HEES

E-RECHNUNG
SICHER? SICHER NICHT.

Agenda

Vorstellung

Warum E-Rechnung und was ist das?

Cybercrime in DEU

Gefahren der Nutzung

Mögliche Abwehrmaßnahmen

Wenn es passiert ist & Fazit

FÜR DAS BESSERE ARBEITEN.

Über mich...

Karsten Peter
Geschäftsleitung Prozesse & IT

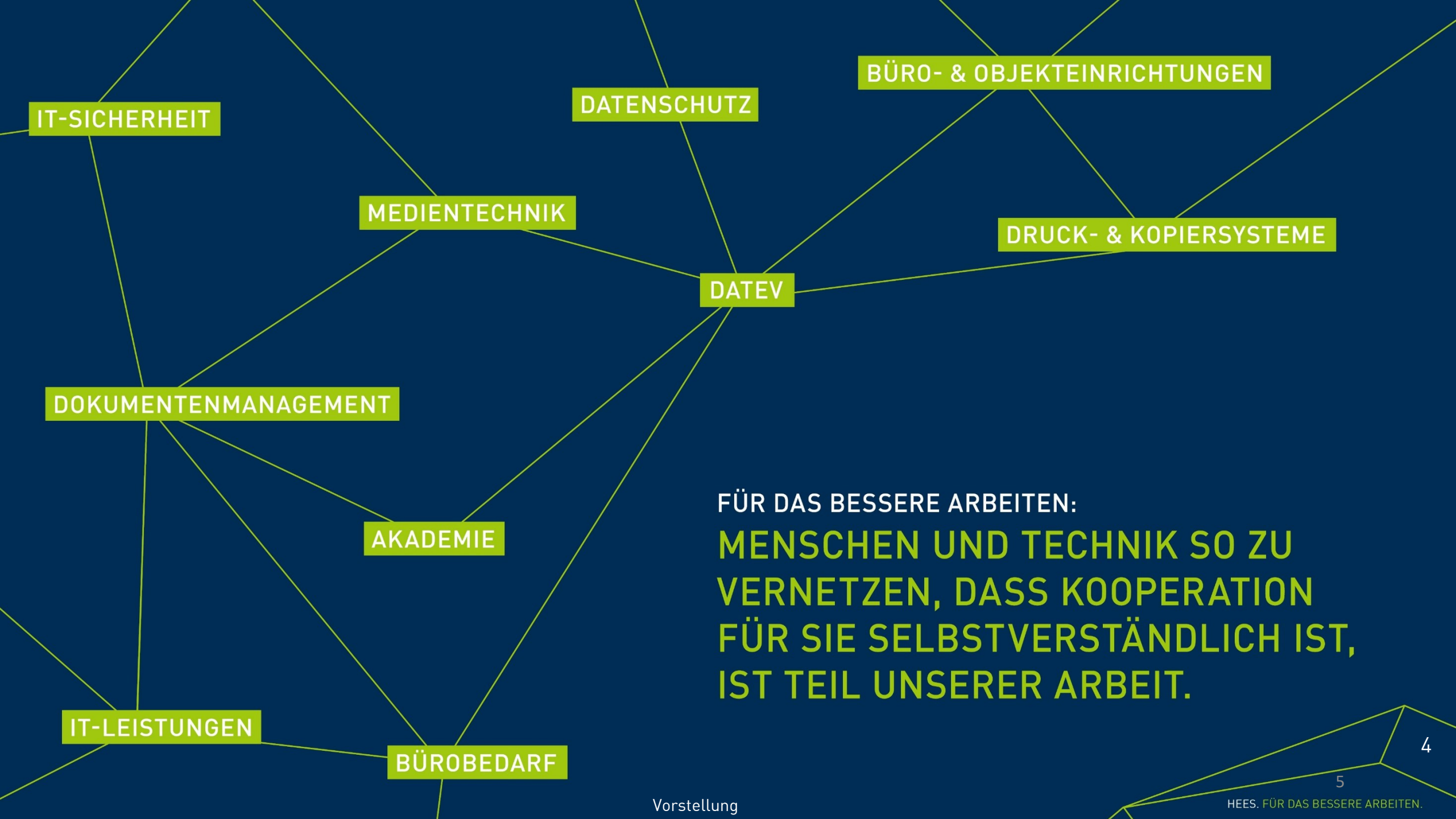
Seit März 2015 bei HEES

Geprüfter Wirtschaftsinformatiker
CISO (TÜV NORD CERT)

FF Siegen & IHK Prüfungsausschüsse

...über HEES

UNSERE STANDORTE
AUF EINEM BLICK.



FÜR DAS BESSERE ARBEITEN:

MENSCHEN UND TECHNIK SO ZU VERNETZEN, DASS KOOPERATION FÜR SIE SELBSTVERSTÄNDLICH IST, IST TEIL UNSERER ARBEIT.

Warum E-Rechnung und was ist das?

