

2020-09-07

Wir als modzoro sehen seit einem Jahrzehnt Sicherheitsschwachstellen und Datenschutzvergehen in verschiedensten Variationen. Unabhängig von der Art oder Komplexität einer Schwachstelle sehen wir sehr oft einen wenig risikobewussten Umgang mit Daten und Ressourcen. Wir schreiben das Jahr 2020, und noch immer werden Applikationen mit der heissen Nadel gestrickt. Time-to-Market hat eine so hohe Priorität, dass nicht einmal grundlegende Sicherheitsprinzipien in die Lösungsarchitektur oder das individuelle Applikationsdesign einfließen. Man findet an jeder Ecke Applikationen und Datenververarbeitungssysteme, die schlecht, d.h. unsicher, mit den ihnen anvertrauten Daten umgehen. Dies ist umso gravierender, wenn es sich um personenbezogene Daten oder gar Gesundheitsdaten handelt.

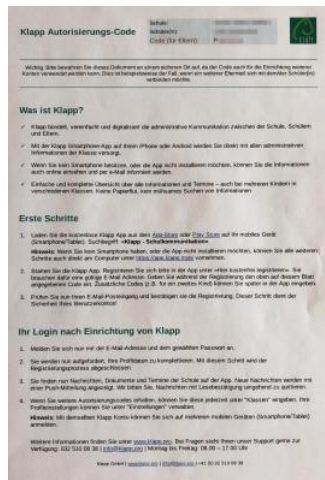
In unserem Artikel [Mit Webapps gegen COVID-19](https://www.modglo.com/modlog/archives/2020/07/05/mit_webapps_gegen_covid-19/index.html) (https://www.modglo.com/modlog/archives/2020/07/05/mit_webapps_gegen_covid-19/index.html) wollten wir darauf aufmerksam machen, dass jeder eine Verantwortung hat, dass Software angemessen sicher wird. Heute möchten wir dieses Thema mit einem weiteren Beispiel erneut aufgreifen. Die anhaltende Corona-Pandemie eröffnet neue Herausforderungen aber auch Möglichkeiten bei der Digitalisierung und der Datenverarbeitung. In allen Bereichen sucht man nach Lösungen, und spätestens während des totalen Lockdowns haben auch Schulen festgestellt, dass sie noch mehr auf die Digitalisierung angewiesen sind. Heute wird alles eingesetzt was verfügbar war: Zoom, Teams, WhatsApp, Facebook Messenger, und die Schweiz wurde bereits vor drei Jahren eine schweizerische Plattform namens Klapp ins Leben gerufen, welche insbesondere die Kommunikation zwischen Eltern und Schule und LehrerInnen vereinfachen soll. *Einfache Kommunikation, die klappt!*, so der Slogan des Unternehmens. Zu Zeiten von Corona hat diese Plattform einen massiven Nutzer-Zuwachs erhalten. Unter den Nutzern ist auch eine unserer MitarbeiterInnen.

Bei Klapp handelt es sich um ein schweizerisches Start-Up mit dem Sitz in Fislisbach (AG). Zum Zeitpunkt der Veröffentlichung gibt das Unternehmen an mehr als 200 Schulen, 8'600 Lehrpersonen und 45'000 Eltern eine Plattform zur Kommunikation zu bieten. Hier werden gemäss seinen Angaben täglich rund 3'000 individuelle Nachrichten versendet. (siehe hierzu Angaben durch Klapp (<https://www.klapp.pro/>)) Die Daten werden ausschliesslich in der Schweiz gespeichert. Neben der Benutzung im Browser kann die App kann auch mit dem Smartphone (iOS und Android) genutzt werden.

Aus technischer Sicht ist Klapp eine cordova-basierte Web- und Mobile-App. Zur Registrierung als Elternteil oder Schüler benötigt man einen sogenannten Autorisierungs-Code. Nach erfolgreicher Registrierung ist der Zugriff auf die jeweilige Klasse und die damit verbundenen Funktionalitäten möglich. Während der Kurzanalyse wurden folgende Haupt-Funktionen als angemeldetes Elternteil identifiziert:

- Gruppen und individual Chats
- Versand von Dateien zwischen Kommunikationspartnern
- Kalenderfunktionen
- Informationen über die Klassenmitglieder
- Namen der Kinder und registrierte Eltern
- E-Mail-Adressen und Rufnummern (wenn freigegeben)

Damit Schulen die Klapp-Plattform nutzen können, wird zunächst ein Ex- und Import von Stammdaten vorgenommen. Zu diesem notwendigen Ex- und Import Prozess hat Klapp diverse **Anleitungen** (<https://www.klapp-prof.de/lehrerforce>) veröffentlicht. Nach erfolgreichem Daten-Import können die Lehrpersonen Einladungsschreiben für die Eltern generieren. Diese enthalten Informationen über Klapp und sind personalisiert. Jedes dieser Einladungsschreiben hat nämlich zusätzlich den Namen des Kindes und einen Autorisierungs-Code für die Eltern aufgedruckt.




