universität wien

Kommunikationsplattformen und andere Kooperations-Tools

Risiko-Aspekte und Handling

Dr. Sebastian Schrittwieser

universität wien

Kommunikationsplattformen und -tools

- Viele verschiedene Tools mit unterschiedlichen Funktionalitäten
  - Textnachrichten, Audio/Video, Dokumentenkollaboration, Dateiaustausch, etc.
- Die Pandemie hat bei vielen Tools zu massiven Funktionserweiterungen geführt
  - Laufend Updates und Vorstellung neuer Tools
- Eine Risikobewertung ist herausfordernd aufgrund des ständig erweiterten Funktionsumfangs der Programme
- Ziel dieses Vortrags: Vorstellung einfacher Methoden zur Evaluierung des Sicherheitslevels einer Kommunikationsplattform

universität wien

Kommunikationsplattformen und -tools

Verschlüsselung

Standort

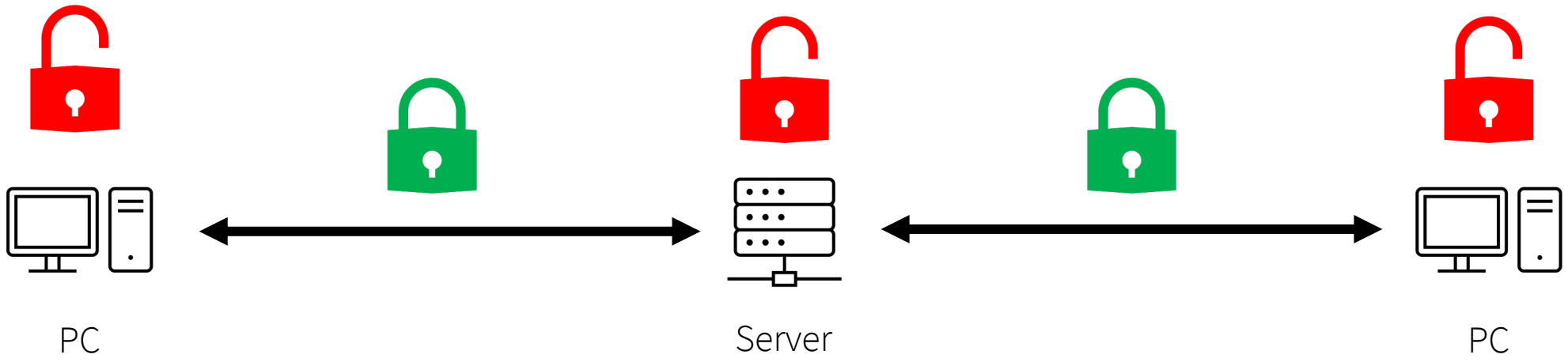
Client

universität wien

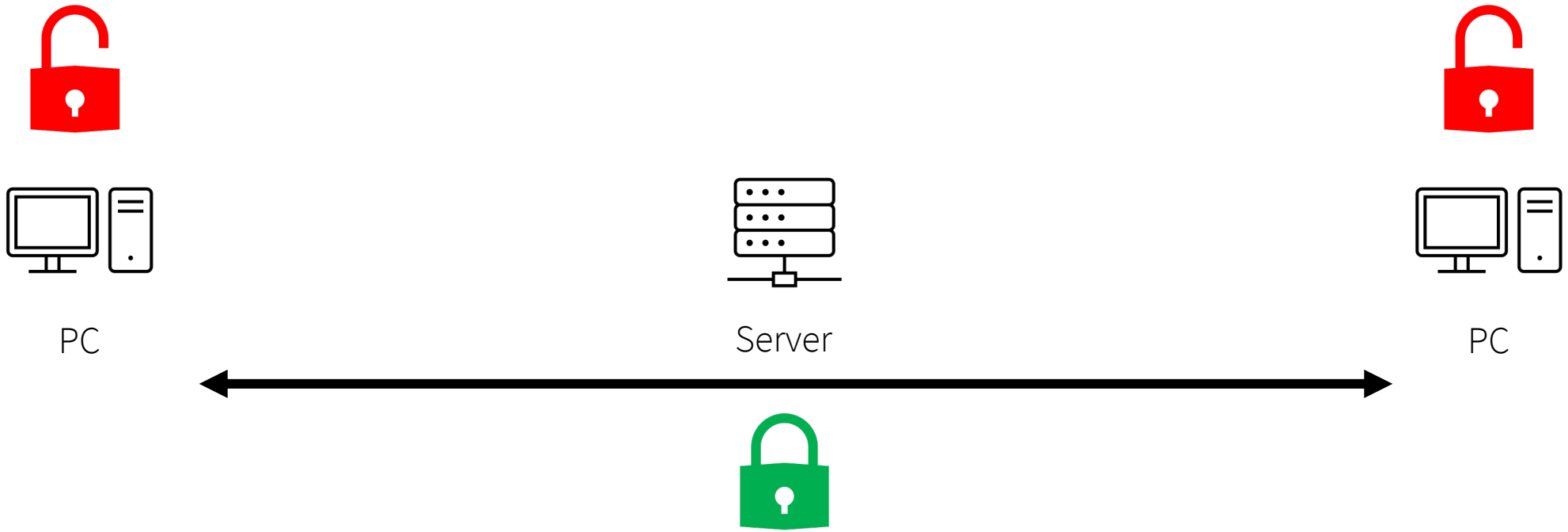
Verschlüsselung ist nicht gleich Verschlüsselung!

