




# SI Cyberschutz

## Ihr Schutz vor finanziellen Risiken

Markus Zahlfeld, Spezialist „Gewerbe absichern“ GD Essen

1

**Heute ist bei Ihnen zum Thema Cyberversicherung**

### Markus Zahlfeld

**47 Jahre**

**Spezialist für gewerbliche Versicherungen  
in der SIGNAL IDUNA Gebietsdirektion Essen**

Technischer Underwriter (DVA)  
Haftpflicht Underwriter (DVA)  
Brandrisiko-Manager (VdS)

**Beratung, Risiko-/Bedarfsanalyse, Risikobesichtigungen im Bereich der gewerblichen**

**- Sachversicherung**  
insbesondere

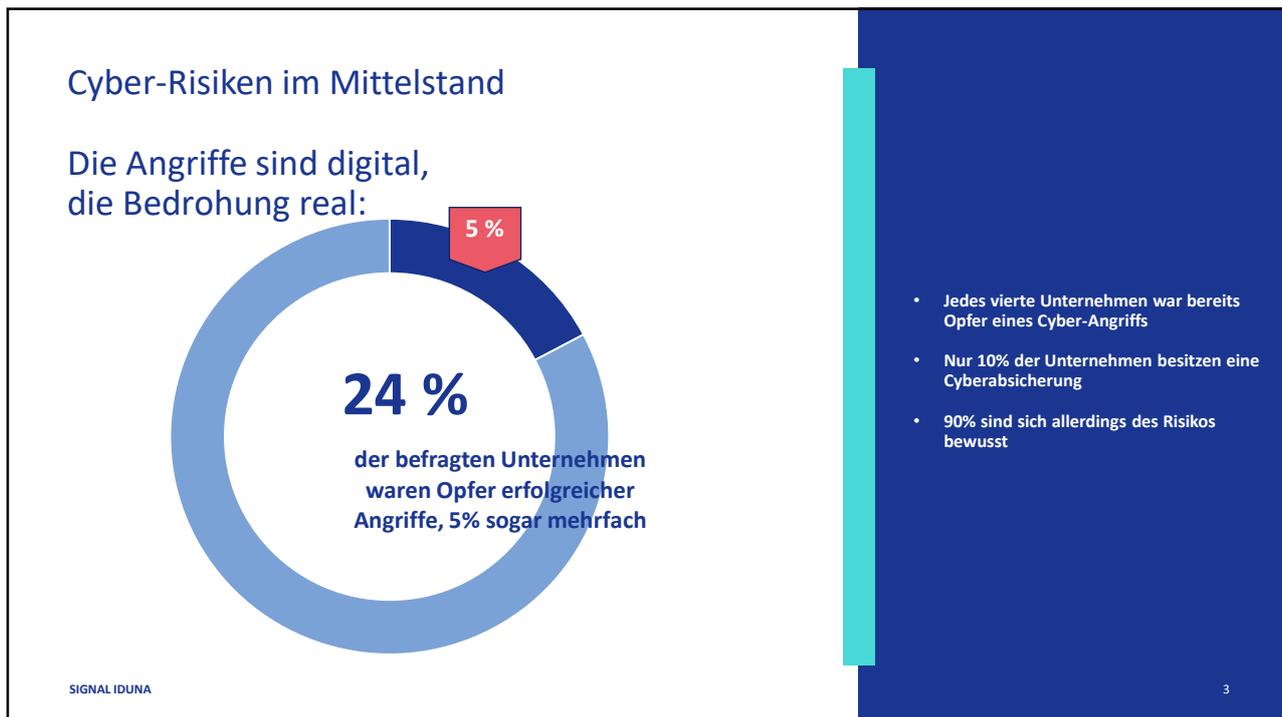
- Inhaltsversicherung
- Betriebsunterbrechungsversicherung
- Elektronikversicherung
- Maschinenversicherung (stationär und/oder fahrbar)
- Transportversicherung
- u.w.

