TÜV SÜD Sec-IT

Mehr Sicherheit.
Mehr Wert.

Cyber Security – versäumen Sie nicht den Angriff auf Sie!

Thierstein, 27.04.2017

Unsere Geschichte: Erfolg seit 150 Jahren

Sec-IT

1866 Am 6. Januar gründen 22 Dampfkesselbesitzer in Mannheim den ersten Dampfkessel-Revisions-Verein.

1881 Die ersten bindenden Sicherheitsstandards für Kesselsicherheit werden verabschiedet und ebnen den Weg für einheitliche technische Inspektionen.

1906 Erstmalige Durchführung von regelmäßig wiederkehrenden Fahrzeuguntersuchungen.

1951 TÜV-Organisationen werden mit der Durchführung regelmäßiger Inspektionen aller motorisierten Fahrzeuge beauftragt.

1989 TÜV Product Service GmbH wird ins Leben gerufen und nimmt dabei eine Vorreiterrolle für internationale Prüfungen ein.

1996 Die TÜV-Gesellschaften Süddeutschlands werden zu TÜV SÜD.

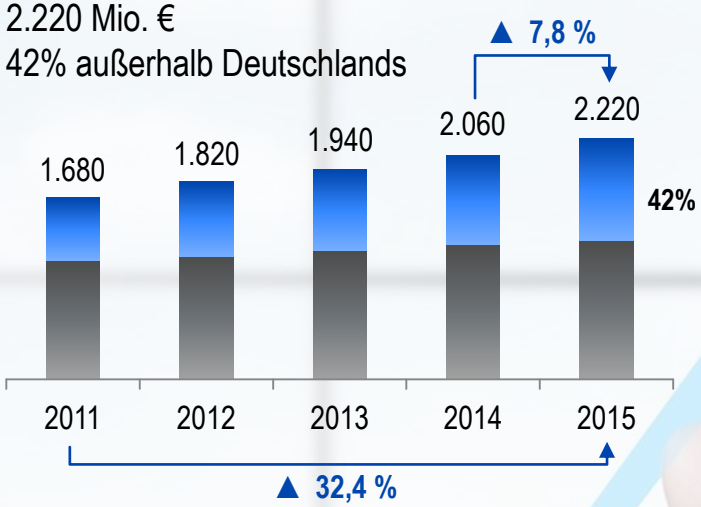
2001 Das TÜV SÜD-Oktagon wird als einheitliches Prüfzeichen eingeführt.

Heute TÜV SÜD verfolgt weiter seine erfolgreiche Internationalisierungs- und Wachstumsstrategie.

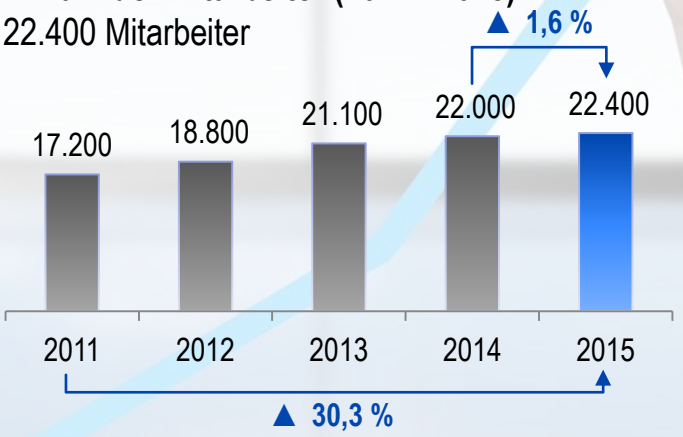
TÜV SÜD Übersicht – Zahlen & Fakten

1	Dienstleister für alle technischen Lösungen
150	Jahre Erfahrung
850	Standorte weltweit
2.220	Millionen Euro Umsatz 2015
24.000	Mitarbeiter weltweit Stand Februar 2016

