

IT Security Talk: Wird E2EE Standard bei E-Mails?



Nationale Initiative für Informations- und Internetsicherheit NIFIS
davit AG IT-Recht im Deutschen Anwaltverein

Aktueller Fall – Zahlung an Hacker

Kaufvertrag über einen gebrauchten Pkw Daimler Typ E200T zum Preis von 13.500 €

Auf Wunsch der Käuferin wird die Rechnung vom Geschäftsführer der Verkäuferin per E-Mail gesendet

Rechnung nennt in Briefkopf und Fußzeile ein Konto der Verkäuferin bei der Sparkasse T

OLG Karlsruhe, Urteil vom 27. Juli 2023 – 19 U 83/22 –, juris

Hacking: der Angriff

Zwei Minuten nach dieser Mail mit der Rechnung erhält die Käuferin eine erneute Mail

Absender ist E-Mail-Adresse der Verkäuferin

neue Rechnung mit gleichem Briefkopf
(incl. Bankverbindung)

Schaden

Käuferin zahlt auf das Konto des P.D. bei der S-Bank, das in der Fußzeile der zweiten Rechnung angegeben war

→ Geld ist weg

Verkäuferin verlangt weiter Zahlung des Kaufpreises

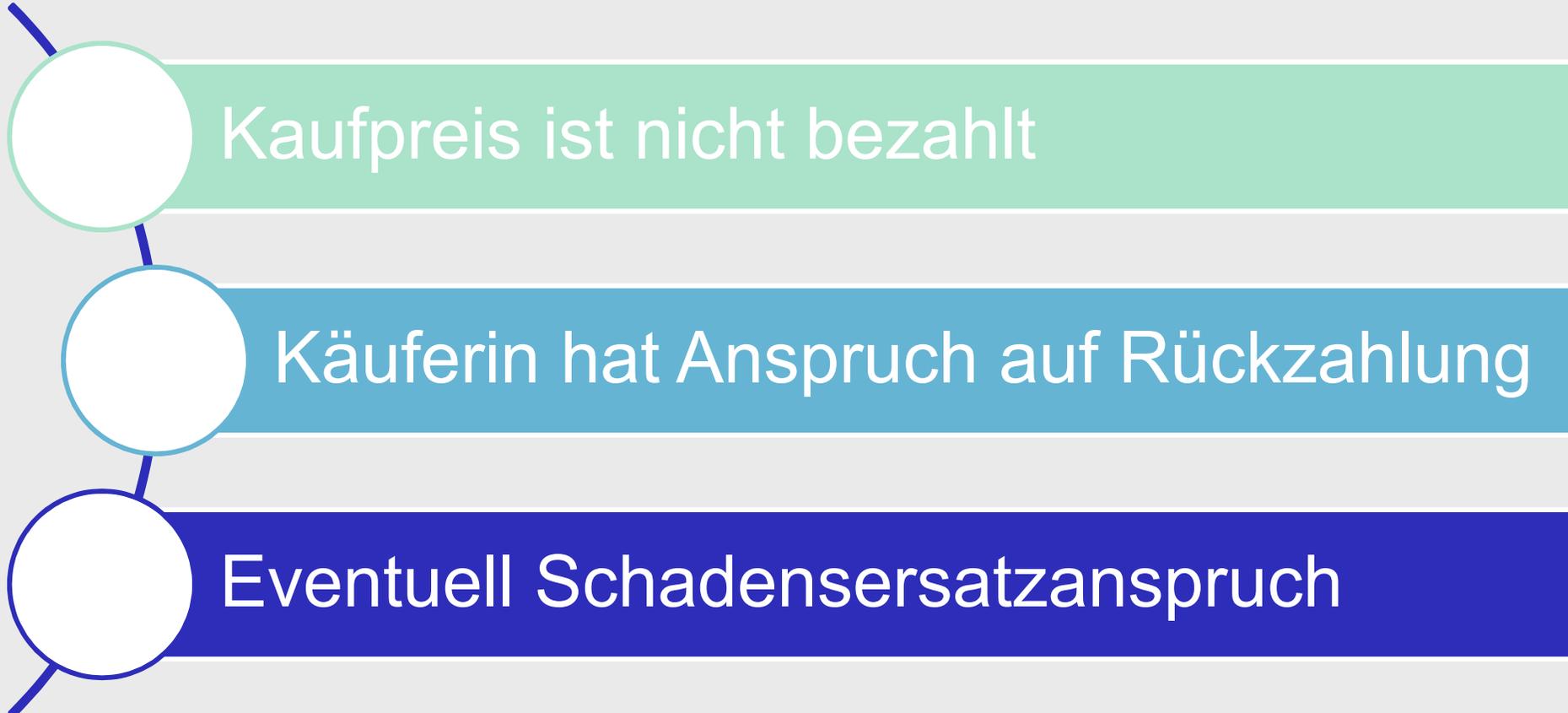
Käuferin will Kaufpreis nicht doppelt zahlen

