HISCOX

Gefährdet.Gefordert.Geschützt?
Was KMU jetzt über Cyberprävention wissen müssen.

Ihre Experten

Claudia von Pawel

Head of Proposition Management, Hiscox

Robin Schröter

Sales Underwriter Commercial Lines, Hiscox

Agenda

1. Cyber-Bedrohungen für KMUs weiter hoch
2. Warum klassische Versicherungen zu kurz springen
3. Wie Hiscox Ihre Kunden vor, während und nach einem Angriff schützt
4. Präventionstools und Krisenhilfe im Detail
5. Hiscox - Ihr Partner für starken Cyber-Schutz

1. Erkenntnisse des Cyber Readiness Report 2025

Risikolage weiter hoch – Lösungen gefragt

67% der deutschen KMUs haben in den letzten 12 Monaten einen Cyber-Angriff festgestellt

60% der Unternehmen sind gar nicht oder nicht angemessen gegen Cyber-Risiken versichert

34% der befragten Unternehmen planen, Investitionen in Cyber-Sicherheit in den nächsten zwölf Monaten signifikant zu erhöhen

1. Cyber-Versicherung:
Warum ist sie so wichtig?

HISCOX

Cyberangriff sind keine Einzelfälle mehr

Unternehmen jeder Branche/ Größe betroffen – vom kleinen Handwerker bis zum DAX-Konzern

Auslöser sind oft einfache Fehler:

- Klick auf Phishing-Mails
- Nicht gepatchtes System
- Offene Zugriffsmöglichkeit (z.B. Remoteverbindung nie deaktiviert oder Cloud-Ordner falsch freigegeben)

Gravierende Folgen wie:

- Betriebsunterbrechung
- Datenverlust
- Kosten für IT
- Rechtliche Risiken

→ Hohe Kosten

2. Klassische Versicherungen greifen zu kurz
Umfassende Lösungen sind gefragt!

	Vor dem Angriff	Während des Angriffs	Nach dem Angriff
Was eine klassische Versicherung leistet	✕	✕	Regulierung von Haftungsansprüchen und Betriebsunterbrechungen
Was wirklich wichtig ist	– Technische Lösungen wie z. B. Virenschutz – Schwachstellenanalysen – Cyber-Trainings	– Soforthilfe insbesondere IT-Forensik – Krisenplan – Expertenhilfe	– Regulierung von Haftungsansprüchen, Betriebsunterbrechungen – Übernahme cyberspezifische Eigenschäden wie z.B. Krisenmanagement, Wiederherstellungskosten, Sicherheitsanalysen & -verbesserungen – Unkomplizierte Abwicklung der Betriebsunterbrechung, vor allem bei Massenschäden

3. CyberClear by Hiscox
Zielgerichtete Prävention & starke Krisenhilfe

	Vor dem Angriff		Während des Angriffs		Nach dem Angriff	
Das leistet CyberClear by Hiscox	Cyber-Training & Phishings-Test	Risikominimierung	Krisenplan	Roter Faden im Ernstfall	Haftpflicht	Abwehr & Erfüllung, inkl. Medienhaftpflicht …
	Cyber-Sicherheits-Scan	Schwachstellenanalyse	Soforthilfe 24/7	Führende IT Forensiker als Partner	Eigenschäden	**Nur bei Hiscox:** Forderungsausfall-deckung bei manipu-lierten Zahlungsdaten …
	Norton-Schutzpaket[1]	Umfassender Schutz für Geräte und Daten	Experten-netzwerk	Fachanwälte & PR-Krisenberater	Betriebsunter-brechung	**Nur bei Hiscox:** Tagessatzentschädigung für schnelle Leistung ohne komplizierten Nachweis des Ertragsausfalls …

