



Mobile App Security for the Real World

Sichere Kundenschnittstelle – technische und regulatorische Herausforderungen

Build38 stellt sich vor

- Gegründet Ende 2018 von 8 Mobile Security und SaaS Experten
- Spin-off der Giesecke+Devrient (G+D) mit über 165 Jahren Security Erfahrung
- HQ in München (Germany), Töchter in Barcelona (Spain) und Singapore
- Referenzkunden in Europa und Asien aus den Bereichen Versicherungen, Financial Services, Digital Health, Automotive, Digital Plattform und Ticketing
- Millionen von Apps weltweit werden bereits von Build38 als Self-Defending App geschützt



**Vertrauen. Risiken.
Online. Digitalisierung.
Kunde. Kommunikation. Information.
Sicher oder doch eher unsicher?
Brauch ich das?
Vorteile. Umsetzung.**

Vertrauen (Trust)

Die Basis einer jeden geschäftlichen Beziehung!

An ongoing journey

There will never be a perfect solution to building trust. By definition, trying to earn trust across multiple stakeholders will almost always involve compromises, as the needs of one party will rarely be fully aligned with the needs of another.

Yet a few truths are clear. One is that being trustworthy will not hurt a business – but not being trustworthy certainly will.



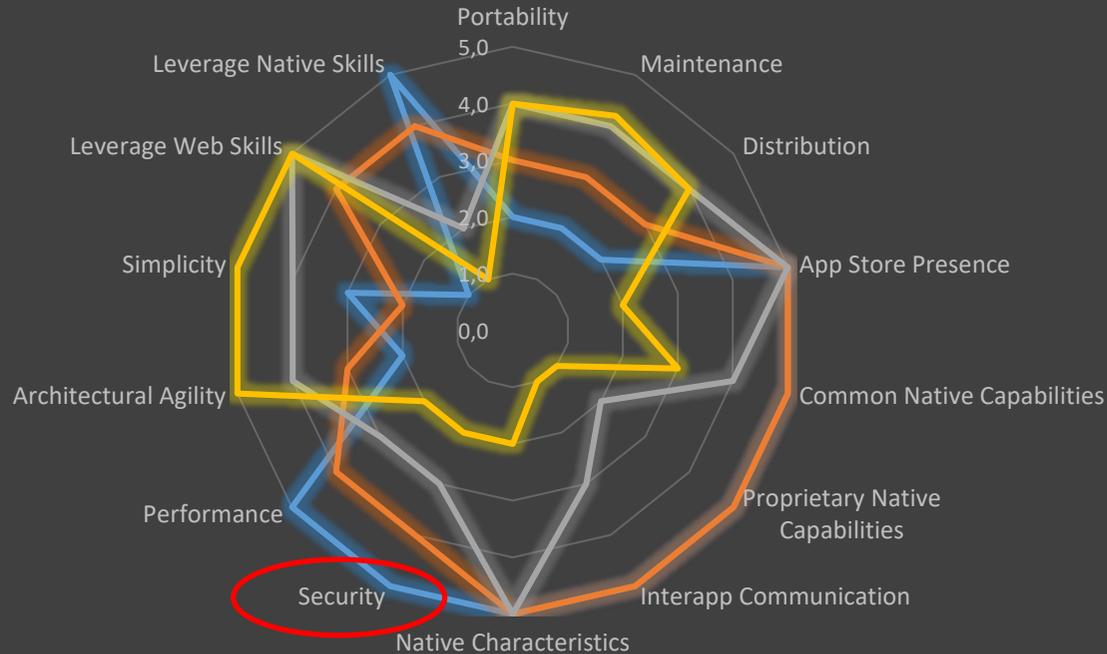
Quelle:

http://www3.weforum.org/docs/WEF_EvolutionTrustBusinessDeliveryValues_report_2015.pdf

Haben Sie folgendes schon einmal gehört?

