Schutzranzen®

Stellungnahme zum Blogbeitrag des Vereins Digitalcourage 22.01.2018

Diese Stellungnahme bezieht sich auf den folgenden Artikel:
https://digitalcourage.de/blog/2018/schutzranzen-amazon-google-und-co-bekommen-daten#Screenshots.

Wir haben in diesem Artikel einige falsche technische Darstellungen gelesen, die wir im Folgenden aufklären wollen. Die Vorwürfe von Digitalcourage bezüglich der Weitergabe persönlicher Daten sind nicht auf Fakten basiert, da nur anonymisierte Kontakte zu anderen Servern stattfinden, durch die keine persönlichen Daten übermittelt werden. Die Datensicherung wird nochmals von unserem technischen Team auf Mängel überprüft. Wir können jedoch erst auf die Spekulationen des Vereins Digitalcourage antworten, wenn sie uns dazu entsprechende Details offenlegen.

1) *Aussage Digitalcourage: "Was weiterhin fehlt: An keiner Stelle wird darüber aufgeklärt, dass die größten Datensammel-Konzerne der Welt Daten bekommen. Die Apps kontaktieren nach unseren Beobachtungen Server bei 1&1, Akamai, Amazon, Facebook, Google und Microsoft; die Website übermittelt ungekürzte IP-Adressen für Nutzungsanalysen an Google-Server in den USA."*

Stellungnahme Schutzranzen:

- Dass ein Server kontaktiert wird, bedeutet nicht, dass darüber Daten geschickt werden – persönlich oder nicht. Im Folgenden erklären wir die vorhandenen Kontakte unserer App und Webseite zu oben genannten Servern.
- Unsere Apps funktionieren über einen Cloud-Server, und kontaktieren deswegen Server von anderen Unternehmen, die diese Dienstleistungen anbieten. Die Server von der Coodriver GmbH sind bei **1&1** und bei **Azure (Microsoft)** gehostet, und deswegen kontaktieren die Schutzranzen Apps Datenzentren dieser Unternehmen. Alle Verbindungen zu unseren Servern werden über Transport Layer Security (TLS) gesichert, die Standard-Sicherheitslösung für das Web. Dies erlaubt nicht, dass die von oder an die Apps übertragenen Daten außerhalb der Apps oder Server gelesen werden können. Somit können die Unternehmen, die uns die Übertragung der Daten oder Hosting der Server anbieten, diese Daten nicht lesen.
- Unsere Apps benutzen Google Maps für die Kartefunktionalität, daher müssen sie **Google-Server** regelmäßig kontaktieren. Zusätzlich, wenn die Familien-Funktion aktiviert wird (es ist ein opt-in), werden Push-Nachrichten benutzt, die auch über Server von Google funktionieren. Dazu gelten die Datenschutzbestimmungen des Dienstes. Push-Nachrichten sind eine gängige Praxis, und die Funktionsbeschreibung ist online und frei zugänglich dokumentiert.
- Die Apps benutzen zusätzlich Google Play Services App Indexing, um Statistiken über die Benutzung der App – konkret, welche Screens wie oft aufgerufen werden – zu sammeln. Hier werden nur Daten an **Google Server** geschickt, die keinen Person- oder Smartphone-Bezug haben (Zähler), die somit anonym sind und nur in einer großen Menge insgesamt bewertet werden. Hierfür kontaktieren auch die Apps Google Server.
- Die Apps benutzen Crashlytics, ein gängiges Werkzeug, um das technische Verhalten von Apps zu überwachen, z.B. was zu einem Crash geführt hat. Crashlytics wird in der **Amazon AWS-Plattform** gehostet, daher kontaktieren die Apps diese Plattform. Crashlytics hat eigene Datenschutzbestimmungen. Außerdem dient der Einsatz des Werkzeugs alleine der Fehlerbehebung (Bug-Fixing), es werden keine persönlichen Daten oder Positionsdaten versendet.
- Die Fahrer App bietet die Möglichkeit, die App über **Facebook** zu empfehlen. Hierzu wird in der derzeitigen Android Version der App ein SDK von Facebook benutzt, das sich sofort bei Anschaltung der App mit Facebook in Verbindung setzt. Diese Verbindung findet nur einmal statt. Somit können keine Positions- oder anderen Daten regelmäßig an Facebook Server

weitergeleitet werden, wie der Text glauben machen will. Eine erneute Verbindung zu Facebook wird erst erstellt, wenn der Benutzer die App tatsächlich weiterempfehlen will. In der zukünftigen Version der App wird eine lokale Lösung zur Weiterempfehlung benutzt werden, nämlich das lokale Aufrufen der Facebook App. Damit wird mit dem Update Facebook nicht mehr beim Starten der App kontaktiert. Die Möglichkeit, die App zu empfehlen, gibt es aus Datenschutzgründen nicht in der Kinder App, und wird es auch weiterhin nicht geben.