1) Optional abschließbar mit CyberClear Plus

4. Cyber-Training und Phishing Simulationen
Mitarbeiter und Cyber-Resilienz stärken

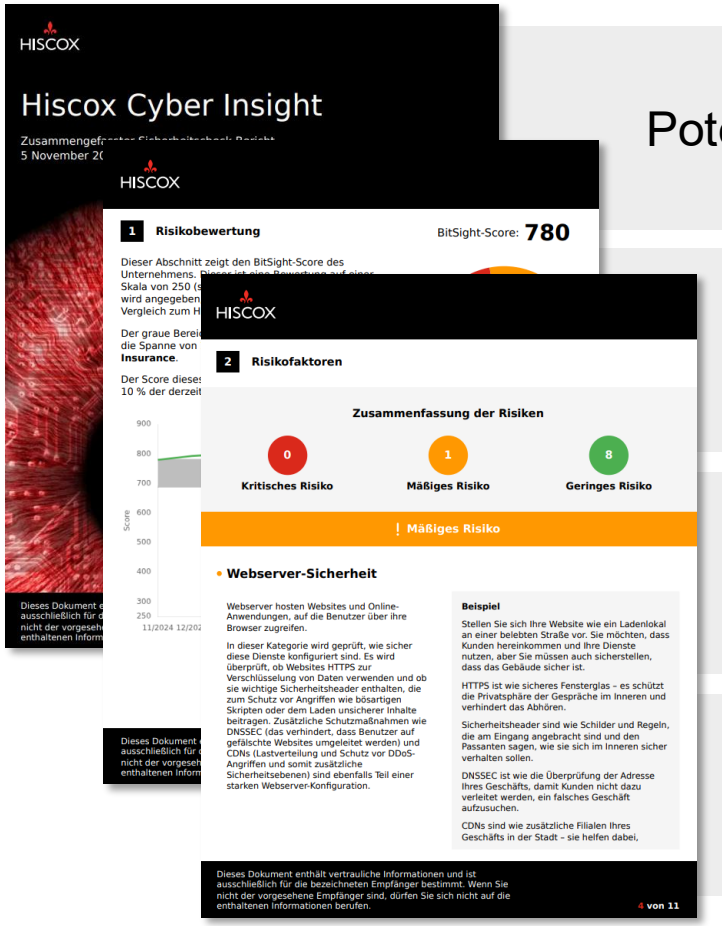
Cyber-Training

- Sensibilisierung zu aktuellen Cyber-Risiken für Geschäftsführer und Mitarbeiter
- Online-Training zu Themen wie Phishing, Social Engineering & KI
- Bis zu 100 Lizenzen ohne zusätzliche Kosten enthalten
- Ihr Vorteil! Bei einer Teilnahmequote von 80% reduziert sich der Selbstbehalt im Schadenfall um 25%

Phishing-Simulationen

- Praxistest für Mitarbeiter
- Mehr als 300 Vorlagen ermöglichen die Erstellung von Phishing-Kampagnen innerhalb weniger Minuten
- Individualisierungen und Erstellung eigener Phishing-Templates ebenfalls möglich

4. Cyber-Sicherheits-Scan
Schwachstellen erkennen und gezielt schließen



Potenzielle Sicherheitslücken schließen, bevor Angreifer sie ausnutzen

Individueller Report – Sie müssen nur die Domain angeben

Der Cyber-Sicherheits-Scan steht auch Interessenten und Maklern zur Verfügung

Besuchen Sie unsere Cyber-Produktseite und probieren Sie es aus!

4. Norton Small Business Premium
Maximale Sicherheit für Geräte und Daten

Umfangreiche Schutzfunktionen

- Gerätesicherheit
- Cloud-BackUp
- Dark Web Monitoring
- Secure VPN

Tools zur Produktivitäts-steigerung

- PC Optimierung
- Treiber Updater
- Software Updater

Rund-um-die-Uhr-Unternehmenssupport

24/7

Das Norton-Schutzpaket können Sie optional im Paket CyberClear Plus abschließen

4. Norton Small Business Premium
Professioneller Schutz, aber einfach!

Das macht Norton zur perfekten Lösung für KMUs:

1

- *Professionelle Software*
- *Mehrere Schutzebenen*
- *Präventiver Schutz vor unterschiedlichen Risiken*

2

- *Einfache Installation*
- *Kinderleichter Betrieb*
- *Kein IT-Personal notwendig*

