HSA_innos
Institut für innovative Sicherheit

Technologie-transferzentrum Data Analytics

Hochschule Augsburg University of Applied Sciences

# ALARM! Oder doch nicht? So sicher sind Funk-Alarmanlagen zum Selbsteinbau

**Eine Studie des Instituts für innovative Sicherheit (HSA_innos) und des Technologietransferzentrums (TTZ) Data Analytics der Technischen Hochschule Augsburg.**

HSA_innos
Institut für innovative
Sicherheit

Technologie-
transferzentrum
Data Analytics

Hochschule
Augsburg University of
Applied Sciences

Die beiden Forschungsinstitute HSA_innos
und TTZ Data Analytics arbeiten für den Transfer
von wissenschaftlichen Erkenntnissen
in die gesellschaftliche und wirtschaftliche Praxis.
Sie sind Teil der Technischen Hochschule Augsburg.
Die folgende Studie ist in enger Zusammenarbeit
beider Institute entstanden.

Autor: Florian Ernst
Betreuer: Prof. Dr. Dominik Merli

# Über das Institut für innovative Sicherheit (HSA_innos)

HSA_innos unterstützt Organisationen aller Größen dabei, sicher und erfolgreich in einer vernetzten Welt zu agieren. Durch die innovativen Ansätze des Instituts werden Systeme, Produkte und Personal widerstandsfähig gegenüber digitalen Bedrohungen von Wirtschaft und Gesellschaft. Hierzu bildet HSA_innos Sicherheitsexpert:innen aus, entwickelt angewandte Technologien und Prozesse für die IT-Sicherheit und schafft Sicherheitsbewusstsein in der Gesellschaft.

**www.hsainnos.de**

**HSA_innos**
Institut für innovative
Sicherheit

# Über das Technologie-transferzentrum (TTZ) Data Analytics in Donauwörth

Das TTZ Data Analytics macht das Potenzial von Daten und Digitalisierung für Unternehmen nutzbar. Forschung und Industrie entwickeln gemeinsam datenbasierte Lösungen und Konzepte zur sicheren und digitalen Wertschöpfung. Im Donau-Ries entstehen so Innovationen – nicht nur für den Landkreis, sondern den gesamten Freistaat Bayern.

**www.ttz-data-analytics.de**

Technologie-
transferzentrum
Data Analytics

# Inhaltsverzeichnis

# Vorwort

Das drahtlose Übertragen von Informationen gibt es nun schon seit mehr als 125 Jahren. Nikola Tesla, ein bekannter Erfinder auf dem Gebiet der Elektrotechnik, steuerte bereits Ende des 19. Jahrhunderts ein Modellboot per Funk. Seit der Erfindung der Halbleitertechnik in den 1960er-Jahren werden batteriebetriebene Sender und Empfänger für unzählige Fernsteuerungen eingesetzt. Mittlerweile sind elektronische Sende- und Empfangsmodule sehr klein und preiswert. Sie werden dort genutzt, wo Verbindungen per Kabel nicht gewünscht oder sehr aufwendig sind: zum Beispiel in Wetterstationen, ferngesteuerten Drohnen oder Autoschlüsseln.
Doch neben dem Komfort und der Möglichkeit zur Datenübertragung birgt die Funk-Technologie auch Risiken. Denn je nach technischem Aufbau des Senders und den Gegebenheiten in der Umgebung kann die Reichweite der gesendeten Signale von wenigen Metern bis zu mehreren Kilometern variieren.
Kriminelle können so unentdeckt aus großer Entfernung die Übertragungen abhören und aufzeichnen, die gesendeten Daten dekodieren, Störungen erzeugen oder sogar aktiv in die Funk-Kommunikation eingreifen.

Aufgrund dieser Gefahren sollte die Sicherheit der Datenübertragung gegenüber Angriffen ein zentrales Anliegen der Hersteller von Funk-Lösungen sein.
Die IT-Sicherheit bietet zahlreiche Maßnahmen mit unterschiedlichen Zielen, um genau solche Angriffe zu verhindern. Beispielsweise lassen sich Daten verschlüsseln, um sie für Dritte unlesbar zu machen (Vertraulichkeit). Oder man lässt sich über digitale Signaturen bestätigen, dass es sich um einen legitimen Sender (Authentizität) mit einer unversehrten Nachricht (Integrität) handelt. Allerdings sind diese Schutzmechanismen auch in aktuellen Produkten mit Funksteuerung nicht immer vorhanden, wie aktuelle Studien und Schwachstellenmeldungen zeigen [1].
Dies ist besonders bedenklich, da Störsender mittlerweile zum Beispiel bei Amazon, AliExpress und ähnlichen Marktplätzen günstig und leicht erhältlich sind.
Die vorliegende Studie betrachtet, inwieweit Funk-Alarmanlagen für den privaten Gebrauch gegen funkbasierte Angriffe geschützt sind. Dies erfolgt anhand von fünf auf dem Markt erhältlichen Produkten.

# Ausgangslage

Funkgeräte mit integriertem Sender und Empfänger waren lange Zeit komplexe, kostspielige und unhandliche Geräte. Nur eine kleine Gruppe von Expert:innen hatte Zugang zu diesen Geräten und die Bedienung erforderte fundiertes und umfangreiches Fachwissen. Seit einigen Jahren gelten jedoch kleine Software Defined Radios (SDRs) als aktueller Stand der Technik. Das eigentliche „Funkgerät“ besteht dabei oft nur noch aus einem einzigen Mikrochip. Die zur Steuerung notwendige Software ist zumeist frei und offen verfügbar sowie durch Anleitungen, Erklärungen und Foren gut dokumentiert.

### Günstig und funktional: SDRs

SDRs sind preiswert und ermöglichen es, analoge und digitale Signale per Funk sowohl zu senden als auch zu empfangen. Sie eignen sich daher hervorragend, um unbekannte Signale in einem großen Frequenzbereich zu erkennen, aufzuzeichnen und auszusenden. Allerdings ist die Sendeleistung von SDRs mit zirka einem Milliwatt sehr gering, für Angriffe unter Laborbedingungen aber absolut ausreichend. Um SDRs für echte Angriffe zu nutzen, sind zusätzliche Verstärker erforderlich, die jedoch einfach zu beschaffen sind.

### Viel Leistung und Reichweite: fertige Störsender

Ganz anders sieht es bei Störsendern, sogenannten *Jammern*, aus. Diese sind bereits für unter 200 Euro für verschiedene Frequenzbereiche und mit sehr hoher Sendeleistung erhältlich. Sie ermöglichen auch Kriminellen ohne Vorwissen, Funkübertragungen über Entfernungen von bis zu 100 Metern zu stören. In der vorliegenden Studie wurden derartige Störsender nicht verwendet. Allerdings unterstreicht die Tatsache, dass Störsender mit hoher Sendeleistung einfach zu beschaffen sind die Notwendigkeit von Gegenmaßnahmen umso mehr.