Beispielhaftes Einladungsschreiben mit Autorisierungs-Code und Vor- Nachname des Kindes

Dieser Autorisierungs-Code wird bei der Registrierung benötigt. Hiermit autorisiert sich die Anwenderin als Elternteil eines bestimmten Kindes. Der Autorisierungscode stellt somit das eindeutige Merkmal dar, um die betreffende Person zu identifizieren.

12:43

DE



Einmalige Registrierung

Meine E-Mail *

Mein Vorname (Zus.)

Mein Nachname (Zusatz)

Ich bin: ☒ Elternteil ☐ Schüler/in

Autorisierungscode ([Wichtige Info](#))

Pin

REGISTRIEREN

ZURÜCK

Der Autorisierungs-Code hat das folgende Format: P-ABCDE1. Das Präfix "P-" steht für "Parent", Autorisierungs-Codes von Schülerinnen haben das Präfix "S-", was für "Student" steht. Die darauffolgenden Werte sind sechs alphanumerische Zeichen. Das bedeutet, dass es maximal 2.17 Milliarden mögliche "Parent" oder "Student" Codes gibt - Bei einer Anfrage pro Sekunde an den Klapp-Server benötigt man 3,7 Wochen um alle möglichen Autorisierungs-Codes zu erraten. Geht man von aktuell 45'000 verfügbaren Autorisierungs-Codes aus, trifft man mit einer Wahrscheinlichkeit von 52.49%, bei der selben Anfragerate, nach 10 Stunden mindestens einen gültigen Autorisierungs-Code. Würde man den möglichen Raum von Zeichen um Kleinbuchstaben und die Länge des Autorisierungs-Codes auf 10 erweitern, so bräuchte man, bei der angenommenen Anzahl an Anfragen pro Sekunde, 16 Millionen Jahre um alle durchzuprobieren. Die Annahme, dass nur eine Anfrage pro Sekunde möglich ist gilt als sehr konservativ, nicht selten können aktuelle Webserver bis zu 1000 Anfragen/Sekunde abarbeiten.

Wie steht es bei Klapp um den Datenschutz?

Die Daten der Applikation (Nachrichten, Chats und Bilder) werden zwar über einen *verschlüsselten Kanal* auf den Klapp-Server übertragen, werden auf dem Server aber *unverschlüsselt gespeichert*. Das heisst, dass mindestens der Betreiber und alle Involvierten, welche die Daten prozessieren, Informationen mitlesen und manipulieren könnten. Im Falle eines Klassenverbundes heisst das im einfachsten Fall, dass die Klapp GmbH sowie die Dienstleister für den Nachrichtenversand über die registrierten Kinder und Eltern sowie Klassengruppierungen und die versendeten Informationen Bescheid wissen. Werden sensible Informationen wie Krankheiten oder vielleicht Kritik- oder Entwicklungspunkte der Kinder zwischen Personen ausgetauscht, sind diese nicht umfassend gesichert und es ist nicht ersichtlich ob man mit dem legitimen Kommunikationspartner Daten austauscht.

In Ihrer Datenschutzerklärung (<https://www.klapp.pro/datenschutz>), verspricht die Klapp GmbH:

"Wir geben keine Personendaten an Dritte weiter und erzielen auch keinen kommerziellen Nutzen daraus. Ihre Personendaten, die Sie uns zur Verfügung stellen, werden von uns weder verkauft, vermietet noch gehandelt".

Weiter schreibt die Klapp GmbH:

"Ihre Daten speichern wir in der Schweiz. Benutzerdaten werden in der Schweiz gespeichert und verarbeitet und unsere Partner halten die schweizerischen und europäischen Datenschutzverordnung ein".

