RANSOMWARE AS A SERVICE - SCHADSOFTWARE AUS SOFTWAREFABRIKEN

KNF-KONGRESS 2022

ROLAND WAGNER

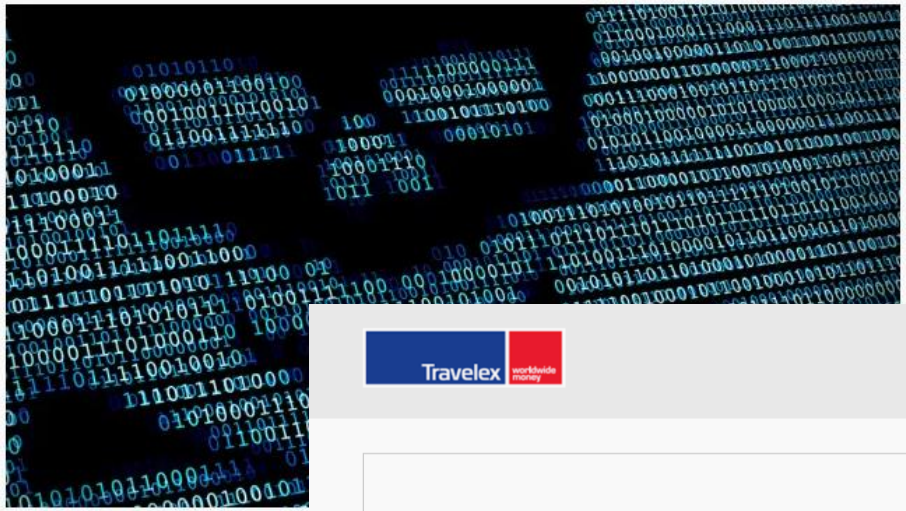
ROLAND@DATEVNET.DE


Abfahrt
Linie
Ziel
Gleis
Zeit
Über
Nach
Gleis
22:10 RB81 Flöha - Pockau-Lengefeld Olbernhau 8
22:30 RB30 Flöha - Frei - Fährt heut Hbf 11
22:31 RB30 Hohenstein (S) Hbf 10
22:36 RB80 Flöha - Zsc g-B. Süd 8
22:36 RB45 rt heute von Geithain - B Hbf 9
22:44 RE6 Einsiedel - Thalheim (Erzgeb) Aue (Sachs) 5
22:45 RB89 Flöha - Freiberg (Sachs) - Tharandt Dresden Hbf 14
23:30 RB30 Fährt heute von Gleis 11 - 11
Ooops, your files have been encrypted!
bitcoin
Check Payment
Decrypt
BMG | MIS

Frankfurt City Officials Shut Down IT Network Over Malware

Dominique Adams

20 December 2019, 04.02pm



The financial hub h
systems following

FRANKFURT, DARMSTADT, MAINZ

Stadtwerke und ÖPNV mit Ransomware angegriffen

Ein IT-Dienstleister mehrerer Energieversorger sowie Betreiber des öffentlichen Nahverkehrs wurde mit einer Ransomware angegriffen. Die Ermittlungen dauern an.

in Pocket speichern | merken

14. Juni 2022, 14:03 Uhr, Moritz Tremmel/dpa

(Bild: Mohamed Hassan/Pixabay)

Travelex

This website will be back online soon!

This website is temporarily unavailable while we make upgrades to improve our service to you.

We are sorry for any inconvenience and thank you for your patience.

Thank you for using Travelex!

velex UK Limited - Registered Number 01985596. Registered Office - 65 Kingsway, London WC2B 6TD.

HR0cHM6Ly93d3cuZ29vZ2xlLmRlLw&guce_referrer_sig=AQAAAJzgKC1N1bNDjYNmi6nT9lVwxz_r748bEBv
Yuqe-
t5_khCoNQCR5OatkETLdZUCtDyNOpDWmQUVWs5dfx6TQtDzTG-qiW_X4O0StELGUDE

Travelex Ransomware Attack Enters Its Third Week

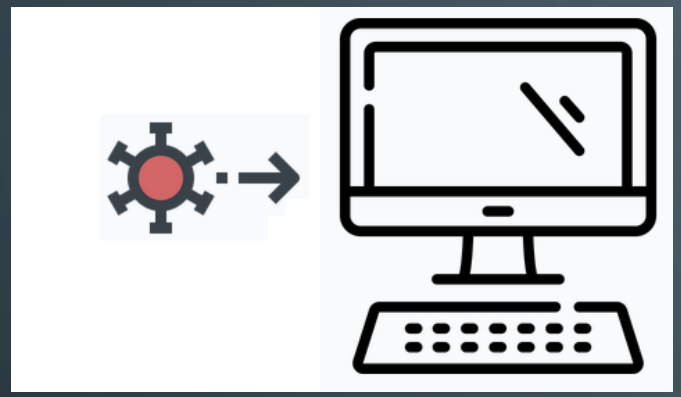
Hutsix

BREACH OF THE MONTH

WAS IST „RANSOMWARE“

„ransom“ = Lösegeld „ware“ (Software / Hardware)

WIE FUNKTIONIERT „RANSOMWARE“ ?