3

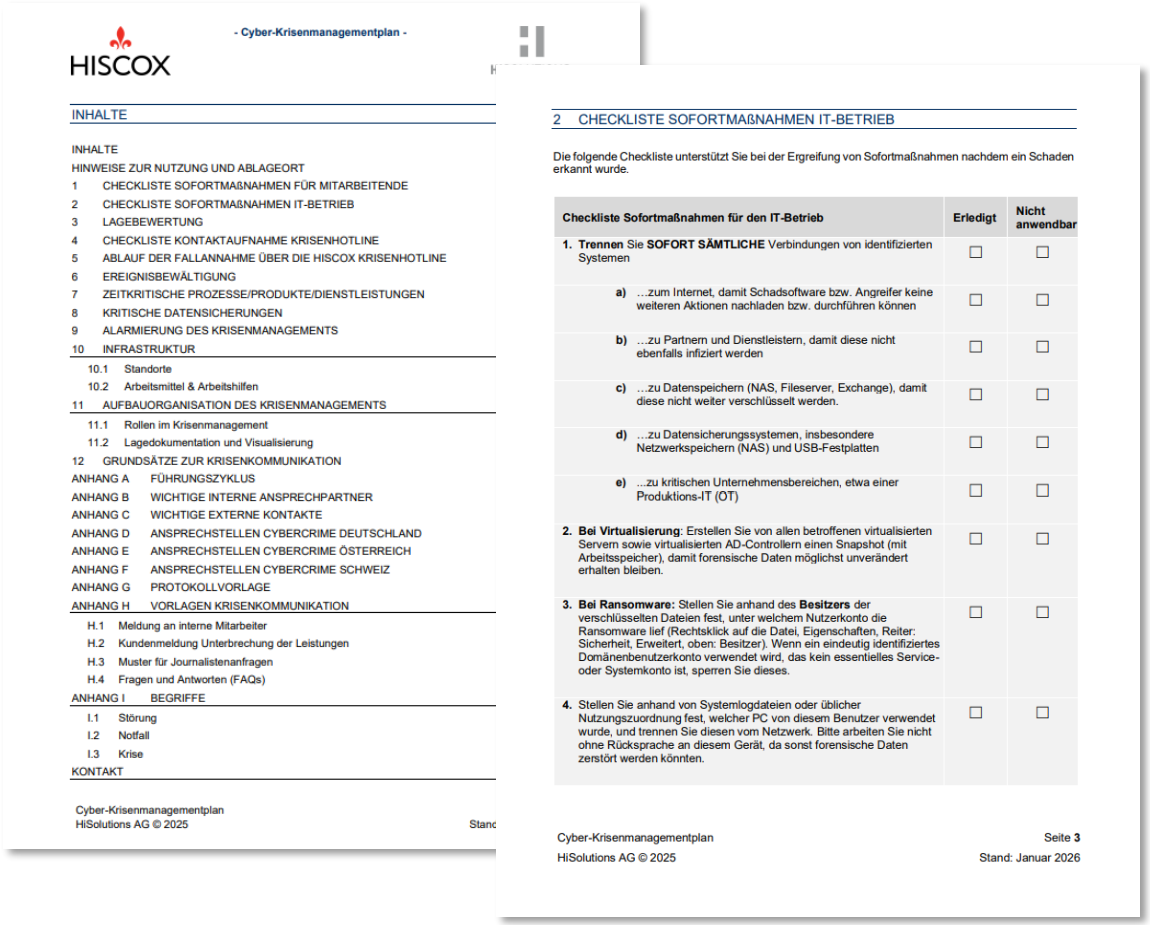
- *24/7 Ansprechpartner bei Problemen*
- *Kostenersparniss (Lizenzen, neue Hardware, IT Beratung)*

4. Cyber-Krisenmanagementplan
Der rote Faden für Ihre Kunden, wenn es ernst wird

Strukturierter Krisenplan inkl. Checklisten, Vorlagen und Handlungsempfehlungen:

- Sofortmaßnahmen für Mitarbeitende
- Sofortmaßnahmen IT Betrieb
- Vorlagen zur Krisenkommunikation
- Muster für Journalistenanfragen
- ...und vieles mehr

Für schnelle, sichere Entscheidungen in den entscheidenden ersten Stunden



- Cyber-Krisenmanagementplan -

HISCOX

INHALTE

Cyber-Krisenmanagementplan
HiSolutions AG © 2025

2 CHECKLISTE SOFORTMAßNAHMEN IT-BETRIEB

Die folgende Checkliste unterstützt Sie bei der Ergreifung von Sofortmaßnahmen nachdem ein Schaden erkannt wurde.

