Informationssicherheit neu gedacht

Machen ist wie wollen – nur besser

REFERENTENVORSTELLUNG

Referent: Christoph Kopper

- Schon immer: Menschliches „Schweizer Taschenmesser“
- Seit 2003 CISO bei der Sparkasse Lörrach-Rheinfelden (Unternehmen unterliegt der Kritis-VO
- Seit 2006 Datenschutzbeauftragter – s.oben
- Mitglied im Themenarbeitskreis „Regulatorik“ der Allianz für Cybersicherheit beim BSI
- Mitglied im Themenarbeitskreis „Awareness“ der Allianz für Cybersicherheit beim BSI
- Mitglied im Themenarbeitskreis „Auswirkung aktueller Krisen und Ereignisse“ der Allianz für Cybersicherheit beim BSI
- Mitglied des ERFA-(Informationssicherheitsclusters) Südbaden eine Ansammlung von KMU zum Informationsaustausch
- Mitglied im GDD-ERFA-Kreis Freiburg

COPYRIGHT - URHEBERRECHTSHINWEIS

TUN SIE ETWAS ABER MACHEN SIE NICHTS

Tägliche Herausforderung:

IT-BY-WILDWEST – Beschaffen was man will und nicht was man braucht oder darf, am Kopf kratzen, verwundert die Äuglein reiben, jemand mit Aufwischen oder Vertuschen beauftragen…

Herr Kopper eine Frage:

„Wieviel Geld verdienen wir mehr durch den ganzen InformationssicherheitsDatenschutz-Voodoo?"

Antwort:

„Die Frage muss lauten: was ist Voodoo? Der Verordnungsgeber ist da recht präzise. IS und DS steht da drin….Von Facebook, TikTok, Instagrammability steht da nichts….. Außerdem: Ohne ISM/DSM verdienen Sie ab Morgen gar nichts mehr."

Spionage „CHIPS-Tüte" !!!

Wer kann, der kann, der darf dann auch:

Spionage: Wenn die Chipstüte auspackt | ZEIT ONLINE

TUN SIE ETWAS ABER MACHEN SIE NICHTS

Tägliche Herausforderung:

Herr Kopper ?

Ich bin ein Fähiger gefangen im Körper eines Unwilligen.

Ich lebe in einer Parallel-Welt zwischen Disneys Lustige Taschenbücher und schreib zack/bumm/knuff und soll aber Kaffka-eske Sätze ausformulieren und Besinnungsaufsätze zu Sachverhalten schreiben die mich intellektuell an meine Grenzen bringen…

Dokumentenhierarchie ISM mit zu erstellenden Richtlinien.pdf

TUN SIE ETWAS ABER MACHEN SIE NICHTS

Tägliche Herausforderung:

Diskussion letzte Woche im TAK (Themenarbeitskreis) Regulierung:

NIS2-Richtlinie:

Thema :Schulung der Geschäftsführung –

Ach nööööööööö….die bocken dann immer so……

AHA – die bocken also !

Wohl und Wehe eines überregulierten Unternehmens: Vorhandensein eines Schulungskonzeptes geclustert nach Art der zu verarbeitenden Informationen.

Mitarbeiter ist nicht mit Datenverarbeitung beschäftigt (Hausmeister) hoher Schulungsumfang

S1-Daten (darf jeder lesen) erhöhter Schulungsumfang

S2-S3-Daten SUPER-DUPER-MEGA-GIGA Schulungsumfang

Und Sie ahnen es bereits

S4-Daten (streng Vertraulich) E.S.K.A.L.A.T.I.O.N.

DATENSCHUTZ PRAXISGERECHT ?

Vom Wunsch und der Wirklichkeit …
Oder wie kommt man vom Hölzchen aufs Stöckchen?