Ab dem 1. Januar 2025 werden **deutsche Unternehmen im B2B-Bereich schrittweise gesetzlich zur E-Rechnung verpflichtet:***

Empfang von E-Rechnungen verpflichtend

ab 01.01. **2025**

Papier- und PDF-Rechnungen zulässig, bei PDF-Rechnungen muss der Empfänger zustimmen

bis 31.12. **2026**

Papier- und PDF-Rechnungen nur bedingt zulässig (bei Zustimmung des Empfängers und Vorjahresumsatz des Rechnungsstellers von max. 800.000 €)

bis 31.12. **2027**

E-Rechnungspflicht für jeden Unternehmer (Erstellung, Übermittlung, Empfang)

ab 01.01. **2028**

* auf Basis des Wachstumschancengesetzes
Quellen: Bundesministerium der Finanzen, Agenda Software

Quelle: Statista

Warum E-Rechnung und was ist das?

Einhaltung der gesetzlichen Vorgaben ab Januar 2025

- ☑ **Annahmepflicht:** Unternehmen müssen über ein System verfügen, **das die Annahme und Verarbeitung von E-Rechnungen ermöglicht** und der europäischen Norm entspricht. (EN 16931)
- ☑ **Digitale Aufbewahrungspflicht:** E-Rechnungen müssen mindestens **zehn Jahre lang elektronisch unverändert und lesbar archiviert werden** (PDF oder Papierform genügt nicht).*