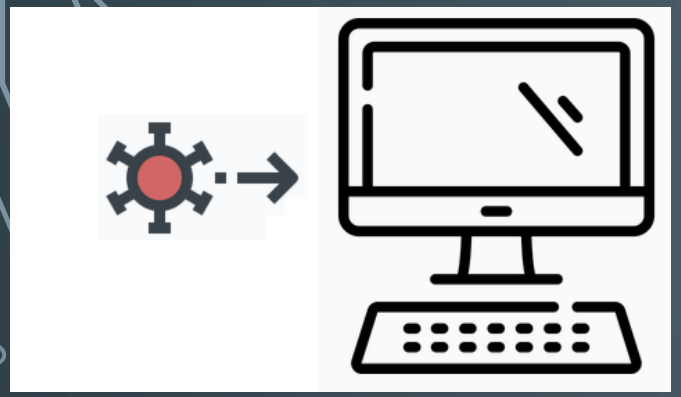


- Mail-Attach
- Drive-By-Download
- Schwachstellen

HTTPS, IRC, Tunnel
(SSH, DNS, ICMP) zu C&C-Server

- automatisiert
- manuell
- IBAN, Kreditkarten, Keys, Wallet, persönliche Daten …
- Kommunikation zu C&C-Server

Autostart, Scheduler, Service,
Plugins, (DLL-) Injection, …
(„Bekannte Methoden“)