Und "Privacy by Design" wird ebenfalls als Merkmal benannt. Die Aussage "Wir wollen mit Ihren Daten kein Geld verdienen. Ihre Benutzerdaten werden unter keinen Umständen an Dritte verkauft oder für Werbung verwendet." wirkt vertrauensweckend.

Auch die Schulen scheinen von der Lösung und deren Sicherheit überzeugt. Auf Anfrage, warum Vor- und Familienname an Dritte ohne Zustimmung mitgeteilt werde teilte eine Schule mit:

"Die Firma Klapp hat nach der Registrierung nur Name und Vorname plus Schule Ihres Kindes. Diese gehören nach meinem Wissen nicht zu den besonders schützenswerten Daten. Es ist uns aber bewusst, dass ein sorgfältiger Umgang mit Daten zentral ist. Daher haben wir uns bei der App auch für die Firma Klapp entschieden, die einen hohen Standard bei der Datensicherheit garantiert".

Bei einer technischen Betrachtung zeigt sich ein anderes Bild. Klapp verwendet beispielsweise für die Übermittlung der Daten Push-Nachrichten, welche über den US-Amerikanischen Dienst OneSignal versendet werden. Hier werden neben dem Vor- und Familiennamen des Absenders und der Betreff der Nachricht auch weitere Metainformationen über das verwendete Gerät und das Betriebssystem und des Netzwerkbetreibers gesammelt.

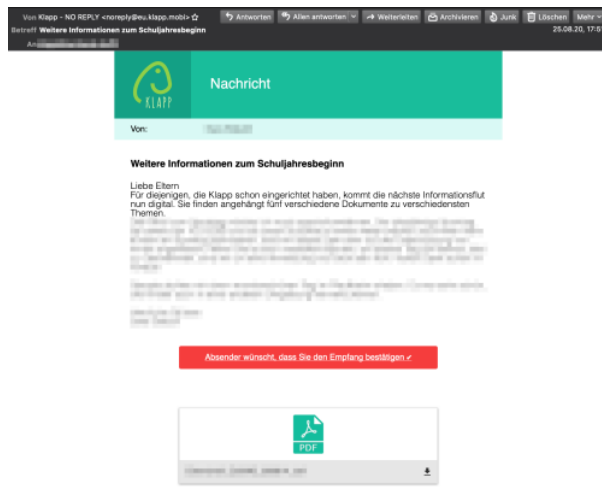


Push-Benachrichtigung enthält Informationen über den Absender sowie Betreff der Nachricht

```
POST /players/8a77f111-c146-402b-88f3-18d874c19872/on_session HTTP/1.1
Host: api.onesignal.com
Content-Type: application/json
Cookie: __cfduid=dd2b3c2801e2179392b0232eac71bf6bf1597813825
Connection: close
If-None-Match: W/"698f061ae145e46b912b7e8e00450320"
Accept: application/vnd.onesignal.v1+json
SDK-Version: onesignal/ios/021402
Accept-Language: de-ch
Content-Length: 434
Accept-Encoding: gzip, deflate
User-Agent: Klapp/2.0.1 CFNetwork/1126 Darwin/19.5.0

{
  "app_id" : "bb3877cc-afc0-4d81-ac73-9339554c7686",
  "net_type" : 0,
  "device_type" : 0,
  "sdk" : "021402",
  "identifier" : "b5c9f6956a9606a93f564ac0677342ffa9d9540b6c34ba170da574fd3f77dc08",
  "language" : "de-CH",
  "device_os" : "13.5.1",
  "game_version" : "2.0.1",
  "timezone" : 7200,
  "ad_id" : "CF7A0B86-311E-4EF7-A469-F7A5322B206A",
  "notification_types" : 31,
  "carrier" : "Salt",
  "device_model" : "iPhone11,2"
}
```

Bei dem Versand via E-Mail verwendet Klapp den Dienstleister Mailgun - ebenfalls ein US-Unternehmen (siehe Datenschutzerklärung (<https://www.klapp.pro/datenschutz>)). Im Gegensatz zu den Push-Nachrichten beinhalten die E-Mail-Nachrichten auch die versendete Information, sowie Hyperlinks zu den allenfalls angehängten Dokumenten. Was bedeutet, dass neben Klapp auch Mailgun in der Lage ist, sämtliche E-Mail-Inhalte zu lesen oder zu manipulieren. Ob diese Firmen sich der hiesigen Gesetzeslage und Richtlinien unterwerfen, ist für uns aktuell nicht prüfbar. Wir möchten aber auch darauf hinweisen, dass die Daten auch ungewollt als Folge eines Erpressungsversuches oder eines Hacker-Angriffes bei dem Dienstleister geleakt werden könne.