- ✓ Richtlinie als Teil der Strategie
  - DatenschutzRichtlinie_Sparkasse Lörrach-Rheinfelden.docx
- ✓ Datenschutzmanagementkonzept als Teil der Richtlinie
  - Datenschutzmanagementkonzept - Sparkasse Lörrach-Rheinfelden_Version_3_Stand_01.03.2023.docx
- ✓ Datenschutzarbeitsanweisung als der Teil der schriftlich fixierten Ordnung also DSMK
  - 2.13.20 Datenschutz (1).pdf
- ✓ Datenschutzfolgeabschätzung-Vorprüfung als Teil der Arbeitsanweisung
  - Datenschutzfolgeabschätzung_Vorpruefung.xlsx
- ✓ Interessenabwägung falls die Vorprüfung nicht hilft
  - DSGVO_Pruefschema_Interessenabwägung1.xlsx
- ✓ DIE DSFA des Todes – der Genickschuss für den Prozessverantwortlichen
  - DSFASIEMHauptpruefung.docx
  - 07DSFAVideoueberwachung_mit_DSGVO_TOM_bereinigt.docx
  - 17202104DSFAWhistleblowingfuerAK_DSSPmitallgemRisikomatrixfinal.docx

MIETEN SIE EIN KINO

Wenn dann alles fertig geprokelt ist, beginnt der Spaß.
Die ganzen Ergüsse dürfen dann ins VVT……

„MUSTER gefällig?"

Ich höre kein wirkliches *„NEIN …*".
Wir sollten allerdings in den großen Saal umziehen, denn wir brauchen einen wirklich großen Bildschirm ….

WIRKLICH GROSS ….

Gurte stramm ziehen:

20210318Muster_VVT_v2.4_mit_Änderungskennung.xlsx

WER JETZT …

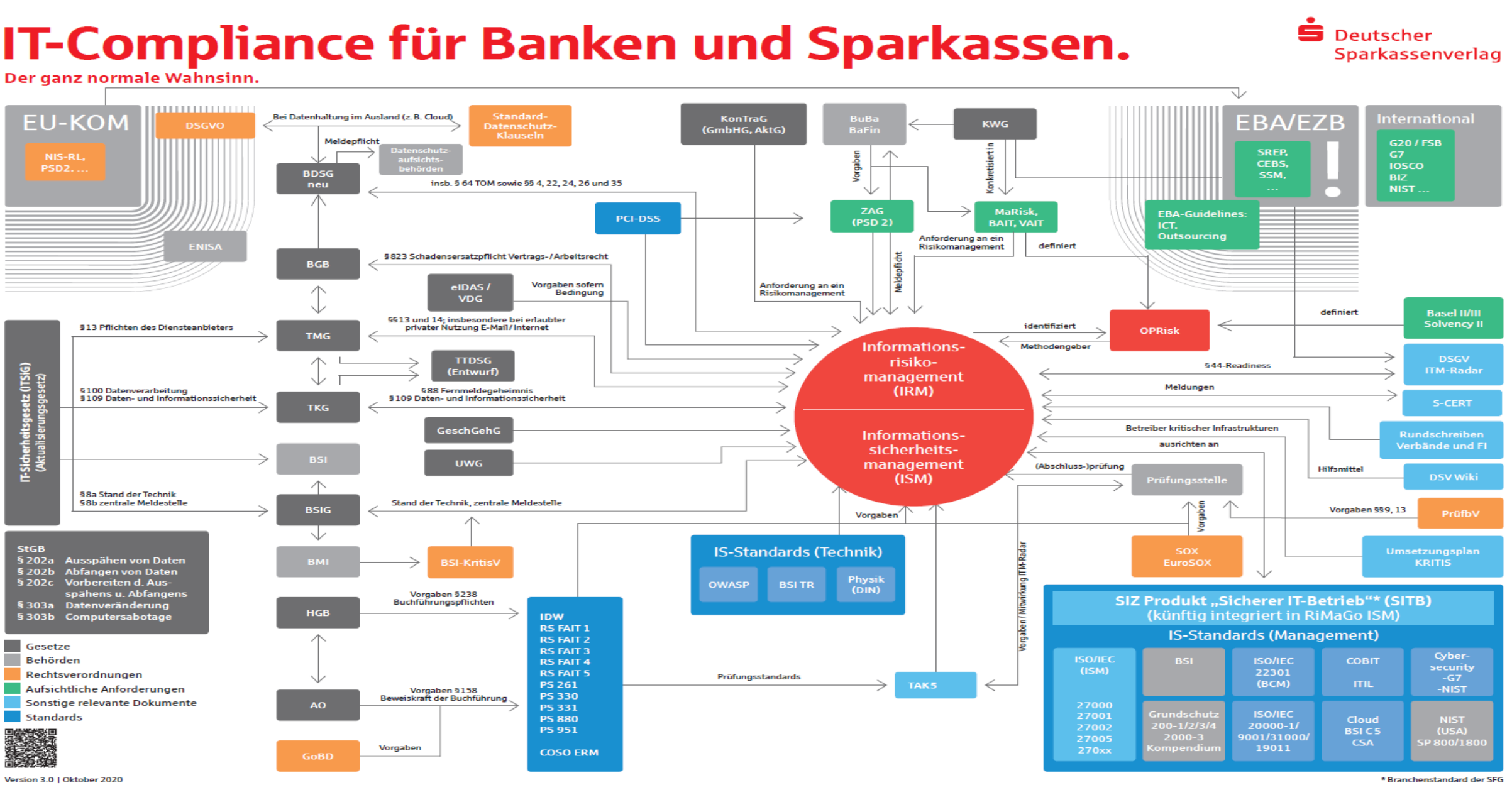
… noch nicht in der Nervenheilanstalt gelandet ist … oder
– schreiend das Gebäude verlässt….

