Definitionen - Cybersicherheit

Wirtschaftslexikon

Cybersecurity ist der Schutz von Netzwerken, Computersystemen, cyber-physischen Systemen und Robotern vor Diebstahl oder Beschädigung ihrer Hard- und Software oder der von ihnen verarbeiteten Daten sowie vor Unterbrechung oder Missbrauch der angebotenen Dienste und Funktionen.

Bundesamt für Sicherheit in der Informationstechnik

Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik.

Kaspersky

Als Cybersicherheit bezeichnet man die Praktik der Verteidigung von Computern, Servern, Mobilgeräten, elektronischen Systemen, Netzwerken und Daten vor böswilligen Angriffen.

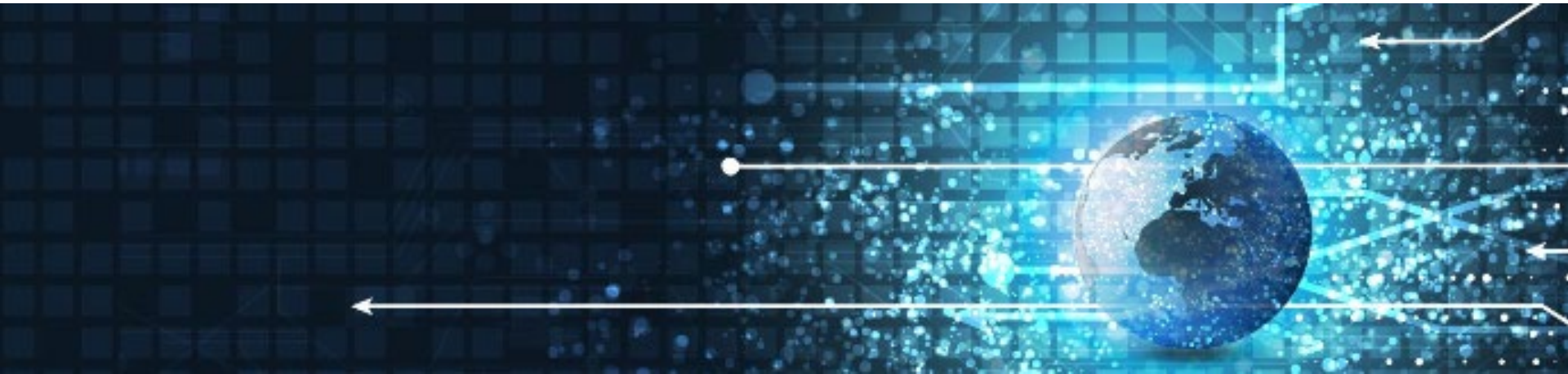
AMT FÜR INFORMATIK
FÜRSTENTUM LIECHTENSTEIN

«Cyber Security»
wo fängt es an
und was ist es wirklich?

"Wenn man Cybersicherheit nur als Informatik-Problem betrachtet,
glaubt man auch, dass die gesamte Belegschaft eines Unternehmens -
vom CEO hinunter - nur ein grosses HR-Problem darstellt.»

Steven Chabinsky

24. September 2019



Zu meiner Person

Thoma Patrik

- Information Security Manager – Liechtensteinische Landesverwaltung
  - patrik.thoma@llv.li
  - +423 236 76 07

Aufgaben

- Sicherheitskonzepte & -analysen überprüfen
- Aufbau, Einführung & Weiterentwicklung ISMS
- Awareness
- Ausarbeitung & Anpassung von Sicherheitsvorschriften
- Umsetzung & Weiterentwicklung der Sicherheitsvorschriften
- Security-Audits
- Risikoeinschätzungen

Agenda

1. IT-Sicherheit / Informationssicherheit
2. Cyber-Sicherheit
3. Cyber-Strategie
4. NIS-Richtlinie

IT-Sicherheit / Informationssicherheit

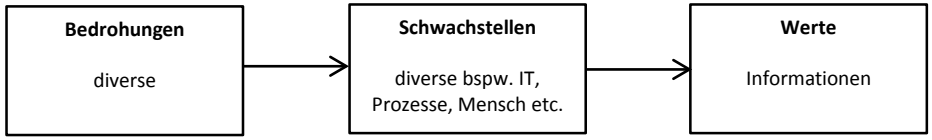
IT-Sicherheit

Die IT-Sicherheit befasst sich grundsätzlich mit dem Schutz der technologie-basierten Systeme und Infrastrukturen, auf welchen digitale Informationen allgemein gespeichert und/oder übertragen werden.