E-Mail erhalten über Mailgun enthält den genauen Text sowie Links zu den angehängten Dateien

Wir geben der Firma Klapp recht. Privacy by Design ist wichtig... und zwar genau aus dem Grund, dass niemand unautorisiertes Drittes unsere Daten einsehen können sollte. Genau deshalb sollte konsequent Ende-zu-Ende-Verschlüsselung eingesetzt werden, wie es zum Beispiel im [Leitfaden des Datenschutzbeauftragten des Kantons Zürich](https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/publikationen/leitfaeden/leitfaeden_datenschutzlexikon_volksschule.pdf) (https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/publikationen/leitfaeden/leitfaeden_datenschutzlexikon_volksschule.pdf) empfohlen wird. Deshalb werden Instant-Messengers wie Signal oder Threema von vielen bevorzugt, da der Transportweg sowie jede Zwischenspeicherung verschlüsselt ist und erst am eigentlichen Endgerät entschlüsselt werden kann.

Nachdem wir uns dem Datenschutzversprechen der Firma Klapp GmbH und dem Thema Datenschutz gewidmet haben, möchten wir auf einige der technischen Unzulänglichkeiten eingehen. Viele der identifizierten Fehlerklassen sind trivial und bekannt. Auch wenn die Auswirkungen bei dieser Applikation möglicherweise gering ausfallen, möchten wir diese aufführen, weil wir diese immer wieder sehen.

Und wie steht es um die Informationssicherheit?

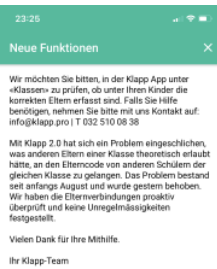
Datenschutz und Informationssicherheit sind eng miteinander verbunden und das Befolgen von Sicherheitsempfehlung wichtig, um den Datenschutz überhaupt zu implementieren. Eine oberflächliche Betrachtung der Plattform hat gezeigt, dass grundlegende Sicherheitsprinzipien der Informationstechnik sowie der sicheren Entwicklung für mobile Anwendungen nicht befolgt wurden. Dies ist leider auch im Jahr 2020 immer noch häufig anzutreffen. Gerade in frühen Projektphasen ist die Erarbeitung von Bedrohungsmodellen und das Definieren von Sicherheitsanforderungen ein Kernpunkt, um später beim Lösungsdesign sowie der eigentlichen Entwicklung die richtigen Massnahmen und Methoden zu ergreifen. Gerade die gefundenen Trivialfehlerklassen zeigen, dass Datenschutz und Sicherheit während der Entwicklung der Plattform keine Schwerpunktthemen waren.

Während der Nutzung der Applikation konnte beobachtet werden, dass nicht nur der eigene Autorisierungs-Code vom Klapp-Server übermittelt wird, sondern auch die Autorisierungs-Codes, welche es den anderen Eltern ermöglichen sich eindeutig zu identifizieren.

```
{
  "students": [
    {
      "id": "5efe",
      "first_name": "M",
      "last_name": "B",
      "email": null,
      "telephone_numbers": null,
      "parents": [
        {
          "id": "5d6d",
          "first_name": "P",
          "last_name": "B",
          "email": "",
          "telephone_numbers": ""
        },
        {
          "id": "5d7",
          "first_name": "Y",
          "last_name": "S",
          "email": "",
          "telephone_numbers": ""
        }
      ],
      "code_parent": "P-"
    },
    {
      "id": "5efe",
      "first_name": "M",
      "last_name": "B",
      "email": null,
      "telephone_numbers": null,
      "parents": [
        {
          "id": "5f3b",
          "first_name": "S",
          "last_name": "B",
          "email": "",
          "telephone_numbers": ""
        }
      ],
      "code_parent": "P-"
    }
  ]
}
```

Auszug aus der Server-Antwort. Zu sehen ist ein JSON-Objekt mit Informationen zu Kindern und Eltern. Ausserdem sind die Autorisierungs-Codes der Eltern enthalten.

