AKTIONSTAG: DIGITALE SICHERHEIT IM BETRIEB

SESSION:
IMMER SICHER VERBUNDEN

– EIN SICHERER ZUGRIFF AUFS INTERNET – AUCH UNTERWEGS UND IM HOME-OFFICE – GELINGT MIT EINEM VPN. WIE ZEIGEN IHNEN, WIE'S GEHT.

NRW, 11. MAI 2022, 12:10 – 12:50 Uhr

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

WAS SIE IN DER HEUTIGEN SESSION ERWARTET?

EINFÜHRUNG

LIVE DEMO

LEARNINGS

FRAGEN & ANTORTEN


EINFÜHRUNG

WARUM IST EINE „SICHERE VERBINDUNG“ NÖTIG?

- Es besteht mehr oder weniger eine Notwendigkeit, zu jedem Zeitpunkt von jedem Gerät aus von überall auf meine Informationen zugreifen zu können
- Die Informationen können in der Cloud liegen, dann werden die Informationen meist zwangsläufig über das Internet abgerufen
- Die Informationen können im lokalen Rechenzentrum liegen:
  - Datenbanken (z.B. selbst entwickelt)
  - Kundeninformationen
  - Geschäftszahlen, etc.

► Es müssen sensible Daten aus einem sicheren Netzwerk über ein unsicheres Netzwerk (Internet) übertragen werden

WARUM IST EINE „SICHERE VERBINDUNG“ NÖTIG?

- Die Nutzung von **öffentlichen WLAN´s** (Freifunk, Flughäfen, Hotels, etc) geschieht **meist unverschlüsselt**.
- Hier muss insbesondere auf eine hinreichende Verschlüsselung geachtet werden.
- Da außerdem in den meisten Fällen die Geräte eines WLAN´s untereinander sichtbar sind, muss besonders auf die Absicherung des Gerätes geachtet werden, z.B. durch eine lokale Firewall.

JEDER(!) HAT DIE PFLICHT, DURCH SEIN EIGENES HANDELN NIEMANDEM SCHADEN ZUZUFÜGEN.

DEMO: KLARTEXT-PROTOKOLLE

- Zu den Anfangszeiten des Internet hat man sich nicht wirklich Gedanken über einen sicheren Transport gemacht
- Viele Protokolle übertragen daher Informationen im Klartext:
  - Web-Protokoll: HTTP
  - Datei-Übertragungen: FTP
  - E-Mail Transport: SMTP
  - Tool zum Konfigurieren von Komponenten: TELNET
  - etc.

