



Cyber-Risiken 2026: Ganzheitlicher Schutz dank Präventionstools und Krisenhilfe

Wir schützen,
was Sie schätzen.

Ihre Experten

Claudia von Pawel



*Head of Proposition Management,
Hiscox*

Unser Gast:

Matthias Arnegger



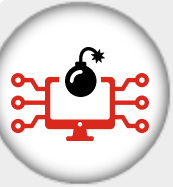
*Business Development Executive,
Gen*

Agenda

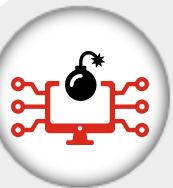
- 
- A background graphic on the right side of the slide showing a blue and white globe with binary code (0s and 1s) and orange curved lines, suggesting a digital or cyber theme.
1. Cyber: Risikolage weiter hoch
 2. Warum klassische Versicherungen zu kurz springen
 3. Wie Hiscox Ihre Kunden vor, während und nach einem Angriff schützt
 4. Wie zielgerichtete Prävention & starke Krisenhilfe im Bedrohungsfall hilft
Highlight: Norton Small Business Premium
 5. Hiscox - Ihr Partner für starken Cyber-Schutz

1. Erkenntnisse des Cyber Readiness Report 2025

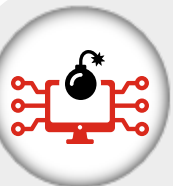
Risikolage weiter hoch – Lösungen gefragt



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?



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

Das leistet CyberClear by Hiscox

Vor dem Angriff

Cyber-Training
& Phishings-
Test



Risikominimierung

Cyber-
Sicherheits-
Scan



Schwachstellenanalyse

Norton-
Schutzpaket¹



Umfassender Schutz für
Geräte und Daten

Während des Angriffs

Krisenplan



Roter Faden im Ernstfall

Soforthilfe
24/7



Führende IT Forensiker
als Partner

Experten-
netzwerk



Fachanwälte & PR-
Krisenberater

Nach dem Angriff

Haftplicht



Abwehr & Erfüllung, inkl.
Medienhaftpflicht
...

Eigenschäden



Nur bei Hiscox:
Forderungsausfall-
deckung bei manipu-
lierten Zahlungsdaten
...

Betriebsunter-
brechung



Nur bei Hiscox:
Tagessatzentschädigung
für schnelle Leistung ohne
komplizierten Nachweis
des Ertragsausfalls
...

4. Bedrohungsszenario A

Phishing

Ein Mitarbeiter erhält eine E-Mail mit dem Link zu einer Sharepointseite mit dem Titel „Budgetplanung“, zu der seine Chefin ihn vermeintlich eingeladen hat.

Beim Klick auf den Link landet er jedoch auf einer gefälschten Microsoft-Loginseite und gibt dort seine Zugangsdaten ein.

Die Angreifer übernehmen daraufhin sein Konto und versenden weitere Phishing-Nachrichten an Kollegen und externe Partner.



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%

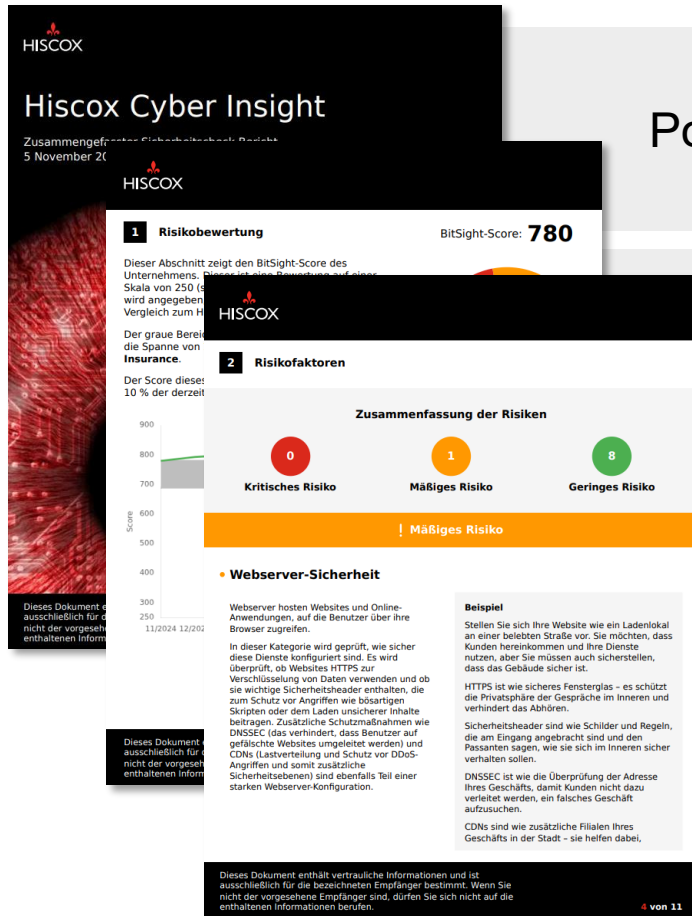
Phishing-Simulationen



- 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. Bedrohungsszenario B

Versäumtes Patchmanagement

Ein mittelständisches Unternehmen versäumt es, einen bereits veröffentlichten Sicherheits-Patch für eine Software zu installieren.

Cyber-Kriminelle nutzen genau diese bekannte Schwachstelle aus, dringen unbemerkt ins Netzwerk ein und installieren Schadsoftware.

In der Folge werden Server verschlüsselt und zentrale Systeme müssen komplett heruntergefahren werden.



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



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*
- *Kostenersparnis (Lizenzen, neue Hardware, IT Beratung)*

4. Bedrohungsszenario C

Der Ernstfall tritt ein

Ein Unternehmen wird Opfer eines Cyberangriffs: Kundendaten werden gestohlen, interne Systeme beschädigt.