Quelle: Statista

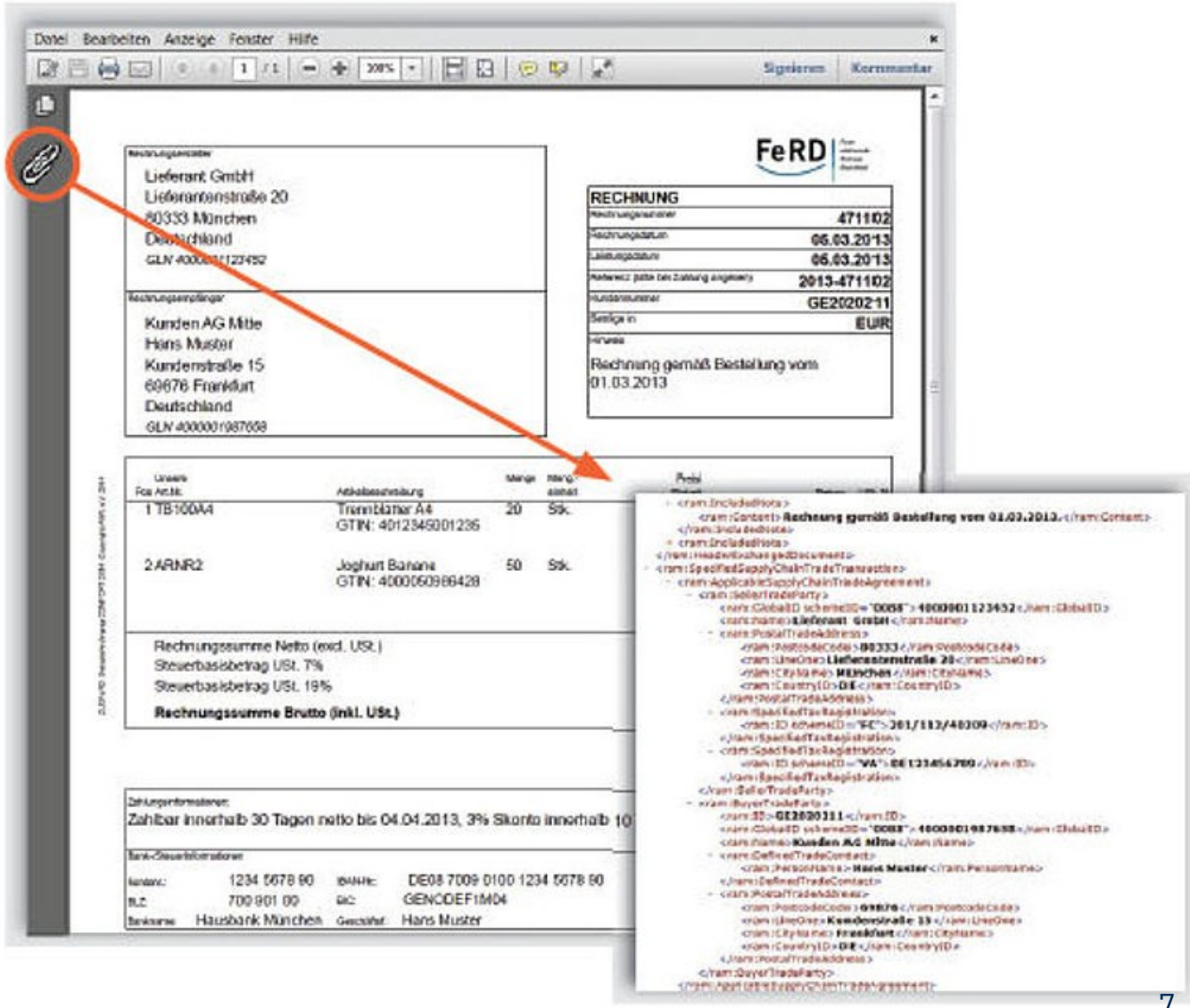
Ausnahmen

- Steuerfreie RG
- RG bis 250 €
- Fahrausweise

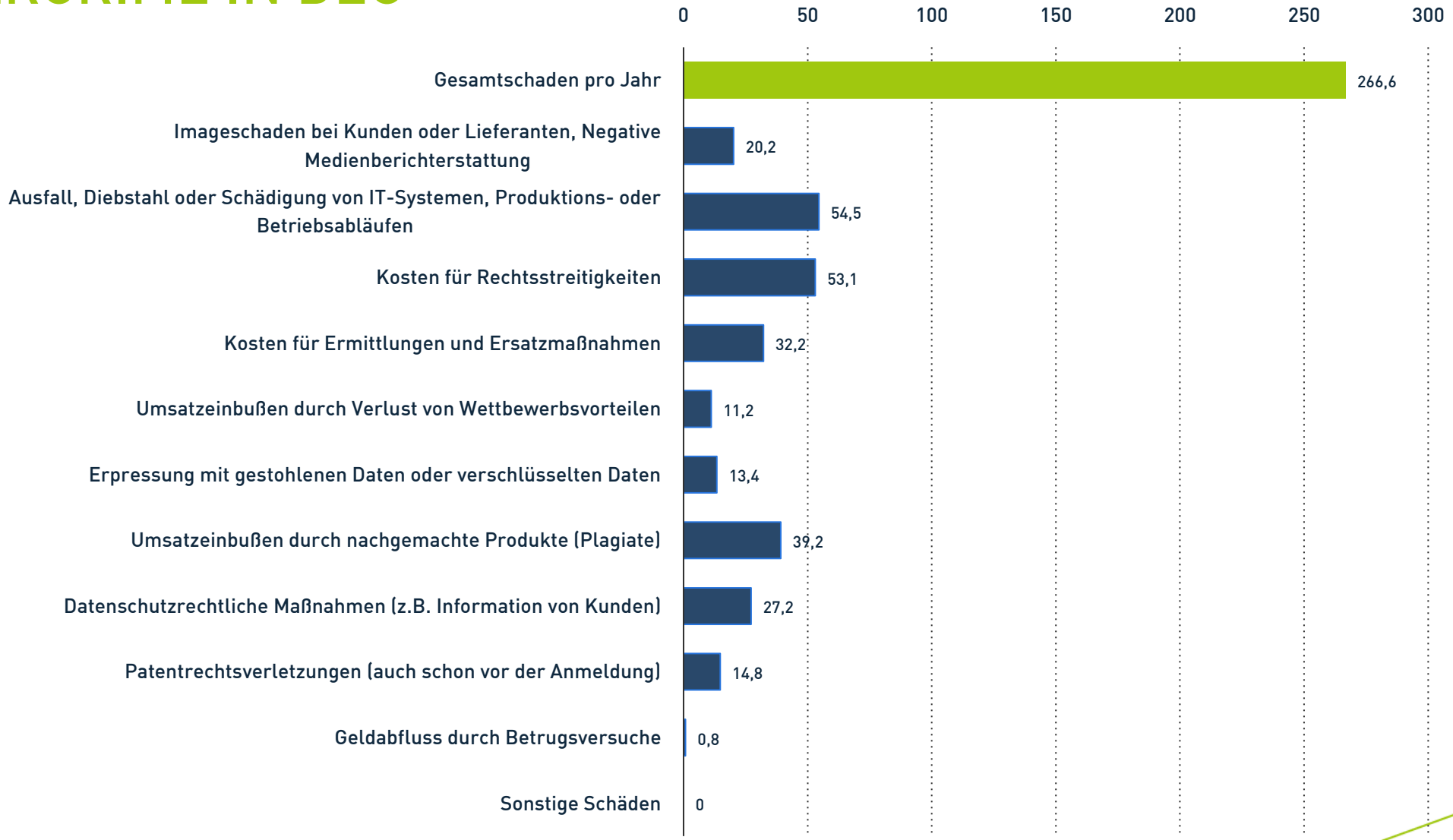
Formate

- ZUGFeRD ab 2.0.1
- XRechnung (3.0.1)
- EDI (Bsp.: EDIFACT)

Warum E-Rechnung und was ist das?



