

Cyberattacke auf Meier Tobler

Martin Schäppi
Leiter Unternehmenskommunikation
9. März 2020

Agenda

1. **Profil Meier Tobler AG**
2. Cyberangriff 24. Juli 2019
3. Konsequenzen, Erkenntnisse
4. Ihre Fragen

Meier Tobler in Zahlen

meier
tobler

1300 Mitarbeitende

500 Mio. CHF Umsatz

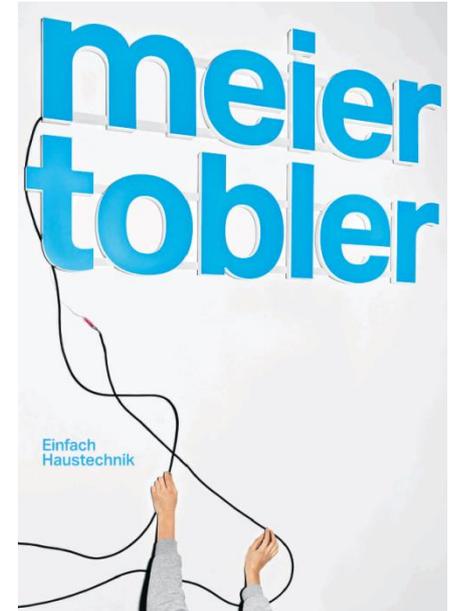
75000 Artikel im Sortiment