# Grundlagen von Funk-Alarmanlagen

Alarmanlagen im professionellen Bereich unterscheiden sich hinsichtlich der an sie gestellten Anforderungen stark von solchen für die private Nutzung.

Professionelle Alarmanlagen werden verwendet, um Gebäude oder Anlagen mit hohem Wert zu schützen. Dazu gehören zum Beispiel Museen, Banken oder Industrieanlagen. Speziell geschultes Fachpersonal übernimmt hier die Installation. Denn diese ist oft mit hohem technischem Aufwand verbunden, weil beispielsweise Kabel verlegt werden müssen. Falls derartige Alarmanlagen dennoch eine Funk-Verbindung zu den Sensoren verwenden, können sie nach der Norm DIN EN 50131-5-3:2017 zertifiziert werden. Diese definiert, welche Störungen die Anlage erkennen und melden muss. Eine solche professionelle Alarmanlage ist jedoch sehr kostenintensiv und für private Anwender:innen daher nur selten geeignet.

## Funk-Alarmanlagen für die private Nutzung

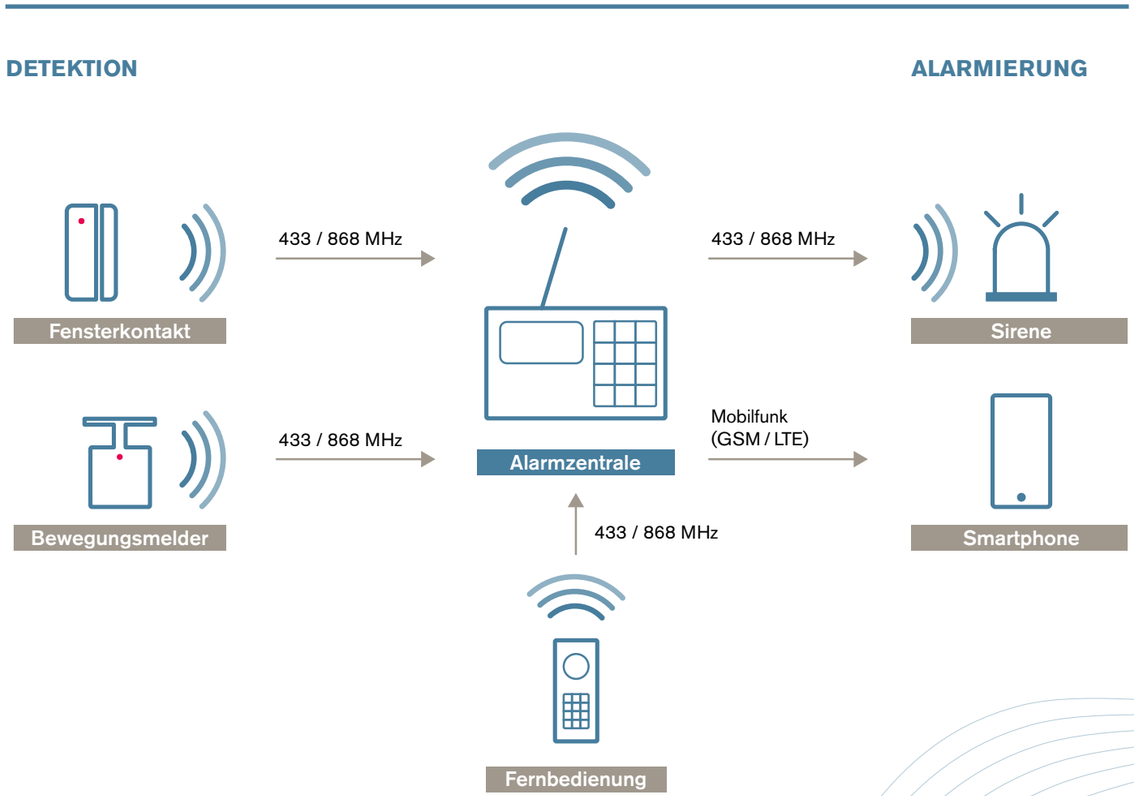
Für private Anwender:innen gibt es ein entsprechend auf ihre Bedürfnisse angepasstes Angebot an Alarmanlagen. Diese sollen zum Beispiel die eigene Wohnung oder eine Gartenlaube schützen. Erkennt die Anlage einen Einbruch, löst sie auf Wunsch einen akustischen Alarm aus, um die Einbrechenden von ihrem Vorhaben abzubringen. Zudem ist auch ein stiller Alarm möglich. In jedem Fall soll die Alarmanlage ihre Besitzer:innen über den Einbruchsversuch informieren und eine Benachrichtigung zum Beispiel über das Mobilfunknetz an eine Smartphone-App schicken.

Die Alarmzentrale selbst ist meist über Funk mit Sensoren wie Fensterkontakten, Bewegungs- oder Rauchmeldern verbunden (siehe Abb. 1). Denn gerade im privaten Bereich ist es meist nicht erwünscht, Kabel zu verlegen. Dabei können bewährte Funk-Standards, zum Beispiel WLAN, ZigBee oder Bluetooth, zum Einsatz kommen. Richtig konfiguriert verfügen sie über integrierte Funktionen zur Verschlüsselung, Authentifizierung und zum Manipulationsschutz.

## Beliebt: 433 und 868 MHz

Einfache und preiswerte Funkmodule sind eine Alternative hierzu. Diese müssen eine ausreichende Reichweite bieten und auf allgemein zugelassenen, lizenz- und gebührenfreien Frequenzen arbeiten. Meist werden dafür die Frequenzen 433 MHz oder 868 MHz genutzt. Bei der Verwendung dieser Module muss der Hersteller ein eigenes Protokoll für die Übertragung definieren. Allerdings liegt es damit in der Verantwortung des Herstellers, die Funkübertragung gegen Angriffe abzusichern.

Die vorliegende Studie testet ausschließlich Geräte, die derartige einfache Funkmodule verwenden. Sie unterliegen allerdings ausdrücklich nicht der DIN-Norm für professionelle Anlagen. Die durchgeführten Tests lehnen sich jedoch bezüglich Art und Dauer der Störsignale teilweise an diese Norm an, um Vergleichbarkeit zu schaffen. Die Analyse soll herauszufinden, ob Funk-Alarmanlagen für den privaten Gebrauch einfache oder gegebenenfalls sogar ausgefeiltere Funk-Angriffe erkennen können. Oder: ob diesen Produkten solche Schutzmechanismen gänzlich fehlen und sie damit private Anwender:innen einem gewissen Risiko aussetzen.