Zwischenergebnis

Kaufpreis ist nicht bezahlt

Käuferin hat Anspruch auf Rückzahlung

Zwischenergebnis



Kaufpreis ist nicht bezahlt

Käuferin hat Anspruch auf Rückzahlung

Eventuell Schadensersatzanspruch

Sicherheit bei der Verkäuferin

Passwort zum E-Mail-Konto neun Stellen aus Buchstaben und Zahlen

Firewall von Microsoft

Vollversion des Antiviren-Programms von X-Security mit eingestellter automatischer Updatefunktion

„Zwei-Faktor-Authentifizierung“ für den Zugang zum E-Mail-Postfach sei wohl möglich, aber nicht eingerichtet

Sicherheit bei der Verkäuferin

Passwörter waren ausschließlich auf den PCs des Geschäftsführers und eines Mitarbeiters S. hinterlegt, zu denen nur diese beiden Personen Zugang hatten

Start des PC nur mit Passwort

Sicherheit bei der Käuferin

Kennwort zum E-Mail-Konto aus Zahlen und Sonderzeichen und 20 Stellen

Zugriff haben der Geschäftsführer, beide IT-Administratoren sowie Mitarbeiter des genutzten Diensteanbieters N.

Zweifaktorauthentifizierung war nicht möglich und wurde auch nicht für erforderlich gehalten

Sicherheit bei der Käuferin

Laptops mit Bitlocker verschlüsselt

Windows Passwort: mind. acht Zeichen mit Klein- und Großbuchstaben, Sonderzeichen und Zahlen