**- Haftpflichtversicherung**  
insbesondere

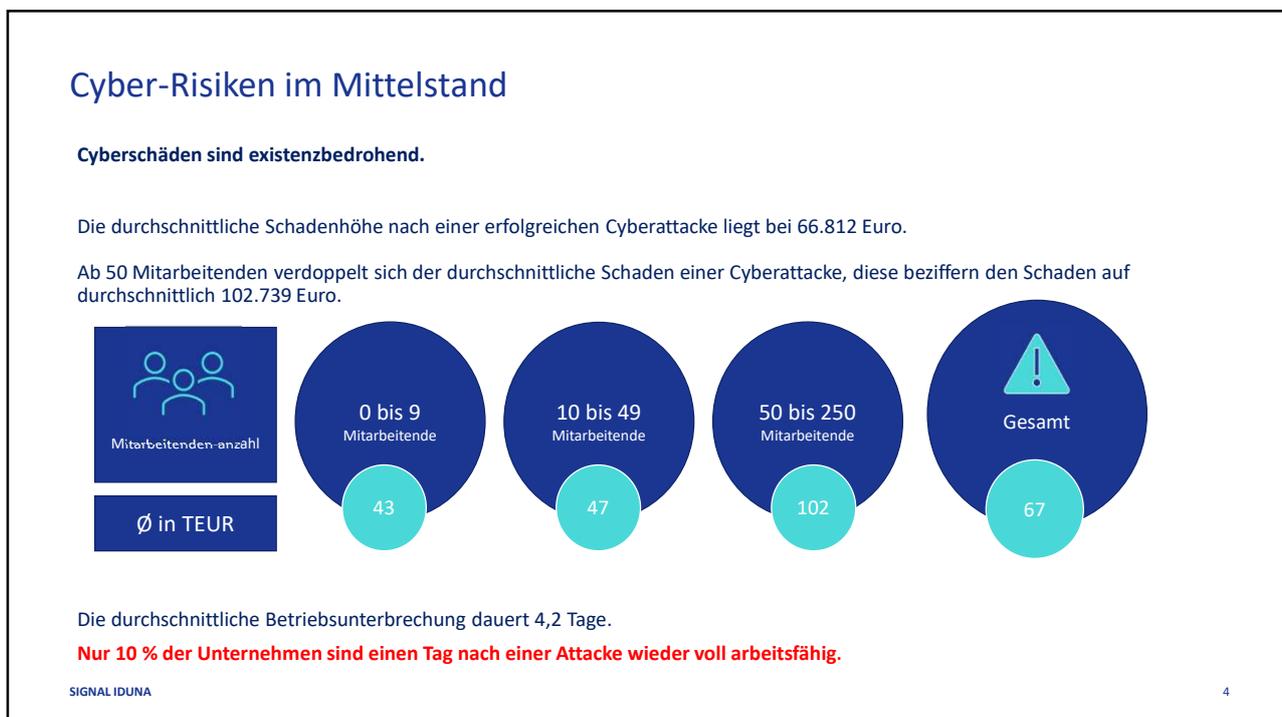
- Betriebs-Haftpflichtversicherung
- Berufs-/Vermögensschaden-Haftpflichtversicherung
- Umwelt-Haftpflichtversicherung
- Cyber-Versicherung
- u.w.

SIGNAL IDUNA

2



3



4

## Cyber-Risiken

### Bedrohungslandschaft

Die Bedrohungslandschaft für Cyber-Risiken ist vielfältig und ständig im Wandel. Es gibt verschiedene Arten von Bedrohungen, wie z.B. Malware, Phishing und Denial-of-Service-Angriffe. Eine detaillierte Analyse der Bedrohungslandschaft ist wichtig, um geeignete Sicherheitsmaßnahmen zu ergreifen.

### Arten von Cyberrisiken

Art der Bedrohung	Beschreibung
Malware	Schädliche Software, die entwickelt wurde, um Systeme zu infiltrieren und Schaden zu verursachen.
Phishing	Betrügerische Methode, bei der Cyberkriminelle versuchen, persönliche Informationen wie Passwörter und Kreditkarteninformationen zu stehlen.
Denial-of-Service-Angriffe	Angriffe, bei denen der Zugriff auf ein Netzwerk oder eine Website verhindert wird, indem die Ressourcen überlastet werden.
Social Engineering	Manipulative Taktiken, bei denen Angreifer versuchen, Menschen dazu zu bringen, vertrauliche Informationen preiszugeben oder unerwünschte Handlungen auszuführen.
Ransomware	Eine Art von Malware, die Daten verschlüsselt und Lösegeld fordert, um die Daten wiederherzustellen.
Fake President Fraud	Eine spezifische Art von Cyberangriffen, bei dem Betrüger sich als hochrangige Führungskräfte oder GF ausgeben, um Mitarbeiter dazu zu verleiten, Gelder oder vertrauliche Informationen preiszugeben.

SIGNAL IDUNA

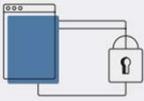
5

5

## Ransomware

ist weiterhin die größte Bedrohung.

**2** Ransomware-Angriffe auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



**68** erfolgreiche Ransomware-Angriffe auf Unternehmen wurden bekannt.

**15** davon richteten sich gegen IT-Dienstleister.



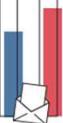
**2.000** Mehr als Schwachstellen in Software-Produkten (15 % davon kritisch) wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein Zuwachs von 24%.



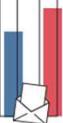
**Eine Viertelmillion** neue Schadprogramm-Varianten wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



**66%** aller Spam-Mails im Berichtszeitraum waren Cyberangriffe: 24% Erpressungsmails, 32% Betrugsmails



**84%** aller betrügerischen E-Mails waren Phishing-E-Mails zur Erhebung von Authentisierungsdaten, meist bei Banken und Sparkassen.