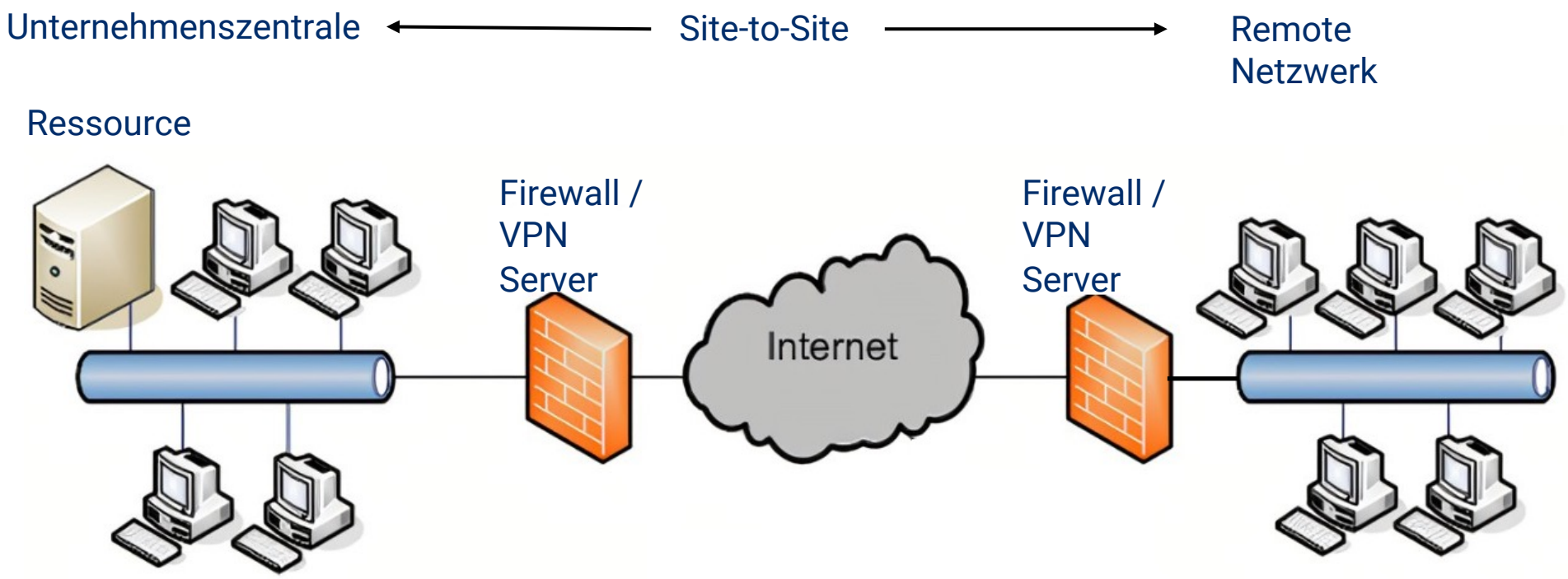
DEMO: KLARTEXT-PROTOKOLLE

- Erst im Laufe der letzten Jahre wurden diese Protokolle „sicher“ gemacht:
- HTTP ► HTTPS
- FTP ► FTPS oder S-FTP
- SMTP -> bis heute ein Klartext-Protokoll, welches aber meist in entsprechende sichere Pakete eingebettet wird (TLS) oder es wird gleich die ganze E-Mail verschlüsselt
- TELNET ► SSH (Secure Shell)

ERLÄUTERUNG DES BEGRIFFES VPN

- VPN bedeutet „Virtuelles privates Netzwerk“
- Ursprünglich entwickelt, um zwei oder mehrere komplette, private Netzwerke zu verbinden
- VPN bedeutete nicht zwangsläufig „verschlüsselt“, das ist heute anders

VPN – URSPRÜNGLICHE VERWENDUNG



Vorteile:

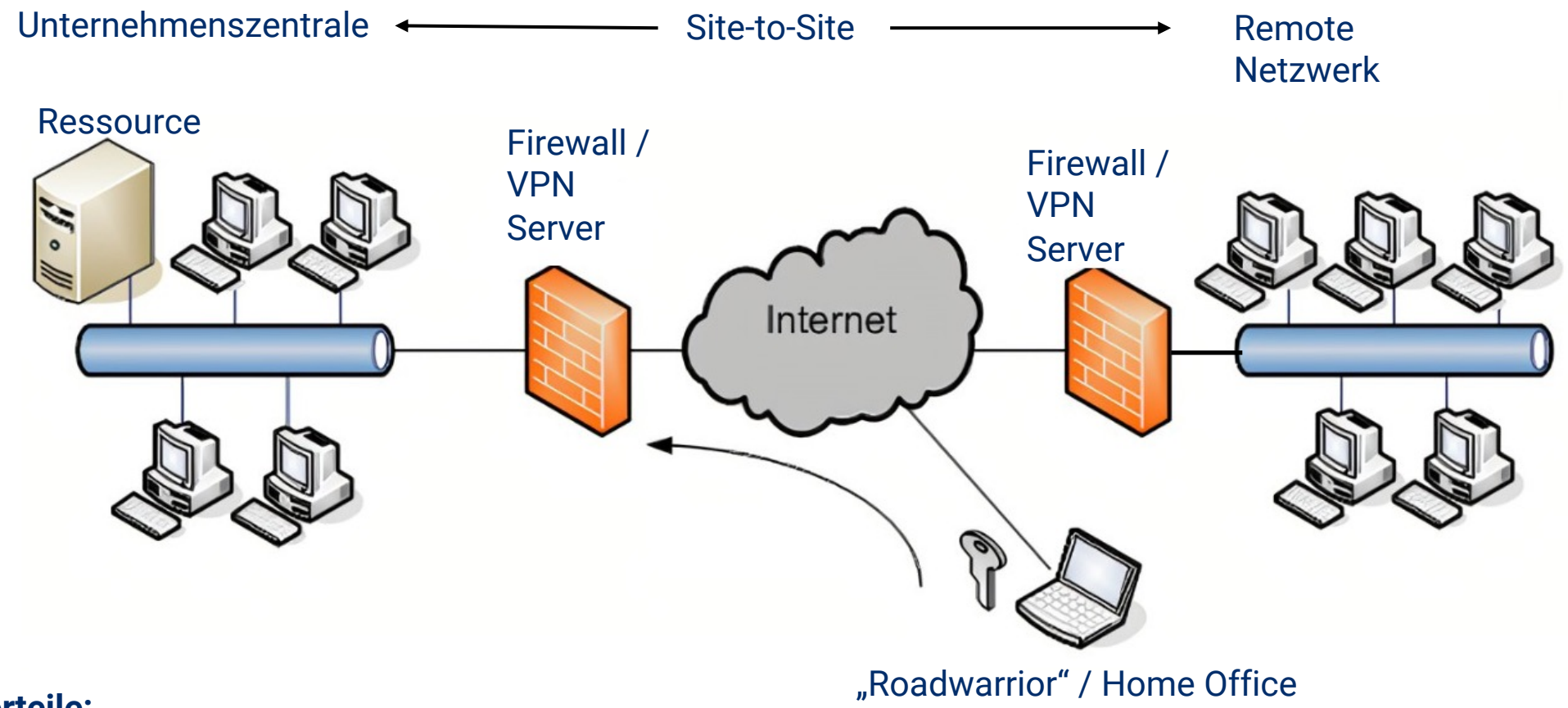
- sehr sichere Verbindung durch implementierte Verschlüsselungs- und Authentifizierungsmechanismen
- transparent für den Anwender

Nachteil:

- relativ schwierig zu implementieren. Durch die Netzwerkstrukturen ergibt sich möglicherweise eine hohe Komplexität

Tipp: Immer VPN-Gateways vom selben Hersteller/Entwickler nehmen.

VPN – ALLGEMEINE VERWENDUNG



Vorteile:

- sehr sichere Verbindung durch implementierte Verschlüsselungs- und Authentifizierungsmechanismen

Nachteil:

- Unterstützung durch den Anwender benötigt (Installation und Konfiguration des VPN Clients)

Tipp: Meistens bieten die Hersteller der VPN-Gateways auch die passenden VPN-Clients an


PRAXISGUIDE

ENTSCHEIDUNGS-MATRIX

Der Farbverlauf stellt sowohl den Grad der Sensitivität der Informationen als auch die Komplexität der Konfigurationen dar.

ZUGRIFF AUF	STANDORT	ART DER VERBINDUNG	EINSATZ VON
Unkritische Informationen im Internet (surfen)	Öffentlicher Ort, Home Office	WLAN, kabelgebunden	Mindestens https Verschlüsselung
Sensible oder personenbezogen Daten im Internet (Kontendaten, etc)	Öffentlicher Ort, Home Office	WLAN, kabelgebunden	Kommerzielle VPN Anbieter (NordVPN, etc)
Firmendaten im Internet	Öffentlicher Ort, Home Office	WLAN, kabelgebunden	Kommerzielle VPN Anbieter, Firmen-VPN (Fritz.Box, etc)
Firmendaten im lokalen Rechenzentrum	Öffentlicher Ort, Home Office	WLAN, kabelgebunden	Firmen-VPN