Die Bankenaufsicht in unheilvoller Kombination mit der EU

Das Damoklesschwert über dem greisen Haupt schwebend und

Tränenblind nehmen wir zur Kenntnis:

WAHNSINN


IT-Compliance für Banken und Sparkassen.
Der ganz normale Wahnsinn.
Deutscher Sparkassenverlag
EU-KOM
NIS-RL, PSD2, ...
DSGVO
ENISA
Bei Datenhaltung im Ausland (z. B. Cloud)
Standard-Datenschutz-Klauseln
Meldepflicht
Datenschutz-aufsichts-behörden
BDSG neu
insb. § 64 TOM sowie §§ 4, 22, 24, 26 und 35
BGB
§ 823 Schadensersatzpflicht Vertrags-/Arbeitsrecht
eIDAS / VDG
Vorgaben sofern Bedingung
TMG
§ 13 Pflichten des Diensteanbieters
§§ 13 und 14; insbesondere bei erlaubter privater Nutzung E-Mail/Internet
TTDSG (Entwurf)
TKG
§ 100 Datenverarbeitung
§ 109 Daten- und Informationssicherheit
§ 88 Fernmeldegeheimnis
§ 109 Daten- und Informationssicherheit
GeschGehG
UWG
BSI
BSIG
§ 8a Stand der Technik
§ 8b zentrale Meldestelle
Stand der Technik, zentrale Meldestelle
BMI
BSI-KritisV
IT-Sicherheitsgesetz (ITSiG) (Aktualisierungsgesetz)
StGB
§ 202a Ausspähen von Daten
§ 202b Abfangen von Daten
§ 202c Vorbereiten d. Ausspähens u. Abfangens
§ 303a Datenveränderung
§ 303b Computersabotage
Gesetze
Behörden
Rechtsverordnungen
Aufsichtliche Anforderungen
Sonstige relevante Dokumente
Standards
HGB
Vorgaben §238 Buchführungspflichten
AO
Vorgaben §158 Beweiskraft der Buchführung
GoBD
Vorgaben
IDW
RS FAIT 1
RS FAIT 2
RS FAIT 3
RS FAIT 4
RS FAIT 5
PS 261
PS 330
PS 331
PS 880
PS 951
COSO ERM
KonTraG (GmbHG, AktG)
BuBa BaFin
KWG
Vorgaben
Konkretisiert in
PCI-DSS
ZAG (PSD 2)
MaRisk, BAIT, VAIT
Anforderung an ein Risikomanagement
definiert
Meldepflicht
Anforderung an ein Risikomanagement
EBA/EZB
SREP, CEBS, SSM, ...
EBA-Guidelines: ICT, Outsourcing
International
G20 / FSB
G7
IOSCO
BIZ
NIST ...
Informations-risiko-management (IRM)
Informations-sicherheits-management (ISM)
identifiziert
Methodengeber
OPRisk
definiert
Basel II/III Solvency II
§ 44-Readiness
DSGV ITM-Radar
Meldungen
S-CERT
Betreiber kritischer Infrastrukturen
ausrichten an
Rundschreiben Verbände und FI
(Abschluss-)prüfung
Prüfungsstelle
Hilfsmittel
DSV Wiki
Vorgaben §§ 9, 13
PrüfbV
Vorgaben
SOX EuroSOX
Umsetzungsplan KRITIS
Vorgaben
IS-Standards (Technik)
OWASP
BSI TR
Physik (DIN)
Vorgaben / Mitwirkung ITM-Radar
Prüfungsstandards
TAK5
SIZ Produkt „Sicherer IT-Betrieb"* (SITB)
(künftig integriert in RiMaGo ISM)
IS-Standards (Management)
ISO/IEC (ISM)
27000
27001
27002
27005
270xx
BSI
Grundschutz 200-1/2/3/4 2000-3 Kompendium
ISO/IEC 22301 (BCM)
ISO/IEC 20000-1/ 9001/31000/ 19011
COBIT
ITIL
Cloud BSI C5 CSA
Cyber-security -G7 -NIST
NIST (USA) SP 800/1800
* Branchenstandard der SFG
Version 3.0 | Oktober 2020