SIGNAL IDUNA

Die Bedrohung ist so groß wie nie zuvor

2.000 Schwachstellen pro Monat

250.000 Schadprogramme pro Tag

6

## Cyberangriff – Wie Hacker vorgehen



SIGNAL IDUNA

7

7

## Kommt Ihnen das bekannt vor?

„Bei uns ist noch nie etwas passiert!“

- Vielleicht hat bei früheren Sicherheitsvorfällen niemand etwas bemerkt.

„Wir haben keine geheimen Daten, bei uns ist nichts zu holen!“

- Auch mit oberflächlich betrachtet „ungefährdeten“ Daten kann erheblicher Missbrauch entstehen, wenn sie in die falschen Hände gelangen.

„Unser Netz ist sicher!“

- Die Fähigkeiten potentieller Angreifer werden oft unterschätzt.
- Jeder kann Fehler machen, auch erfahrene Netzwerk- und Sicherheitsspezialisten!

SIGNAL IDUNA

8

8



**Es ist nicht die Frage, für wie interessant ich mich halte.**

Jeder hat Daten, die sich mitzunehmen lohnen

- Kundendaten
- Adresslisten der Schule
- uvm.

Und wenn das System still steht, kann man nicht mehr arbeiten:

- Keine Bestellung beim Großhandel
- Keine Termini- und -vereinbarungen
- Keine Rechnungsschreibung

SIGNAL IDUNA

9

9

**Unser SI Cyberschutz,  
ein gutes Team  
für Ihre Sicherheit**

**SIGNAL IDUNA**

- Absicherung Ihres Cyber-Risikos**  
Eigenschäden  
Drittschäden  
Service / Kosten
- Notfallhilfe**  
Schadenshotline  
Soforthilfe  
Expertennetzwerk
- Prävention**  
Online-Trainings für Mitarbeitende  
Phishing-Simulationen

**perseus**  
technologies



10

10

## Absicherung Ihres Cyber-Risikos

### Eigenschaden

#### Daten-/Software-Schäden

- Daten/Programme werden beschädigt, gestohlen, verschlüsselt oder gehen verloren und müssen...
  - ...rekonstruiert oder wieder eingegeben werden
  - ...neu installiert und konfiguriert werden (z.B. von Beratern des Softwarehauses oder eigenen Mitarbeitern)
  - ...neu angeschafft werden

#### Mehrkosten und Ertragsausfall aufgrund Betriebsunterbrechung

- Das IT-System ist offline...
  - ...es kann nicht mehr auf Konstruktionsdaten aus CAD/CAM zugegriffen werden, die Produktion steht still
  - ...es können keine Auftragsengänge und Angebotsabgaben bearbeitet werden
- Aufgrund eines Datenlecks kommt es durch behördliche Anweisung zum Stillstand des Betriebes

11

## Absicherung Ihres Cyber-Risikos

### Folgekosten

#### Kosten für Forensik

- Kosten, die durch Ursachenermittlung und Behebung des Schadens entstehen
- Im Schadenfall stehen über eine Experten-Hotline IT-Spezialisten (Forensiker) zur Seite

#### Reputations- und Imagesicherung

- Negativschlagzeilen verursachen Kosten für Rufwiederherstellung (z.B. Anzeigenschaltung)
- Kundenverluste und -misstrauen nach Veröffentlichung vertraulicher Daten

#### Informationspflicht

- Kosten für die Information/Benachrichtigung geschädigter Kunden

12

## Absicherung Ihres Cyber-Risikos



Haftpflicht-Ansprüche

### Befriedigung berechtigter oder Abwehr unberechtigter Ansprüche Dritter

- Aufgrund eines Hackerangriffs werden Kreditkartendaten Ihrer Kunden gestohlen. Die Payment Card Industrie wie z.B. Master Card / Visa macht Schadenersatzforderungen und Vertragsstrafen geltend
- Vertrauliche Daten werden versehentlich im Internet veröffentlicht, es kommt zu einer Datenvertraulichkeitsverletzung
- Es werden Listen mit sensiblen Kundendaten über den normalen Müll entsorgt. Die Listen werden gefunden und die Daten gelangen so in die Öffentlichkeit. Es kommt zu behördlichen Ermittlungen im Zusammenhang mit Datenschutzverletzungen sowie zu Schadenersatzforderungen der betroffenen Personen
- Veröffentlichung von Fotos auf Ihrer Homepage, zu deren Nutzung Sie nicht berechtigt sind

13

## Die gehackte Datenbank

Ein Beispiel aus der Praxis:

Vor zwei Jahren hatte der Geschäftsführer in eine elektronische Kundenkartei und einen Server zur zentralen Datenspeicherung investiert. Die Server- und Datenbanksoftware war jedoch nicht auf dem neuesten Stand und hatte Sicherheitslücken. Hackern gelang es durch diese Sicherheitslücken in das System einzudringen und hunderte von Kundendatensätzen, Kreditkartendateien und Rechnungen abzugreifen, zu verändern und zu löschen.