Viren

Trojaner

Würmer

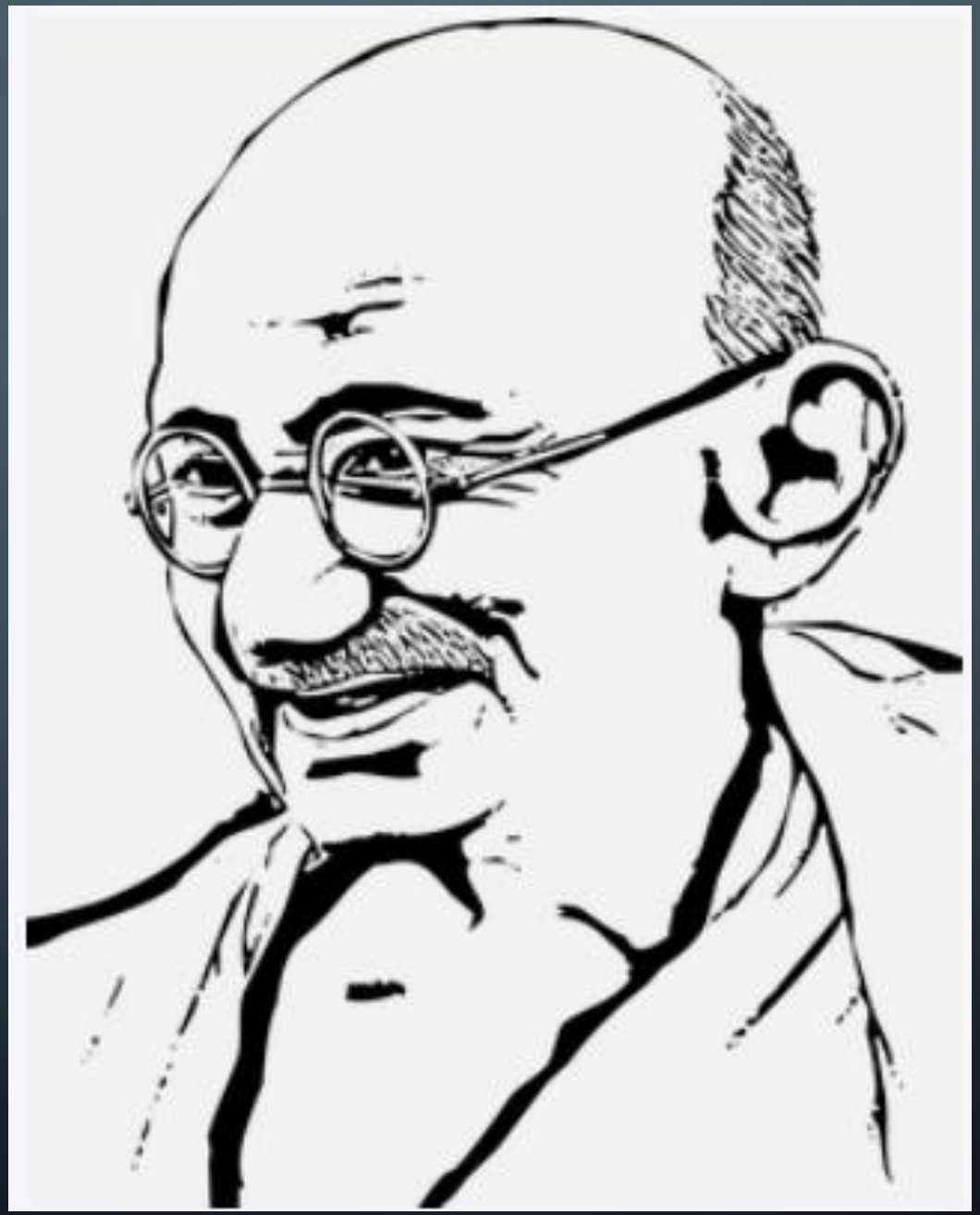
Schadsoftware

Botnetz

„SPEZIALFUNKTION“

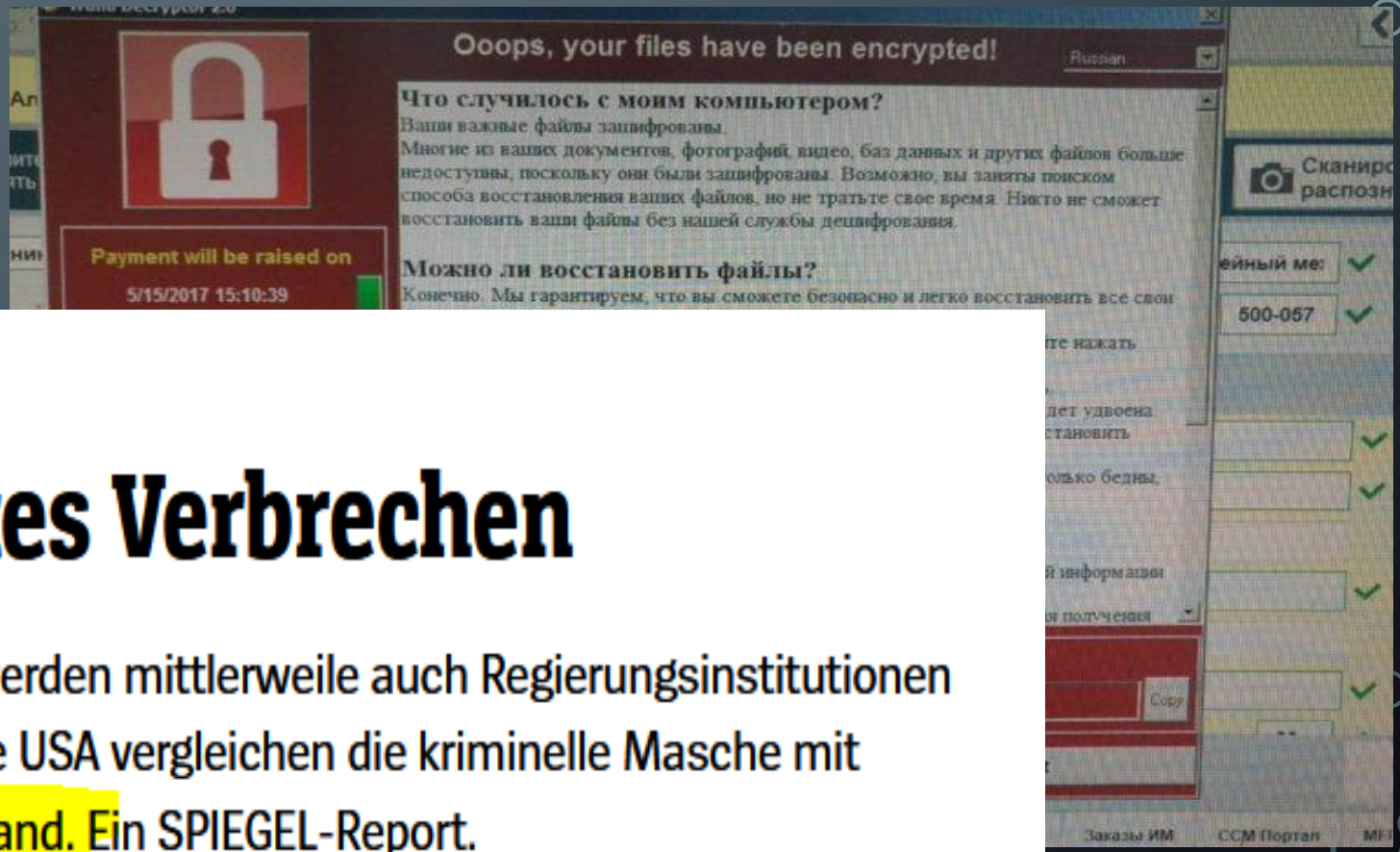
https://www.hackread.com/russian-postal-service-hit-by-wannacry-ransomware/