**1** Abbildung: Der grundlegende Aufbau einer Funk-Alarmanlage. Die Zentrale ist die Hauptschnittstelle für die einzelnen Komponenten. Quelle: Florian Ernst / Hochschule Augsburg

# Zum Test verwendete Hard- und Software

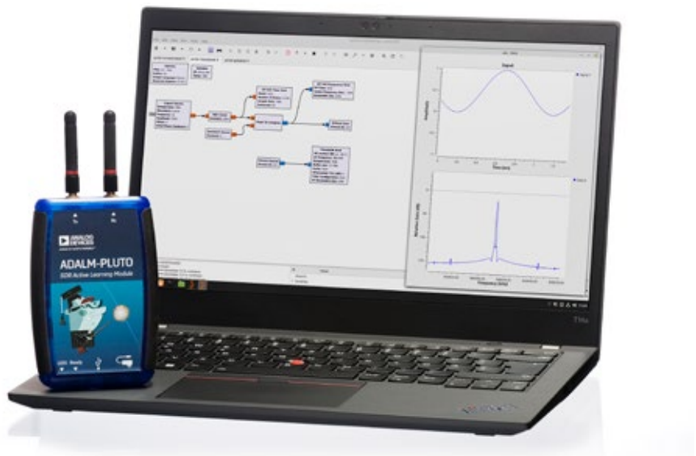
Um Funk-Alarmanlagen zu manipulieren, braucht es spezielle Hardware. Diese ist einfach und kostengünstig auf dem freien Markt erhältlich. Software und passende Anleitungen sind frei im Internet verfügbar.

Für die vorliegende Studie wurden handelsübliche SDR-Hardware und -Software beschafft, um einen tieferen Einblick in die von den Herstellern verwendeten Protokolle zur Datenübertragung zu gewinnen. Die oben genannten Störsender *(Jammer)* wurden nicht verwendet. Aufgrund der technischen Gegebenheiten ist allerdings davon auszugehen, dass die Verwendung solcher Störsender unter denselben Voraussetzungen zu ähnlichen Ergebnissen führt. Alles, was im Test als Störsender bezeichnet wird, basiert auf der hier beschriebenen Hard- und Software. Es handelt sich ausdrücklich nicht um Störsender als Komplettlösungen.

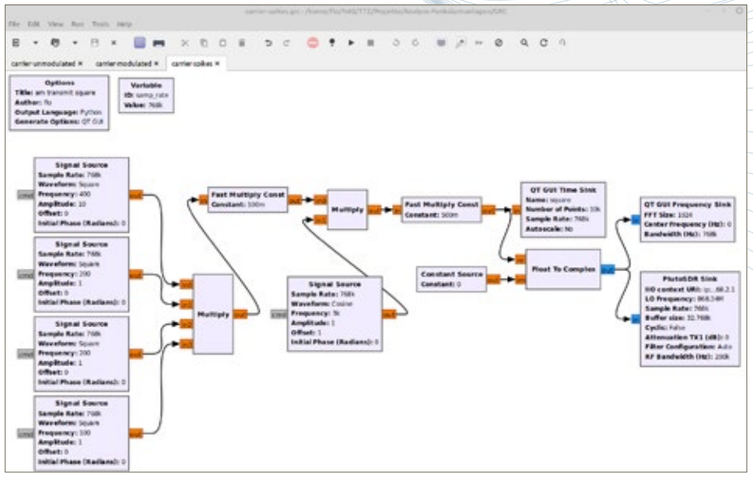
Als SDR wurde ein Adalm-Pluto Rev. C [2] des Herstellers AnalogDevices verwendet (siehe Abb. 2). Dieses preiswerte (ca. 300 Euro, Stand 01/2023) und sehr handliche Gerät ermöglicht den Empfang und das Senden beliebiger Signale zwischen 70 MHz und 6 GHz. Zur Steuerung des Adalm-Pluto ist lediglich ein gewöhnlicher PC mit USB-Schnittstelle notwendig.

Die Erzeugung und Aussendung protokoll-unabhängiger Störungen geschah mittels „GNU RADIO“ [3] (siehe Abb. 4). Dies ist ein freies Programmierwerkzeug, das beliebige Formen von Signalen erzeugen und zum Senden bereitstellen kann.

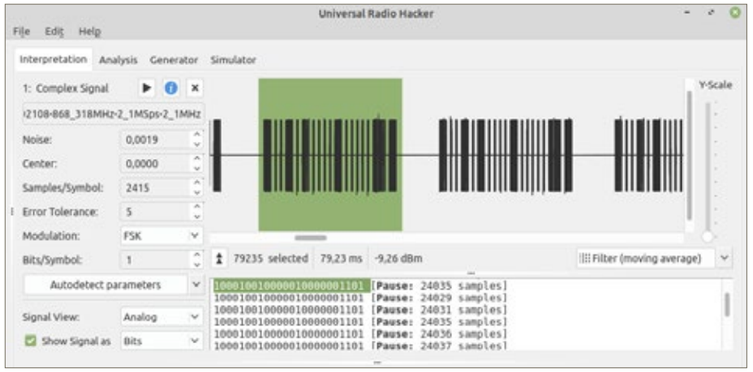
Zum Aufzeichnen, Dekodieren, Manipulieren und Aussenden von Meldungen wurde die Software „Universal Radio Hacker“ [4] verwendet (siehe Abb. 4). Dieses frei verfügbare Programm ist einfach bedienbar. Zudem ermöglicht es die verwendeten Protokolle einer Anlage innerhalb kurzer Zeit zu analysieren.




**2** Abbildung: Die verwendete Hardware:
Ein Adalm-Pluto und ein gewöhnliches Notebook.
Bild: Florian Ernst / Hochschule Augsburg.




**3** Abbildung: Die verwendete Software:
das Programm „GNU Radio“. Bild: Screenshot.
Quelle: Florian Ernst / Hochschule Augsburg




**4** Abbildung: „Universal Radio Hacker“ mit dekodierter Meldung eines Sensors. Bild: Screenshot.
Quelle: Florian Ernst / Hochschule Augsburg

# Szenarien und Testablauf

Es wurden drei realistische Szenarien für Einbrüche mit verschiedenen Zielen, Vorgehensweisen und Schwierigkeitsgraden erstellt. Alle nutzen die Funk-Kommunikation der Alarmanlagen aus, um den Einbruch zu verbergen.

### Szenario 1: Einbruch bei scharf geschalteter Alarmanlage

Ziel ist es, den Alarm beim Einbruch nicht auszulösen. Hierzu versenden die Kriminellen Störsignale, damit die Zentrale die Meldungen der Sensoren wie zum Beispiel das Öffnen eines Tür- oder Fensterkontakts nicht mehr auswerten kann. Der Schwierigkeitsgrad variiert hier je nach verwendeter Methode. Wird ein fertiger Störsender *(Jammer)* verwendet, braucht es wenig Know-how und der Vorgang ist damit einfach. Soll die Manipulation über die Protokoll-Ebene stattfinden, wird spezielles Wissen benötigt und der Vorgang ist damit als eher schwierig einzustufen.