10000 Kunden Installateure HLKS

1500 Kunden Planer HLKS

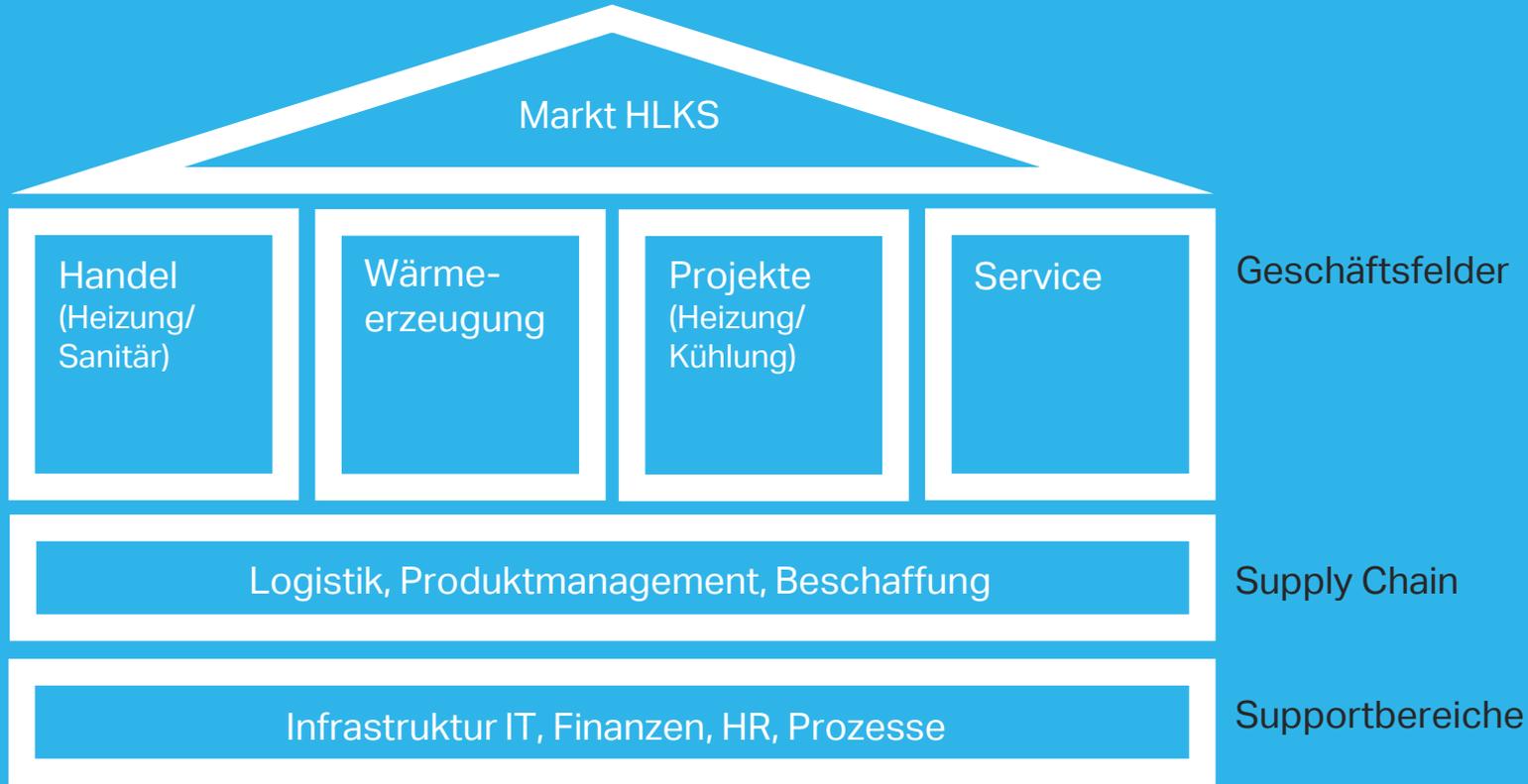
250000 Kunden Liegenschaftsbesitzer

Meier Tobler AG



Der erste Prototyp unseres
leuchtenden Logos.

Vier Säulen tragen das Geschäftsmodell





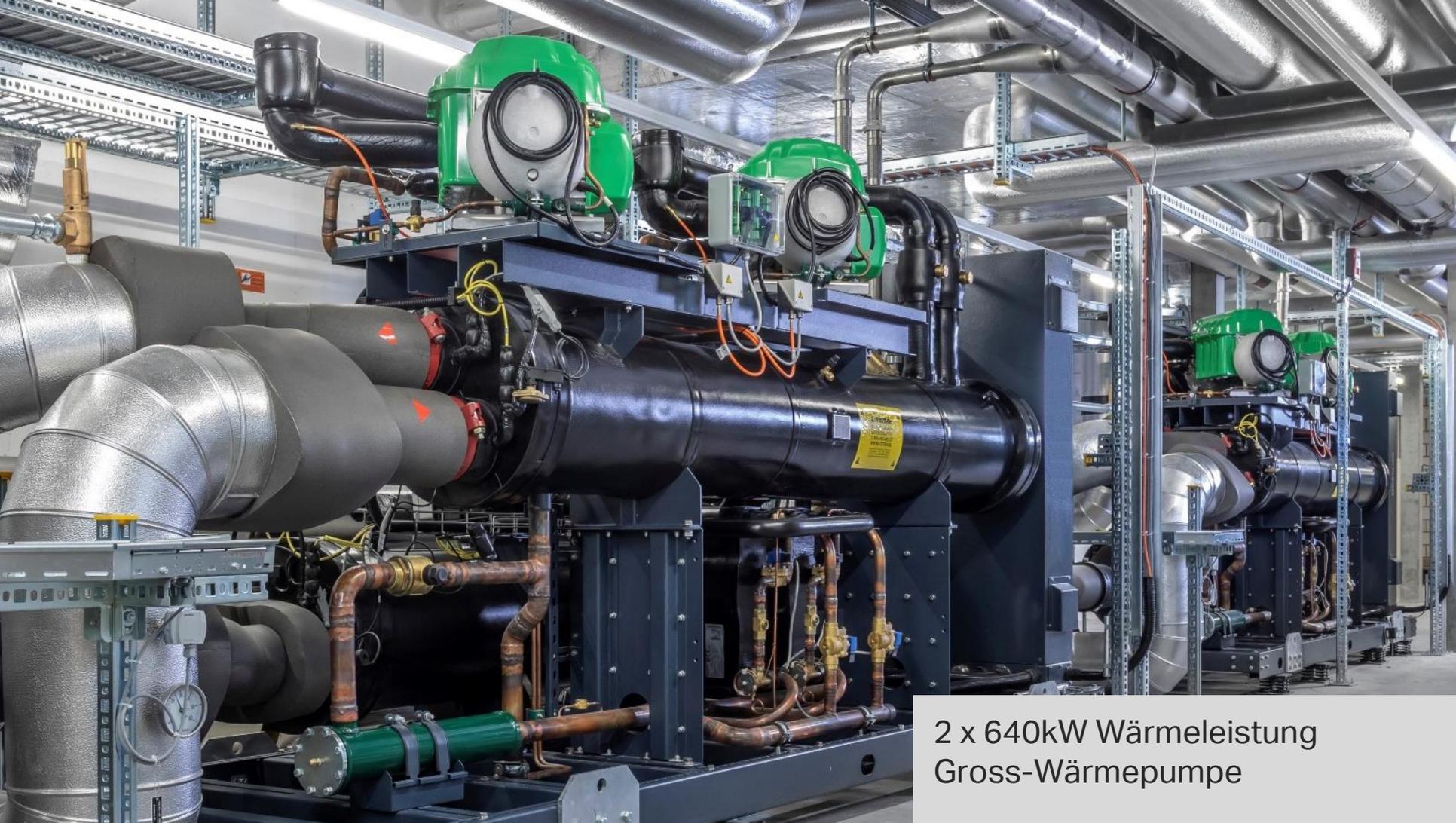
Der jüngste Marché in Bulle:
Eröffnung Mai 2019