WER MACHT DENN SOWAS?



WER MACHT DENN SOWAS?

WER MACHT DENN SOWAS?



Die Erpressungstrojaner russischer Hacker

S+ Ein nahezu perfektes Verbrechen

Neben Unternehmen und deren Kunden werden mittlerweile auch Regierungsinstitutionen zum Opfer von Ransomware-Angriffen. Die USA vergleichen die kriminelle Masche mit Terrorismus. Die Spur führt oft nach Russland. Ein SPIEGEL-Report.

https://www.spiegel.de/netzwelt/netzpolitik/ransomware-die-erpressungstrojaner-russische-hacker-a-8749c550-120b-482b-8732-c9e01c945461

WER MACHT DENN SOWAS?
RAAS (RANSOMWARE AS A SERVICE)

- „Crimeware-Kits“ / „Rent an Attack“
- Spezialisten für jeden Bereich
- Kein IT-Wissen notwendig
- Professionelle Software-Entwicklung (9to5)
- Professioneller Service (Chat, 14 Tage: Key kostenlos, …)
- Erpressung: Target dependent amount !

WER MACHT DENN SOWAS?
RAAS (RANSOMWARE AS A SERVICE)

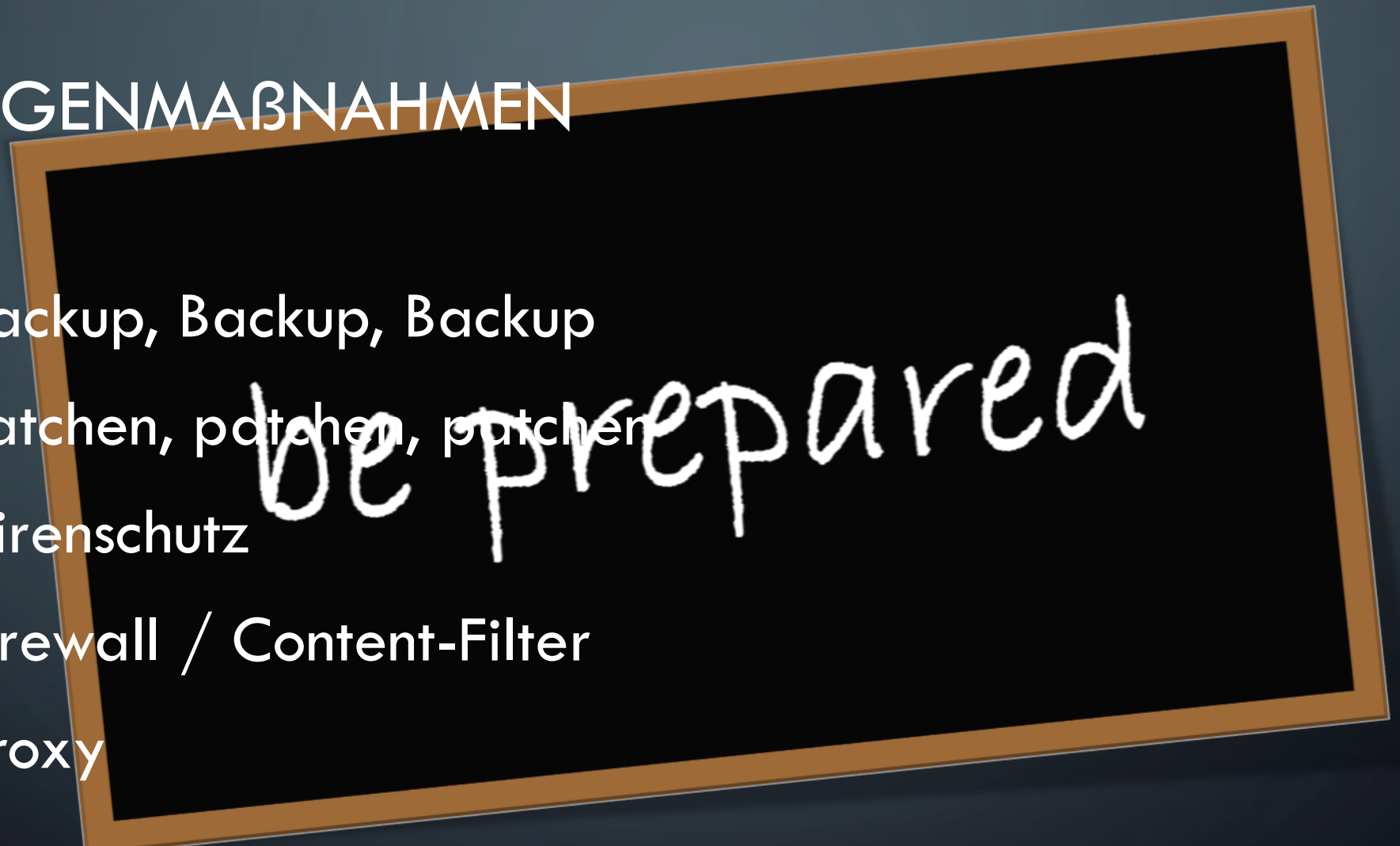
DarkSide:

"… our goal is to make money, and not creating problems for society…"

FunFact: Juni 2019: „GandCrab geht in Rente"

GandCrab seit Januar 2018; mehr als 2 Milliarden $

GEGENMAßNAHMEN



- Backup, Backup, Backup
- Patchen, patchen, patchen
- Virenschutz
- Firewall / Content-Filter
- Proxy
- Awareness

GEGENMAßNAHMEN

- Internet trennen / Segmente trennen
- Rechner ausschalten
- Neustart nutzlos! (persistence)
- von USB booten
- Kill Switch
- „Root cause“ finden !

GEGENMAßNAHMEN

- „Bezahlen oder nicht bezahlen, das ist hier die Frage“
  - „**Nicht bezahlen !!!**“
  - bezahlt? „Schlüssel oder nicht Schlüssel, das ist …“
- Temporäre Dateien
- Schlüssel extrahieren
- Teilverschlüsselung
- „Sicheres“ Backup verwenden

GEGENMAßNAHMEN

No More Ransomware & bleib-Virenfrei

NO MORE RANSOM

bleib-Virenfrei

Achtung double extorsion (Multiple extorsion) !

GEGENMAßNAHMEN - PRIVAT

- Backup, Backup, Backup
- Patchen, patchen, patchen
- Nur vertrauenswürdige Software
- Virenschutz
- Administrator? → User !
- Keine persönlichen Daten
- Keine unbekannten USB-Sticks

GEGENMAßNAHMEN - PRIVAT

- Lokale Firewall
- (externe Firewall / Content-Filter) -> pfSense (auch virtuell)
- (Proxy) -> pfSense , squid (auch virtuell)
- Awareness
- Anzeige erstatten!

Stopp, nicht nachmachen

Infraud: US-Justiz gelingt Schlag gegen Cybercrime-Ring

Ukrainische Cyberpolizei verhaftet Ransomware-Bande Cl0p

Behörden der Ukraine und Südkoreas feiern einen Schlag gegen die Ransomware-Bande Cl0p in Kiew. 6 Personen sind verhaftet, Bargeld, Kfz, Computer beschlagnahmt.

RANSOMWARE

Revil-Mitglieder verhaftet

Ermittlern ist ein Schlag gegen die Ransomware-Gruppe Revil gelungen. Diese hatte unter anderem den IT-Dienstleister Kaseya gehackt.

AUSGESCHALTET: GLOBALE RANSOMWARE-ERPRESSER ENDLICH GEFASST

LockBit: Russisch-kanadischer Ransomware-Operator festgenommen

Nach jahrelangen Ermittlungen konnten amerikanische Behörden einen Operator der LockBit-Gruppe verhaften. Der russisch-kanadische Bürger Mikhail Vasiliev wurde in Kanada festgenommen und könnte demnächst in die Vereinigten Staaten ausgeliefert werden.


Any
Questions