

SECU INFRA

Cyber Defense. Made in Germany.

8. BDL-Forum Digitalisierung

Cyber Security im Focus



Ramon Weil
Founder & CEO - SECUINFRA

Cyberangriff auf Rheinmetall

14. April 2023, 19:39 Uhr | Lesezeit: 1 min | [Kommentare](#)

Polizei und Armee indirekt von Cyberangriff betroffen

Ein auf IT für innere Sicherheit spezialisiertes Unternehmen ist von Hackern

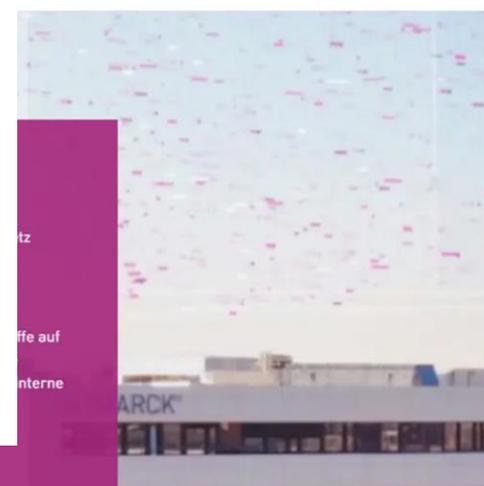
Ferrari von Hackern angegriffen

AKTUALISIERT AM 21.03.2023 - 11:42



r ist Opfer eines Hackerangriffs geworden. ir Kontaktinformationen von Kunden, teilte

n-Dienstleister



Störungen bei Versicherungen
Cyberangriff auf Krankenkassen-Dienstleister

Kunden- oder Versicherten-Daten abgeflossen?

Stand: 27.04.2023 13:08 Uhr

Deutsche Leasing AG

Sparkassen-Tochter wird Opfer eines Hackerangriffs

Das Unternehmen hat nach dem Vorfall den Zugriff auf die Systeme abgeschaltet. Ob Daten abgegriffen wurden, ist noch unklar.

Michael Maisch
06.06.2023 - 18:51 Uhr



Rhein-Main

Cyberangriff auf Kunden-Daten

KRANKENKASSEN

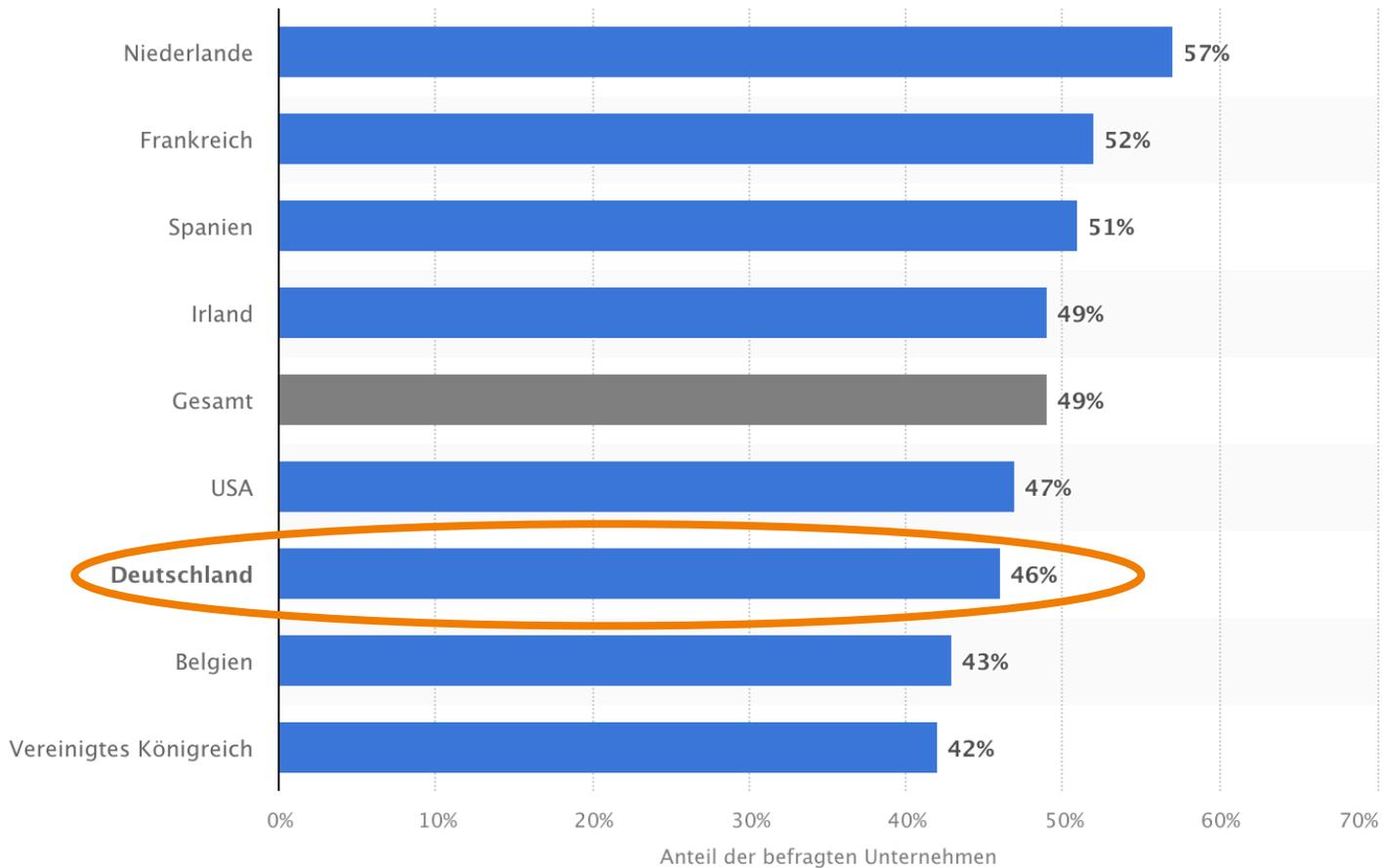
AOK meldet Sicherheitsbruch: Millionen Versicherten-Daten abgegriffen