In Szenario 1 wurden vier Varianten in den Schwierigkeitsgraden leicht, mittel und schwer getestet, die sich in den ausgesendeten Störsignalen unterscheiden:

- Unmodulierte Trägerfrequenz (Schwierigkeitsgrad: leicht)
- Einfache, amplitudenmodulierte Trägerfrequenz (Schwierigkeitsgrad: leicht)
- Kurze, nadelförmige, amplitudenmodulierte Impulse (Schwierigkeitsgrad: mittel)
- Manipulierte Originalmeldung: ein Datenpaket wurde aufgezeichnet und ohne Pause ausgesendet (Schwierigkeitsgrad: schwer)

Diese Störsignale wurden jeweils für mindestens 30 Sekunden ausgesendet. Dabei sind zwei Ergebnisse möglich:

✓ Die Alarmanlage erkennt den Angriff. Alarm wird ausgelöst und die Besitzer:innen werden informiert.

✗ Die Alarmanlage erkennt den Angriff nicht. Der Alarm wird nicht ausgelöst und der Einbruchsversuch bleibt unbemerkt.

### Szenario 2: Kriminelle übernehmen die Steuerung der Anlage

Ziel der Einbrechenden ist es in diesem Fall, die Anlage unscharf zu schalten. Hierfür zeichnen die Kriminellen die Signale der Fernbedienung auf, während der oder die Besitzer:in die Anlage per Fernbedienung unscharf schaltet. Zu einem späteren Zeitpunkt senden sie die unveränderten Signale erneut aus, um die Alarmanlage zu deaktivieren. Die Kriminellen müssen hierzu über längere Zeit in der Nähe der Anlage sein und gute SDR-Kenntnisse besitzen. Die Methode liegt damit im mittleren Schwierigkeitsgrad.

Für diesen Test wurde in der Studie die Originalmeldung der Fernbedienung mit der Anweisung „unscharf schalten“ aufgezeichnet. Nach der Aktivierung der Anlage wurde die aufgezeichnete Meldung unverändert vom Störsender ausgesendet. Dies kann zu zwei möglichen Ergebnissen führen:

✓ Die Anlage bleibt im Zustand „scharf“ und die Meldung wird entweder vollständig ignoriert oder als Angriffsversuch erkannt und von der Anlage als Manipulationsversuch gemeldet.

✗ Die Anlage wechselt in den Zustand „unscharf“ und löst damit bei einem nachfolgenden Einbruchsversuch keinen Alarm aus.

### Szenario 3: Manipulation am Menschen

Ziel dieses Szenarios ist, die Besitzer:innen dazu zu bringen, die Alarmanlage selbst abzuschalten oder Alarm-Meldungen zu ignorieren. Hierzu lösen Kriminelle absichtlich und wiederholt Fehlalarme und technische Warnmeldungen aus. Die Besitzer:innen gehen dann von einem Defekt der Anlage aus. Sie sollen dadurch die Zuverlässigkeit der Anlage bezweifeln und nicht mehr auf Meldungen reagieren oder die Anlage selbst abschalten. Dieses Vorgehen benötigt spezielles Wissen und technisches Know-how zur Manipulation auf der Protokoll-Ebene des Gerätes. Deswegen ist der Schwierigkeitsgrad als schwer zu bewerten.

Für diesen Test wurden die Originalmeldung des Fensterkontakts mit der Information „Fensterkontakt geht auf“ aufgezeichnet. Diese wurde unverändert vom Störsender ausgesendet, während die Zentrale scharf geschaltet war. Dabei wurde beobachtet, ob die Zentrale dadurch einen Alarm auslöst. Ein Teil der überprüften Alarmanlagen bietet zudem die Funktion, eine zu geringe Batterieladung der Sensoren zu melden. Bei diesen Geräten wurde im Test versucht, die Zentrale zur Ausgabe einer Warnmeldung zu bringen, indem eine vorher aufgezeichnete Meldung „Batterie schwach“ eines Fensterkontakts ausgesendet wurde.

Beide Meldungen haben jeweils zwei mögliche Ergebnisse:

✓ Die Anlage erkennt die Manipulation und meldet diese.

✗ Die Manipulation wird nicht erkannt. Die Besitzer:innen werden informiert, obwohl weder ein Einbruchsversuch vorliegt noch ein Batteriewechsel nötig ist.

# Getestete Geräte

Es wurden fünf Alarmanlagen mit Funksteuerung getestet, die im ersten Quartal 2022 erhältlich waren.

In der Studie wurden die auf dieser Doppelseite dargestellten Funk-Alarmanlagen erworben und den beschriebenen Tests unterzogen. Maßgeblich für die Auswahl der Funk-Alarmanlagen waren folgende Kriterien:

- Sie liegen in etwa im gleichen Preissegment.
- Sie sind laut Hersteller ausschließlich für den Schutz geringer Sachwerte geeignet.
- Sie unterliegen nicht der Norm DIN EN 50131-5-3:2017 für professionelle Geräte.
- Sie verwenden als Funk-Frequenzen entweder 433 MHz oder 868 MHz.
- Sie waren alle auf dem freien Markt als Neuware erhältlich (auch wenn sie zum Kaufdatum teils nicht mehr hergestellt wurden).


**Blaupunkt**
**SA 2900-R**
**179 €**
**Mitgeliefertes Zubehör:**
**1x Fernbedienung, 1x Fensterkontakt, 1x Bewegungsmelder**

**BurgWächter**
**BurgProtect 2210**
**266 €**
**Mitgeliefertes Zubehör:**
**1x Fernbedienung, 2x Fensterkontakt, 1x Bewegungsmelder**

**Abus**
**SMARTVEST**
**229 €**
**Mitgeliefertes Zubehör:**
**1x Fernbedienung, 2x Fensterkontakt, 1x Bewegungsmelder**

**Berghoch**
**Funk-Alarmanlage**
**420 €**
**Mitgeliefertes Zubehör:**
**2x Fernbedienung, 8x Fensterkontakt, 2x Bewegungsmelder, 1x Außensirene**


**Olympia**
**ProHome 8762**
**149 €**
**Mitgeliefertes Zubehör:**
**1x Fernbedienung, 4x Fensterkontakt, 1x Bewegungsmelder, 1x Schalt- / Messsteckdose**

# Ergebnisse der Untersuchung

Die Ergebnisse der einzelnen Anlagen sind hier anonymisiert dargestellt. Alle Hersteller wurden über die identifizierten Schwachstellen informiert.

Tabelle 1 zeigt, dass selbst bei geringem oder mittlerem Aufwand zur Erzeugung von Störsignalen nur eines der fünf Geräte in der Lage ist, den Jamming-Angriff zu erkennen und Besitzer:innen über die Störung der Funkfrequenz zu informieren. Bei hohem Aufwand zur Erzeugung des Störsignals erkennt auch diese Anlage den Angriff nicht.

