Version (November 2023):
https://web.archive.org/web/20231113155108/https://kuno-sperrdienst.de/Home/displayDataProtection



6. Umfang und Änderungen dieser Datenschutzerklärung

Diese Datenschutzerklärung gilt ausschließlich für die Nutzung der von uns angebotenen Internetseite. Für fremde mit unserem Internetauftritt nicht im Zusammenhang stehenden Erklärungen und Richtlinien übernehmen wir keine Verantwortung und Haftung. Wir behalten uns das Recht vor, die vorstehenden Datenschutzbestimmungen von Zeit zu Zeit entsprechend künftiger Änderungen hinsichtlich der Erhebung und Verarbeitung von personenbezogenen Daten anzupassen.

(Stand: 26.06.2018)

Abbildung 18: Auszug aus der Datenschutzerklärung (inkl. Datum zum Stand)

4.2.4.1 Empfehlung

Die Datenschutzerklärung sollte aktualisiert und gemäß aktuellem Recht angepasst werden. Die Erklärung zu Cookies ist recht kurz. Es könnte nützlich sein, mehr Details darüber zu geben, welche Arten von Cookies verwendet werden, zu welchem Zweck und wie Benutzer die Verwendung von Cookies steuern können (siehe Fund zu Google Fonts). Es empfiehlt sich die Datenschutzerklärung umfassend zu bearbeiten und durch einen Rechtsanwalt im Bereich Datenschutz zu prüfen.

[30] https://kuno-sperrdienst.de/Home/displayDataProtection