Checkliste Sofortmaßnahmen für den IT-Betrieb	Erledigt	Nicht anwendbar
1. **Trennen** Sie **SOFORT SÄMTLICHE** Verbindungen von identifizierten Systemen	☐	☐
a) ...zum Internet, damit Schadsoftware bzw. Angreifer keine weiteren Aktionen nachladen bzw. durchführen können	☐	☐
b) ...zu Partnern und Dienstleistern, damit diese nicht ebenfalls infiziert werden	☐	☐
c) ...zu Datenspeichern (NAS, Fileserver, Exchange), damit diese nicht weiter verschlüsselt werden.	☐	☐
d) ...zu Datensicherungssystemen, insbesondere Netzwerkspeichern (NAS) und USB-Festplatten	☐	☐
e) ...zu kritischen Unternehmensbereichen, etwa einer Produktions-IT (OT)	☐	☐
2. **Bei Virtualisierung**: Erstellen Sie von allen betroffenen virtualisierten Servern sowie virtualisierten AD-Controllern einen Snapshot (mit Arbeitsspeicher), damit forensische Daten möglichst unverändert erhalten bleiben.	☐	☐
3. **Bei Ransomware:** Stellen Sie anhand des **Besitzers** der verschlüsselten Dateien fest, unter welchem Nutzerkonto die Ransomware lief (Rechtsklick auf die Datei, Eigenschaften, Reiter: Sicherheit, Erweitert, oben: Besitzer). Wenn ein eindeutig identifiziertes Domänenbenutzerkonto verwendet wird, das kein essentielles Service- oder Systemkonto ist, sperren Sie dieses.	☐	☐
4. Stellen Sie anhand von Systemlogdateien oder üblicher Nutzungszuordnung fest, welcher PC von diesem Benutzer verwendet wurde, und trennen Sie diesen vom Netzwerk. Bitte arbeiten Sie nicht ohne Rücksprache an diesem Gerät, da sonst forensische Daten zerstört werden könnten.	☐	☐

Cyber-Krisenmanagementplan Seite 3
HiSolutions AG © 2025 Stand: Januar 2026

4. Cyber-Soforthilfe
Ausgezeichnete Experten bereits im Verdachtsfall zur Stelle

HISCOX

Soforthilfe im Notfall
Direkter Zugang zu **führenden IT-Forensikern**

Wann
Leistung schon bei Verdacht, dass ein Cyber- oder Datenschutzvorfall vorliegen könnte!

Wie
24/7 Zugriff auf **Krisenhotline** mit unmittelbarer **Unterstützung durch IT-Experten und weitere Krisen-Experten**.

Was
Unmittelbare Unterstützung u.a bei **Situationsanalyse, Sofortmaßnahmen, Sicherung von Spuren, DSGVO-Meldungen**

Ziel

- Keine Zeit verlieren
- Keine unnötigen Fehler
- Schaden sofort begrenzen

HISCOX

Ihr Partner für starken Cyber-Schutz!

5. Erkenntnisse des Cyber Readiness Report 2025
KMUs investieren massiv – Vertriebschance

75% der deutschen KMUs planen neue Mitarbeiterschulungen

Cyber-Training und Phishing-Simulationen

62% der Unternehmen wollen spezialisiertes Personal einstellen

34% der befragten Unternehmen haben vor, in moderne Sicherheitssoftware zu investieren

Norton Schutzpaket

5. Warum sollten sich Kunden und Makler für Hiscox entscheiden?

Branchenpionier
15 Jahre Cyber-Expertise – wir wissen, was wir tun!

Expertennetzwerk
Zugriff auf Top-Spezialisten wie HiSolutions und msg im Ernstfall.

Awareness & Training UPDATE
Mitarbeiterschulungen und Phishing-Simulationen zur Stärkung der Cyber-Resilienz.

Cyber-Sicherheits-Scan NEU
Schwachstellen entdecken – bevor Angreifer sie ausnutzen.

Technisches Schutzpaket (optional) NEU
Cyber-Sicherheitssoftware mit Virenschutz, Cloud-Back-up und mehr powerd by Norton

Forderungsausfalldeckung (nur bei Hiscox!) NEU
Schutz bei manipulierten Zahlungsdaten.

Tagessatzentschädigung (nur bei Hiscox!)
Kein komplizierter Nachweis des Ertragsausfalls nötig, schnelle Leistung auch im Kumulfall

Attraktive Prämien UPDATE
Wettbewerbsfähige Prämien, speziell für kleine und mittlere Unternehmen

Auszeichnungen & Awards
Schwachstellen entdecken – bevor Angreifer sie ausnutzen

HISCOX

Vielen Dank für Ihre Aufmerksamkeit