CYBERCRIME IN DEU

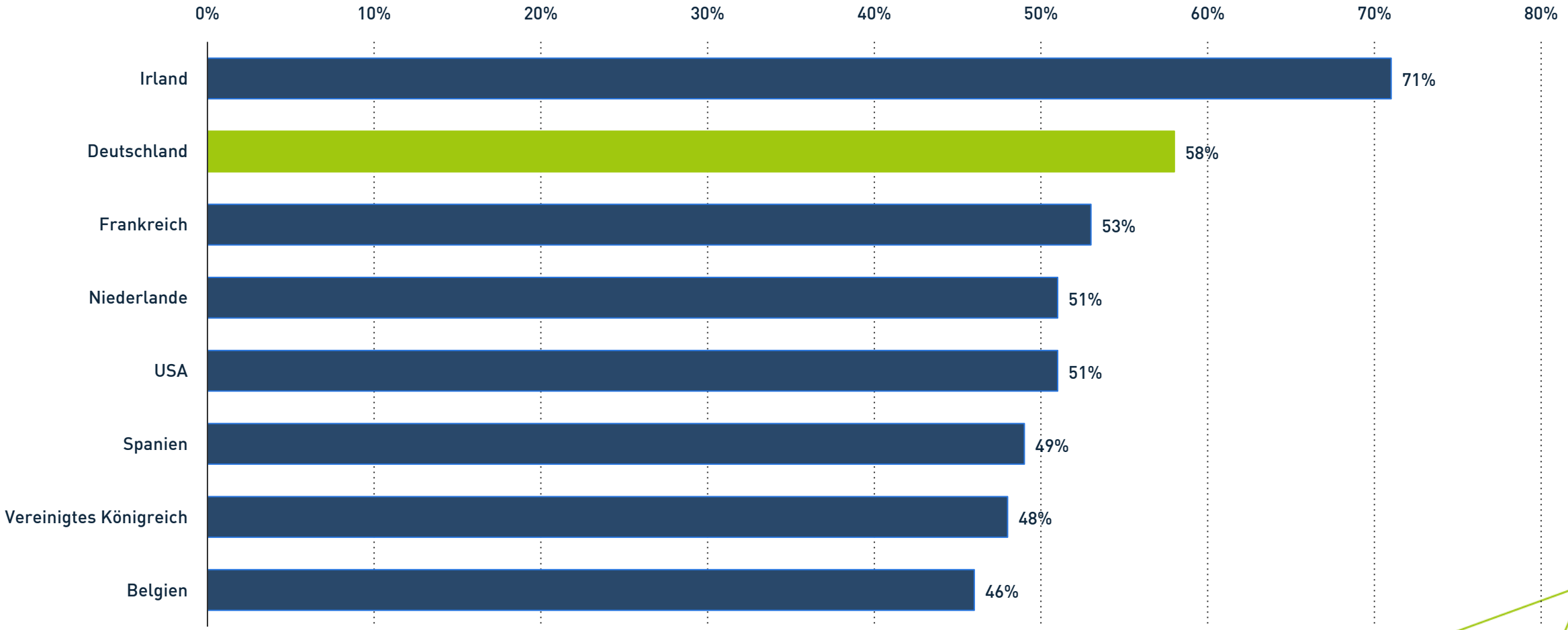


Hinweis(e): Deutschland; KW16 bis KW24 2024; 1.003 Befragte
Quelle(n): Bitkom; ID 444719