Umsatz (2011 - 2015)
2.220 Mio. €
42% außerhalb Deutschlands



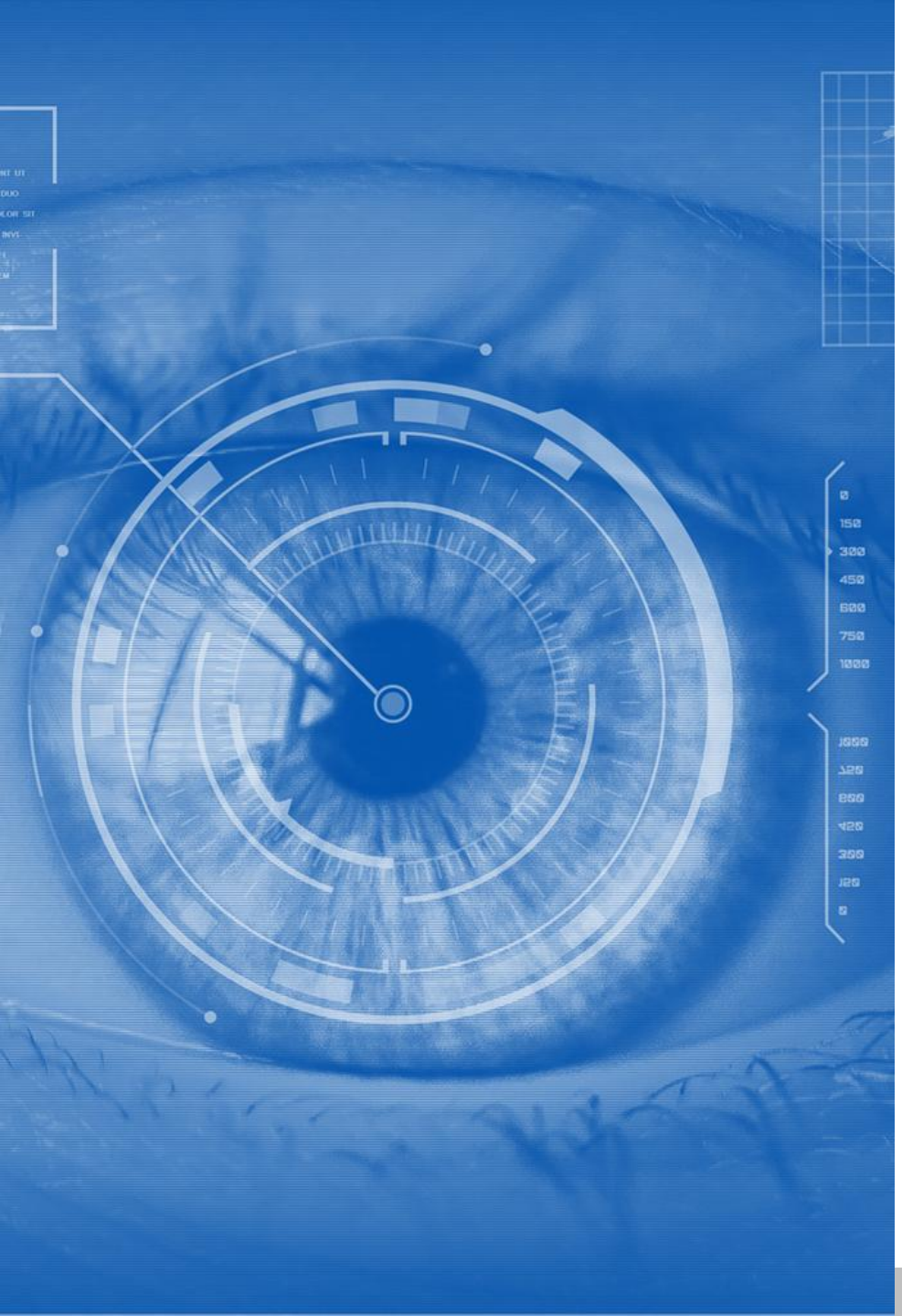
Anzahl der Mitarbeiter (2011 - 2015)
22.400 Mitarbeiter



Leistungsspektrum der TÜV SÜD Sec-IT GmbH

Sec-IT

Positions-Bestimmung	Detail-Prüfungen		Umsetzung	Zertifizierung	Ökonomischer Erfolg
					
Einstieg zur Risikoermittlung Grober Handlungsbedarf	Vor- Ort und Remote-Audits Ggf. mit technischer Unterstützung	**Spezifischer Handlungs-bedarf** Technische Anforderungen Organisatorisch & rechtliche Anforderungen	Hebung des Reifegrads	Nachgewiesene Erfüllung von Standards	**Sicherheit** **Vertrauen** **Umsatz-Wachstum**
• **Cyber-Security-Check** • **Datenschutz-Check** • **Schwachstellen-Scans** • **Hacking-Lab**	• **Penetrationstests** • **Prüfung von Rechenzentren** • **Website-Checks** • **Payment-Card-Industry-Checks**		• **Validierung von Maßnahmen** • **Best Practices**	• **s@fer-shopping** • **PCI** • **Rechenzentren** • **Auftragsdaten-verarbeitung**	



TÜV SÜD Sec-IT

Mehr Sicherheit.
Mehr Wert.