- Transportverschlüsselung
  - Daten werden am Transportweg verschlüsselt
  - Beispiel Webshop:
    - Kreditkartendaten werden am PC verschlüsselt, zum Server geschickt und dort wieder entschlüsselt
    - Am Transportweg zwischen PC und Server kann nicht mitgelesen werden
  - Beispiel MS Teams:
    - Die Nachrichten werden am PC verschlüsselt, zum Server geschickt, dort wieder entschlüsselt, dann erneut verschlüsselt und zum Empfänger geschickt
    - Am Transportweg zum Server und vom Server kann nicht mitgelesen werden, jedoch am Server schon!

Transportverschlüsselung



Ende-zu-Ende-Verschlüsselung



universität wien

Ende-zu-Ende-Verschlüsselung

- Ende-zu-Ende-Verschlüsselung garantiert eine durchgängige Verschlüsselung der Daten auch über einen bzw. mehrere Server hinweg
- Aus Sicht der Informationssicherheit erstrebenswert, jedoch in der Praxis oft mit Herausforderungen verbunden
  - Speicherung des geheimen Geräteschlüssels
    - Wo wird dieser abgespeichert? Wie sicher ist er dort?
    - Was geschieht im Falle eines Verlusts des Schlüssels? Gibt es ein Backup? Wenn ja, wo liegt dieses Backup?
  - Multi-Device-Fähigkeit
  - Webansicht

universität wien

Praxisbeispiele (Ende-zu-Ende-Verschlüsselung)

- WhatsApp
  - (Optionales) unverschlüsseltes Backup aller Nachrichten in der Cloud
  - Multi-Device-Fähigkeit wurde erst letzte Woche eingeführt
- Signal
  - Kein Cloud-Backup, Verlust alter Nachrichten bei Hardwaredefekt
- Apple iMessage
  - Sicherheit der Nachrichten hängt am iCloud-Account
- Zoom
  - Optionale Ende-zu-Ende-Verschlüsselung deaktiviert eine Reihe von Funktionen wie Breakout-Räume

universität wien

Lokal gespeicherte Daten bei Ende-zu-Ende-Verschlüsselung

- Ende-zu-Ende-Verschlüsselung schützt Daten nur während der Übertragung
- Risiko Endpunkte
  - Wie sind die Daten am PC/Smartphone geschützt?
  - Beispiel Signal Desktop
    - Eine Schadsoftware könnte Signal-Nachrichten aus der lokal gespeicherten Datenbank extrahieren (diese sind zwar verschlüsselt, der Schlüssel ist aber auch für alle anderen Programme zugänglich abgespeichert)

universität wien

Erkennung von Ende-zu-Ende-Verschlüsselung

- Wie kann ich feststellen, welche Art der Verschlüsselung verwendet wird?
  - Nicht direkt erkennbar, aber manche Funktionalitäten sind mit Ende-zu-Ende-Verschlüsselung nicht umsetzbar
- Indizien, die gegen (richtig implementierte) Ende-zu-Ende-Verschlüsselung sprechen
  - Weboberfläche mit Zugriff auf die Daten nach Login
  - Zugriff auf alte Nachrichten nach Neuinstallation und Login