Im Fall der IT-Sicherheit scheint klar, dass die technologische Infrastruktur (IT) als der (Vermögens-)Wert betrachtet wird, welcher geschützt werden muss.

Informations-Sicherheit

Die internationale Sicherheits-Norm ISO/IEC 27001 definiert Informationssicherheit als Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen unabhängig der entsprechenden Darstellungsform oder Ausprägung der jeweiligen Information (Digital, Papier, Wort, Bild, usw.).



Schutzziele - CIA

Confidentality

Gewährleistung, dass Informationen nur für diejenigen zugänglich sind, die dazu berechtigt sind

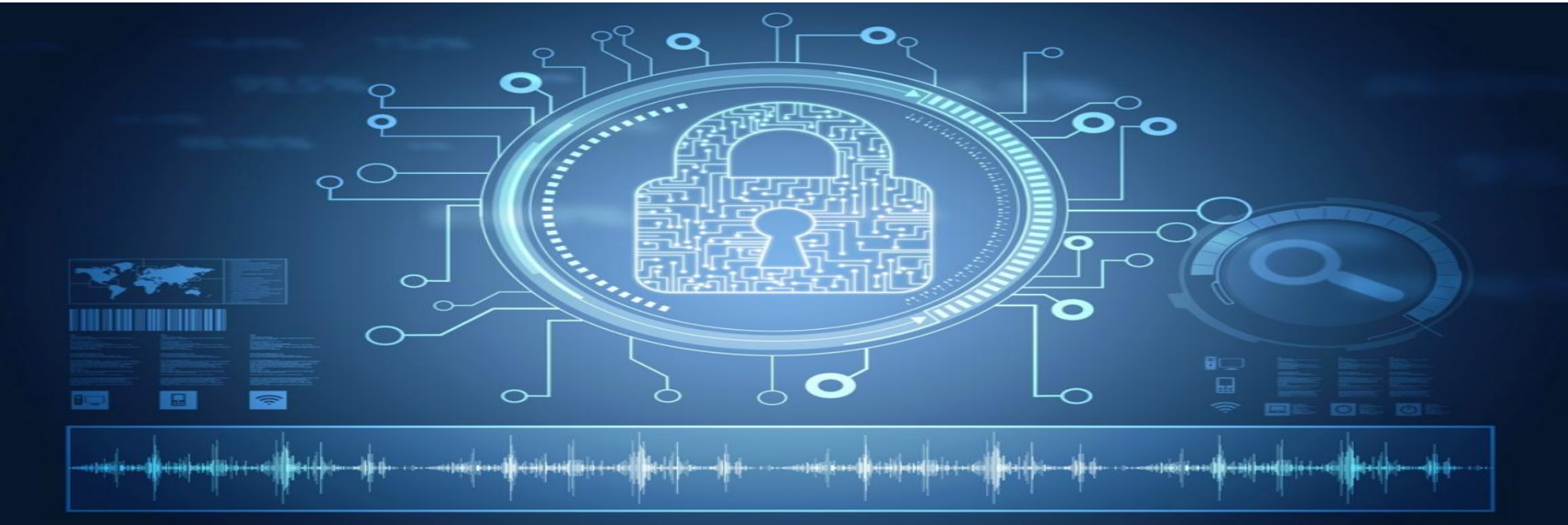
Integrity

Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden

Availybility

Gewährleisten, dass autorisierte Benutzer zu definierten Zeiten Zugriff auf Informationen haben