Ein Pfund Gehacktes

„Live-Hacking“ mit Google
Warum werden Unternehmen angegriffen?
Wie werden Unternehmen angegriffen?

Googlen = Hacken?

Sec-IT

Google ist die beliebteste und meist genutzte Suchmaschine.

Google lernt aus Suchanfragen, findet und erarbeitet täglich terabyteweise neue Inhalte mit automatisierten Mechanismen

Google bietet neben der Standardsuche verschiedene Suchparameter

…die setzen wir sinnvoll ein…

…und finden Verborgenes!

Googlen = Hacken?

Sec-IT

Wir verwenden z.B. „inurl“ vor dem Suchbegriff, um speziell in der Webadresse zu suchen oder mit „intitle“ Begriffe im Namen der Webseite zu finden.

In Kombination und mit speziellen interessanten Suchbegriffen finden sich so sehr viele kritische Dinge.

Googlen = Hacken?

Sec-IT

Warum finden wir so etwas?

- Unsichere „Out-of-the-Box“-Produkte wie Überwachungskameras oder Multifunktionsdrucker

- Unsichere Cloud-Services

- Fehlendes Fachwissen beim Einrichten eigener „Dienste“ (Vom Webserver bis zur FritzBox)

Sie sehen: Die Angriffspunkte finden sich auch bei KMU und Kleinstunternehmen!

Googlen = Hacken?

Sec-IT

Beispiele:

intitle:“index of“ inurl:”cv.pdf”

Googlen = Hacken?

Sec-IT

Beispiele:

intitle:“index of“ inurl:”Bewerbungen”

Googlen = Hacken?

Sec-IT

Beispiele: filetype:reg intext:“internet account manager“

Googlen = Hacken?

Sec-IT

Beispiele: intitle:“Officejet Pro 8600“

Googlen = Hacken?

Sec-IT

Beispiele: intitle:“Kontoauszug“

Googlen = Hacken?

Sec-IT

Beispiele: intitle:“Kontoauszug“

Warum werden Unternehmen angegriffen

Motivation von Angreifern

Sec-IT

- Abgreifen und Kopieren von Daten zum Verkauf
  - Kreditkartendaten
  - Kundenadressen
- Erpressung von Unternehmen
  - Ransomware
  - Veröffentlichung schutzwürdiger Daten
- Abgreifen und Kopieren von Daten zur Eigennutzung
  - Provisionsmodelle (TK- und Energiebranche), Kundenabwerbung
  - Wettbewerbsausspähung
- Beschädigung des Unternehmens
  - Rache, Unzufriedenheit
  - Vandalismus

Wie werden Unternehmen angegriffen

Motivation von Angreifern

Sec-IT

Externe Angriffe:

- Social Engineering und Informationsbeschaffung
  - Facebook, Google, Twitter, Vereinsseiten, Diskussionsforen…
- Ausnutzen von Sicherheitslücken über das Internet
  - Webserver, SSL/TLS, PHP, Datenbanken, Blogsysteme…
- Nutzen erbeuteter Authentifizierungsmerkmale auf externen Zugängen
  - Backendsysteme, Redaktionssysteme, Datenbanken…
- Einschleusen von Schadcode z.B. per Mail, Download, BYOD oder USB-Devices
  - Mitarbeiterhandys, Tablets, Heim-PCs, USB-Sticks, E-Zigaretten…
- Abhören/Abgreifen von Informationsübermittlungen aus dem Umfeld heraus
  - DECT-Anlagen, unverschlüsselte Internetkommunikation, Monitore, öffentliche Gespräche

Wie werden Unternehmen angegriffen

Motivation von Angreifern

Sec-IT

Interne Angriffe:

- Unzufriedene Mitarbeiter werden „eingekauft“
- Angreifer kommt direkt als „Handwerker“ ins Haus
- Manipulierte Hardware
- Einbruch
- …