Das bedeutet, dass jeder Empfänger das eindeutige Identifizierungsmerkmal aller Klassenteilnehmer besitzt und deren Identität übernehmen kann. Die Auswirkung eines Missbrauchs erscheint vielleicht aktuell nicht weiter schlimm bei einer solchen Verwendung. Soziales Schadenspotenzial ist auf jeden Fall vorhanden und Vertrauensmissbrauch ist möglich. Wichtig ist jedoch zu verstehen, dass eine zukünftige Funktionserweiterung der Plattform noch andere betrügerische Aktivitäten ermöglichen könnte, die heute vielleicht noch nicht absehbar sind. Hätte Klapp eine Implementierung nach den eigens aufgestellten Prinzipien der Datensparsamkeit und Need-to-Know Basis gewählt, wäre dieser Fehler gar nicht aufgetreten. Diese Schwachstelle wurde umgehend dem Klapp-Team gemeldet und Sie wurde am Abend des 24. August 2020 durch ein serverseitiges Update behoben. Daraufhin hat das Klapp-Team auch eine interne Nachricht an die BenutzerInnen versendet in der zu einer manuellen Überprüfung der registrierten Elternteile aufgerufen wird.



In-App Benachrichtigung des Klapp-Teams nachdem die Autorisierungs-Code-Leck Schwachstelle behoben wurde.

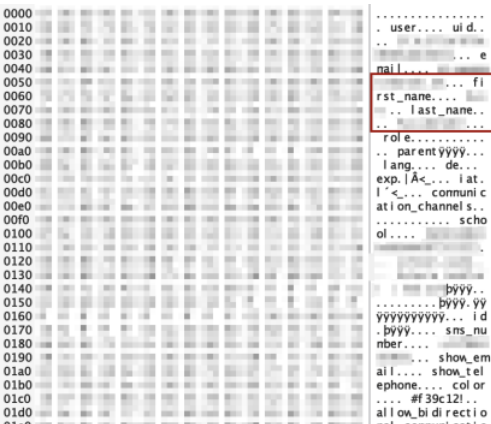
Ebenfalls ein Klassiker unter den trivialen Fehlern in Applikationen ist eine Vertrauensstellung durch sehr langlebige Authentisierungsmerkmale. Im Falle der Klapp-Applikation sind es JSON-Web-Tokens ohne Ablaufzeitpunkt. Jeder, der in den Besitz eines solchen Tokens gelangt, kann ohne zusätzliche Merkmale wie Benutzername oder Passwort andere Nutzer imitieren und hat somit automatische die Identität und Berechtigungen des legitimen Eigentümers. Bei der Klapp-Applikation werden diese Tokens auf dem Endgerät ohne zusätzliche Schutzmassnahmen abgelegt und gelangen so auch auf Backup-Datenträger oder Cloud-Dienste. Auch hier möchten wir darauf hinweisen, dass die Auswirkungen zum Glück in dem heutigen Anwendungsfall moderat ausfallen. Bekannte Schwachstellen zu implementieren ist auf jeden Fall eine schlechte Praxis, auch wenn sie aktuell wenig Relevanz haben.

```
JWT
Headers = {
  "alg": "HS256",
  "typ": "JWT"
}

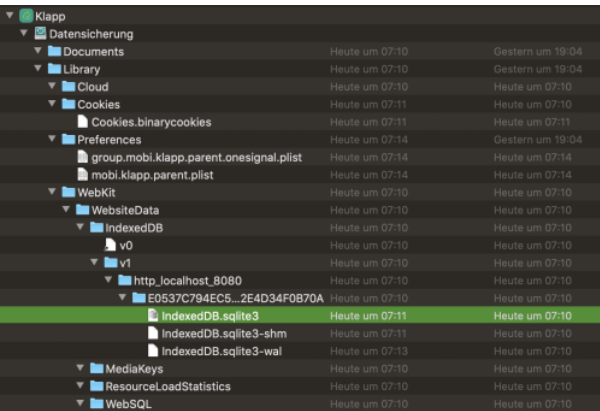
Payload = {
  "uid": "..."
}

Signature = "..."
```

Unsterblicher JSON-Web-Token da kein Ablaufzeitpunkt (exp) angegeben ist.)



Die SQLite Datenbank ist nicht verschlüsselt. Auch die darin enthaltenen Informationen sind nicht durch die App verschlüsselt.



Die SQLite Datenbank befindet sich in einem Geräte Backup.