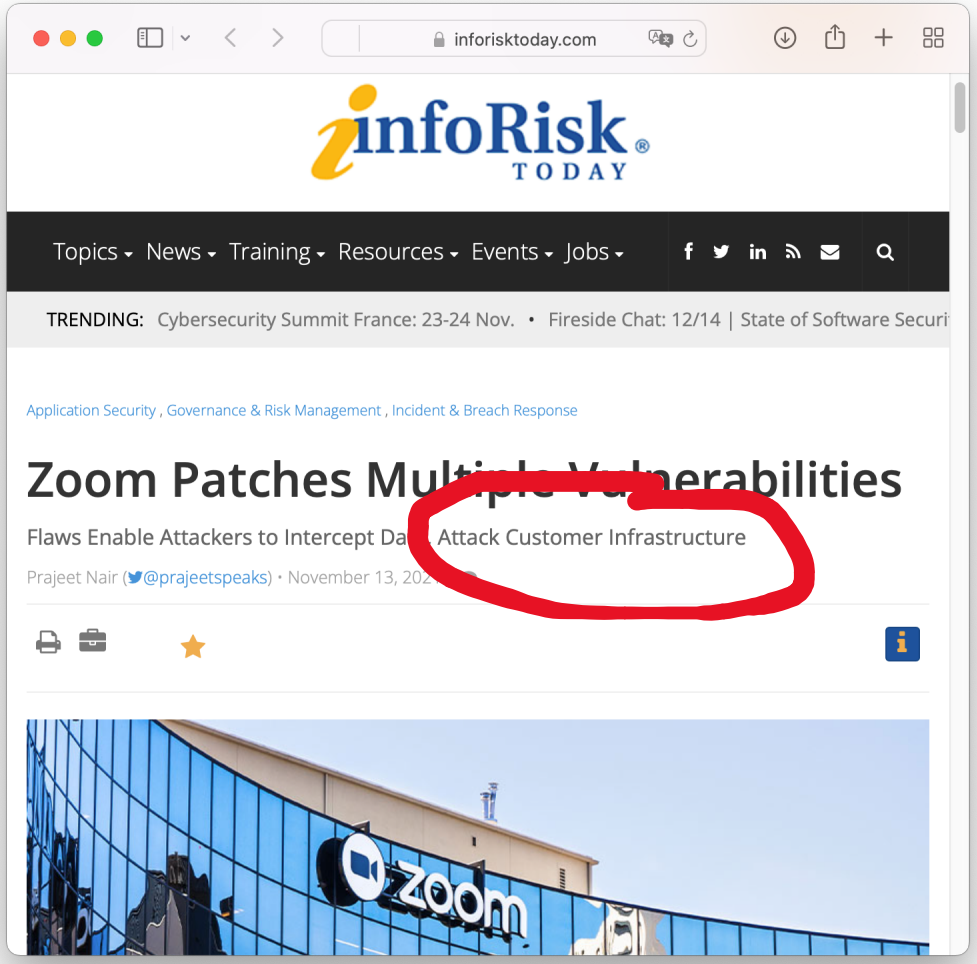
universität wien

Risikoabschätzung On-premise vs. Cloud

- Was ist mein Ziel?
  - Datensouveränität
  - Datensicherheit
  - Datenschutz
- On-premise schneidet bei der Datensicherheit nicht immer besser ab
  - Beispiel: Schwere Sicherheitslücke wird am 24. Dezember um 16 Uhr bekannt und bereits aktiv ausgenützt
  - Kann sich rechtzeitig jemand in meinem Unternehmen darum kümmern?

Praxisbeispiel

- Schwachstellen in der On-premise-Version von Zoom
- *„The now patched vulnerabilities could have enabled attackers to obtain **server access with maximum privileges and navigate further on the company's network**, as well as compromise the Zoom software's functionality“*
- Auswirkungen auf die ganze IT-Infrastruktur eines Unternehmens



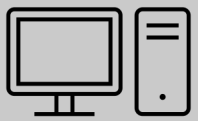
https://www.inforisktoday.com/zoom-patches-multiple-vulnerabilities-a-17906

universität wien

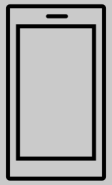
Risikoabschätzung Verschlüsselung und Standort

	Datensouveränität	Datensicherheit	Datenschutz	
Cloud, transportverschlüsselt				Teams, Google Meet, Dropbox Slack, Zoom (Cloud)
On-premise, transportverschlüsselt				Jitsi (On-premise)
Cloud, Ende-zu-Ende verschlüsselt				WhatsApp, Signal
On-premise, Ende-zu-Ende verschlüsselt				Matrix/Element

Risikoabschätzung Client



Native Software für Desktop-Systeme



Native Software für Mobilsysteme

Web-Applikation

universität wien

Risikoabschätzung Client

- Mobil vs. Desktop
  - Android und iOS haben mehr Sicherheitsfunktionen als Desktop-Betriebssysteme
    - App-Sandboxing
    - Codesignatur
    - Verschlüsselter bzw. sicherer Speicher im Mobiltelefon
    - Automatische Updates
  - Allerdings größere Gefahr durch Einsatz in potentiell unsicheren Umgebungen
    - Verlust und Diebstahl
    - Verbindung mit unsicheren Drahtlosnetzwerken

universität wien

Risikoabschätzung Client

- Mobil vs. Desktop
  - Erhöhtes Risiko durch kleinere Benutzeroberfläche
    - Unbeabsichtigte Bedienungsfehler (Einladung als falsche Person geschickt, versehentliche Aktivierung von Funktionalitäten, etc.)
    - Geringere Übersichtlichkeit (wer ist in einem Call dabei?)
- Native Applikation vs. Web-Applikation
  - Etwas geringeres Schadenspotential bei Web-Applikationen, da in modernen Webbrowsern der ausgeführte Code abgeschirmt wird und es weniger Schnittstellen zum Betriebssystem gibt
  - Für die Web-Applikationen ist keine Updatestrategie erforderlich
    - Allerdings sehr wohl für den Webbrowser

universität wien

Zusammenfassung

- Aktuell viel Bewegung im Markt für Kommunikationsplattformen
  - Regelmäßig neue Funktionen und Programmupdates
  - Risikobewertung aufgrund der vielen Veränderungen herausfordernd
- Technische Details der Implementierung einer Software nur mit tiefgehender Programmanalyse evaluierbar
- Die verwendete Verschlüsselung, der Standort und der Client können jedoch mit einfachen Mitteln recht zuverlässig bestimmt werden und bieten eine gute Grundlage für die Risikobewertung eines Systems

universität wien

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Sebastian Schrittwieser | sebastian.schrittwieser@univie.ac.at