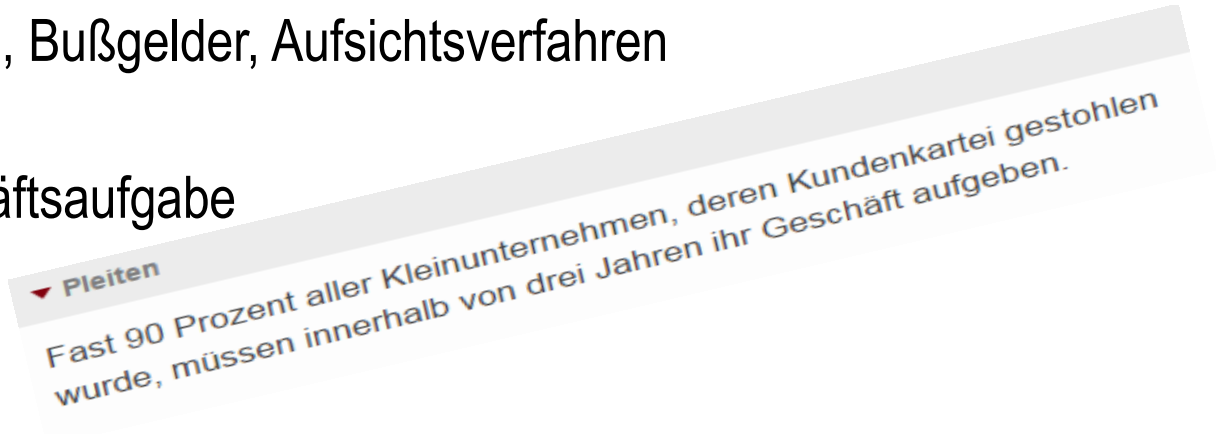
Wie werden Unternehmen angegriffen

Motivation von Angreifern

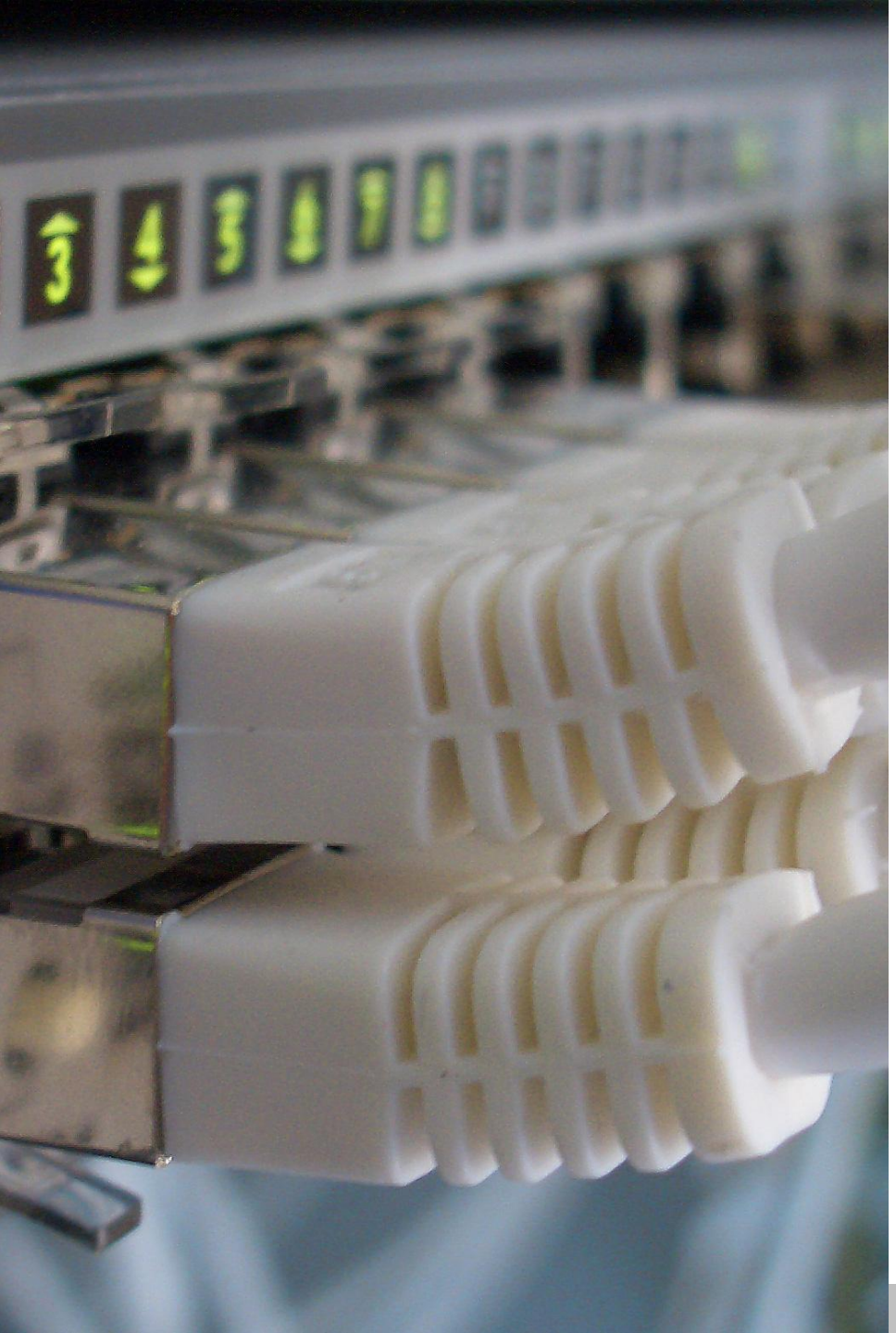
Sec-IT

Folgen:

- Direkter Finanzieller Verlust z.B. durch Erpressung
- Finanzieller Aufwand durch Schadensbehebung
- Imageverlust, Reputationsmaßnahmen