Wärmepumpe

Brauchwarmwasser-Speicher

Heizwasser-Speicher



2 x 640kW Wärmeleistung
Gross-Wärmepumpe

«smart-guard» Fernüberwachung Wärmepumpen

**meier
tobler**



**Gewinner des
diesjährigen
«Swiss Industry
4.0 Award»**

Agenda

1. Profil Meier Tobler AG
2. **Cyberangriff 24. Juli 2019**
3. Konsequenzen, Erkenntnisse
4. Ihre Fragen

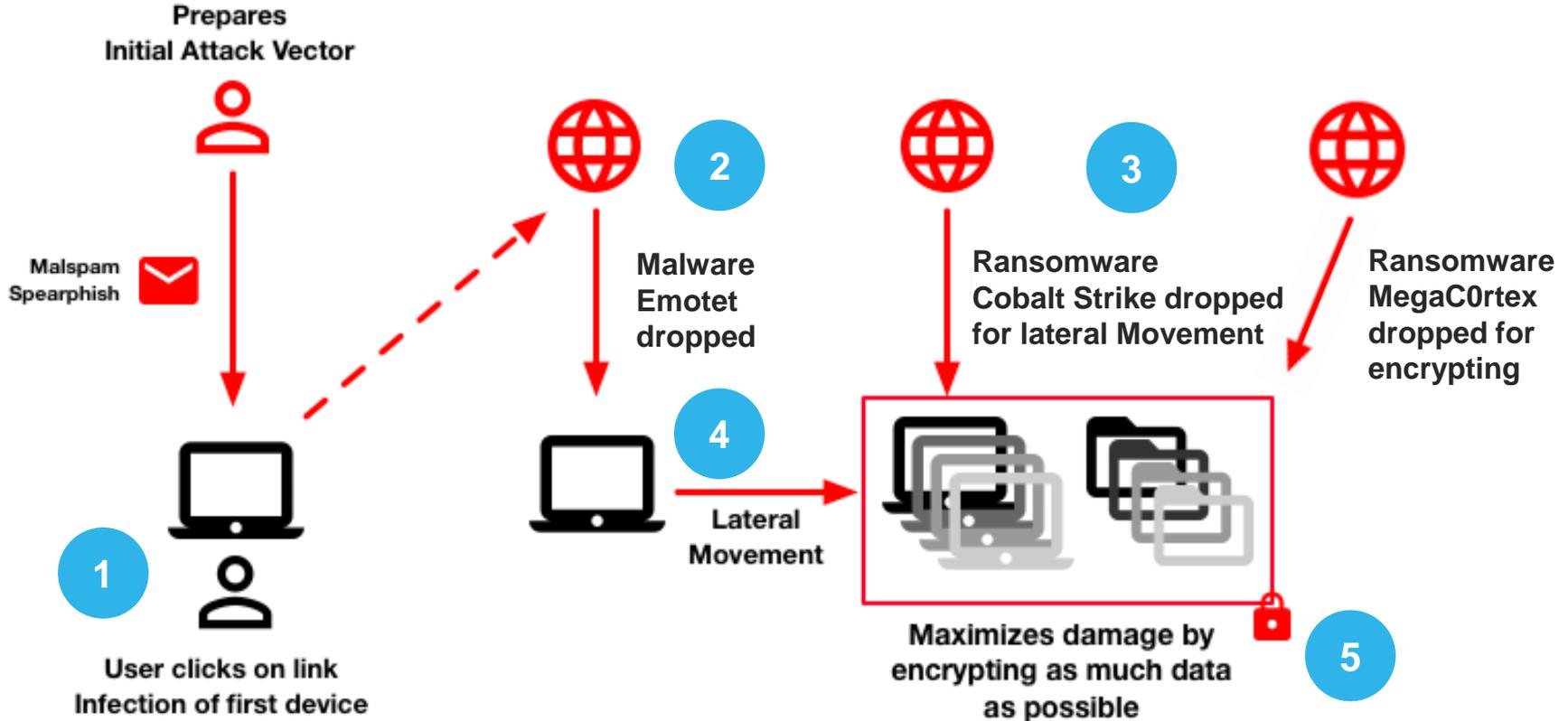
Cyberangriff 24. Juli 2019

Link auf Video:

https://vimeo.com/352427866/9c4d525a67?utm_content=CEOnewsletter%20%E2%80%93%20August%202019%20-%20DE



Cyberangriff



Emotet

- Seit 2014 bekannt
- Ursprünglich Banking Trojaner
- Etabliert Initialzugang für Verkauf im Darknet
- Ermöglicht Nachladen anderer Malware
- schwer erkennbar, mutiert im Wochentakt
- Seit April 2019 nutzt Emotet veränderte E-Mails echter Konversationen
«Dynamit Phishing»

Cobalt Strike

- Werkzeugkasten für Angriff
- Etabliert Operationsbasis
- Erlaubt die Ausbreitung im Netz