Mail-Konto auch auf einem iPhone

Schleswig-Holsteinisches Oberlandesgericht

Werkvertrag – § 631 BGB Bauvertrag

drei Abschlagsrechnungen an Zeugen

Schlussrechnung – 15.385,78 €

Zahlung auf Konto eines Dritten

Urt. v. 18.12.2024 – 12 U 9/24

Schleswig-Holsteinisches OLG

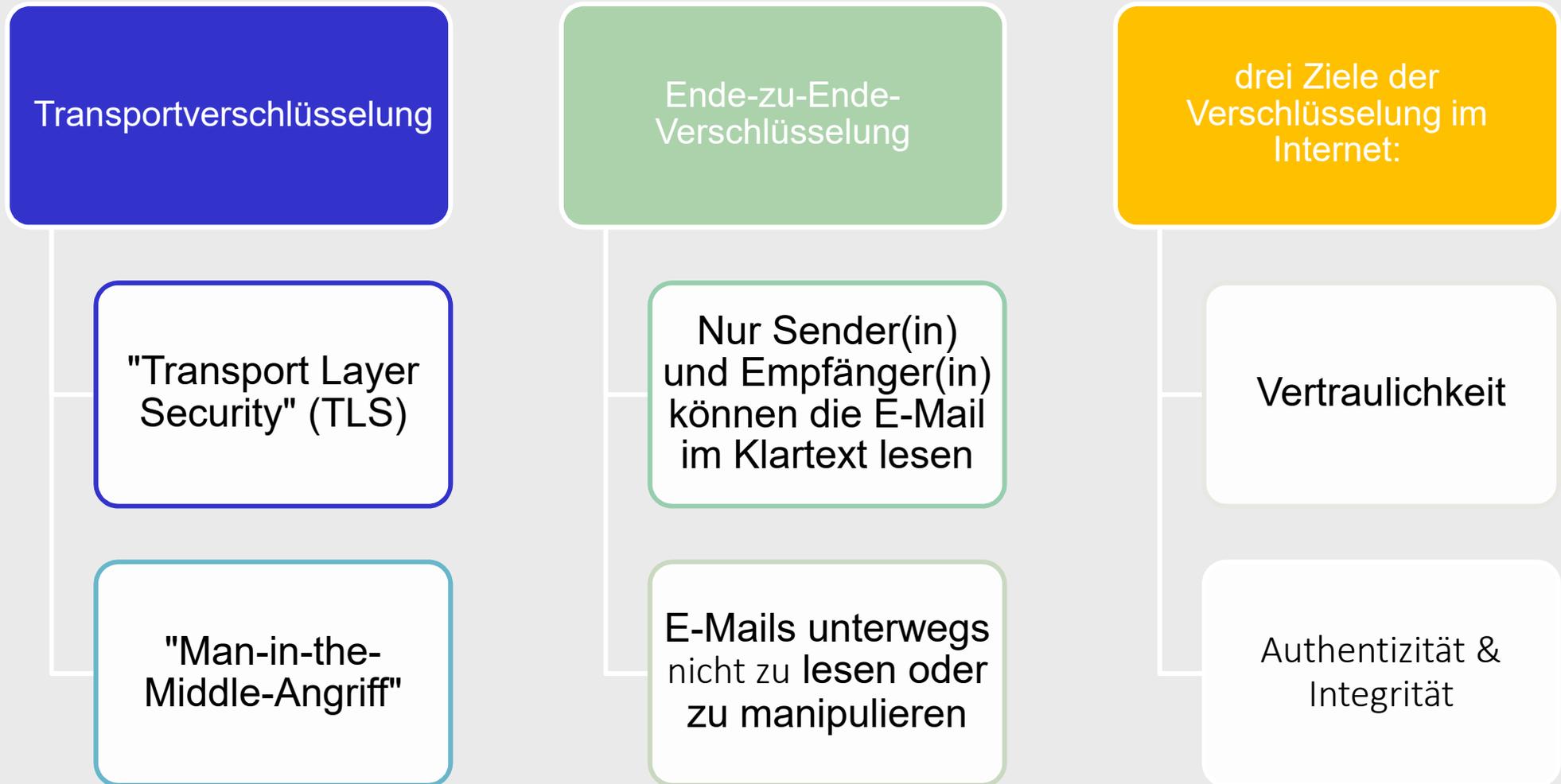
Zeuge x erhält manipulierte SchlussRe

Kto bei Neo/Onlinebank, „Account No.“

ohne QR Code, Siegel, GF und SteuerNr.

abw. Farbgestaltung, kein Wasserzeichen

Schleswig-Holsteinisches Oberlandesgericht



Schleswig-Holsteinisches Oberlandesgericht

E2EE bedeutet technischen Aufwand, incl. Technischer Beratung und Programme

Auch von kleineren Unternehmen zu erwarten

nicht unmöglich, E2EE einzuführen

Sonst muss halt Papier versendet werden

Fehlverständnis Schleswig-Holsteinisches OLG

Vertraulichkeit

Verschlüsselung

E2EE oder TLS

Authentizität -
Integrität

Signatur/Siegel

fortgeschritten
oder qualifiziert

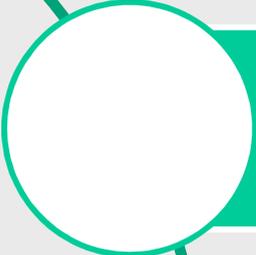
Authentizität und Integrität nach § 14 Abs. 3 UStG