Cybercrime in DEU

CYBERCRIME IN DEU

Unternehmen, die in den letzten 12 Monaten eine Cyber-Attacke erlebt haben 2023

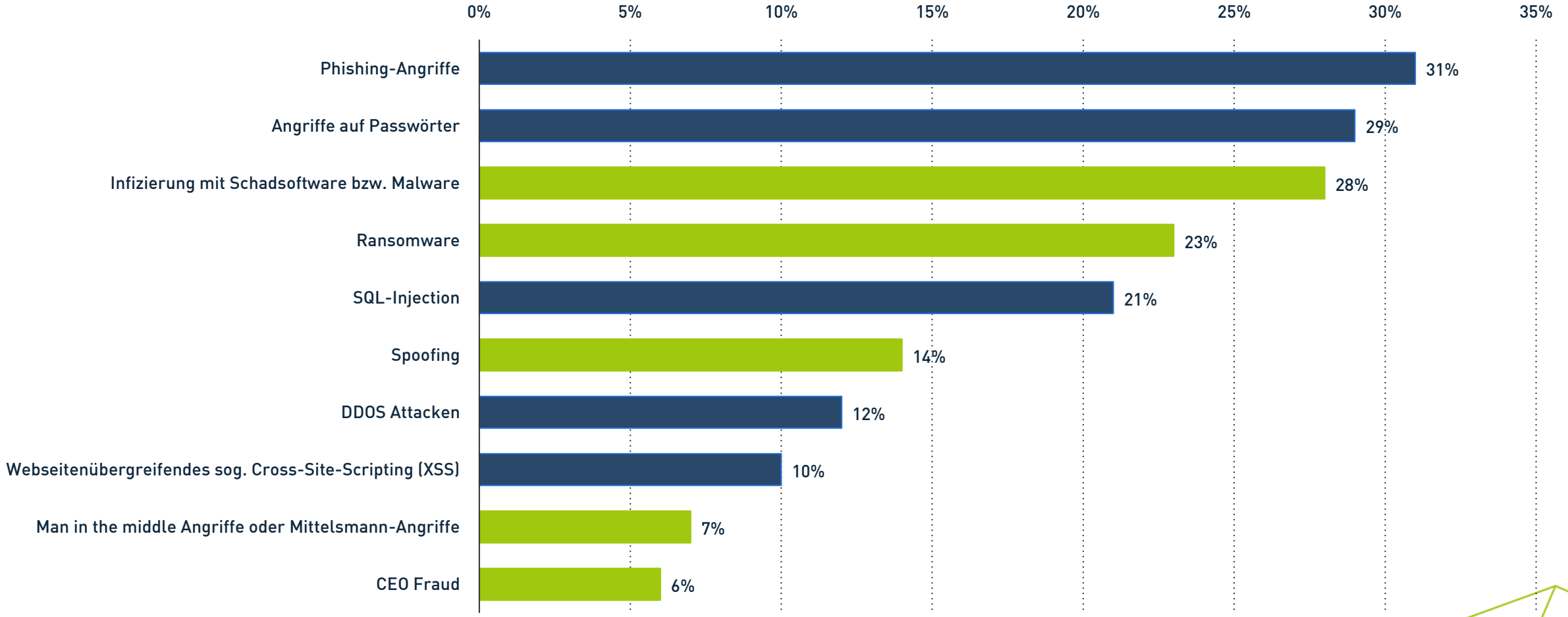


Hinweis(e): Weltweit, Belgien, Frankreich, Deutschland, Irland, Niederlande, Spanien, Vereinigtes Königreich, USA; 9. Januar 2023 bis 2. Februar 2023; 5.005 Befragte; Cybersecurity-Personal

Quelle(n): Hiscox; ID 1230157

CYBERCRIME IN DEU

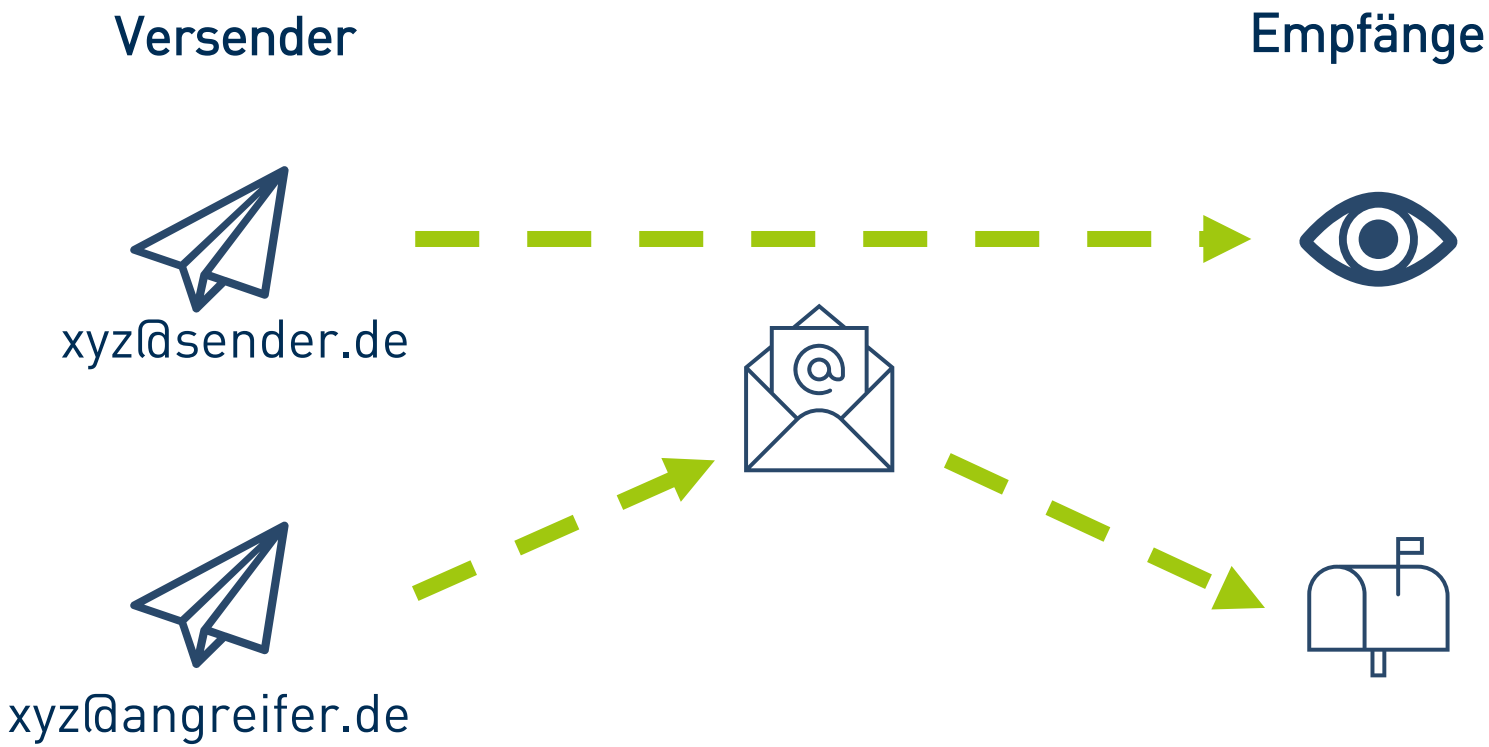
Anteil der von Cyberangriffen betroffenen Unternehmen nach Art des Angriffs 2023