MegaCortex

- Verschlüsselungssoftware
- Erlaubt Daten zu verschlüsseln

Chronologie Cyberangriff 24. Juli 2019

Datum, Zeit	Ereignis
24.07.19 / 0200	Meier Tobler durch GIA alarmiert. Entscheid: Systeme herunterfahren
24.07.19 / 0645	Krisenstab einberufen (Sofortmassnahmen, Kommunikation)
24.07.19 / 0700	Kader wird informiert, Rückholen von Schlüsselpersonen (Ferienzeit)
24.07.19 / 0800	Krisenstab bezieht «War Room», Cyber Security Experten aufgeboten
25.07.19 / 1100	Telefonie wiederhergestellt, Not-Website online, MA-Info nach Hause
26.07.19 / 1000	20 Not-Arbeitsplätze SAP in Betrieb, Kundenanfragen werden bearbeitet
27.07.19 / 1400	E-Mail-Verkehr über Webmail online
28.07.19 / 1600	Betriebsaufnahme Lager Däniken und Nebikon, erste Auslieferungen

Agenda

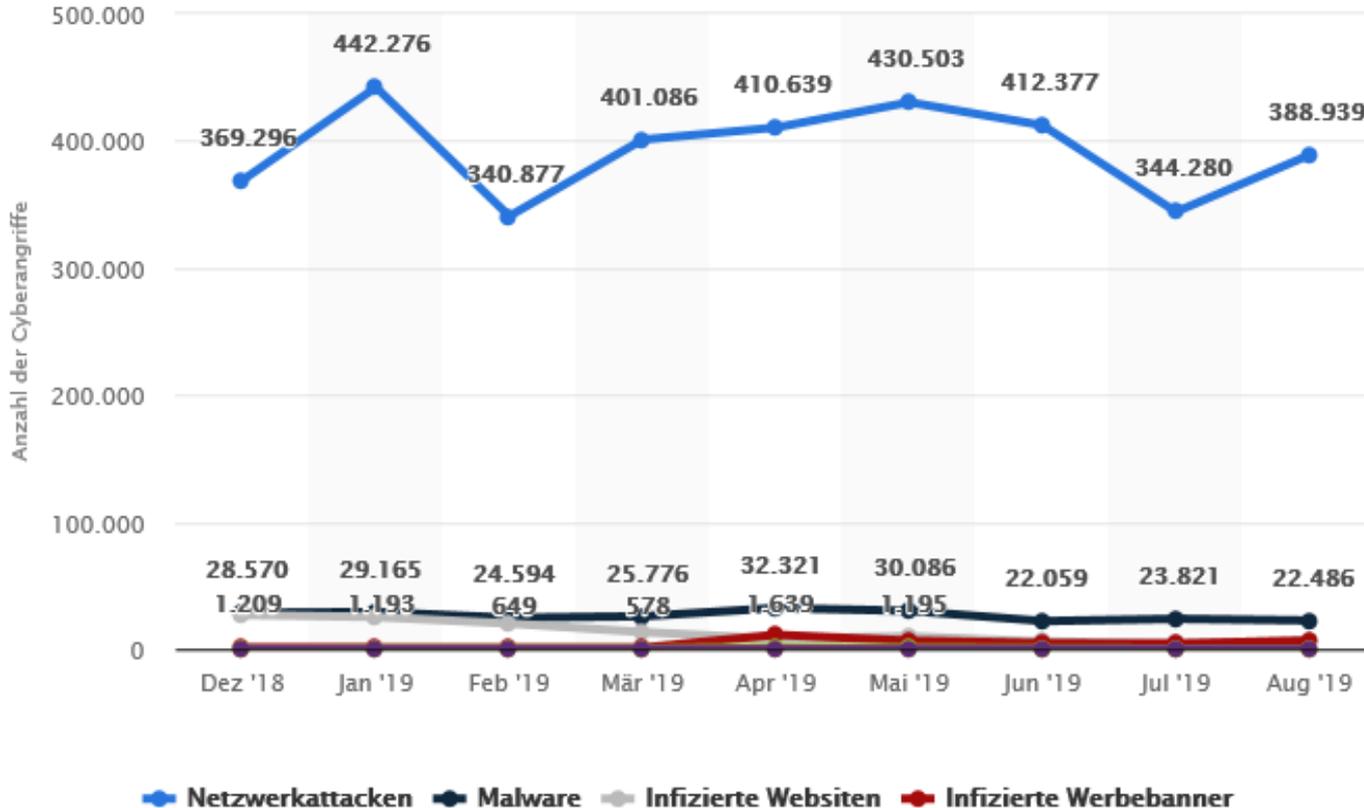
1. Profil Meier Tobler AG
2. Cyberangriff 24. Juli 2019
- 3. Konsequenzen, Erkenntnisse**
4. Ihre Fragen