Krankenkassen der AOK in zehntausend Bundesländern: Unbefugte womöglich auf sensible Daten von Versicherten zugegriffen haben

Lukas Hoffmann, Jürgen Klöckner, Dietmar Neuerer, Britta

02.06.2023 • Update: 02.06.2023 - 21:01 Uhr





46%
aller befragten
Unternehmen
in Deutschland
haben 2022
einen Cyberangriff
erlebt.

[Details zur Statistik](#)

© Statista 2023

[Quellen anzeigen](#)

Schaden durch Cybercrime jährlich >200 Mrd. €

Schaden durch...	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)	Schadenssummen in Mrd. Euro (2021)
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	35,3	23,6	12,3
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	35,0	41,5	61,9
Kosten für Rechtsstreitigkeiten	29,8	16,2	12,4
Kosten für Ermittlungen und Ersatzmaßnahmen	25,2	10,1	13,3
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	21,5	41,5	29,0
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	16,1	10,7	24,3
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	15,3	21,1	22,7
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	12,4	18,5	17,2
Patentrechtsverletzungen (auch schon vor der Anmeldung)	10,4	18,8	30,5
Geldabfluss durch Betrugsversuche	3,9		
Sonstige Schäden	1,1	0,9	0
Gesamtschaden pro Jahr	205,9	202,7	223,5

**Schaden bei ca. 5%
des BIP Deutschlands!**

Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich | rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen. |
Quelle: Bitkom Research 2023