- Rechtliche Folgen, Bußgelder, Aufsichtsverfahren
- Insolvenz, Geschäftsaufgabe



Quelle: http://www.wiwo.de/technologie/hacker/wir-kaempfen-um-unsere-existenz-wir-haben-ihre-rechnung-erhalten-aber-den-auftrag-nie-erteilt/12733898-2.html



TÜV SÜD Sec-IT

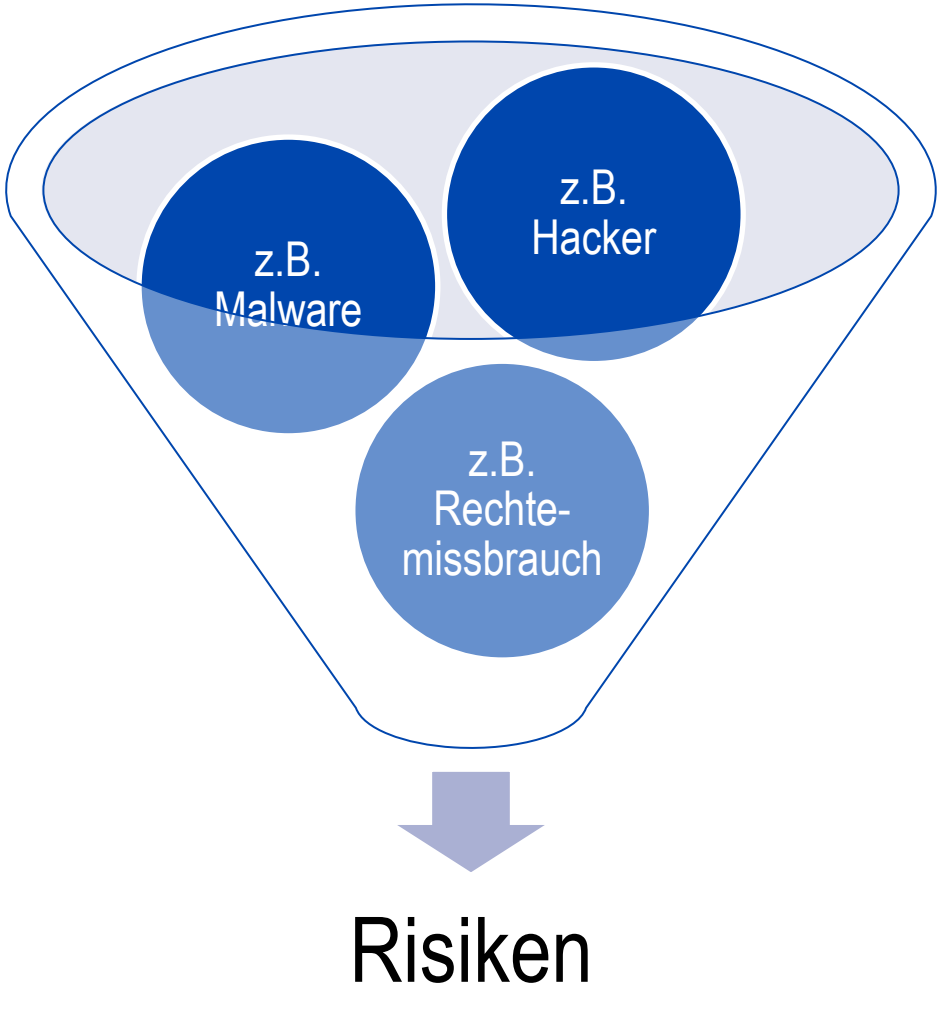
Mehr Sicherheit.
Mehr Wert.

