SIGNAL IDUNA

Fachverband Metall Nordrhein-Westfalen

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-/Vermögenschaden-Haftpflichtversicherung
  - Umwelt-Haftpflichtversicherung
  - Cyber-Versicherung
  - u.w.

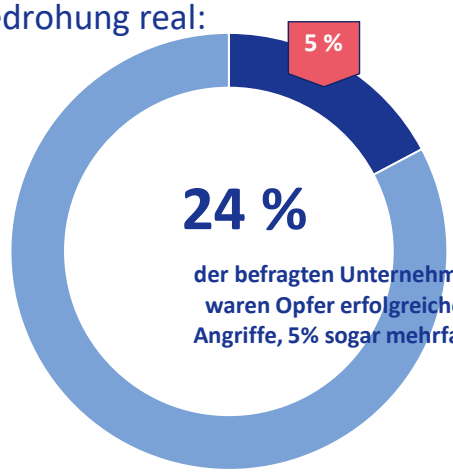
SIGNAL IDUNA

2

2

Cyber-Risiken im Mittelstand

Die Angriffe sind digital, die Bedrohung real:



- Jedes vierte Unternehmen war bereits Opfer eines Cyber-Angriffs
- Nur 10% der Unternehmen besitzen eine Cyberabsicherung
- 90% sind sich allerdings des Risikos bewusst

SIGNAL IDUNA 3

3

Cyber-Risiken im Mittelstand

Cyberschäden sind existenzbedrohend.

Die durchschnittliche Schadenhöhe nach einer erfolgreichen Cyberattacke liegt bei 66.812 Euro.

Ab 50 Mitarbeitenden verdoppelt sich der durchschnittliche Schaden einer Cyberattacke, diese beziffern den Schaden auf durchschnittlich 102.739 Euro.

Die durchschnittliche Betriebsunterbrechung dauert 4,2 Tage.

Nur 10 % der Unternehmen sind einen Tag nach einer Attacke wieder voll arbeitsfähig.

SIGNAL IDUNA 4

4

Cyber-Risiken

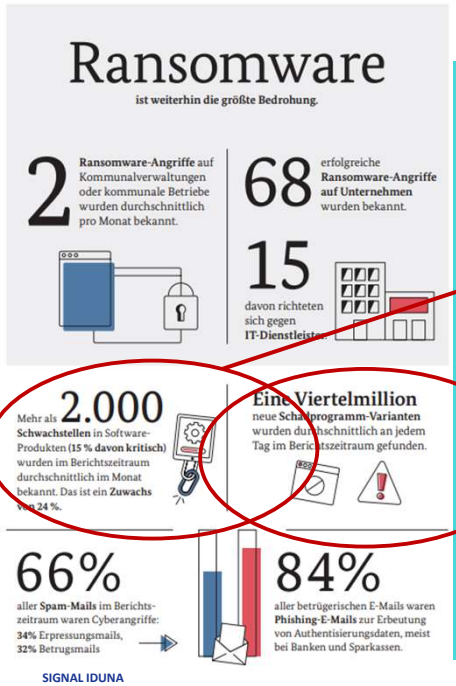
Bedrohungslandschaft

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.

5



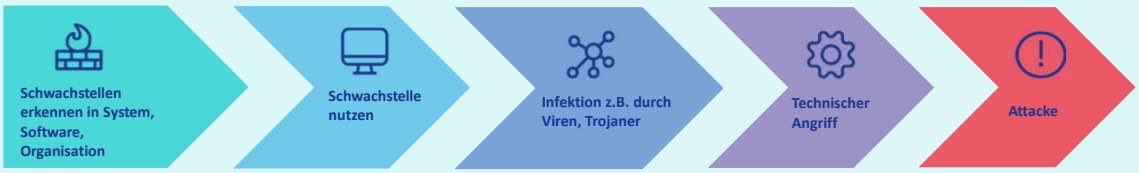
Die Bedrohung ist so groß wie nie zuvor

2.000 Schwachstellen pro Monat

250.000 Schadprogramme pro Tag

6

Cyberangriff – Wie Hacker vorgehen



7

Kommt Ihnen das bekannt vor?