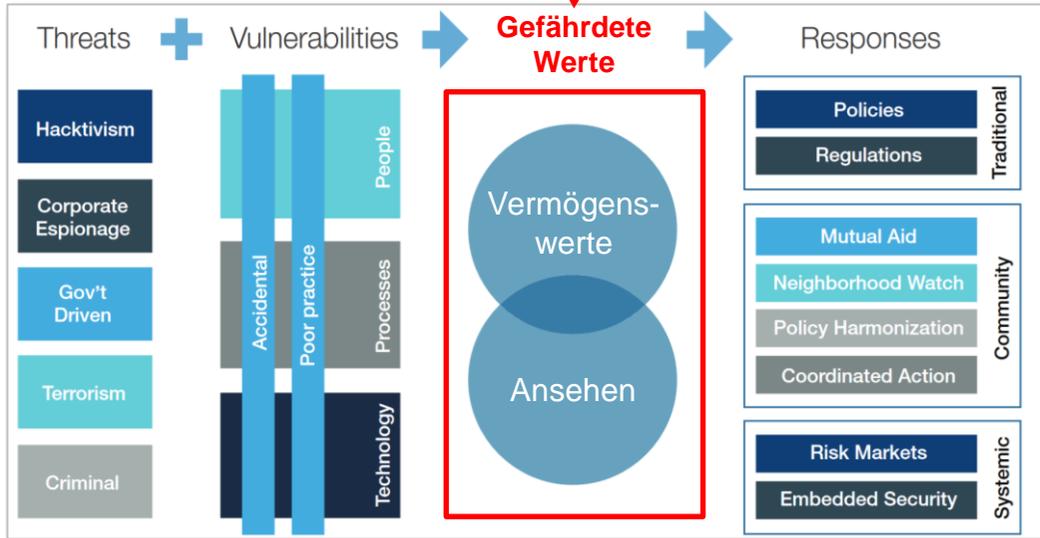
- “Wir und unsere Kunden sind sicher!”
- “Wir sind zu klein und unbedeutend um Angriffsziel zu sein.”
- “Keiner interessiert sich für uns.”

Sicht des Handels / der Industrie: Sicherheit ist oft ein (technisches) Kriterium. App Sicherheit darf kein Luxus sein!



Kennen Sie ihre Geschäftsrisiken in 2020?

Rank		Percent	2019 rank	Trend
2	Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)	44%	2 (44%)	⊖



Quellen:

World Economic Forum, 2012, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf

Allianz Risk Barometer 2020, <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020-Appendix.pdf>

Digitales Geschäftsmodell gescheitert

7-Eleven Japan, „7-pay“ nach 2 Monaten Nutzung eingestellt

COMPANIES

Seven-Eleven mobile pay hack hits Japan's drive to go cashless

Troubled start for 7pay after convenience store chain chased front-runners



The hackers that broke into accounts of Seven & I's 7pay mobile payment service are believed to have been aided by the app's lack of two-step authentication.

Nikkei staff writers
July 6, 2019 16:48 JST

7-Pay

- 900 Kundenkonten betroffen, ¥ 55 million (US\$500,000) Verlust
- Automatisierter Angriff:
Notwendige Daten zum zurücksetzen des Accounts and eine andere Email-Adresse: Name, Geburtsdatum (default Wert ausreichend), Telefonnummer

Quellen:

<https://www.sej.co.jp/company/important/20190704.html>

<https://asia.nikkei.com/Business/Companies/Seven-Eleven-mobile-pay-hack-hits-Japan-s-drive-to-go-cashless>

<https://www.theverge.com/2019/7/6/20684386/7-eleven-japan-shut-mobile-payments-app-7pay-security-flaw-cybersecurity>

Mangelnde Sorgfaltspflicht mit großer Wirkung

Untersuchung ended mit hoher Strafzahlung



2016
9000 Kunden um
£2.5 Millionen erleichtert

2018
£16.4 Millionen Strafe wegen
Verletzung der Sorgfaltspflicht

Quellen:

<https://www.bankinfosecurity.com/tesco-bank-confirms-massive-account-fraud-a-9501>

<https://www.itproportal.com/features/is-the-tesco-bank-hack-the-wakeup-call-needed-to-make-mobile-security-a-priority/>

<https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack>

Digitalisierung. Schleichend? Die Erweiterung des bekannten, oder etwas völlig neues?

Oft ist Sicherheit regulatorisch oder organisatorisch vorgeschrieben.

WeChat ist mehr als ein Soziales Netzwerk.

Die SuperApp bietet Bezahldienste, ist Plattform für den Handel, etc.