Tabelle 2 zeigt, dass drei von fünf Anlagen den Replay der aufgezeichneten Meldung akzeptieren und die Anlage unscharf geschaltet haben. Die anderen beiden ignorierten die Nachricht, jedoch wurde kein Alarm ausgelöst und die Besitzer:innen wurde nicht über den Angriffsversuch informiert.

Tabelle 3 zeigt, dass alle getesteten Anlagen im scharfgeschalteten Zustand durch einen Replay der Sensor-Meldung „Fenster geht auf“ einen Alarm auslösten. Bei drei Anlagen konnte durch den Replay einer entsprechenden Meldung der Warnhinweis „Batterie schwach“ ausgelöst werden. Zwei Anlagen verfügten nicht über diese Funktion und konnten damit nicht überprüft werden.

Basierend auf diesen Ergebnissen wurden die entsprechenden Hersteller der Funk-Alarmanlagen vor Veröffentlichung der Studie mehrmals kontaktiert und detailliert über die gefundenen Schwachstellen informiert. Vier der fünf Hersteller haben daraufhin Kontakt zu den Testern aufgenommen. Drei Hersteller waren bereit, die Schwachstellen gemeinsam zu besprechen.

Ein Hersteller meldete sich trotz mehrmaliger Nachfragen zu den Schwachstellen nicht zurück. An der Anlage konnte das Fehlen eines auf der Website beworbenen Sicherheitsmerkmals nachgewiesen werden, das Angriffe nach Szenario 2 und 3 sehr wahrscheinlich verhindert hätte. Allerdings löschte der Hersteller, nachdem er aufgrund der vorliegenden Ergebnisse kontaktiert wurde, den Hinweis auf dieses Produkt-Feature auf der entsprechenden Internetseite.

### SZENARIO 1: WURDE JAMMING ERKANNT UND GEMELDET?

| ANLAGE | UNMODULIERTE TRÄGERFREQUENZ (LEICHT) | AMPLITUDEN-MODULIERTE TRÄGERFREQUENZ (LEICHT) | KURZE, AMPLITUDENMODULIERTE STÖRIMPULSE (MITTEL) | MANIPULIERTE ORIGINALMELDUNG (SCHWER) |
|---|---|---|---|---|
| A | ✓ | ✓ | ✓ | ✗ |
| B | ✗ | ✗ | ✗ | ✗ |
| C | ✗ | ✗ | ✗ | ✗ |
| D | ✗ | ✗ | ✗ | ✗ |
| E | ✗ | ✗ | ✗ | ✗ |

**1** Tabelle: Die Ergebnisse aus Szenario 1. Nur eines der Geräte erkennt die Angriffe mit Störsignalen.

### SZENARIO 2: WURDE DAS AUFGEZEICHNETE SIGNAL „UNSCHARF SCHALTEN“ DER FERNBEDIENUNG IGNORIERT ODER ALARM AUSGELÖST?

| ANLAGE | REPLAY ABGELEHNT |
|---|---|
| A | ✓ |
| B | ✓ |
| C | ✗ |
| D | ✗ |
| E | ✗ |

**2** Tabelle: Die Ergebnisse aus Szenario 2. Lediglich zwei Anlagen ignorieren die ausgesendete Nachricht.

### SZENARIO 3: WIRD EINE STÖRMELDUNG ALS MANIPULATION ERKANNT?

| ANLAGE | „FENSTER AUF“ | „BATTERIE SCHWACH“ |
|---|---|---|
| A | ✗ | (nicht ermittelbar) |
| B | ✗ | ✗ |
| C | ✗ | (nicht ermittelbar) |
| D | ✗ | ✗ |
| E | ✗ | ✗ |

**3** Tabelle: Die Ergebnisse aus Szenario 3. Alle Anlagen lösten Fehlalarme aus.

# Fazit

Günstige Funk-Alarmanlagen für den privaten Gebrauch sind zum Großteil nicht gegenüber Angriffen per Funk abgesichert. Hersteller sollten bei der Produktentwicklung darauf achten, dass sichere Verfahren oder moderne Funktechnologien zum Einsatz kommen.

Funk-Equipment wird immer preiswerter und immer häufiger in Consumer-Produkten eingesetzt. Dadurch werden Angriffe auf diesen Kommunikationskanal für Kriminelle immer interessanter. In dieser Studie wurde untersucht, ob günstige Funk-Alarmanlagen gegenüber solchen Angriffen abgesichert sind.

Um einen Überblick über den Markt zu erhalten, wurden fünf Funk-Alarmanlagen für private Anwender:innen mit ähnlichem Preis und Funktionsumfang analysiert. Alle Anlagen wurden ausschließlich mit Funk-Technik angegriffen und hinsichtlich ihrer Reaktionen getestet.

**Diese Szenarien wurden untersucht**

- Szenario 1:
  Kriminelle verhindern, dass ein Alarm ausgelöst wird, obwohl die Anlage scharf geschaltet ist.
- Szenario 2:
  Kriminelle können die Alarmanlage von außen unscharf schalten.
- Szenario 3:
  Kriminelle bringen die Besitzer:innen dazu, die Alarm-Meldungen zu ignorieren oder die Anlage selbst abzuschalten.

**Ergebnisse der Studie**

Vier der fünf Anlagen ermöglichen Einbrüche mit leichtem Schwierigkeitsgrad. Hierfür benötigen Einbrechende lediglich einen geringen technischen Aufwand und geringe bis mittlere technische Kenntnisse. Obwohl die Anlagen voll funktionsfähig und scharf geschaltet waren, konnten sie die Besitzer:innen nicht zuverlässig alarmieren.

Nur eine Anlage bietet grundsätzlich die Möglichkeit, Störsignale wie in Szenario 1 zu erkennen und die Besitzer:innen entsprechend zu informieren.

Zwei Hersteller haben die Kommunikation zwischen Fernbedienung und Zentrale geschützt und können Replay-Angriffe wie in Szenario 2 beschrieben zuverlässig verhindern. Allerdings setzt keines der untersuchten Produkte diese Schutzmaßnahmen auch zum Schutz der Kommunikation zwischen Sensoren und Zentrale ein, wie die Ergebnisse von Szenario 3 zeigen.

**Darauf sollte man beim Kauf achten**

Wer Interesse an solchen Funk-Alarmanlagen hat, sollte aufgrund dieser Ergebnisse folgende Punkte beachten:

- Die Anlagen sollten nur zum Schutz geringer Sachwerte eingesetzt werden. So wird es auch von den Herstellern der untersuchten Produkte angegeben. Denn ein größerer Sachwert rechtfertigt für Kriminelle den Mehraufwand, auf mehr Technik und Wissen zurückzugreifen.
- Gerade bei Funk-Alarmanlagen im privaten Sektor sollten sich Anwender:innen darüber bewusst sein, dass Funkverbindungen zwar die Installation des Alarmsystems erleichtern, zugleich aber auch eine große Angriffsfläche bieten.
- Funkprotokolle im 433 und 868 Mhz Bereich sollten zumindest grundlegende Schutzmaßnahmen gegen funkbasierte Angriffe aufweisen.
- Bewährte Technologien wie WLAN, ZigBee oder Bluetooth haben bereits integrierte Maßnahmen, die einen gewissen Schutz bieten können.
- Zum Schutz höherer Sachwerte sollte auf professionelle DIN-zertifizierte Anlagen zurückgegriffen werden. Denn diese bieten aufgrund ihres höheren technischen Standards mehr Sicherheit gegen funkbasierte Angriffe.