Der Versand von individual Nachrichten an Lehrer ist eine von der Plattform vorgesehene Funktionalität. Wählt man "Neue Nachricht" aus so erscheint eine Auflistung der Lehrer, welche zum Empfang von Nachrichten autorisiert sind. Jeder Lehrer hat in der Plattform eine eindeutige Benutzerkennung, Beispielsweise 5f3bf6370452c910612c71be. Diese wird beim Versand der Nachricht angegeben. Eine solche Benutzerkennung haben auch Eltern und Schüler. Tauscht man die Benutzerkennung des Lehrers mit der eines anderen Elternteils aus, so wird die Nachricht an den gewünschten Empfänger übermittelt.



In-App Nachricht an ein anderes Elternteil versendet.

Soweit modzero bekannt, ist dies keine vorgesehene Funktionalität. Auch hier müssen wir erneut darauf verweisen, dass solche Fehlerklassen üblich sind. Nur weil eine Benutzeroberfläche eine Einschränkung vorsieht, muss diese von der Applikation nicht zwingend umgesetzt worden sein. Eine Einschränkung in der Benutzeroberfläche ersetzt nicht ein striktes Umsetzen eines ordentlichen Benutzer- und Rollenkonzeptes auch im Backend.

Beiläufig sind noch weitere Probleme aufgefallen, welche hier nicht im Detail beschrieben werden, aber auch mit dem Klapp-Team besprochen wurden:

- Sensible Informationen in lokaler SQLite-Datenbank (iOS)
- SQLite Datenbank (iOS) in einem Backup vorhanden
- Fehlendes Zertifikats-Pinning und Jailbreak-Erkennung
- Keine Möglichkeit den Zugriff auf die App durch Pass Code oder biometrische Merkmale zu beschränken

Fazit

Dies soll kein Aufruf zur Verhinderung von Innovation oder Digitalisierung sein, jedoch bitten wir jeden einzelnen Entwickler, Architekt, CEO... JEDEN Involvierten... seine Verantwortung wahrzunehmen und im Zweifelsfall jemanden hinzuzuziehen, der die Sachlage neutral beurteilen kann.

Natürlich kann in diesem Beispiel argumentiert werden, dass die Auswirkungen der Schwachstellen ja überschaubar sind und die Schutzmassnahmen für das Anwendungsgebiet möglicherweise ausreichen. Das Problem einer solchen Argumentation liegt dabei, dass sich die Umgebung, der Funktionsumfang, die Entwicklungsprozesse sowie die Firmen selbst zukünftig wandeln werden. Selbst wenn zum jetzigen Zeitpunkt ein Unternehmen ehrbare Ziele verfolgt oder eine Applikationsschwachstelle nur eine verhältnismässig geringe Auswirkung aufweist, so kann sich dies schon Morgen ändern. Es ist daher wichtig bereits früh in der Projektphase die richtigen Entscheidungen zu treffen und Fehlfunktionen, Schwachstellen und Bedrohungsmodelle als integral wichtigen Bestandteil zu behandeln.

Zeitlicher Ablauf

- 2020-08-18 Einladungsschreiben der Schule erhalten.
- 2020-08-18 Schwachstellen aufgedeckt.
- 2020-08-19 Klapp kontaktiert. Klapp hat sich zurückgemeldet.
- 2020-08-21 Schwachstellen telefonisch an Klapp übermittelt. Schwachstellen akzeptiert.
- 2020-08-24 Rückmeldung von Klapp erhalten, dass die Autorisierungs-Code Schwachstelle behoben wurde

Posted by Sven Fassbender, Max Moser | [Permanent link \(https://www.fassbender.ch/archives/2020/09/07/knapp-daneben-ist-auch-vorbei/index.html\)](https://www.fassbender.ch/archives/2020/09/07/knapp-daneben-ist-auch-vorbei/index.html) | File under: [mobile \(https://www.fassbender.ch/archives/mobile/index.html\)](https://www.fassbender.ch/archives/mobile/index.html), [security \(https://www.fassbender.ch/archives/security/index.html\)](https://www.fassbender.ch/archives/security/index.html), [software \(https://www.fassbender.ch/archives/software/index.html\)](https://www.fassbender.ch/archives/software/index.html), [exploit \(https://www.fassbender.ch/archives/exploit/index.html\)](https://www.fassbender.ch/archives/exploit/index.html), [advisory \(https://www.fassbender.ch/archives/advisory/index.html\)](https://www.fassbender.ch/archives/advisory/index.html)