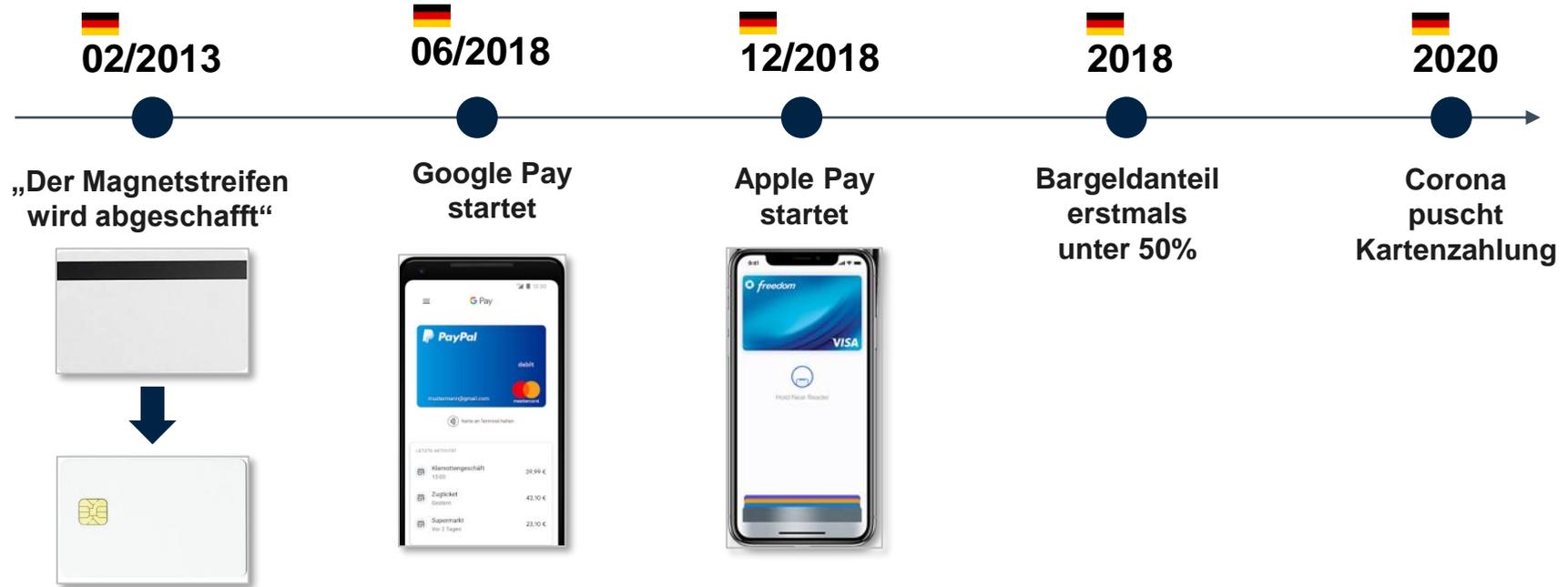
WeChat (微信),
„winzige Nachricht“

WeChat:

- 1,17 Milliarden MAU in Q1 / 2020
- 1,1 Milliarden tägliche Transaktionen mit Mini Programs (01/2019)

Quelle:
<https://www.businessofapps.com/data/wechat-statistics/>

Auch bei digitalen Bezahlvorgängen ist überall Sicherheit drin! (auch wenn es keiner sieht)



Quellen:

<https://www.welt.de/finanzen/article160307831/Der-Magnetstreifen-wird-abgeschafft.html>
<https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfcrel&hl=de>
<https://support.apple.com/de-de/HT201239>

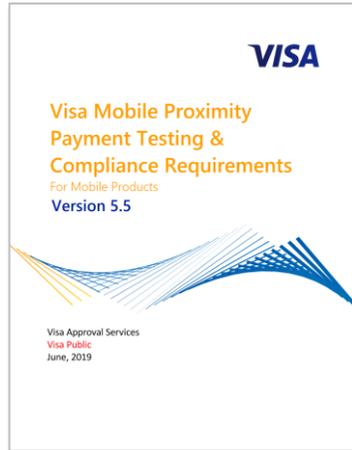
Das eRezept kommt. Schnell, einfach, fälschungssicher!