WER JETZT …

GESETZE UND VERORDNUNGEN

Und es kommt immer etwas NEUES:

- Die deutsche Cyberabwehr folgt einer dezentralen Logik und ist vor allem auf die Sicherheit der eigenen Systeme fokussiert. Deutschland und Europa gehen davon aus, durch zusätzliche Verordnungen die Cyberabwehr und Datensicherheit zu stärken und die Resilienz der beteiligten Akteure aus Wirtschaft und Staat dadurch zu erhöhen, in dem man neue Verordnungen und vor Allem neue Bußgeldvorschriften erlässt.

- Cyberarmee der Volksrepublik China im Zeitstrahl
  - 2004 ca. 30 „Elite-Hacker"
  - aktuell ca. 100.0000 Soldaten

- Deutschland „Nationales Cyber-Abwehrzentrum" aufgestellt 2011
  - Dienstposten geplant „10" aktuell besetzt „10" „Hackback" nicht zulässig!!!

- Länder wie Russland, China, aber auch Frankreich haben zum Beispiel „Wirtschaftsspionage" als offizielles Staatsziel in ihrer Verfassung stehen.

GESETZE

- BAIT (Bankaufsichtliche Anforderungen an die IT)
- DORA (Digital OperationalRessilienceAct)
- IT-SIG 2.0 (reines Artikelgesetz hier werden bestehende Rechtsnormen entweder verschärft oder konkretisiert oder oder oder)
- BSI-Gesetz
- KRITIS-VO (wenn eine Regelung nicht reicht)
- CRA (CyberResillianceAct) (dann darf noch Europa mitmischen)
- NIS-Richtlinie (und hier kommt der Rest der Rasselbande in den Fokus)

GESETZE

https://www.swr.de/swraktuell/baden-wuerttemberg/karlsruhe/hackerangriff-rastatt-umgang-100.html

Gerade ist zu merken, dass die Kommunen und Landratsämter – generell öffentliche Stellen - recht hektische Flecken bei diesen ganzen üblen Nachrichten – ich meine nicht die Cyberbedrohungen - bekommen…

ABER…

Der deutsche Beamte neigt zum Glück nicht zum übereifrigen und unbedachtem Handeln…

Ruhe kehrt ein sobald man merkt, dass man von den Bußgeldvorschriften ausgenommen ist…

Das bringt dann alle wieder ins ruhigere Fahrwasser und lässt sie wieder ruhig schlafen.