bitkom

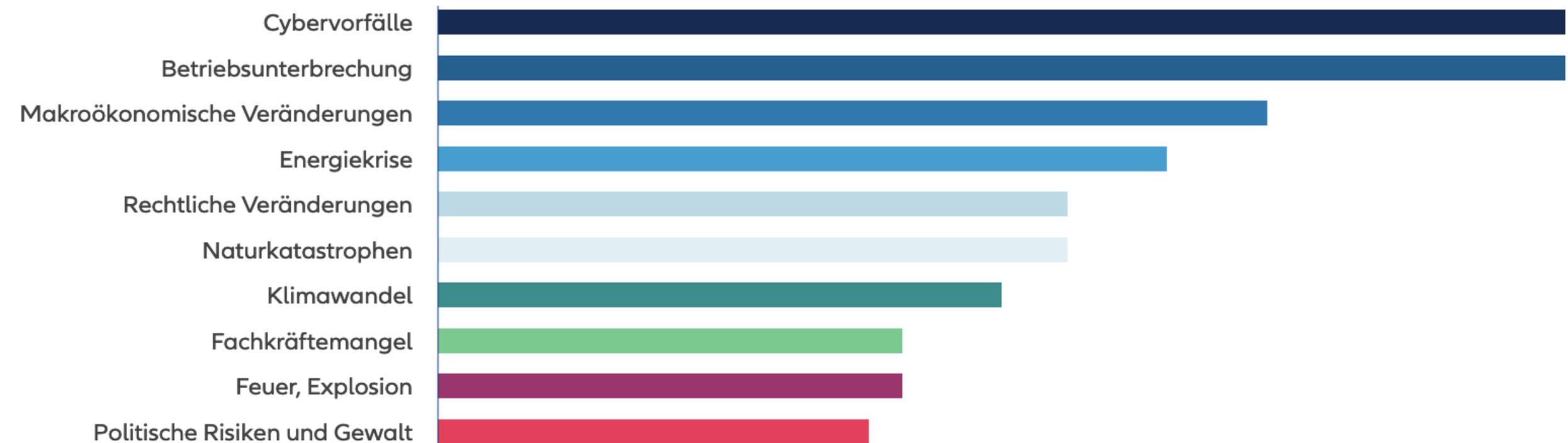
Größtes Geschäftsrisiko: Cyberangriffe!



Top 10 Geschäftsrisiken weltweit in 2023

Allianz Risk Barometer 2023

Basierend auf den Antworten von 2.712 Risikomanagement-Experten aus 94 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



Erfahrungen aus der Praxis

SECUINFRA Cyber Defense. Made in Germany. **Focus:** Erkennung/Analyse/Abwehr von Cyberangriffen seit 2010

Täglich melden sich **Opfer von Cyberangriffen** bei uns!

- **Kleinigkeiten:**
 - CEO Fraud
 - Webseite, Social Media Account übernommen
 - Bankaccount übernommen
 - Einzelne Rechner/Telefone gehackt

Erfahrungen aus der Praxis

SECUINFRA Cyber Defense. Made in Germany. **Focus:** Erkennung/Analyse/Abwehr von Cyberangriffen seit 2010

Täglich melden sich **Opfer von Cyberangriffen** bei uns!

- **Existenzen:**

- **RANSOMWARE**

- IT-Systeme verschlüsselt
 - keine Produktion/Vertrieb/Angebote/Rechnungen/Buchungen/Kommunikation...
 - für Stunden/Tage/Wochen...
- Massenhaft Daten gestohlen

YOUR SYSTEM HAS BEEN PENETRATED by LV



Your company documents, databases and other important files have been **encrypted**



Your confidential documents, personal data and sensitive info have been **downloaded**



All the downloaded info will be **published and put up for sale in darknet** if you don't pay

You have
2 days 23:59:34

Your price
\$500,000

STOP IT !

**IF YOU DO NOT PAY ON TIME, ALL THE DOWNLOADED INFORMATION WILL BE PUBLISHED AUTOMATICALLY
JOURNALISTS AND DATA PROTECTION AUTHORITY WILL BE NOTIFIED ABOUT PERSONAL DATA LEAK**

IT'S JUST A BUSINESS

We'll receive money anyway: from you or from the darknet

IF YOU DO NOT PAY

IF YOU PAY ON TIME

Live chat

W***** C***** A***** D***** D*****

The company that operates in the Government appraiser industry.

Revenue: > \$5 Million

Data Volume: > 800 GB

.....

Data description:

- * Personal Data.
 - * Accounting, budget, financial data.
 - * Payroll data.
 - * Contract data.
 - * Operational and business files.
 - * Email and msg archives.
-

**„Serviceseite“
im Darknet**

This company's data will become available in days. Contact us if you want to get it or if you want to protect it.

Erfahrungen aus der Praxis

SECUINFRA Cyber Defense. Made in Germany. **Focus:** Erkennung/Analyse/Abwehr von Cyberangriffen seit 2010

Täglich melden sich **Opfer von Cyberangriffen** bei uns!