# Addendum: Wie gefährlich sind Funk-Jammer?

Kriminelle können fertige, kommerzielle Störsender ohne technisches Vorwissen nutzen. Sie sind einfach anwendbar und haben eine enorme Sendeleistung.

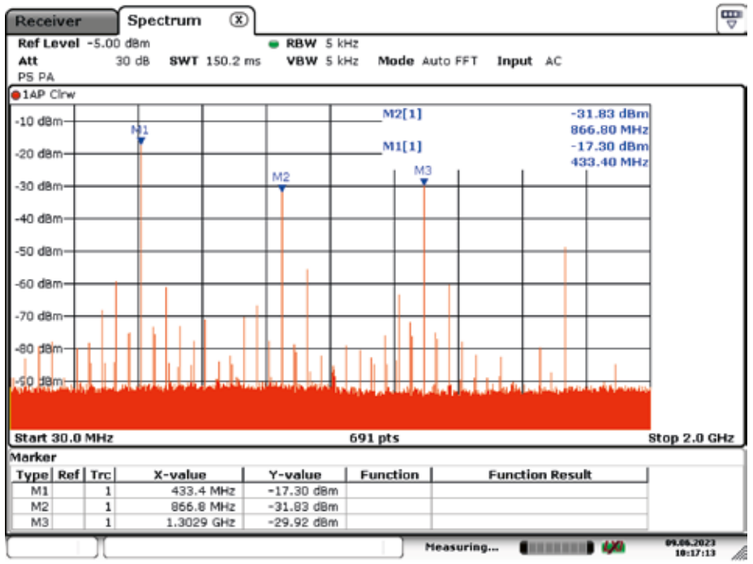
Die Studie „ALARM! Oder doch nicht? So sicher sind Funk-Alarmanlagen zum Selbsteinbau“ des Instituts für innovative Sicherheit (HSA_innos) und des Technologietransferzentrums Data Analytics untersuchte Funkangriffe mit Software Defined Radios (SDRs). Wollen Kriminelle diese für reale Angriffe auf Funk-Alarmanlagen nutzen, benötigen sie zumindest Knowhow und Verstärker. Anders sieht es bei kommerziellen Störsendern, sogenannten Jammern, aus. Sie sind günstig, für verschiedene Frequenzbereiche und mit sehr hoher Sendeleistung erhältlich. Fertige Störsender ermöglichen es Kriminellen auch ohne Vorwissen Funkübertragungen über Entfernungen von bis zu 100 Metern zu stören. Deshalb bewertet dieses Addendum zur ursprünglichen Studie die Gefahr, die von kommerziell angebotenen Störsendern ausgeht.

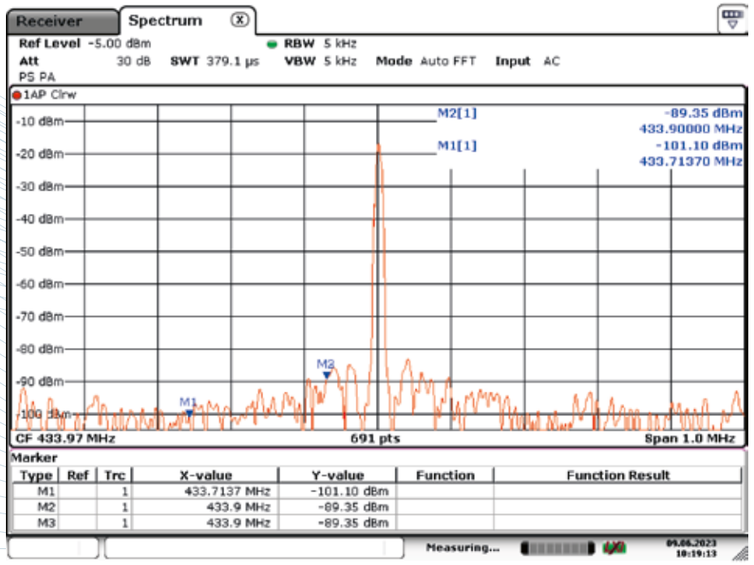
## Ziel und Vorgehensweise

Insgesamt wurden zehn Jammer untersucht. Sechs der Geräte zur Störung von 433 MHz Kommunikation wurden hierzu auf einem Online-Portal gekauft. Zudem stellte eine Bayerische Sicherheitsbehörde vier beschlagnahmte Geräte zu Forschungszwecken zur Verfügung. Diese blockieren zum Beispiel WLAN, GPS oder Bluetooth. Alle Geräte wurden zusammen mit dem Labor für Nachrichtenübertragungstechnik der Technischen Hochschule Augsburg vermessen. Anschließend konnte die davon ausgehende Gefahr bewertet werden.

Die Jammer 1 bis 6 wurden über ein 40dB-Dämpfungsglied an einen Spektrumanalysator angeschlossen und per Labornetzteil mit der angegebenen Betriebsspannung versorgt, um dann den Stromverbrauch ablesen zu können. Mit dem Spektrumanalysator wurde bei jedem Jammer eine Darstellung über einen großen Frequenzbereich erzeugt und die Sendeleistung gemessen (Abbildung 4, oben) sowie die Signalform im Bereich um 433 MHz dargestellt (Abbildung 4, unten).

Die Jammer 7 bis 10 wurden ebenfalls mit dem Spektrumanalysator hinsichtlich ihres Frequenzbereichs analysiert (Abbildung 4, oben), wobei die Sendeleistung hierbei aus technischen Gründen nur grob abgeschätzt werden konnte. Anschließend wurde die Signalform in einem ausgewählten Bereich dargestellt (Abbildung 5, unten). Bei den Jammern 7 bis 9 wurde ein einzelner Frequenzbereich bei 0,9 GHz bzw. 1,8 GHz gewählt. Bei Jammer 10 lagen die Frequenzen bei 1,2 und 1,6 GHz.