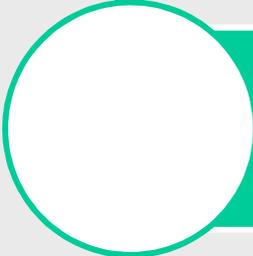
EU DIW

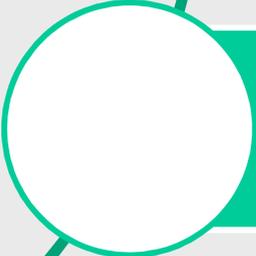
Fernsignatur

Rechnung
mit qeS

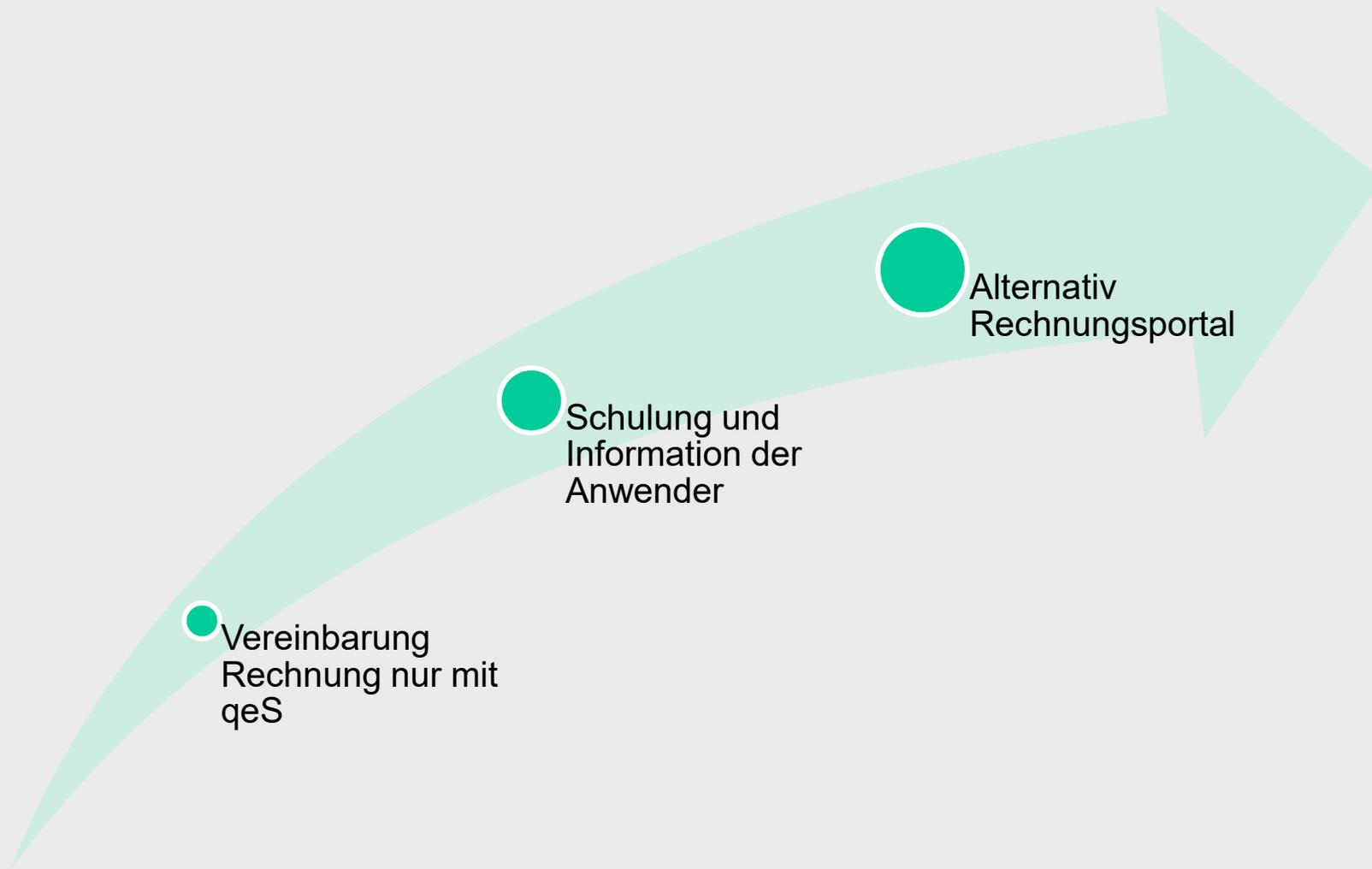
Problem noch nicht gelöst

 Empfänger waren sorglos, haben

 erkennbare Signale nicht beachtet

 hätten auch ohne qeS bezahlt

Lösung



Kontakt

☾ Dr. Thomas Lapp - Rechtsanwalt, Fachanwalt für IT-Recht und
zertifizierter QVM-Mediator

davit – AG IT-Recht im Deutschen Anwaltverein e.V.

Vorsitzender der NIFIS e.V. – Nationale Initiative für
Informations- und Internetsicherheit

IT-Kanzlei dr-lapp.de GbR

Berkersheimer Bahnstraße 5, 60435 Frankfurt am Main

anwalt@dr-lapp.de

The background of the slide features a central image of a globe showing the continents of Europe and Africa. The globe is surrounded by a field of binary code (0s and 1s) and dashed lines, suggesting a digital or network environment. The overall color scheme is blue and white.

**Vielen Dank für Ihre
Aufmerksamkeit!**

Dr. Thomas Lapp
Rechtsanwalt, Fachanwalt für IT-Recht und zertifizierter QVM-Mediator
Vorsitzender der NIFIS e.V. Nationale Initiative für Informations- und
Internetsicherheit

Weitere Informationen unter www.nifis.de