ZUM
VIDEO
Einrichten einer
FRITZ Box für VPN

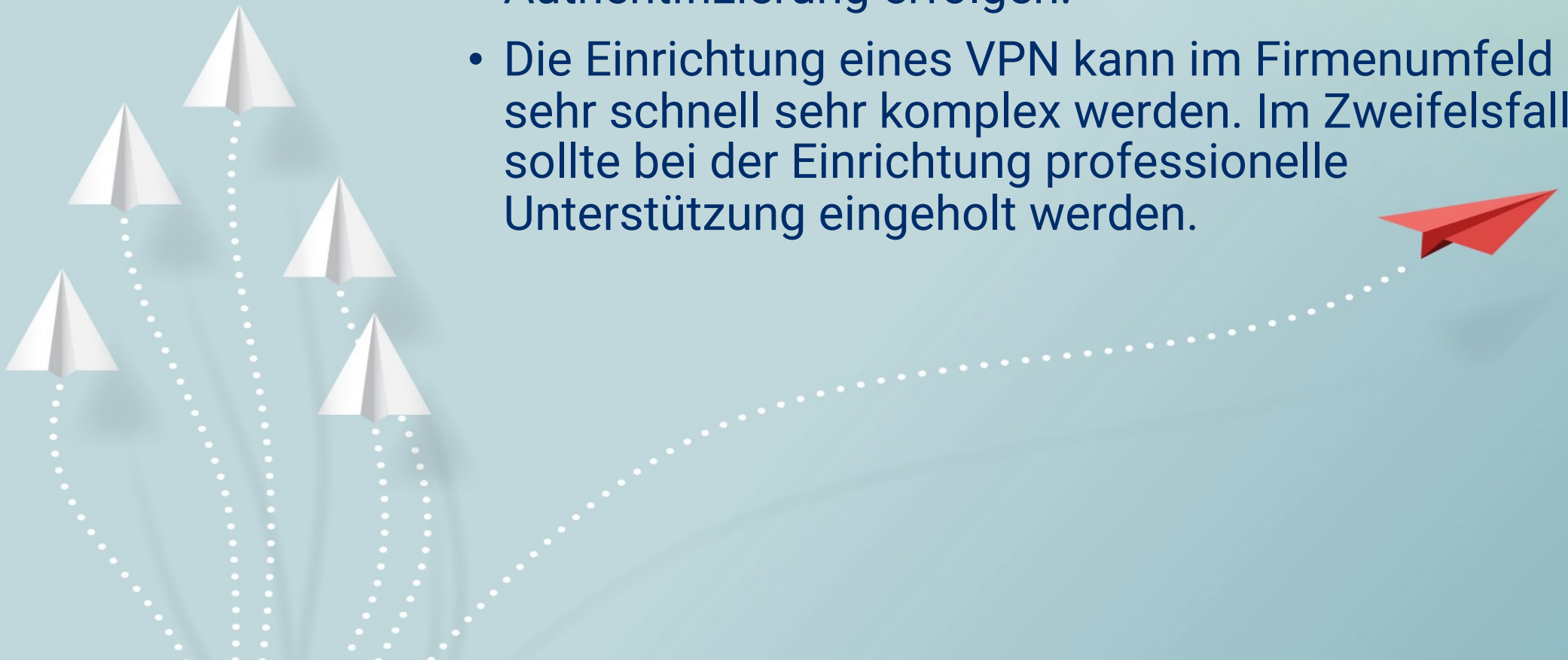

ZUM
VIDEO
Konfiguration eines Windows Server 2016 für VNP

LEARNINGS

LEARNINGS

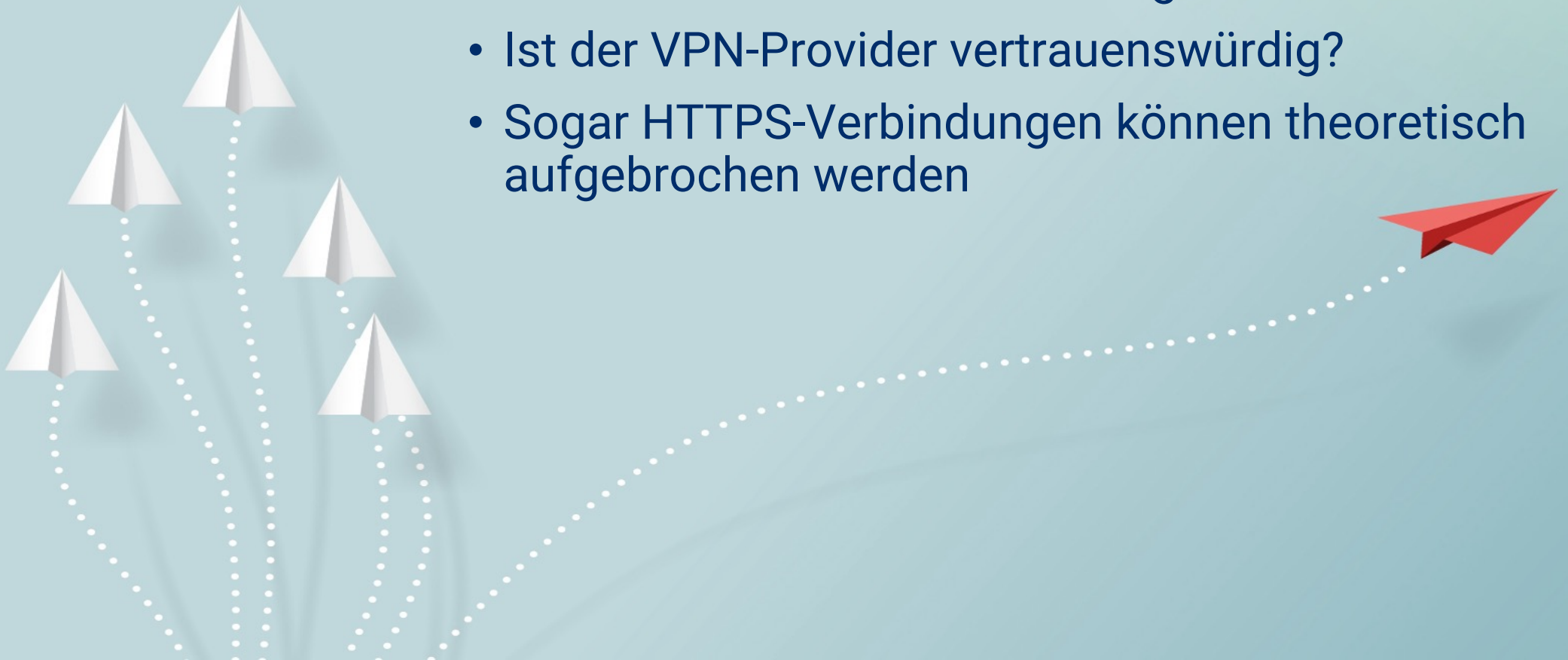
- Die Technologien, die sich hinter dem Begriff „VPN“ verbergen, sind bereits seit Jahren etabliert und gelten als ausreichend sicher
- VPN ist daher eine geeignete Lösung, um auch sensible Daten über ein unsicheres Netzwerk zu übertragen

LEARNINGS



- Die Authentifizierung beim Zugriff auf ein VPN sollte nicht nur durch ein einzelnes Kennwort erfolgen. Hier sollte mindestens eine sog. 2-Faktor Authentifizierung erfolgen.
- Die Einrichtung eines VPN kann im Firmenumfeld sehr schnell sehr komplex werden. Im Zweifelsfall sollte bei der Einrichtung professionelle Unterstützung eingeholt werden.

LEARNINGS



Letztendlich ist alles eine Frage des Vertrauens:

- Ist das WLAN vertrauenswürdig?
- Ist der VPN-Provider vertrauenswürdig?
- Sogar HTTPS-Verbindungen können theoretisch aufgebrochen werden