**4** Abbildung: Beispielhafte Darstellung der Hochfrequenz-Analyseergebnisse anhand von Jammer 1. Quelle: Technische Hochschule Augsburg

# Die untersuchten Jammer im Überblick

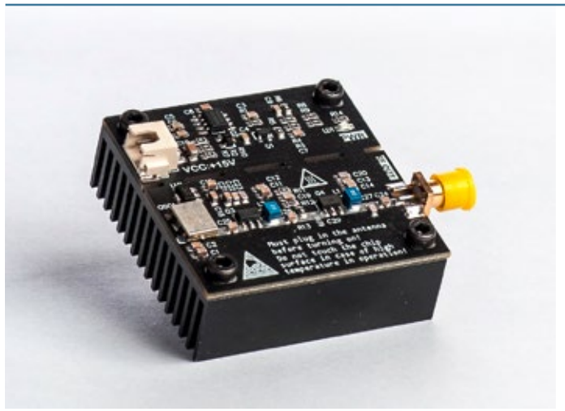
Kommerzielle Störsender als fertige Lösung gibt es in vielen Varianten. Sie unterscheiden sich in Preis, Leistung, Sendefrequenz und Signalform – und stellen daher eine vielseitige Gefahr dar.


**JAMMER 1**

| | |
|---|---|
| Preis: | 38,06 € |
| Frequenz: | 433,4 MHz |
| Signalform: | einzelner unmodulierter Träger und Oberwellen |
| Sendeleistung: | 0,2 W |
| Stromverbrauch: | 5 V / 0,25A |
| Verwendeter PA-Chip: | unbekannt |

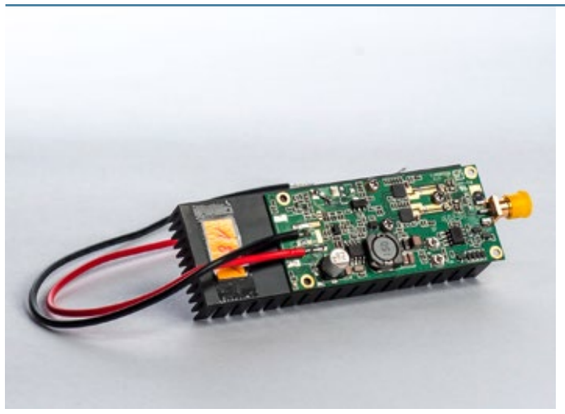
**JAMMER 2**

| | |
|---|---|
| Preis: | 24,41 € |
| Frequenz: | 433,5 MHz (Mitte) |
| Signalform: | zahlreiche Peaks innerhalb 26 MHz Bandbreite, Peakabstand 110 kHz |
| Sendeleistung: | 0,025 W |
| Stromverbrauch: | 5 V /0,065A |
| Verwendeter PA-Chip: | SBB5089Z |



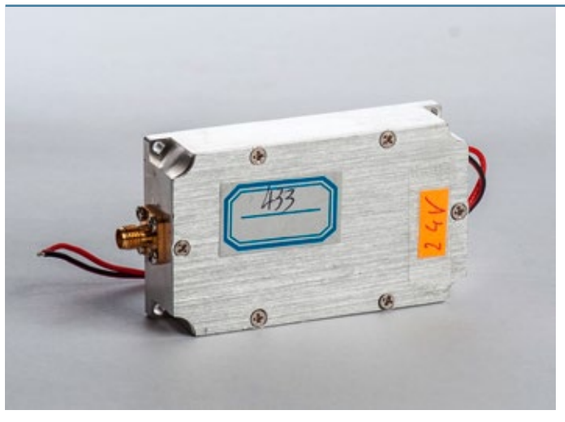
**JAMMER 3**

| | |
|---|---|
| Preis: | 19,63 € |
| Frequenz: | 467 MHz (Mitte) |
| Signalform: | zahlreiche Peaks innerhalb 97 MHz Bandbreite, Peakabstand 25 kHz |
| Sendeleistung: | 4 W |
| Stromverbrauch: | 15 V / 0,615A |
| Verwendeter PA-Chip: | 2x SBB5089Z |



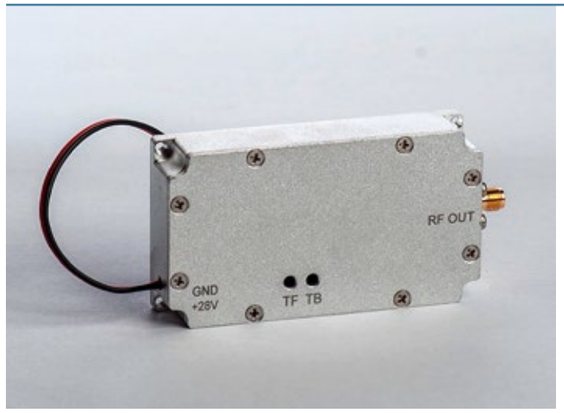
**JAMMER 4**

| | |
|---|---|
| Preis: | 39,67 € |
| Frequenz: | 431,7 MHz (Mitte) |
| Signalform: | zahlreiche Peaks innerhalb 36 MHz Bandbreite, Peakabstand 35 kHz |
| Sendeleistung: | 2 W |
| Stromverbrauch: | 18 V / 0,7 A |
| Verwendeter PA-Chip: | 2x YP3236W |




**JAMMER 5**

| | |
|---|---|
| Preis: | 92,41 € |
| Frequenz: | 430 MHz (Mitte) |
| Signalform: | zahlreiche Peaks innerhalb 10 MHz Bandbreite |
| Sendeleistung: | 10 W |
| Stromverbrauch: | 24 V / 1 A |
| Verwendeter PA-Chip: | YG602020 / M6010GN |




## JAMMER 6

| | |
|---|---|
| Preis: | 97,10 € |
| Frequenz: | 438,5 MHz (Mitte) |
| Signalform: | zahlreiche Peaks innerhalb 47 MHz Bandbreite |
| Sendeleistung: | 8 W |
| Stromverbrauch: | 28 V / 0,7 A |
| Verwendeter PA-Chip: | BLF6G27-10G |

## JAMMER 7

| | |
|---|---|
| Preis: | ca. 300 € |
| Frequenz: | 8 Bereiche, darunter GSM, WLAN und Bluetooth (gemessen bei 950 MHz) |
| Signalform: | zahlreiche Peaks innerhalb 110 MHz Bandbreite |
| Sendeleistung: | 0,3 W HF-Leistung, Spitzenleistung 5 W |
| Stromverbrauch: | 12 V, integrierter Akku |
| Verwendeter PA-Chip: | unbekannt |

## JAMMER 8

| | |
|---|---|
| Preis: | ca. 300 € |
| Frequenz: | 6 Bereiche, darunter GSM, WLAN und Bluetooth (gemessen bei 963 MHz und 1,8 GHz) |
| Signalform: | zahlreiche Peaks innerhalb 110 MHz Bandbreite, Pulswiederholungsrate 8 µs |
| Sendeleistung: | 0,3 W HF-Leistung, Spitzenleistung 5 W |
| Stromverbrauch: | 12 V, integrierter Akku |
| Verwendeter PA-Chip: | unbekannt |

## JAMMER 9

| | |
|---|---|
| Preis: | ca. 300 € |
| Frequenz: | 6 Bereiche, darunter GSM, WLAN und Bluetooth (gemessen bei 1,8 GHz) |
| Signalform: | zahlreiche Peaks innerhalb 160 MHz Bandbreite |
| Sendeleistung: | 1 W HF-Leistung, Spitzenleistung 25 W |
| Stromverbrauch: | 12 V, integrierter Akku |
| Verwendeter PA-Chip: | unbekannt |

## JAMMER 10

| | |
|---|---|
| Preis: | ca. 15 € |
| Frequenz: | GPS (1,2 GHz und 1,6 GHz) |
| Signalform: | Einzelne Peaks in kurzer Folge |
| Sendeleistung: | ca. 10 mW |
| Stromverbrauch: | 12 V, Fahrzeugsteckdos |
| Verwendeter PA-Chip: | 2x YP3236W |

# Ergebnisse und Fazit

Acht der zehn untersuchten Jammer sind extrem gefährlich.