**Als Folge davon mussten die IT-Systeme sowie die Kundendaten bereinigt und neu aufgesetzt werden.**

### Schadenaufwand:

Kosten für IT-Spezialisten (Ursachenermittlung):	10.000€
Kosten für IT-Spezialisten (System-/Datenwiederherstellung):	20.000 €
Kosten für Kundenkommunikation:	25.000 €
<hr/>	
Gesamt =	55.000 €
<hr/> <hr/>	

#### Schnell-Check SI Cyberschutz

- ✓ Service-/Kosten-Baustein und Eigenschaden-Baustein
- ✓ Kosten für IT-Spezialisten zur Schadenfeststellung
- ✓ Mehrkosten für die Kundenkommunikation
- ✓ Kosten für IT-Spezialisten zur System- und Datenwiederherstellung

14

## Der Bedienungsfehler

Ein Beispiel aus der Praxis:

Während das Geschäft brummt, kommt es zu einer hohen Arbeitsbelastung bei den Mitarbeitenden. Aufgrund eines falschen Klicks wird das Computerprogramm für die Warenbestellungen „zerschossen“.

Durch die nur noch manuell mögliche Bestellungsbearbeitung, können nicht alle Aufträge in der geplanten Zeit abgearbeitet werden. Überstunden werden angesetzt.

SIGNAL IDUNA

### Schadenaufwand:

Kosten für Soforthilfe:		3.000 €
Kosten für IT-Spezialisten:		4.000 €
Kosten für den Mehraufwand der Mitarbeiter:		5.000 €
<b>Gesamt</b>	<b>=</b>	<b>12.000 €</b>

#### Schnell-Check SI Cyberschutz

- ✓ Versicherungsschutz für Informationssicherheitsverletzungen u.a. durch Bedienfehler.
- ✓ Soforthilfe und Empfehlungen für Sofortmaßnahmen über die Notfallhotline
- ✓ Wiederherstellung der zerstörten Software durch einen IT-Spezialisten
- ✓ Mehrkosten für die Überstunden der Mitarbeiter.

15

15

## Produktionsstillstand

Falscher Klick zur falschen Zeit

Ein Beispiel aus der Praxis:

Ein Mitarbeitender klickt versehentlich ein Werbebanner im Internet an. Da die installierte Version des Browsers veraltet ist, hat eine hinter dem Banner befindliche Schadsoftware leichtes Spiel. Sie infiziert sämtliche Endgeräte im Unternehmen: Computer, Mobiltelefone und computergestützte Fertigungsmaschinen.

Die gesamte Produktion steht still, denn sämtliche Dateien und Kundendaten sind nicht mehr zugänglich!

Die vorhandenen Sicherheitskopien können erst nach mehr als 36 Stunden installiert werden, da das Schadprogramm zunächst professionell entfernt werden muss.

SIGNAL IDUNA

### Schadenaufwand:

Kosten für Datenwiederherstellung:		6.000 €
Kosten der Betriebsunterbrechung:		11.000 €
Kosten für IT-Forensiker		7.000 €
Ertragsausfall Auftrag Abnehmer:		2.000 €
<b>Gesamt</b>	<b>=</b>	<b>26.000 €</b>

#### Wie kann man dies verhindern?

- ✓ Browser auf Aktualität prüfen und ggf. aktualisieren!
- ✓ Sicherheitslücken identifizieren und schließen!
- ✓ Mitarbeiter zu Bedrohungen aus dem Internet schulen!

**Die Antwort:** Prävention durch Perseus-Schulungen und Security-Baseline-Check (SBC)!

16

16

## „Erpressung“

Festplatte vergessen

Ein Beispiel aus der Praxis:

Eine unter Zeitdruck stehende Mitarbeiterin lässt eine Festplatte am Server ihres Arbeitgebers stecken und fährt nach Hause, obwohl die Datensicherung noch nicht abgeschlossen ist.

Russische Hacker erlangen Zugriff auf den Server und verschlüsseln sowohl die Daten, als auch die Datensicherung.

Es wird ein Lösegeld in Höhe von 2 Bitcoins gefordert.

Der Lösegeldforderung wird nicht nachgegeben, da das Unternehmen so schnell keine liquiden Mittel aufreiben konnte.

**Folge: Vernichtung der Daten!**

SIGNAL IDUNA

### Schadenaufwand:

Datenwiederherstellung (Notmaßnahme)	22.000 €
Weitere Datenwiederherstellungskosten	18.000 €
Umsatzausfall des Online-Geschäfts	18.000 €
<b>Gesamt</b>	<b>58.000 €</b>

#### Wie kann man dies verhindern?

- ✓ Datensicherung gewissenhaft abschließen und Daten auf externen Datenträgern aufbewahren!
- ✓ Überprüfung und Festlegung der organisatorischen IT-Sicherheit!