„Bei uns ist noch nie etwas passiert!“

- Vielleicht hat bei früheren Sicherheitsvorfällen niemand etwas bemerkt.

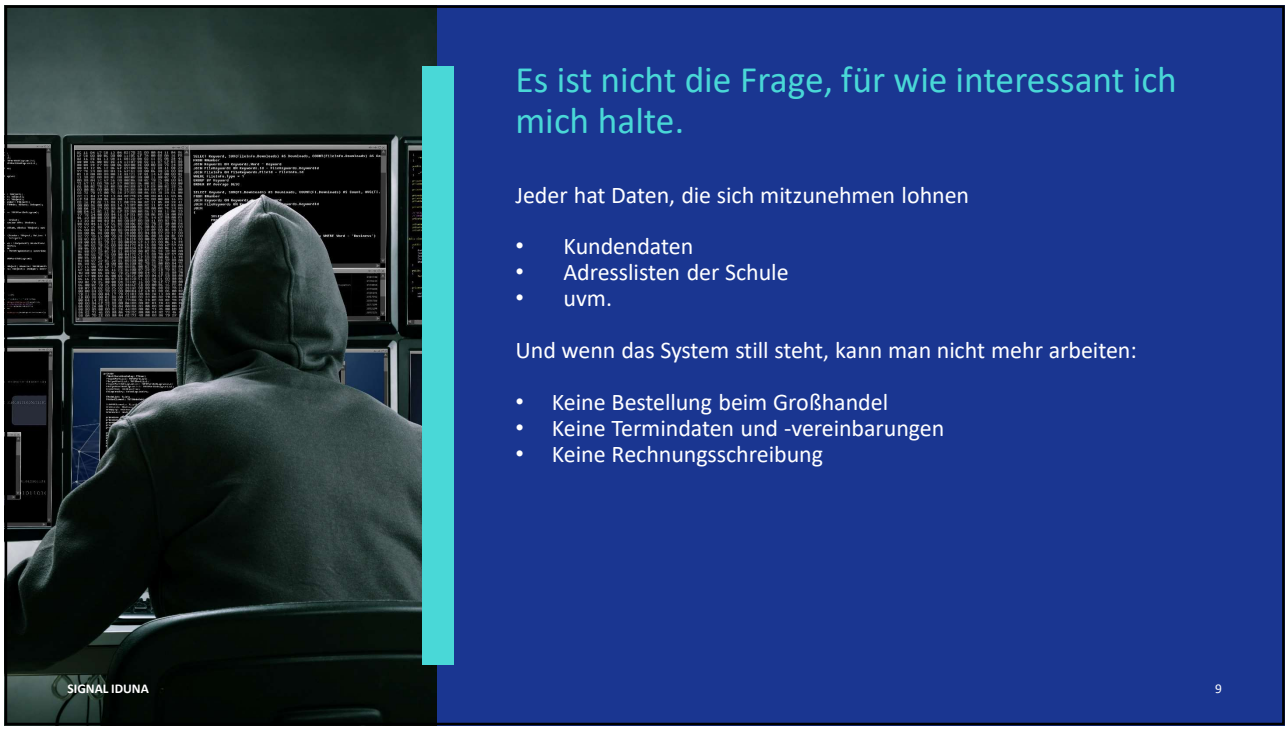
„Wir haben keine geheimen Daten, bei uns ist nichts zu holen!“

- 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!

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 Termindaten 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

SIGNAL IDUNA

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 Auftragseingänge und Angebotsabgaben bearbeitet werden
- Aufgrund eines Datenlecks kommt es durch behördliche Anweisung zum Stillstand des Betriebes

11

Absicherung Ihres Cyber-Risikos

SIGNAL IDUNA

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

SIGNAL IDUNA

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

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 €**
Gesamt =	**55.000 €**

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

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.