Hinweis(e): Deutschland; KW16 bis KW23 2023; 1.002 Befragte; Unternehmen ab 10 Mitarbeitern und Jahresumsatz von 1 Mio. Euro oder mehr
Quelle(n): Bitkom; ID 928943

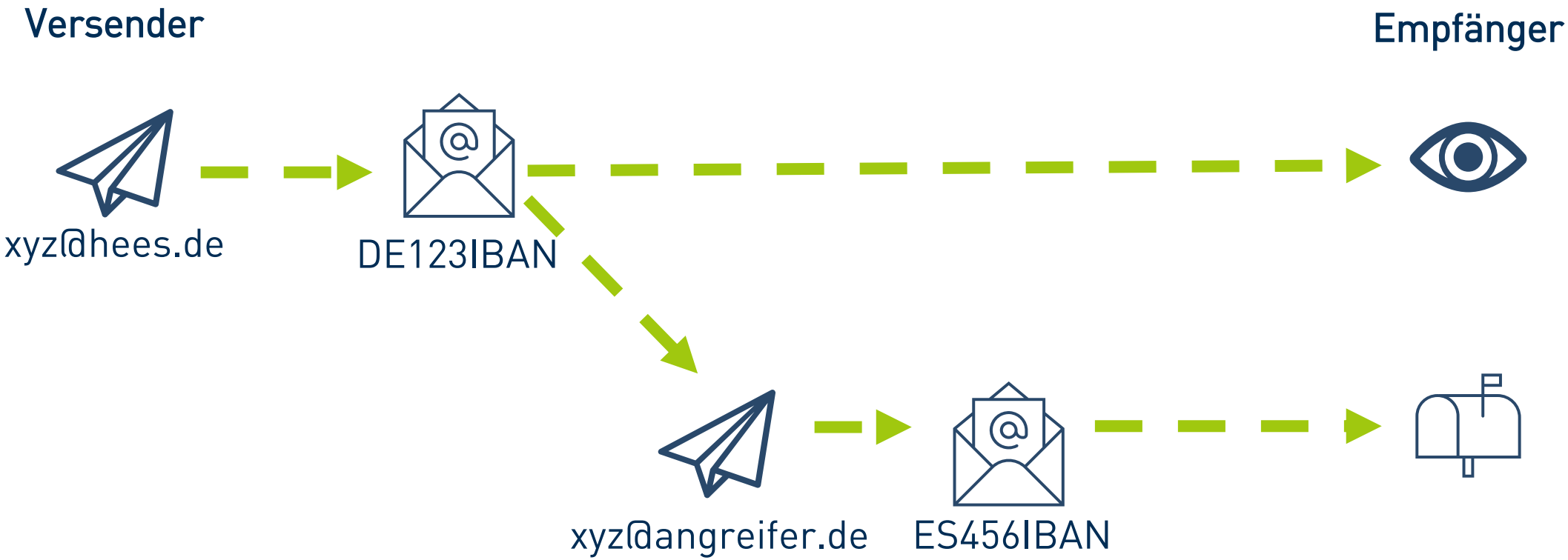
GEFAHREN DER NUTZUNG

Versand unter bekanntem Namen durch Dritte per Mail



GEFAHREN DER NUTZUNG

Falsche / Manipulierte Rechnung per Mail (XML-Datei)



GEFAHREN DER NUTZUNG

Falsche / Manipulierte Rechnung per Mail (XML-Datei)

Zahlungsinformationen:

Zahlbar innerhalb 30 Tagen netto bis 04.04.2013, 3% Skonto innerhalb 10 Tagen bis 15.03.2013