WAS GEHT DA VOR SICH ?

https://cybermap.kaspersky.com/de/

Wer Kaspersky misstraut:

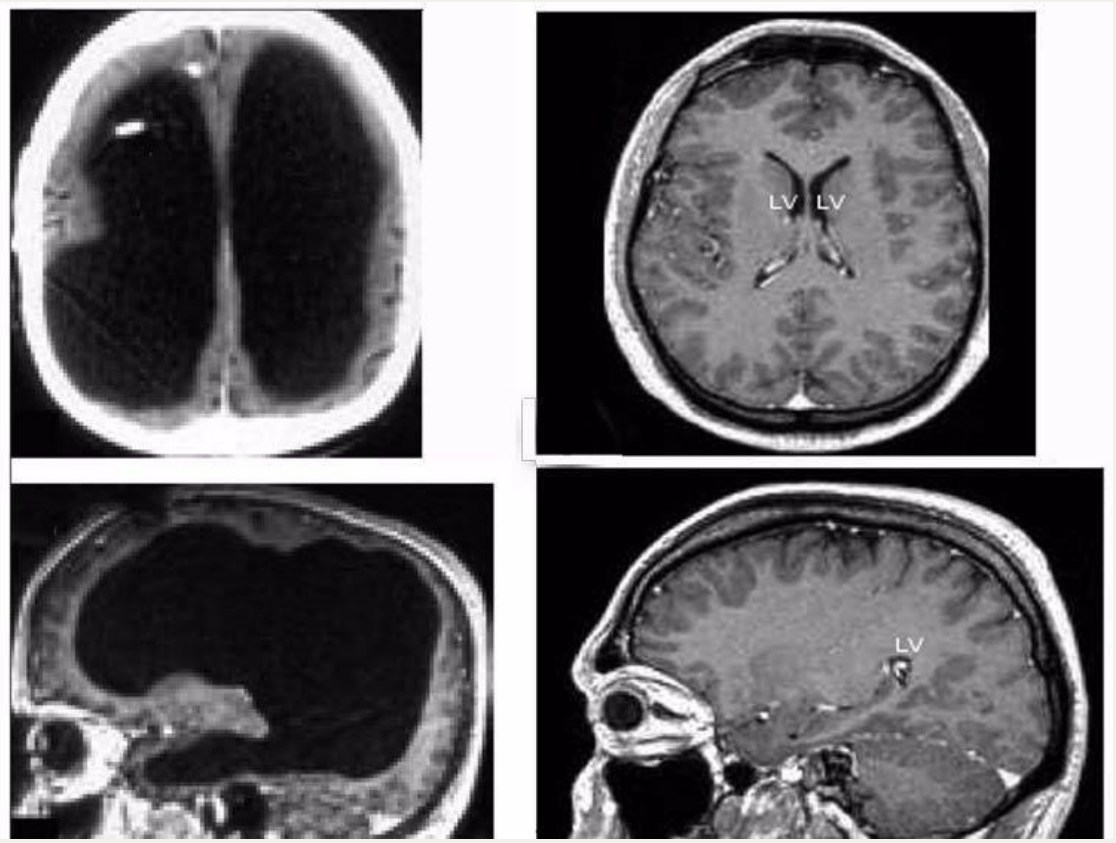
Live Cyber Attack Threat Map | Radware

IST JA NICHT SO ALS WÜRDE NICHTS PASSIEREN

Warnmeldungen\BSI-Tagesbericht\2023

WEIL MAN SO NICHT ARBEITEN KANN

BLUTIGER WIRD ES NICHT



1. **PASSWÖRTER**
2. **Zutritt (by Wildwest, Schlüssel, Smartcard)**
3. **Zugang (by Wildwest)**
4. **Zugriff……**

WENN SICHERHEITSMAßNAHMEN GUT GEMEINT SIND

Das Gegenteil von

gut gemacht,

ist gut gemeint.

NFC-KARTEN.....

BEI BEDARF

RFID/NFC Multi Frequenz ID Karten Replikator IC Keychain Duplicator Englisch Lesen Schreiben Programmer mit 10pcs ID-125KHz Karten + 10pcs ID-125KHz Schlüsselanhänger + 10pcs IC-13,56MHz UID Taste: Amazon.de: Computer & Zubehör

Neuftech USB RFID Reader ID Kartenlesegerät Kartenleser Kontaktlos Card Reader für EM4100: Amazon.de: Elektronik & Foto

Ihre Fragen ???

Vielen Dank!

Kontakt

Christoph Kopper
Tel.: 07621/411- 0
Email: datenschutz@sparkasse-loerrach.de