Die erste untersuchte Gruppe von Jammern (1 bis 6) zielt auf die Störung im Bereich von 433 MHz ab, den unter anderem auch Funk-Alarmanlagen nutzen. **Jammer 1** erzeugt einen einzelnen unmodulierten Träger mit 0,2 W Sendeleistung bei 433,4 MHz. Hier besteht eine Gefahr, falls das zu störende Gerät die exakt gleiche Frequenz verwendet. Die von **Jammer 2** erzeugte Signalform ist prinzipiell in der Lage, alle Geräte im 433 MHz-Bereich zu stören. Jedoch ist die Sendeleistung mit 0,025 W sehr gering und verteilt sich über zahlreiche Oberwellen. Daher besteht eine Gefahr nur im nahen Umfeld.

**Jammer 3** bis **6** erzeugen eine Signalform, die prinzipiell alle Geräte im 433 MHz-Bereich stören kann. Zudem haben sie eine **hohe Sendeleistung** von bis zu 10 W. Das macht diese Geräte **extrem gefährlich**. Selbst bei Verwendung einer Antenne von geringem Ausmaß ist es möglich, die **Funk-Kommunikation im 433 MHz-Bereich großflächig und vollständig zu unterbinden**.

**Jammer 7** bis **10** erzeugen eine Signalform, die prinzipiell alle Geräte im jeweiligen Frequenzbereich, unter anderem GSM, WLAN, GPS oder Bluetooth, stören kann. Zudem können die Jammer 7 bis 9 gleichzeitig sechs beziehungsweise acht Frequenzbereiche blockieren. Die verwendete Signalform und die **hohe Sendeleistung** machen diese Geräte ebenfalls **extrem gefährlich**. Selbst, wenn nur die mitgelieferten Antennen verwendet werden, kann die **Funk-Kommunikation** in den jeweiligen Frequenzbereichen **großflächig** und **vollständig unterbunden** werden.

Insgesamt lässt sich sagen, dass gefährliche Störsender bereits zu geringen Preisen erworben werden können. Daher setzen Kriminelle sie mit hoher Wahrscheinlichkeit auch in der Praxis ein. Für Systembetreiber und Produktentwickler bedeutet dies: Funkangriffe mit Störsendern dürfen in keiner Bedrohungs- und Risikoanalyse fehlen.

# Quellen und weitere Informationen

## QUELLEN


[1] Trend Micro Research. Attacks Against Industrial Machines via Vulnerable Radio Remote Controllers: Security Analysis and Recommendations. https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/attacks-against-industrial-machines-via-vulnerable-radio-remote-controllers-security-analysis-and-recommendations

[2] Webseite des Adalm-Pluto SDRs: https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/adalm-pluto.html

[3] Webseite des Programmierwerkzeugs GNU Radio: https://www.gnuradio.org/

[4] Pohl, Johannes und Andreas Noack: Universal Radio Hacker: A Suite for Analyzing and Attacking Stateful Wireless Protocols. https://github.com/jopohl/urh


## WEITERFÜHRENDE INFORMATIONEN ZU HSA_INNOS UND TTZ DATA ANALYTICS

Zusammen mit dem DZ.S (Digitales Zentrum Schwaben) und dem aitiRaum e. V. veranstaltet HSA_innos jährlich die AUXINNOS – das Forum für innovative Sicherheit für IT-Fachkräfte und Studierende aus Bayerisch-Schwaben.

Hier finden Sie das Event: www.auxinnos.de

HSA_innos bietet Weiterbildungsmöglichkeiten für Bachelorabsolventinnen und Berufstätige.

Master Industrielle Sicherheit: www.hs-augsburg.de/Elektrotechnik/Industrielle-Sicherheit-Master.html

Zertifikat „Industrial Safety and Security: www.hs-augsburg.de/Informatik/HSA-innos/lehre/Industrial-Safety-and-Security

Das TTZ Data Analytics in Donauwörth veranstaltet die Reihe „Data Analytics im Donau-Ries“ für den regionalen Austausch von Forschung und Wirtschaft in der Region.

Zur aktuellen Veranstaltung:
www.hs-augsburg.de/ttz-data-analytics/im-Donau-Ries



## IMPRESSUM UND KONTAKT


**Herausgeber**
Technische Hochschule Augsburg
Augsburg Technical University
of Applied Sciences
An der Hochschule 1
86161 Augsburg
info@hs-augsburg.de
www.hs-augsburg.de

**Projektleitung**
Prof. Dr. Dominik Merli

**Institut für innovative Sicherheit (HSA_innos)**
Am Technologiezentrum 8
86159 Augsburg
info@hsainnos.de
www.hsainnos.de

**Technologietransferzentrum (TTZ) Data Analytics**
Äbtissin-Gunderada-Straße 4
86609 Donauwörth
ttz-don@hs-augsburg.de
www.ttz-data-analytics.de/

**Redaktion**
Alexander Lehner, M. A.

**Gestaltung**
wppt : kommunikation gmbh
Gesellschaft für visuelle Kultur
Treppenstraße 17 – 19
42115 Wuppertal
Maike Hinz, Rob Fährmann
Tel. +49 202 42966-0
Fax +49 202 42966-29
direkt@wppt.de
www.wppt.de

**Bilder / Grafiken**
Hochschule Augsburg, andere Bildrechte liegen bei den genannten Urheber:innen und Autor:innen.




**Gender-Hinweis**
Wir haben in dieser Publikation – im Sinne einer gendergerechten Sprache – die Schreibweise mit dem Doppelpunkt gewählt.

**Technische Hochschule Augsburg**
Technical University of Applied Sciences
An der Hochschule 1
86161 Augsburg
info@tha.de
www.tha.de

Institut für innovative
Sicherheit (HSA_innos)
Am Technologiezentrum 8
86159 Augsburg
info@hsainnos.de
www.hsainnos.de

Technologietransferzentrum (TTZ)
Data Analytics
Äbtissin-Gunderada-Straße 4
86609 Donauwörth
ttz-don@hs-augsburg.de
www.ttz-data-analytics.de