**Die Antwort:** Der Perseus-Security-Baseline-Check hilft technische und organisatorische Mängel bei der IT-Sicherheit festzustellen

17

17

# PERSEUS – Führende menschliche Firewall.

**perseus.**  
technologies

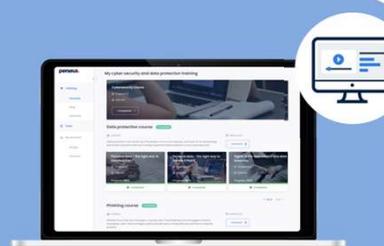
STÄRKSTER SCHUTZSCHILD: PERSEUS AKTIVIERT MITARBEITENDE GEGEN BEDROHUNGEN AUS DEM INTERNET

.....

**46% aller Cyber-Schäden**

**werden durch die eigenen Mitarbeitenden verursacht.**

Perseus bietet Ihnen ein Präventions-Management



18

18

## Die menschliche Firewall als stärkster Schutzschild gegen Cyberrisiken

**perseus.**  
technologies



Erklärung

- Online-Schulungen für Mitarbeitende
- Automatisierte Phishing-Simulation
- Tools & Dienstleistungen: Notfallplan & Richtlinien, Gefahrenwarnungen, Malware-Scan, Browser-Check



USPs

- Nachhaltiger Schutz durch ein umfassendes Sensibilisierungskonzept
- Nahtlose Integration in die Versicherungspolice
- Plug and Play – Einfache Handhabung und sofortige Einsatzfähigkeit



Vorteile

### Unternehmen

- Befähigung der Mitarbeitenden und Verhinderung von Cyberschäden

19

19



SIGNAL IDUNA

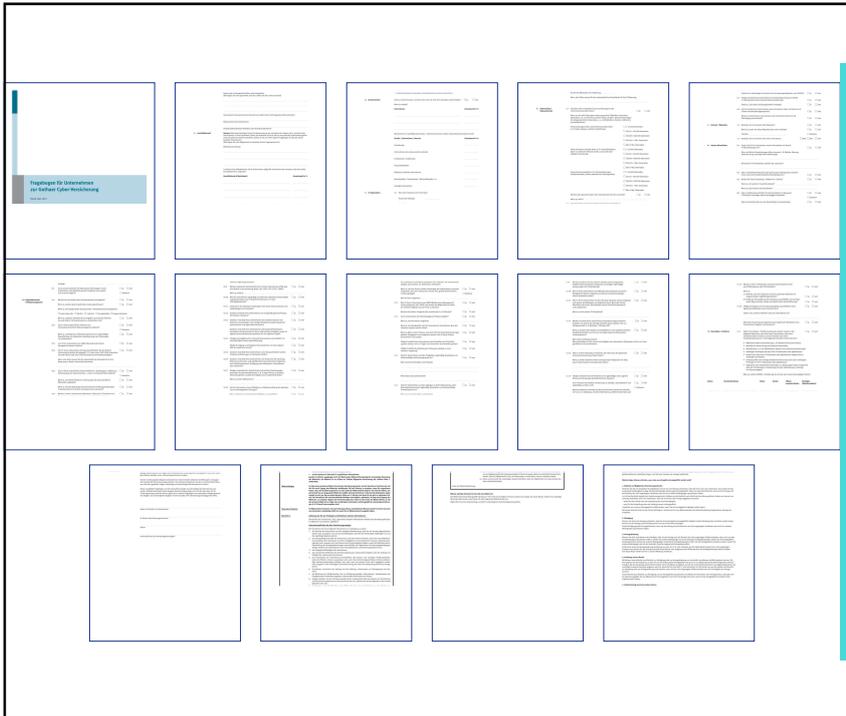
## Risikofragebögen

Welche Informationen benötigen Versicherer für die Kalkulation einer Cyber-Police?

**Das ist sehr unterschiedlich!**

20

20



So sieht ein „Cyber“ Fragebogen der Konkurrenz aus!