Cyber-Sicherheit



Cyber-Sicherheit / Szenarien

- Cyber-Mobbing: Verleumdung, Belästigung, Bedrängung und Nötigung anderer Menschen → Wert: Mensch

- illegales Teilen von digitalen Inhalten (Torrent): Unterhaltungsbranche verliert nach wie vor jedes Jahr grosse Beträge → Wert: Besitzer der Rechte an Inhalten - Wertesystem der Gesellschaft

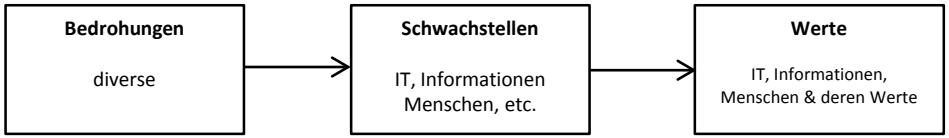
- Cyber-Terrorismus: Cyber-Terroristen greifen über den Cyberspace kritische Infrastrukturen (Elektrizitäts- und Wasserversorgung, Telekommunikationsnetze, Transportinfrastrukturen etc.) an → Wert: Bevölkerung

Cyber-Sicherheit

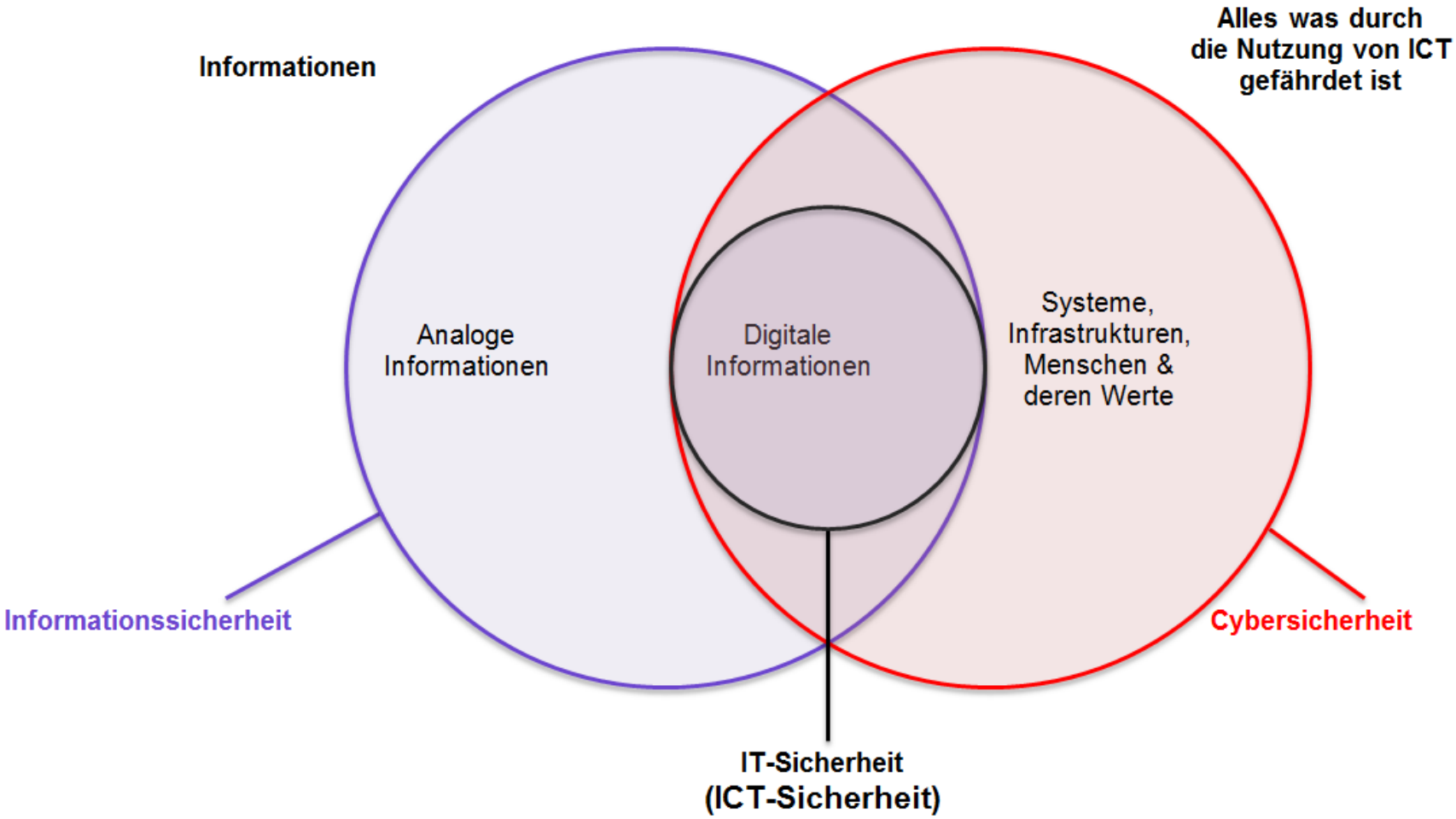
Neben der IT sowie Informationen müssen bei Cyber auch weitere Werte geschützt werden wie bspw.:

- Menschen
- die Interessen der Gesellschaft (z.B. ihr Wertesystem)
- kritischen Infrastrukturen

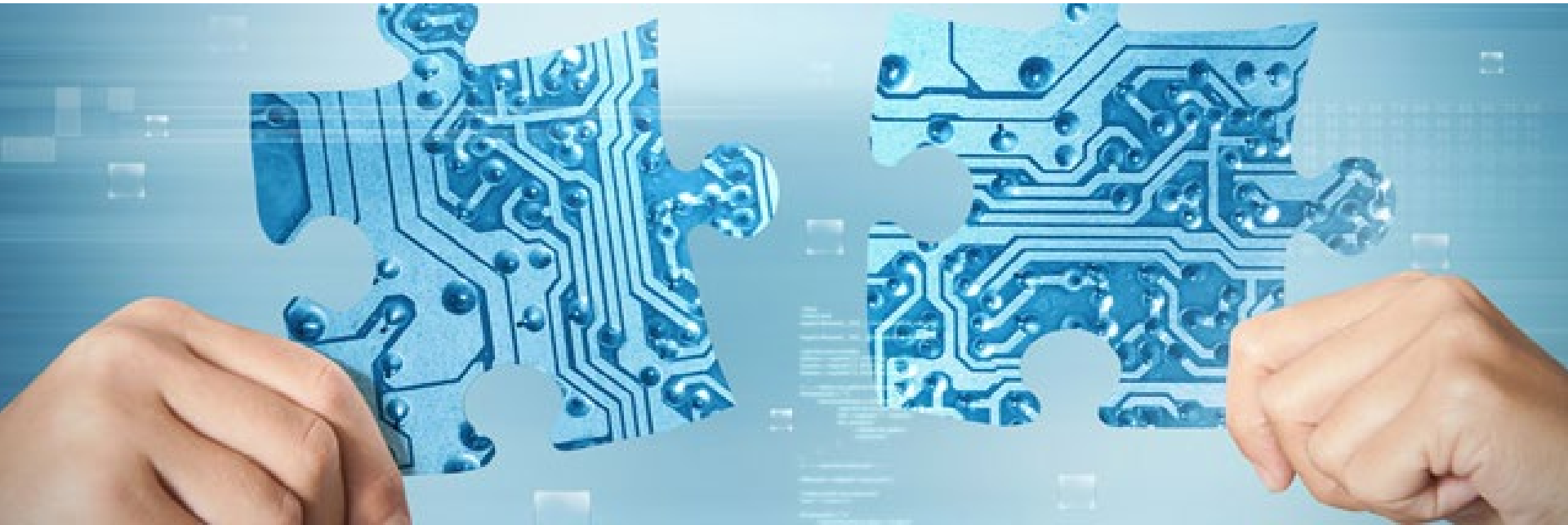
Cyber-Sicherheit wird zu einer Erweiterung der Informationssicherheit. Sie schützt nicht nur Informationen und Systeme, die Informationen verarbeiten, sondern auch die Ressourcen, die wir in einer „Cyberumwelt“ nutzen und macht auch vor der Bevölkerung und gesellschaftlichen Werten nicht halt.