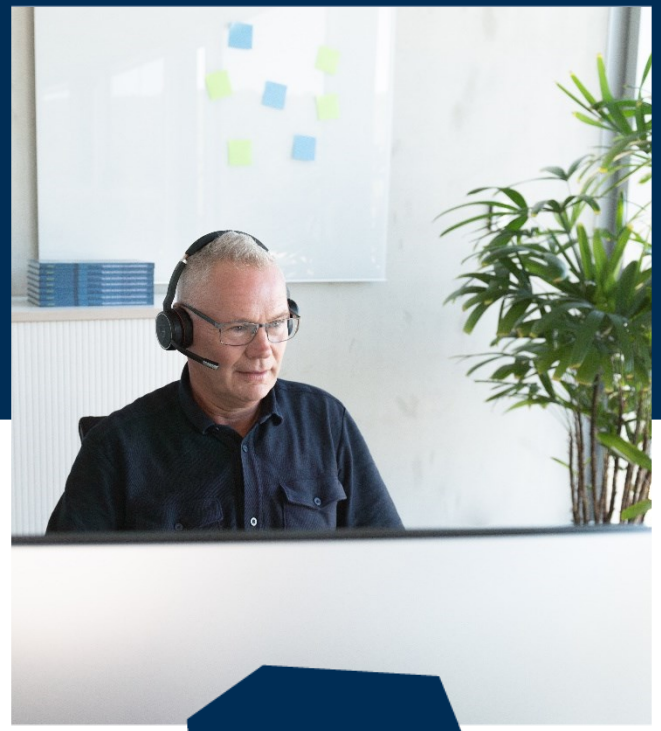
Bank-/Steuerinformationen

Kontonr.:	1234 5678 90	IBAN-Nr.:	DE08 7009 0100 1234 5678 90	Handelsreg.:	H A 123
BLZ:	700 901 00	BIC:	GENODEF1M04	USt.-Identnr.:	DE123456789
Bankname:	Hausbank München	Geschäftsf.:	Hans Muster	Steuernr.:	201/113/40209

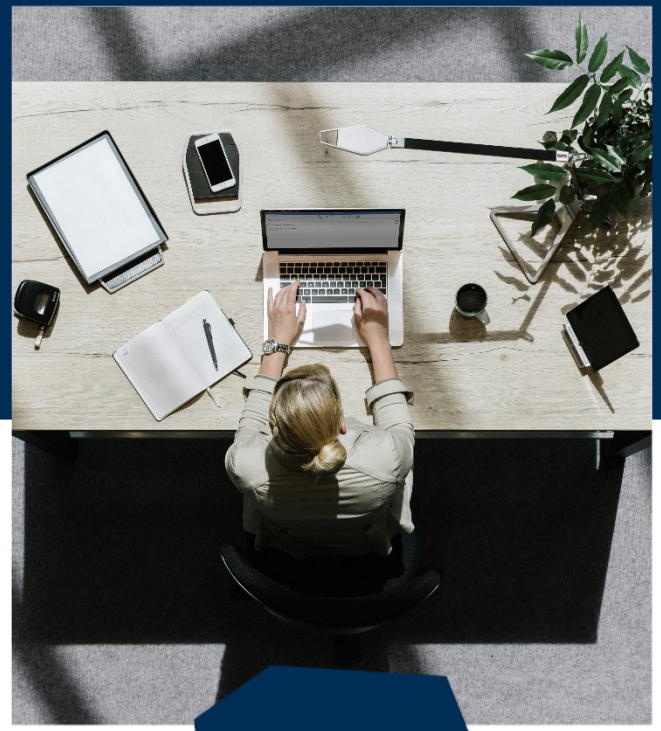
```
<ram:SpecifiedTradeSettlementPaymentMeans>
  <ram:PayeePartyCreditorFinancialAccount>
    <ram:IBANID>DE87009010012345678 90</ram:IBANID>
  </ram:PayeePartyCreditorFinancialAccount>
  <ram:PayeeSpecifiedCreditorFinancialInstitution>
    <ram:BICID>GENODEF1M04</ram:BICID>
  </ram:PayeeSpecifiedCreditorFinancialInstitution>
</ram:SpecifiedTradeSettlementPaymentMeans>
```

Quelle(n): http://www.pdfunit.com/de/documentation/java/testscope/zugferd.html 08.04.2025