14 Seiten!!!  
12 Haupt- und ca. 60 Zusatzfragen sowie diverse weitere Angaben!

**Fragebogen zur Cyber-Risiko-Versicherung**

UVR

Adressat/Versicherungsnehmer (Name) \_\_\_\_\_

Adressat \_\_\_\_\_

Anschrift (Versicherungsgegenstand) \_\_\_\_\_

**Bitte lesen Sie vor Beantwortung der nachfolgenden Fragen die Belehrung im Antrag zu den Rechtsfolgen einer Verletzung der vorvertraglichen Anzeigepflicht.**

**Bezeichnet**

Umsatz \_\_\_\_\_ EUR Anzahl Mitarbeiter \_\_\_\_\_ Anzahl IT-Arbeitsplätze \_\_\_\_\_

Bausteine  Kostenbaustein  Eigenschadenbaustein  Betriebsunterbrechung  Drittschadenbaustein

Gesamtvorsicherungssumme(nicht zu bezahlen)  150.000 EUR  250.000 EUR  500.000 EUR  1.000.000 EUR

Selbstbeteiligung  500 EUR  1.000 EUR  2.500 EUR  5.000 EUR

Mitglied in  Innung  Einzelhandelsverband  DEHOGA  VSV

Person Cyber Security Club  Star Heald (bis 9 FT)  Good Heald (bis 19 FT)  Plain Heald (ab 20 FT)

Die Versicherungen zu den Fragen 1-3 müssen erfüllt oder versichert sein, da ansonsten kein Versicherungsschutz gewährt werden kann.

1) Bei „versichert“ besteht Versicherungsschutz erst, wenn die Umsetzung abgeschlossen ist (jedoch nicht vor dem beantragten Beginn)

1 Haben Sie für jeden Nutzer und Administrator eine benutzerindividuelle Benennung/Zugang mit Passwort vergeben, welches für den Zugang zu jedem System notwendig ist?  Ja  versichert \*  Nein

2 Schützen Sie sich vor dem Verlust der wichtigsten Unternehmensdaten durch eine mindestens wöchentliche Datensicherung (keine Spiegelung) und bewahren Sie die Datensicherung physisch getrennt auf?  Ja  versichert \*  Nein

3 Stellen Sie sicher, dass alle Systeme auf dem aktuellsten Stand sind und verfügen alle Informationssysteme über einen Schutz gegen Schadsoftware, der auf dem aktuellsten Stand gehalten wird (z. B. Virenscanner, Code Signing, Application Firewall oder ähnlich wirksame Maßnahmen) und installieren die zur Verfügung gestellten Sicherheitsupdates?  Ja  versichert \*  Nein

4 Betreiben Sie e-Commerce (z. B. WEB-Shop, Onlinehandel, Onlinebuchungsportal)?  Ja  Nein

Wenn Ja

4.1 Umsatzanteil bis  25 %  50 %  \_\_\_\_\_ %

4.2 Wird der Webshop selbstständig administriert und betrieben?  Ja  Nein

4.3 Werden alle eingehenden bargeldlosen Zahlungsvorgänge über einen Payment-Dienstleister abgerechnet?  Ja  Nein

5 Bearbeiten, speichern oder übermitteln Sie persönlich alle Ihrer rechtmäßig erhaltenen Geschäfts- und Computer-E-Mail-Korrespondenz?  Ja  Nein

Wenn Ja bis  25.000 \_\_\_\_\_ Datenätze pro Jahr

6 Erwirtschaften Sie Umsätze im außereuropäischen Ausland?  Ja  Nein

Wenn Ja auch in USA/Kanada?  Ja  Nein

7 Verarbeiten Sie sensible Daten im Sinne § 3 BDSG - „Berufgeheimnisse, Betriebsgeheimnisse, Daten“?  Ja  Nein

Wenn Ja bzw. ab Umsatz 5 Mio EUR:

7.1 Werden alle externen und externen Mitarbeiter regelmäßig über Maßnahmen zur Informationssicherheit geschult und sind verpflichtet, diese einzuhalten?  Ja  Nein

7.2 Werden Zugriffe für Ihre IT-Infrastruktur konsequent nur gewährt, wenn sie für deren Aufgabenerfüllung notwendig sind?  Ja  Nein

7.3 Werden administrative Zugriffe regelmäßig nach einem festgelegten Turnus auf deren Notwendigkeit überprüft?  Ja  Nein

7.4 Erfolgt der Zugriff auf Ihre interne IT-Infrastruktur über öffentliche oder drahtlose Netze ausschließlich verschlüsselt?  Ja  Nein

7.5 Gibt es einen Verantwortlichen für die Einhaltung datenschutzrechtlicher Vorgaben (Stichtag: \_\_\_\_\_)?  Ja  Nein

7.6 Wird die Installation von Sicherheits-Patches für Ihre IT zentral gesteuert?  Ja  Nein

7.7 Werden sensible Daten (z. B. personenbezogene Daten \* und Geschäftsgeheimnisse) bei Datenverlust verschlüsselt?  Ja  Nein

7.8 Gibt es einen Verantwortlichen für IT-Sicherheit?  Ja  Nein

\* Sensible Daten nach § 2 BDSG sind: rassenethnische Herkunft, politische Meinungen, religiöse/philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben

8 Ist die Nutzung privater Geräte in Ihrer Unternehmens-IT erlaubt?  Ja  Nein

Wenn Ja:

8.1 Befinden sich private Geräte in einem getrennten Netzwerk-Segment?  Ja  Nein

8.2 Haben private Geräte Zugriff auf geschäftliche Dienste oder Infrastruktur?  Ja  Nein

8.3 Ist die Administration von Servern über private Geräte möglich?  Ja  Nein

9 Übertragen Sie Informationsrechtliche Aufgaben an einen Dienstleister bzw. Provider?  Ja  Nein

Wenn Ja:

9.1 Der Dienstleister/Provider (Name) ist in folgenden Bereichen für uns tätig: \_\_\_\_\_

9.2 Existiert ein Dienstleistungsvertrag, in dem Verfügbarkeit, Updates und das Beheben von Sicherheitslücken geregelt sind?  Ja  Nein

9.3 Der Dienstleister (Name) ist in den folgenden Fällen von der Haftung freigestellt: \_\_\_\_\_

9.4 Unterliegt Ihr Dienstleister dem einheitlichen Datenschutzrecht der Europäischen Union?  Ja  Nein

10 Speichern und verarbeiten Sie Daten im Auftrag von Dritten (z. B. als Lohnbuchhalter/Steuerberater)?  Ja  Nein

Wenn Ja:

10.1 Verarbeiten Sie Daten, die besonderen gesetzlichen Verschwiegenheitspflichten unterliegen, wie zum Beispiel Gesundheitsdaten?  Ja  Nein

10.2 Verarbeiten oder speichern Sie Geschäftsgeheimnisse von Dritten?  Ja  Nein

10.3 Verarbeiten oder speichern Sie Finanz- oder Steuerdaten von Dritten?  Ja  Nein

11 Nutzen bzw. betreiben Sie automatisierte Produktions- bzw. Kontrollsysteme (IC-Systeme)?  Ja  Nein

Wenn Ja:

11.1 Befinden sich die IC-Systeme in einem separaten Netzwerk mit eingeschränkter Zugriffsmöglichkeit?  Ja  Nein

11.2 Wird für Systeme, die an IC-Systemen beteiligt sind (insbesondere Terminals), die Einhaltung besonderer Maßnahmsgebühren sichergestellt?  Ja  Nein

11.3 Sollen mobile Geräte an IC-Systeme beteiligt sind, sind diese vor unbefugtem Zugriff durch Verschlüsselung und Passwörter geschützt?  Ja  Nein

11.4 Sollen ein Fernzugriff auf die IC-Systeme möglich ist, erfolgt dieser ausschließlich auf verschlüsseltem Weg und nur mittels 2-faktoriger Authentifizierung?  Ja  Nein

12 Existiert ein schriftliches IT-Nutz- und -Wiederanlauf-Konzept welches auch die Verantwortlichen benennt?  Ja  Nein

13 Besteht eine Voreversicherung/Wenn Ja bei welcher Gesellschaft?  Ja  Nein

Würde eine bestehende Voreversicherung gekündigt/Wenn Ja von wem?  VN  VR  Ja  Nein

14 Schadenjournal (zu den letzten 5 Jahren)

Schadensjahr	Schadenhöhe	Schadensursache
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Die Fragen sind nach bestem Wissen richtig und vollständig beantwortet. Die Rechtsfolgen bei einer Verletzung der vorvertraglichen Anzeigepflicht, die im Antrag stehen, habe ich gelesen und zur Kenntnis genommen.

Datum \_\_\_\_\_ Unterschrift Antragsteller \_\_\_\_\_

So sah unser Fragebogen zur Cyber-Police vorher aus.

2 Seiten,  
14 Haupt- und  
25 Zusatzfragen

## Der SI-Cyberschutz:

### Risikofragebogen „Cyber“

mal ganz anders!

SIGNAL IDUNA

#### 2 Basis-Risikofragen:

1. Frage: **Betreiben Sie E-Commerce > 50 %, Ja = Anfrage (Kurzfragebogen), mit welchem Handelsumsatzanteil und welches Shop-System nutzen / betreiben Sie?**  
Antwort:

2. Frage: **Erwirtschaften Sie Umsätze im außereuropäischen Ausland?**  
Antwort: **Ja! = Beitragszuschlag**

#### 2 zusätzliche Risikofragen bei:

3. **produzierenden Betrieben (Hersteller); Umsatz > 20 Mio. €:**  
Frage: **Nutzen Sie automatisierte Produktions- bzw. Kontrollsysteme (IC-Systeme) ?**  
Antwort: **Ja! - Beitragszuschlag**

4. **nur bei ausgewählte Betriebsarten, sofern Kritis möglich:**  
Frage: **Handelt es sich beim Betrieb um eine KRITIS gemäß BSI-KritisV ?**  
Antwort: **Ja! = Anfrage mit Langfragebogen**

23

23

## Voraussetzungen für den Abschluss des SI-Cyberschutz



Die Betriebsstätten und informationsverarbeitenden Systeme, die Sie selbst betreiben, befinden sich innerhalb der Bundesrepublik Deutschland.