Was jetzt notwendig ist:

IT-Forensik & Sofortmaßnahmen: Experten analysieren den Angriff, stoppen die Schadsoftware, sichern Beweise und stellen Notfall-IT-Spezialisten für mehrere Wochen bereit.

Wiederherstellung der Systeme: Fachkräfte reparieren beschädigte Datenbanken, bauen Server und Netzwerkinfrastruktur neu auf und tauschen kompromittierte Hardware aus.

DSGVO-Folgen & Rechtsberatung: Juristen melden den Vorfall an Behörden, erstellen Kundeninformationen, übernehmen Risikoabschätzung und Dokumentation.

PR- und Krisenkommunikation: Kommunikationsprofis begrenzen den Imageschaden und übernehmen Medien- sowie Kundenkommunikation.

Kundenbenachrichtigung & Monitoring: Das Unternehmen informiert 120.000 betroffene Kunden und stellt einen 12-monatigen Identitätsschutz-Service bereit.



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 -

INHALTE

HINWEISE ZUR NUTZUNG UND ABLAGEORT

- CHECKLISTE SOFORTMAßNAHMEN FÜR MITARBEITENDE
- CHECKLISTE SOFORTMAßNAHMEN IT-BETRIEB
- LAGEBEWERTUNG
- CHECKLISTE KONTAKTAUFNAHME KRISENHOTLINE
- ABLAUF DER FALLANNAHME ÜBER DIE HISCOX KRISENHOTLINE
- EREIGNISBEWÄLTIGUNG
- ZEITKRITISCHE PROZESSE/PRODUKTE/DIENSTLEISTUNGEN
- KRITISCHE DATENSICHERUNGEN
- ALARMIERUNG DES KRISENMANAGEMENTS
- INFRASTRUKTUR
- 10.1 Standorte
- 10.2 Arbeitsmittel & Arbeitshilfen
- 11 AUFBAUORGANISATION DES KRISENMANAGEMENTS
- 11.1 Rollen im Krisenmanagement
- 11.2 Lagedokumentation und Visualisierung
- 12 GRUNDSÄTZE ZUR KRISENKOMMUNIKATION
- ANHANG A FÜHRUNGSZYKLUS
- ANHANG B WICHTIGE INTERNE ANSPRECHPARTNER
- ANHANG C WICHTIGE EXTERNE KONTAKTE
- ANHANG D ANSPRECHSTELLEN CYBERCRIME DEUTSCHLAND
- ANHANG E ANSPRECHSTELLEN CYBERCRIME ÖSTERREICH
- ANHANG F ANSPRECHSTELLEN CYBERCRIME SCHWEIZ
- ANHANG G PROTOKOLLVORLAGE
- ANHANG H VORLAGEN KRISENKOMMUNIKATION
- H.1 Meldung an interne Mitarbeiter
- H.2 Kundenmeldung Unterbrechung der Leistungen
- H.3 Muster für Journalistenanfragen
- H.4 Fragen und Antworten (FAQs)
- ANHANG I BEGRIFFE
- I.1 Störung
- I.2 Notfall
- I.3 Krise
- KONTAKT

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
HiSolutions AG © 2025

Seite 3
Stand: Januar 2026

4. Cyber-Soforthilfe

Ausgezeichnete Experten bereits im Verdachtsfall zur Stelle

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

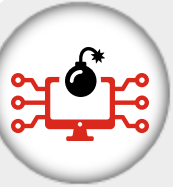




Ihr Partner für
starken Cyber-Schutz!

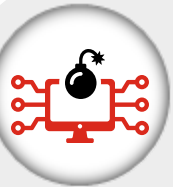
5. Erkenntnisse des Cyber Readiness Report 2025

KMUs investieren massiv – Makler brauchen starke Partner

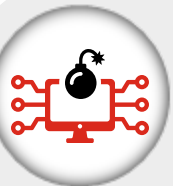


75% der deutschen KMUs planen neue Mitarbeiterschulungen

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

Mitarbeiterschulungen und Phishing-Simulationen zur Stärkung der Cyber-Resilienz.

UPDATE



Cyber-Sicherheits-Scan

Schwachstellen entdecken – bevor Angreifer sie ausnutzen.

NEU



Technisches Schutzpaket (optional)

Cyber-Sicherheitssoftware mit Virenschutz, Cloud-Back-up und mehr powered by Norton

NEU



Forderungsausfalldeckung (nur bei Hiscox!)

Schutz bei manipulierten Zahlungsdaten.

NEU



Tagessatzentschädigung (nur bei Hiscox!)

Kein komplizierter Nachweis des Ertragsausfalls nötig, schnelle Leistung auch im Kumulfall



Attraktive Prämien

Wettbewerbsfähige Prämien, speziell für kleine und mittlere Unternehmen

UPDATE



Auszeichnungen & Awards

Schwachstellen entdecken – bevor Angreifer sie ausnutzen



Bleiben Sie in Kontakt mit uns!

Auch über profino hinaus

Hiscox Makler
News:
Abonnieren &
gewinnen!

- ✓ Stets informiert beraten: Hiscox News & Produktinformationen
- ✓ Unterstützung für Ihren Vertrieb: Unterlagen, Studien, digitale Tools
- ✓ Profitieren Sie von IDD-Webinaren, exklusive Events & mehr!
- ✓ Bei Neuansmeldung Gewinnchance auf die passende Ausstattung zur Fußball-WM (1. Preis JBL-Soundbar, 2. & 3. Preis: Fan-Paket)



Vielen Dank für
Ihre Aufmerksamkeit!