Differenzierung



Cyber-Strategie



Strategien der Nachbarsländer

Österreich

7 Handlungsfelder mit 15 konkreten Massnahmen

Deutschland

4 Handlungsfelder mit insgesamt 29 Massnahmen

Schweiz

7 Handlungsfelder und 16 Massnahmen

→ NCS-II: Ausdehnung über die Verwaltung und Kritische Infrastrukturen hinaus auf die gesamte Wirtschaft (inkl. KMU) und die Gesellschaft

Gemeinsamkeiten

Kompetenzförderung

Forschung & Entwicklung, Bildungsangebot, Awareness etc.

Gesetzgebung

Überprüfung bestehender Rechtsgrundlagen, Strafverfolgung stärken etc.

Koorperation

Bilaterale, regionale, nationale und internationale Unterstützung

Organisation

Einrichtung von Steuerungsgruppen, Schaffung von Strukturen etc.

Kritische Infrastrukturen

Stärkung und Verbesserung der Widerstandsfähigkeit (Resilienz)

Niemand ist eine Insel

- Mehrheit der Kritischen Infrastrukturen hängen europa-/weltweit zusammen
- Cyber stoppt an keiner Landesgrenze
- Vorfälle eines Partners sind auch Bedrohungen für die eigene Sicherheit

➔ Alle haben dieselben Herausforderungen, welche isoliert nicht gemeistert werden können

Strategien für FL als Kleinstaat

- Fokussierung und Pragmatismus
- Priorisierung
  - Bewusst Entwicklungen abwarten
- Internationale Vernetzung
  - Kooperationen anstreben
  - Von guten Beispielen lernen
- Flexibilität nutzen
  - Agilität bringt Geschwindigkeit

Richtlinie (EU) 2016/1148 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Schutzniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie)

NIS-Richtlinie (EU) 2016/1148

Die NIS-Richtlinie soll der Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen dienen. Um dieses hohe Sicherheitsniveau zu erreichen, sieht die Richtlinie folgendes vor:

- die Pflicht für alle Mitgliedstaaten, eine nationale Strategie festzulegen;
- die Schaffung einer internationalen Kooperationsgruppe;
- die Schaffung eines internationalen Netzwerks von Computer-Notfallteams;
- Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste;
- Benennung von nationalen zuständigen Behörden, zentralen Anlaufstellen und Computer Security Incident Response Teams (CSIRTs);
- Einführung von Sanktionen für Verstösse, die wirksam, angemessen und abschreckend sein müssen.

NIS-Richtlinie betrifft

- Betreiber kritischer Infrastrukturen
- wichtige Anbieter von Diensten der Informationsgesellschaft
- Ausgenommen sind:
  - Kleinstunternehmen
  - Telekommunikationsanbieter
  - Vertrauensdienstanbieter (eIDAS-VO)

Definition Cyber-Sicherheit

Definitionen - Cybersicherheit

Wirtschaftslexikon

Cybersecurity ist der Schutz von Netzwerken, Computersystemen, cyber-physischen Systemen und Robotern vor Diebstahl oder Beschädigung ihrer Hard- und Software oder der von ihnen verarbeiteten Daten sowie vor Unterbrechung oder Missbrauch der angebotenen Dienste und Funktionen.

Bundesamt für Sicherheit in der Informationstechnik

Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik.

Kaspersky

Als Cybersicherheit bezeichnet man die Praktik der Verteidigung von Computern, Servern, Mobilgeräten, elektronischen Systemen, Netzwerken und Daten vor böswilligen Angriffen.

→ aus privatwirtschaftlicher Sicht sicherlich korrekt

Fragen

Besten Dank für Ihre Aufmerksamkeit