Cyber Security Check

Unsere Unterstützung zur
Risikoeinschätzung

Cyber Security Check hilft bei Risikoeinschätzung

Sec-IT



Cyber Security Check hilft bei Risikoeinschätzung

Sec-IT

Risikovermeidung

Einstellen risikobehafteter Aktivitäten

…oftmals keine mögliche Option.

Risikobeherrschung

Ergreifen angemessener Schutzmaßnahmen

(z.B. ISO27001 Annex A)

Risikomanagement

Risikoakzeptanz

Genaue Kenntnis und Bewertung der Bedrohungen und daraus resultierender Risiken notwendig

Risikoübertragung

Dritte übernehmen das Risiko, z.B. Outsourcing oder Versicherung des Risikos.

Cyber Security Check hilft bei Risikoeinschätzung

Sec-IT

Cyber Security Check hilft bei Risikoeinschätzung

Sec-IT

- Zur Risikoeinschätzung benötigt:

  Systematischer Ansatz um Struktur von Unternehmen und Technik möglichst vollständig zu erfassen

  Kenntnis von IT-Prozessen und Best Practices

  Kenntnis von IT-Bedrohungen und üblichen Gegenmaßnahmen

-> In KMU und Kleinstunternehmen meist nicht vorhanden.

Cyber Security Check hilft bei Risikoeinschätzung

Sec-IT

- TÜV SÜD Sec-IT bringt als Prüfdienstleister im IT-Umfeld mit:
- mehr als 15-jährige Erfahrung im IT-Security-Umfeld
- Auditoren mit breitem Wissensansatz von Datenschutz über Qualitäts- und Prozessmanagement bis zu ISO27001-Expertise
- Effektive Tools und zuverlässige Abwicklungsprozesse
- Hohe Awareness und sehr hohe Sicherheit der Prüfergebnisse
- regionale Verteilung von Fachexperten

Cyber Security Check hilft bei Risikoeinschätzung

Sec-IT

- TÜV SÜD Cyber Security Check:
- Grundlage ist ISACA-Leitlinie für Durchführung von Cyber-Sicherheits-Checks der Allianz für Cybersicherheit
- Anforderungs- und Prüfkatalog mit
  53 Einzelprüfpunkten aus 13 Bereichen
- Prüfung vor Ort beim Unternehmen

Cyber Security Check hilft bei Risikoeinschätzung

Sec-IT

- 13 Themenbereiche der Prüfung:

A	• Absicherung von Netzübergängen
B	• Abwehr von Schadprogrammen
C	• Inventarisierung der IT-Systeme
D	• Vermeidung von offenen Sicherheitslücken
E	• Sichere Interaktion mit dem Internet
F	• Logdatenerfassung und -auswertung
G	• Sicherstellung eines aktuellen Informationsstands
H	• Bewältigung von Sicherheitsvorfällen
I	• Sichere Authentisierung
J	• Gewährleistung der Verfügbarkeit notwendiger Ressourcen
K	• Durchführung nutzerorientierter Maßnahmen
L	• Sichere Nutzung Sozialer Netzwerke
M	• Durchführung von Penetrationstests