Krankenkasse bzw. Kostenträger AOK Rheinland-Pfalz		Hilfs- mittel- zahl	Impf- stoff	Soz.-St. Beleg	Begr.- Pflanzl	Apotheken-Nummer / IK	
Name, Vorname des Versicherten Mustermann geb. am Erika 12.08.1964 Heidestraße 17 51147 Köln		Zuzahlung	Gesamt-Brutto				
Kassen-Nr.	Versicherten-Nr.	Status	Arztstempel-Informationen				
106415300	A123456789	1000 1	Arztstempel-Nr.	Faktor	Taxe		
Betriebsstätten-Nr.	Arzt-Nr.	Datum	1. Verordnung				
271111100	654321161	10.07.2012	2. Verordnung				
Rp, (Bitte Leeräume durchstreichen)		Vertragsarztstempel					
Antistressin Impfstoff Amp. 10 x 0,5 ml Muster Pharma GmbH		27/1111100 Psychologische Gemeinschaftspraxis Dr. med. Markus Mustermann Dr. rer. nat. Erik Mustermann Dorfriedestraße 1 51069 Köln Tel. 02 21 / 8 87 65 43 <i>[Handwritten Signature]</i> Unterschrift des Arztes Muster 16 (7.2008)					
Bei Arbeitsunfall auszufüllen!		Abgabedatum in der Apotheke					
Unfalltag	Unfallbetrieb oder Arbeitgebernummer						
2711111004							



Quellen:
Wikipedia
<https://www.bundesgesundheitsministerium.de/e-rezept.html>
<https://www.apotheke-adhoc.de/nachrichten/detail/markt/so-funktioniert-das-erezept-von-cgm-spahn-besuch-auf-der-dmea/>

Sicherheit ist oftmals vorgeschrieben: um Risiken zu minimieren oder um Urkunden sicher ausstellen zu können



16. August 2019: „Gesetz für mehr Sicherheit in der Arzneimittelversorgung (GSAV)“



5. Mai 2020: DiGA Fast-Track

Quellen:

<https://technologypartner.visa.com/Download.aspx?id=211>

<https://www.bundesgesundheitsministerium.de/e-rezept.html>

https://www.bfarm.de/SharedDocs/Downloads/DE/Service/Beratungsverfahren/DiGA-Leitfaden.pdf?__blob=publicationFile

[https://de.wikipedia.org/wiki/Verordnung_\(EU\)_Nr._910/2014_\(eIDAS-Verordnung\)](https://de.wikipedia.org/wiki/Verordnung_(EU)_Nr._910/2014_(eIDAS-Verordnung))

eIDAS bezeichnet die EU-Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt



**Und was bringen Sicherheit
und Datenschutz dem
Handel / der Industrie?**

Der Kunde hat eine deutliche Meinung zu Sicherheit und Datenschutz

43%

der Befragten sind von Sicherheit und Datenschutz „besessen“.

77%

der Konsumenten wählen den Händler nach Cyber-Sicherheit und Datenschutz aus.

66% vs 49%

66% der Konsumenten würden mehr kaufen, wenn Zusagen gemacht würden; nur **49%** des Handels führen die entsprechenden Maßnahmen ein.

Anmerkung: Werte gelten für Deutschland.

Quelle: Capgemini 2018: https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2018/05/dti-cybersecurity-in-retail_final_web_-3.pdf

Entsprechende Maßnahmen zu Sicherheit und Datenschutz werden von den Kunden honoriert

>20%

mehr **Umsatz** durch 28% der Kunden, wenn der Handel sicheres Web und App zusichert.

14%

Prozentpunkte mehr **Kundenzufriedenheit** nach der Implementierung von Cyber-Sicherheit und Datenschutz.

Anmerkung: Werte gelten für Deutschland.

Quelle: Capgemini 2018: https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2018/05/dti-cybersecurity-in-retail_final_web_-3.pdf

Was ist zu tun?

Sichere Apps – eine kurze Handlungsempfehlung

Apps sind die wichtige Kundenschnittstelle überhaupt

1 Behandeln Sie App Sicherheit und Datenschutz nicht stiefmütterlich

2 Die sichere App in 3 Schritten – alles ist aus der App heraus überprüfbar

(und natürlich liegt die Schwierigkeit im Detail 😊)

- Die App selber muss manipulationssicher sein
- Die App sollte auf einem „sicheren“ mobilen Endgerät laufen
- Sichere Kommunikation zwischen App und Server!

To the rebels and the
pioneers, the thinkers and
the doers, the dreamers and
believers:

Go for it!

You are safe.

save/d

Thank you!



Getting in touch



torsten.leibner@build38.com
Build38 GmbH, Atelierstr. 29
81671 Munich, Germany

Handelsregister des AG München, HRB 244695