- Neue Dimension der Cyberangriffe ist erreicht «Dynamit Phishing»
- Organisiertes Verbrechen betreibt Arbeitsteilung
- Kombination opportunistischer und gezielter Attacken
- Alle sind betroffen, unabhängig der Grösse
- Frage des Aufwands, den der Angreifer betreiben will
- Beim Angriff ist Mensch schwächstes Glied (Social Engineering)
- Bei Bewältigung des Angriffs ist Mensch das stärkste Element
- Klassische Sicherheits-Vorkehrungen reichen nicht mehr

- Bedrohungslage radikal verändert und verschärft, Schwachstelle Mensch!
- Zusätzliche Sicherheitsmassnahmen wie Verschärfung Policies, Dateianhänge E-Mail, Whitelisting Websites
- Einführung Zwei-Faktor-Authentifizierung
- Einführung 7x24h aktive Überwachung der Systeme (Tanium)
- Sandboxen zur Abklärung potenziell gefährlicher Mails
- Krisenorganisation muss optimiert und trainiert werden
- Notfallorganisation ≠ Krisenorganisation, Verfügbarkeit des Krisenstabs

Bedrohungslage

Registrierte Cyberangriffe in der Schweiz

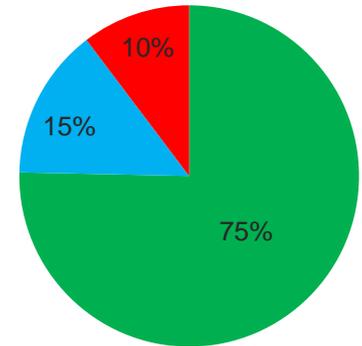


Quelle: <https://de.statista.com/statistik/daten/studie/73932/umfrage/anzahl-registrierter-cyberangriffe-pro-monat-in-der-schweiz/>

Faktor Mensch: Sensibilisierungskampagne

- Sensibilisierungskampagne Cyberkriminalität
Alle rund 1200 Anwender wurden mit fünf simulierten, personalisierten Mails aus 12 Vorlagen kontaktiert
- Auswertung der Reaktionen der Anwender
- Aufklärung der Anwender die einen Link klickten mittels interaktivem E-Learning

Anwenderverhalten



- E-Mails nicht geöffnet
- E-Mails nur geöffnet
- E-Mails geöffnet und Link geklickt

**Ich freue mich
auf Ihre Fragen!**

**Danke für Ihre
Aufmerksamkeit.**

**Alle Infos:
[meiertobler.ch](https://www.meiertobler.ch)**