- **Akamai** ist der weltweit größte Content Delivery Network Anbieter. Er bietet Inhaltslieferung an viele Unternehmen. Dieser Dienst kann keine Daten lesen, solange sie über TLS gesichert sind. Coodriver hat kein geschäftliches Verhältnis mit Akamai, also es geht hier um einen der oben genannten Unterstützungsdienste, die keine persönlichen Daten übermittelt bekommen.

2) *Aussage Digitalcourage: "Auf die Nutzung des Webstatistik-Tools Google Analytics wird in den Datenschutzbestimmungen hingewiesen. Auch Cookies werden dort erklärt und dass damit Nutzungsdaten an Google-Server in den USA gehen. Unverständlich ist jedoch, warum offenbar die für den legalen Einsatz von Google Analytics in der EU erforderliche IP-Anonymisierung nicht aktiviert ist. Der Blick in den Quelltext der Website zeigt, dass Google Analytics genutzt wird, nirgendwo jedoch findet sich das Kürzel für die Anonymisierung der IP-Adressen. In den Datenschutzbestimmungen von Schutzranzen selbst heißt es, dass „in Ausnahmefällen" ungekürzte IP-Adressen an die US-Server geschickt werden. Wieso? Und welche Ausnahmefälle sind das?"*

Stellungnahme Schutzranzen:

- Unsere Webseite hat **Google Analytics** benutzt. Die Übermittlung von ungekürzten IP-Adressen beruht auf einer falschen Konfiguration der Javascript Bibliothek, die inzwischen korrigiert wurde. Wir bedanken uns dafür, dass Digital Courage darauf aufmerksam gemacht hat.

3) *Aussage Digitalcourage: „Schutzranzen"-Apps: 1&1, Akamai, Amazon, Facebook, Google und Microsoft lesen mit. Bereits bei einer ersten Untersuchung mit der freien App „Net Monitor" haben wir festgestellt, dass die Angaben zur Datenweitergabe an Dritte nicht stimmen können: Screenshots belegen, dass die Kinder-App Daten an Amazon-Server in den USA sendet. Außerdem kontaktiert werden Server bei Akamai, Google, Microsoft und 1&1. Die Autofahrer- und Eltern-App kontaktieren sogar Facebook. Womöglich sind es noch mehr, denn je länger die Kinder-App läuft, desto mehr kontaktierte Server kommen unserer Beobachtung nach dazu. Die hier genannten haben wir im Zeitraum bis 17.1.2018 gefunden."*

Stellungnahme Schutzranzen:

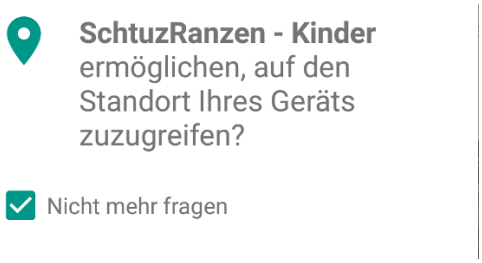
- Warum welche genannte Server kontaktiert werden, wurde im ersten Punkt erklärt.
- Es ist irreführend, anzudeuten, dass es sich um mehr als die tatsächlich erkannten Kontakte handeln könnte, ohne irgendeinen Nachweis zu liefern. Wir können spekulative Kontakte nicht erklären.

4) *Aussage Digitalcourage: "Datensicherheit: mangelhaft. Bei näherer Begutachtung haben wir auch Schwachstellen in der Datensicherheit festgestellt. Die Bestandsdaten der Kinder und anderer App-Nutzer.innen und deren Positionsdaten sind hochsensibel. Deshalb wollen wir darüber keine Details veröffentlichen. Unser Ziel ist nicht, Überwachung von Kindern auf Datensicherheit zu optimieren. Unser Ziel ist eine freie Gesellschaft, in der Kinder zu überwachen und die Positionsdaten in Bediensysteme von Autos einzuspeisen als der Übergriff gesehen wird, der es ist."*

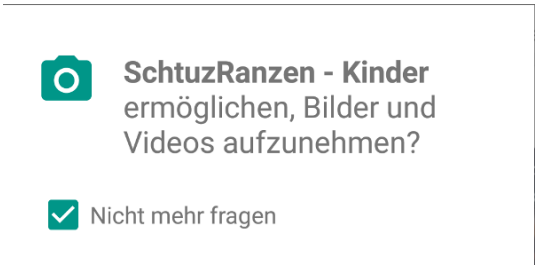
Stellungnahme Schutzranzen:

- Es ist gängige Praxis, bei der Entdeckung von Schwachstellen die Betroffenen schnellstmöglich zu informieren, und Ihnen Zeit zu geben, die Schwachstellen zu korrigieren. Dies haben wir vor kurzem bei der Entdeckung von Spectre und Meltdown beobachten können. Wir würden uns daher freuen, wenn Digitalcourage ihren Beitrag zur IT-Sicherheit leisten würde, und uns von den entdeckten Schwachstellen berichten würde, bevor sie damit an die Öffentlichkeit gehen, oder sogar versucht, sie selbst auszunutzen. In der Zwischenzeit überprüft unser Team gerade alle Komponenten unsere Lösung.
- Wir sichern unsere Kommunikation mit TLS 1.2 und einem Zertifikat, das die folgenden Cypher-Suite-Merkmale aufweist:
    - TLS ECDHE für Schlüsselaustausch
    - RSA zu Authentifizierung des Servers;
    - AES symetrische Verschlüsselung mit 128-Bit Schlüssel
    - GCM cypher mode
    - SHA 256 für die Integritätsgarantie
    - Alle diese Lösungen sind weitverbreitet und akzeptierte Standardlösungen
- Wir wurden gestern von Sicherheitsexperten der Universität Hamburg auf einen möglichen Angriff auf unsere API hingewiesen. Wir haben inzwischen einen Endpoint geschlossen, der zu Debug-Zwecken erstellt worden war. Zusätzlich wird die für Ende Januar geplante neue Version der Apps eine end to end Verschlüsselung als Merkmal haben.

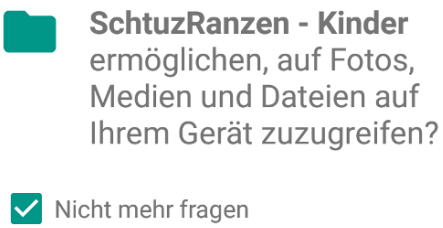
Antwort auf *“Unsere Recherche in Bildern.”*



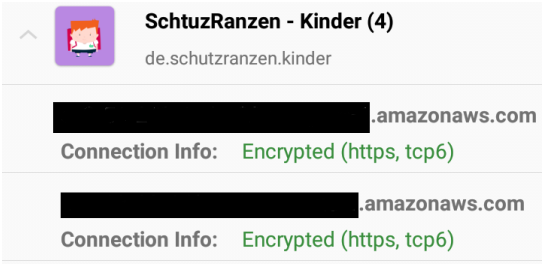
- Die Kinder App muss Zugriff auf den Standort des Smartphones haben, um die Schutzwesten-Funktionalität zu gewährleisten.



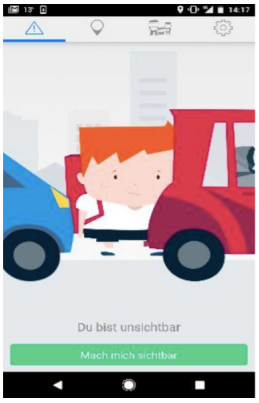
- Die Kinder-App benötigt Zugriff auf die Kamera, um sich mit der Fahrer-App zu verbinden, da dies durch das Lesen eines QR-Codes per Kamera erfolgt. Dies ist die Standardanfrage von Android für den Zugriff auf die Kamera.



- Der Zugriff auf Dateien wird benötigt, um Applikations-Daten persistent zu speichern, z.B. verbundene Eltern-Apps. Dies ist die Android Standardanfrage für den Zugriff auf Dateien.



- Das Bild zeigt, dass die App den Amazon-AWS Dienst kontaktiert, um mit dem Werkzeug Crashlytics zu kommunizieren. Hier werden keine persönlichen Daten geschickt.



- Das Bild zeigt etwas, das Digitalcourage übersehen hat. Die Sichtbarkeit der Kinder-App für die Elternteile ist opt-in, d.h. sie ist nach der Installation nicht angeschaltet und die Eltern können das Kind nicht lokalisieren. Das Kind muss die Funktion selbst anschalten, und kann sie jederzeit wieder ausschalten. Hiermit wollen wir dem Kind jederzeit selbst die Entscheidung überlassen, ob es von den Eltern lokalisierbar sein will.

Ansprechpartner für die Presse:
Schutzranzen by Coodriver GmbH
Walter Hildebrandt +49-172-6611135
b.hildebrandt@coodriver.com

Die Coodriver GmbH ist mit Schutzranzen ein deutsches Start-up-Unternehmen, das sich zum Ziel gesetzt hat, mit innovativen Technologien die Sicherheit von Kindern im Straßenverkehr zu erhöhen. Die Schutzranzen App wurde 2016 mit dem „auto motor und sport-mobility & safety Award“ ausgezeichnet.