MÖGLICHE ABWEHRMAßNAHMEN



SPF



DKIM

DMARC

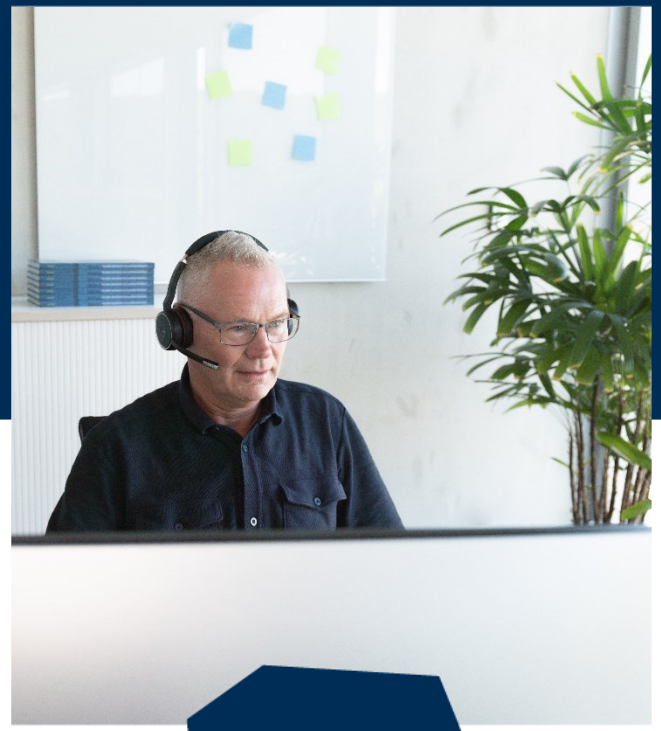
Technische Maßnahmen der Versender

SPF – Wer darf in meinem Namen Mails versenden (IP-Adressen)

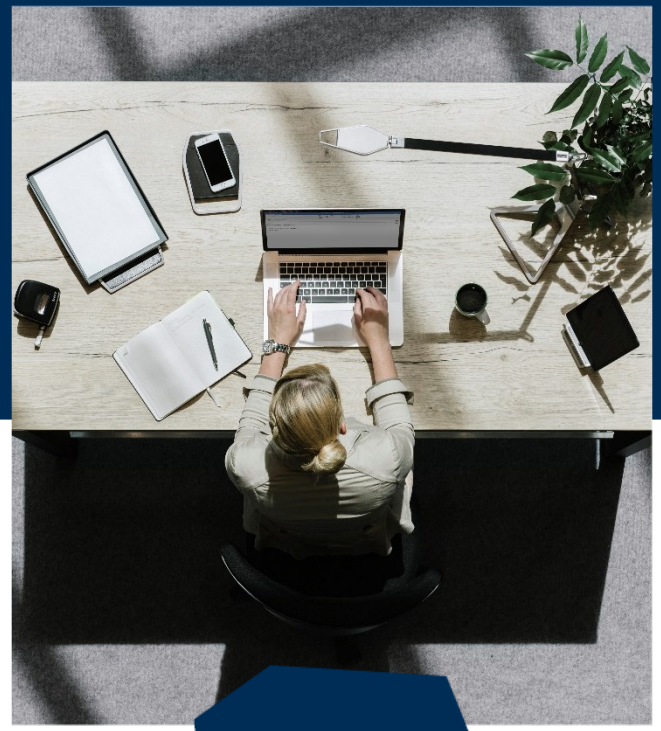
DKIM – Signieren der Mails, um Integrität sicherzustellen

DMARC – Richtlinie zum Umgang mit fehlerhaften Mails

MÖGLICHE ABWEHRMAßNAHMEN



IBAN



SPF/DKIM

Sensibilisierung

<u>Organisatorische Maßnahmen des Empfängers</u>

Bankverbindung prüfen, bei Änderung Rückversicherung – Prozess etablieren

SPF/DKIM prüfen, wenn fehlerhaft – äußerst kritisch sein (Spamfilter) – Prozess etablieren

Sensibilisierungsmaßnahmen der verarbeitenden Personen vornehmen

WENN ES PASSIERT IST

- → OLG Schleswig-Holstein – (Az. 12 U 9/24) , 18.12.2024 - B2C
- → Transportverschlüsselung nicht ausreichend,
  E2E Verschlüsselung wäre notwendig gewesen
- → Widerspricht einem Urteil des OLG Karlsruhe (Az. 19 U 83/22),
- → Mögliche technische Maßnahmen müssen zum Schutz ergriffen werden

- → Dem Kunden durch DKIM und SPF ermöglichen schadhafte Mails besser zu erkennen
- → Im B2C Verkehr bei hohem Risiko auf Post oder E2E Verschlüsselung setzen

FAZIT & ZUSAMMENFASSUNG

- → Empfang & Archivierung von E-Rechnungen ist pflicht
- → Sicherheitsgefährdung ist als hoch bis sehr hoch einzustufen
- → Sicherheitsanbieter unterstützen bei SPF/DKIM/DMARC (Hornetsecurity, MS Exchange Security, Proofpoint, etc.)
- → Verantwortlichen im Unternehmen festlegen
- → Prozesse für die häufigsten kritsichen Fälle etablieren
  - → Geänderte / Abweichende Bankverbindung
  - → Umgang mit verdächtigen Mails
  - → CEO Fraud vorbeugen (telefonische Rückversicherung etc.)
- → Wenn möglich, alternativen Übertragungsweg etablieren (SFTP, EDI, APIs – REST, Soap, WSDL)

Danke fürs Zuhören!

Quellen

E-Rechnung und IT-Risiken: So schützen Sie sich | IHK München

Elektronische Rechnung | IHK

XRechnung & ZUGFeRD: E-Invoicing-Format umsetzen | Comarch

DMARC – Wikipedia, Sender Policy Framework – Wikipedia, DomainKeys Identified Mail – Wikipedia