- **Existenzen:**

- **RANSOMWARE**

- IT-Systeme verschlüsselt
 - keine Produktion/Vertrieb/Angebote/Rechnungen/Buchungen/Kommunikation...
 - für Stunden/Tage/Wochen...
- Massenhaft Daten gestohlen
- Erpresser gut informiert über Finanzen.
 - Lösegeld richtet sich nach Finanzkraft des Opfers! Üblich 1% - 5% des Umsatzes.*

Was tun? Die richtige Balance ist wichtig.



Angriff
verhindern
verlangsamen

Angriff
erkennen
abwehren



GESCHWINDIGKEIT ist der Schlüssel!

Wer ist schneller?
Angreifer oder Verteidiger?

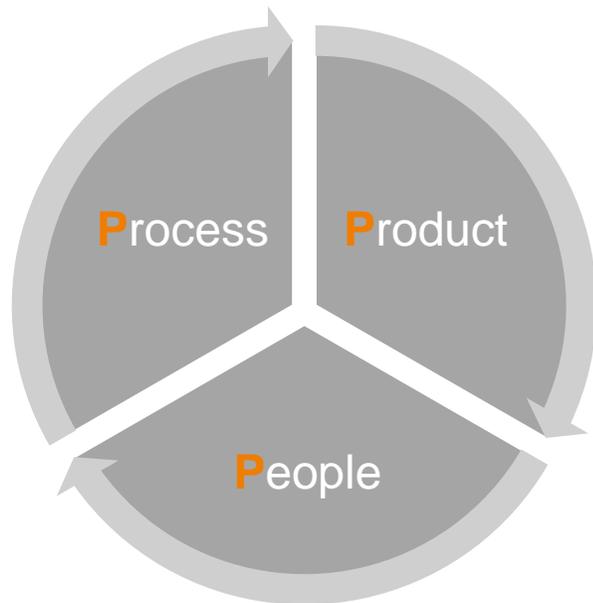


- Angriffsfläche reduzieren
- Zero Trust
- Verschlüsselung
- 2-Faktor Authentifizierung
- ...

- SOC aufbauen/einkaufen
- 24/7 Erkennung, Analyse und Abwehr

Cyberangriffe erkennen, analysieren, abwehren

Selber machen?

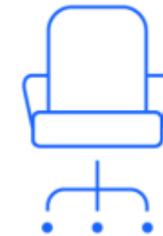
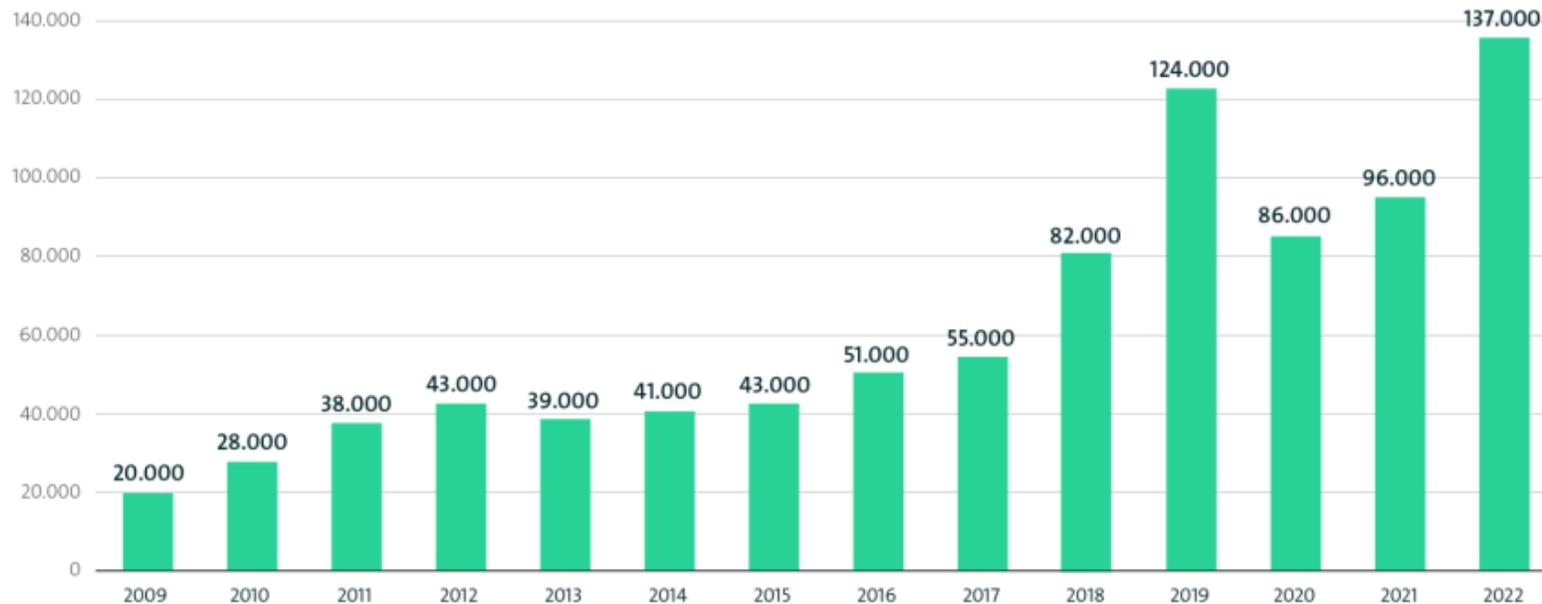