Für jeden Nutzer und Administrator existiert ein individueller Zugang mit Passwort. Dabei wird technisch sichergestellt, dass die Passwörter bestimmte Mindestanforderungen erfüllen (insbesondere Anzahl der Zeichen). Administrative Zugänge sind dabei ausschließlich Administratoren und ausschließlich zur Erledigung administrativer Tätigkeiten vorbehalten.



Die wichtigsten Unternehmensdaten werden durch eine mindestens wöchentliche Datensicherung (keine Spiegelung) vor Verlust geschützt und die Datensicherung physisch getrennt aufbewahrt.



Die informationsverarbeitenden Systeme sind auf dem aktuellen Stand, Sicherheits-Updates (Patch- Management) sind installiert. Ein Schutz gegen Schadsoftware (z. B. Virens Scanner, Code Signing), der auf dem aktuellen Stand gehalten wird, ist vorhanden. Geräte (Server) und/oder Dienste (z. B. Internetseiten, Internet-, Clouddienste), die über das Internet erreichbar sind, verfügen über zusätzliche Schutzmaßnahmen (z. B. Firewall, 2-Faktor-Authentifizierung bei Servern). Mobile Geräte und die darauf befindlichen Daten sind geschützt (z. B. durch Datenverschlüsselung, Diebstahlsicherung).

SIGNAL IDUNA

24

24

# Security Baseline Check.



SEITE 25

## Schritt 1 – Digitale Fragebogen

- Allgemeine Informationen
- Abfrage von relevanten Daten zu organisatorischen und technischen IT-Sicherheitsmaßnahmen

## Schritt 2 – Live Check mit Experten

- Organisation und Sensibilisierung
- Identitäts- und Berechtigungsmanagement
- Datensicherheit
- IT-Systeme und Netzwerke
- Patch- und Änderungsmanagement
- Schutz vor Malware

## Schritt 3 – Abschlussreport

- Individueller Bericht in Ampelform
- Potenzial für Verbesserungen
- Konkrete Handlungsempfehlungen

optional buchbar



25

25

# Security Baseline Check (SBC).



Der SBC prüft auch, ob Ihr Unternehmen die Voraussetzungen zum SI-Cyberschutz erfüllt

Der ...  
Ris ...  
men  
und daisen!

26

26

Im Marktvergleich mit 14 Mitbewerbern bietet die SIGNAL IDUNA das beste Preis-/ Leistungsverhältnis!

HISCOX

RHV

VHV  
VERSICHERUNGEN

ERGO

AIG

baloise

MARKEL

Allianz

württembergische

Gothaer

HDI



COGITANDA®  
CYBER SIND WIR.

PROVINZIAL

AXA

SIGNAL IDUNA

27

27

Warum der  
SI-Cyberschutz?

wählbare  
Versicherungs-summen

- 150.000 Euro
- 250.000 Euro
- 500.000 Euro
- 1.000.000 Euro
- 2.000.000 Euro
- 3.000.000 Euro

wählbare  
Selbstbeteiligungen

- 500 Euro (Standard)  
+ 12 Std. SB bei Betriebsunterbrechung  
alternativ wählbar
- 250 Euro
- 1.000 Euro
- 2.500 Euro
- 5.000 Euro
- 10.000 Euro <- Beitragsvorteil 43 %

SIGNAL IDUNA

28

28

Bei Vereinbarung einer Selbstbeteiligung von 10.000 Euro reduziert sich der Beitrag im Vergleich zur „Standard“ SB 500 Euro um

## -43 % (Beitragsvorteil)

Und wenn:

- 1) mind. 80 % Ihrer Mitarbeiter an den Präventionsschulungen von Perseus teilgenommen haben, reduziert sich die vereinbarte Selbstbeteiligung um 50 %
- 2) Sie mindestens 1 mal jährlich den optionalen Security Baseline Check (SBC) bei Perseus buchen und festgestellte Mängel beseitigen, reduziert sich für 1 Jahr die vereinbarte Selbstbeteiligung um 50 %

**Kosten zurzeit 499,00 Euro netto** für „SIGNAL IDUNA-Kunden“

**Beispiel: 10.000 Euro SB**

1) minus 50 % => - 5.000 Euro SB  
5.000 Euro SB im Schadenfall

2) minus 50 % => - 5.000 Euro SB  
**0 Euro SB im Schadenfall**  
und bis zu 43 % Beitrag gespart

### Warum der SI-Cyberschutz?

Darum lohnt für Sie eine hohe Selbstbeteiligung von 10.000 Euro

Durch aktives Handeln haben die tatsächliche Höhe Ihrer Selbstbeteiligung selbst in der Hand

29

## Fragen, Anregungen und Wünsche

SIGNAL IDUNA

30

30

SIGNAL IDUNA 

Vielen Dank für Ihre Aufmerksamkeit!