Cyber Security Check hilft bei Risikoeinschätzung

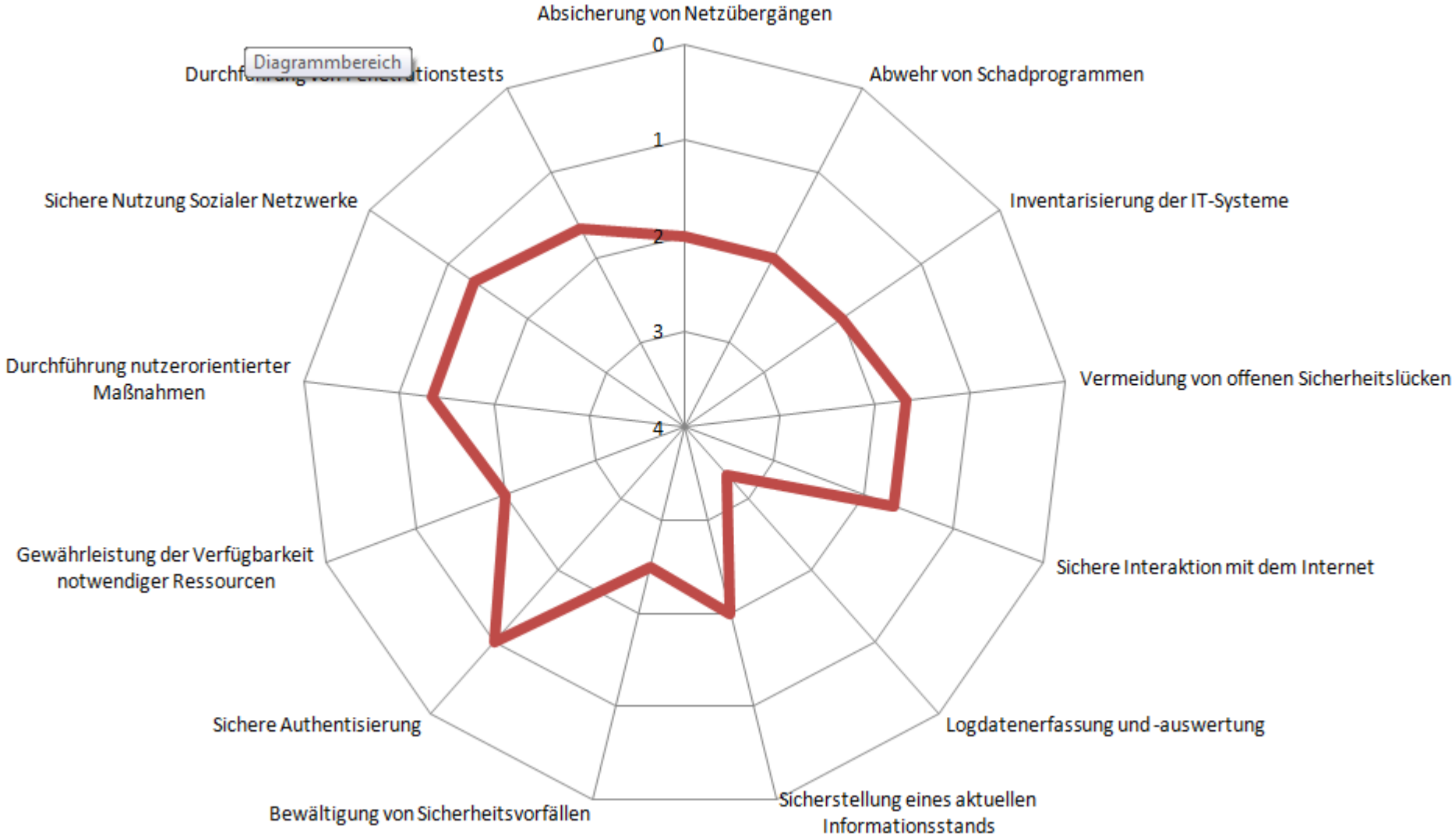
Sec-IT

- TÜV SÜD Cyber Security Check:
  - Konzentrierte und effiziente Prüfung vor Ort beim Unternehmen
  - Bericht gibt schnellen Überblick über Bedrohungslage und Einzelbewertung aller geprüften Punkte.

A	Absicherung von Netzübergängen	2,00	2 - Mittleres Sicherheitsrisiko
B	Abwehr von Schadprogrammen	2,00	2 - Mittleres Sicherheitsrisiko
C	Inventarisierung der IT-Systeme	2,00	2 - Mittleres Sicherheitsrisiko
D	Vermeidung von offenen Sicherheitslücken	1,67	2 - Mittleres Sicherheitsrisiko
E	Sichere Interaktion mit dem Internet	1,67	2 - Mittleres Sicherheitsrisiko
F	Logdatenerfassung und -auswertung	3,33	3 - Hohes Sicherheitsrisiko
G	Sicherstellung eines aktuellen Informationsstands	2,00	2 - Mittleres Sicherheitsrisiko
H	Bewältigung von Sicherheitsvorfällen	2,50	3 - Hohes Sicherheitsrisiko
I	Sichere Authentisierung	1,00	1 - Verbesserungspotenzial
J	Gewährleistung der Verfügbarkeit notwendiger Ressourcen	2,00	2 - Mittleres Sicherheitsrisiko
K	Durchführung nutzerorientierter Maßnahmen	1,33	1 - Verbesserungspotenzial
L	Sichere Nutzung Sozialer Netzwerke	1,33	1 - Verbesserungspotenzial
M	Durchführung von Penetrationstests	1,67	2 - Mittleres Sicherheitsrisiko