Schadenaufwand:

Kosten für Soforthilfe:		**3.000 €**
Kosten für IT-Spezialisten:		**4.000 €**
Kosten für den Mehraufwand der Mitarbeiter:		**5.000 €**
Gesamt	=	**12.000 €**

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.

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.

Schadenaufwand:

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

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)!

„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 nachgekommen, da das Unternehmen so schnell keine liquiden Mittel auftreiben konnte.

Folge: Vernichtung der Daten!

Schadenaufwand:

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

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

SIGNAL IDUNA

17

17

PERSEUS – Führende menschliche Firewall.

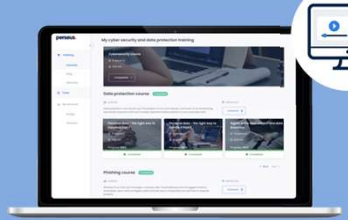
perseus. technologies

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

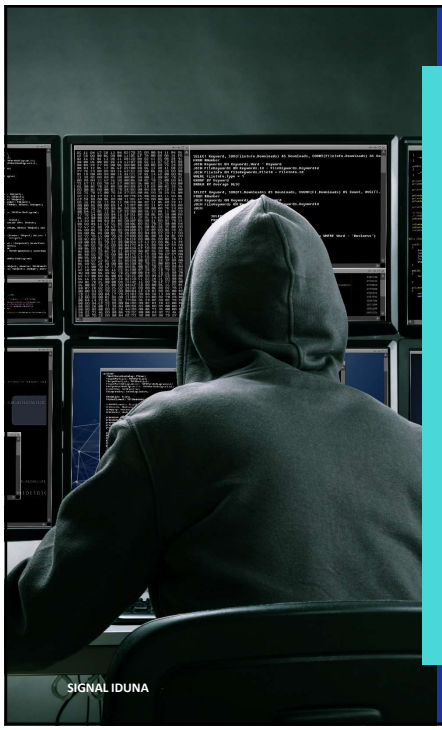
Vorteile

Unternehmen

- Befähigung der Mitarbeitenden und Verhinderung von Cyberschäden

19

19



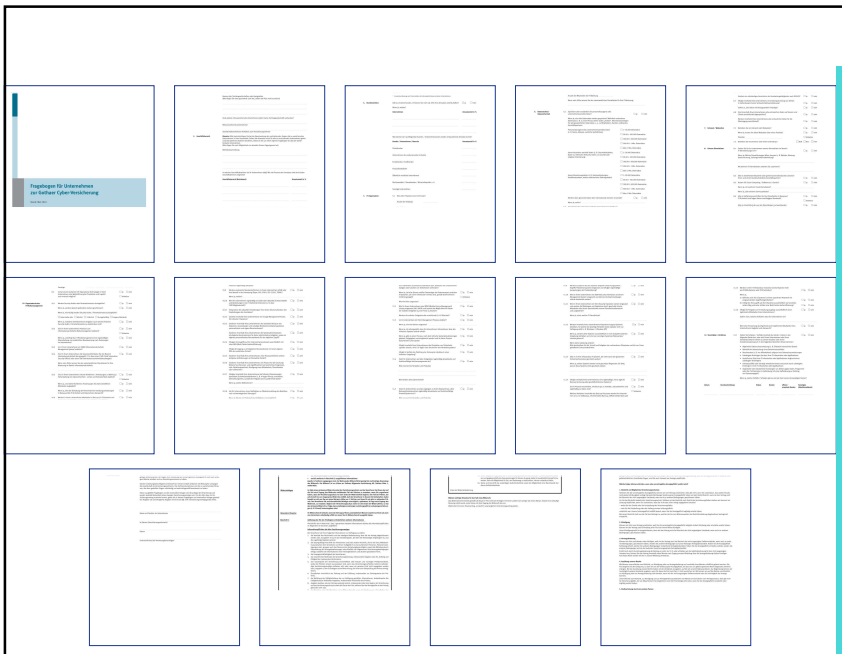
Risikofragebögen

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

Das ist sehr unterschiedlich!