- Teure Tools
- Teure Experten
- **Fachkräftemangel**

SOC – Experten: Fachkräftemangel

Trotz Krieg und Krisen: IT-Fachkräftebedarf zieht an

Anzahl zu besetzender IT-Stellen in der Gesamtwirtschaft



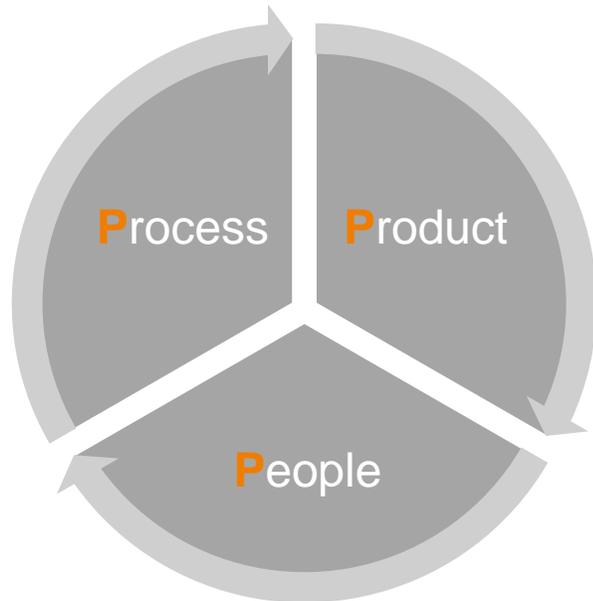
Basis: Unternehmen ab 3 Beschäftigten in Deutschland (n=854) | Datenerhebung: jeweils im September | Quelle: Bitkom Research 2022

bitkom

Studie:
Dienst
140.000

Cyberangriffe erkennen, analysieren, abwehren

Selber machen?



- Teure Tools
- Teure Experten
- **Fachkräftemangel**

Service einkaufen?



- Schnelle Umsetzung
- Deutliche Risikoreduzierung
- **Vorsicht bei der Partnerwahl!**

Mythen rund um IT-Sicherheit

1. Ich bin nicht interessant für Angreifer.

- Können Sie ohne IT arbeiten?
- Wenn Sie nicht ohne IT arbeiten können, sind Sie erpressbar und somit interessant für Angreifer!

2. IT-Sicherheit kostet nur Geld.

- Zukünftig wird es nur noch Unternehmen geben, welche ihre IT-Sicherheit im Griff haben!
- Ohne Digitalisierung verliert man an Wettbewerbsfähigkeit.
- Digitalisierung ohne IT-Sicherheit führt zwangsläufig in die Katastrophe!

3. Mit den richtigen Cyber Defense Produkten bin ich sicher.

- 100% Sicherheit gibt es nicht!
- Security Produkte helfen Cyber Defense Experten bei ihrer Arbeit.
- Ohne die Experten sind Cyber Defense Produkte meist nutzlos!

SECU INFRA

Cyber Defense. Made in Germany.

Vielen Dank