Cyber Security Check hilft bei Risikoeinschätzung

Sec-IT



Cyber Security Check hilft bei Risikoeinschätzung

Sec-IT

- TÜV SÜD Cyber Security Check:

Der zugrundeliegende Leitfaden bietet ein Mapping zu gängigen IT-Sicherheits-Standards:

- ISO 27001
- BSI-Grundschutkatalog
- Cobit 5
- PCI DSS 3.0

	Maßnahmen	Basismaßnahmen	Referenzen
A	**Absicherung von Netzübergängen** Die Absicherung von Netzübergängen ist einer der entscheidenden Faktoren für eine wirksame Abwehr von Angriffen aus dem Internet. Auf Grundlage der Netzwerkarchitektur müssen Abwehrmaßnahmen für alle internen und externen Netzübergänge sowie die entsprechenden Prozesse (wie z. B. ein Change Management) geplant und umgesetzt werden.	» Alle Netzübergänge sind identifiziert und dokumentiert. » Das Netz ist in Segmente aufgeteilt und die Anzahl der Netzübergänge wird minimal gehalten. » Alle Netzübergänge sind durch geeignete Sicherheitsgateways abgesichert und werden regelmäßig überprüft. » Auf Client- und Serversystemen findet eine technische Schnittstellenkontrolle statt, die eine zulässige Nutzung kontrolliert und eine unzulässige Nutzung verhindert. » Zugänge mobiler IT-Geräte sind angemessen abgesichert und auf das erforderliche Mindestmaß beschränkt. » Zugänge für Remote-Administration und -Überwachung sind angemessen abgesichert. » Es werden nur zeitgemäße Verschlüsselungs- und Authentisierungsverfahren eingesetzt.	**BSI IT-GSK 13. Erg.-Lieferung:** B 3.301, B 3.302, B 4.1, B 5.14, M 2.204 **COBIT 5:** DSS05.02, DSS05.03, DSS06.06 **ISO/IEC 27001:2005:** A.10.6, A.10.7.1, A.11.4, A.11.6.2, A11.7, A.12.5.4 **ISO/IEC 27001:2013:** A.6.2, A.8.3.1, A.9.1.2, A.13.1 **PCI DSS 3.0:** 1.1, 1.1.2, 1.1.4, 1.1.6, 1.2, 1.2.3, 1.3, 1.3.1-1.3.8, 1.4, 2.2.3, 2.2.4, 4.1, 4.1.1, 8.3, 11.4, 12.3.8, 12.3.9

Cyber Security Check hilft bei Risikoeinschätzung

Sec-IT

- Aufwand für einen TÜV SÜD Cyber Security Check
  - Kalkulation nach Ausfüllen eines Fragebogens zur Einschätzung des Unternehmens
  - Kleine Unternehmen bis 25 MA: ca. 1.400 EUR bis ca. 1.700 EUR
  - Klassischer Mittelständler 100 MA: ca. 2.000 EUR bis ca. 2.800 EUR
  - Großunternehmen über 250 MA: ca. 3.400 EUR bis ca. 4.100 EUR
  - Penetrationstest immer optional.

Cyber Security Check hilft bei Risikoeinschätzung

Sec-IT

- TÜV SÜD Cyber Security Check:

  Weiterführende Prüfungen / Zertifizierungen durch TÜV SÜD helfen bei der kontinuierlichen Verbesserung:

  - Regelmäßig wiederholter Cyber Security Check
  - IT-Penetrationstests
  - PCI-DSS – Prüfung/Zertifizierung (TÜV SÜD Management Service)
  - ISO27001-Zertifizierung (TÜV SÜD Management Service)
  - IT-Awareness-Schulungen
  - Datenschutzprüfungen /Zertifizierungen

Tipps für den Alltag

Sec-IT

Marko Hoffmann
Information Security and Risk Services

089-5008-4616
marko.hoffmann@tuev-sued.de

tuev-sued.de/csc