20

20

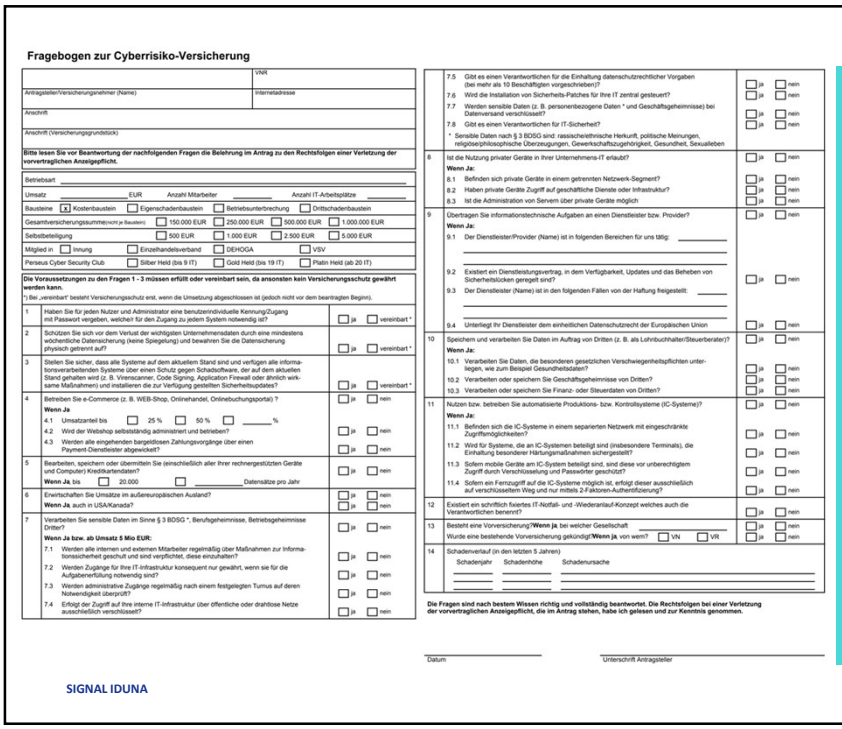


So sieht ein „Cyber“ Fragebogen der Konkurrenz aus!

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

21

21



Fragebogen zur Cyberrisiko-Versicherung

SIGNAL IDUNA

So sah unser Fragebogen zur Cyber-Police vorher aus.

2 Seiten,
14 Haupt- und 25 Zusatzfragen

22

22

Der SI-Cyberschutz:

Risikofragebogen „Cyber“

mal ganz anders!

2 Basis-Risikofragen:

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

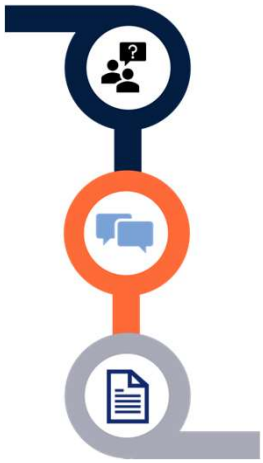
2 zusätzliche Risikofragen bei:

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

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. Virenscanner, 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).

Security Baseline Check.



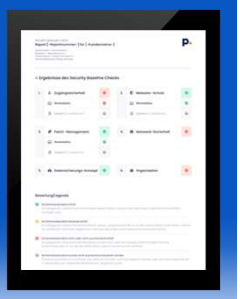
Schritt 1 – Digitale Fragebogen

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

optional buchbar

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

SEITE 25

25

25

Security Baseline Check (SBC).

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

26

26

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

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

SIGNAL IDUNA

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

29

Fragen, Anregungen und Wünsche

SIGNAL IDUNA

30

30

SIGNAL IDUNA

Vielen Dank für Ihre Aufmerksamkeit!

31