# FUNK JOURNAL

Facts zu Risiko-, Vorsorge- und Versicherungsmanagement

## Prävention ist die beste Medizin

Die Pandemie beschleunigt die Digitalisierung. Doch das schafft auch neue Cyber-Risiken. Wie diese angegangen werden können, erklärt Centris-CEO Patrick Progin im Interview.

## Cybertraining die richtige Investition

Von Passwortsicherheit bis hin zum simulierten Phishing-Angriff: Funk CyberAware bereitet Ihre Mitarbeitenden auf den Ernstfall vor.

## Kein Gesichtsverlust im Land des Lächelns

Bei Geschäften mit China können Kulturunterschiede zu regelrechten Stolpersteinen werden. Funk zeigt, auf was es zu achten gilt.

Funk Insurance Brokers AG

Winter 2020

# Risikomanagement ist das A und O

Der IT-Betreiber Centris unternimmt viel, damit Kunden und Geschäftsprozesse gut geschützt sind. Im Interview zeigt CEO Patrick Progin, wie sich Centris mittels Risikomanagement für den Ernstfall rüstet.


## Centris AG

Die Centris AG zählt zu den führenden Dienstleistern für modulare IT-Lösungen im Schweizer Markt der Kranken- und Unfallversicherer. Als Outsourcing-Dienstleister ist Centris auch Berater für Business-Prozesse im Krankenversicherungsumfeld und ein innovativer Partner, der neue Lösungen zusammen mit Kunden und Software-Partnern im Rahmen von Communities konzipiert. Herzstück ist die Digital Swiss Health Platform, ein integriertes und offenes Gesamtsystem, das die wichtigsten Geschäftsprozesse von Kranken- und Unfallversicherern unterstützt. Über die zentral betriebene Lösung werden derzeit Rechnungen von rund der Hälfte aller Versicherten im ganzen Land geprüft.

*Titelbild:*
Patrick Progin ist seit 2004 CEO der Centris AG. Zuvor war er CIO und Verwaltungsrat bei Swiss Life und La Suisse Versicherung.

*Ihr Unternehmen begann in den 40er-Jahren als Lochkarten-Zentrale des Konkordats der Schweizerischen Krankenversicherer. Heute ist Centris ein modernes IT-Unternehmen. Wo sehen Sie die grossen technologischen Entwicklungen in den nächsten fünf bis zehn Jahren? Wie wird sich Centris in dieser Zeit verändern?*

Orientiert man sich an den Schweizer Zukunftsforschern (swissfuture) schreitet die Digitalisierung und alles was damit verbunden ist weiter voran. Immer mehr Prozesse und Produkte existieren ausschliesslich digital. Computer und reale Gegenstände (Internet der Dinge) vernetzen sich immer stärker. Systeme werden offener und anschlussfähiger. Ausserdem ist davon auszugehen, dass die technologische Autonomisierung sehr bald in sehr unterschiedlichen Anwendungsfeldern eine grosse Rolle spielen wird. Für Centris als Integrator und Betreiber gilt die Priorität in erster Linie dem technologischen «Enabling». So schaffen wir die Grundlagen für die Digitalisierungsstrategien der Versicherungskunden. Unser Kernstück, die Digital Swiss Health Platform, ist so gestaltet, dass Anwendungen aus dem gesamten eHealth-Ökosystem eingebunden werden können. Ausserdem arbeiten wir an der Bereitstellung unserer Services auf Cloud-Basis und automatisieren die IT-Backoffice-Prozesse laufend weiter. Das technologische «Enabling» ist jedoch nur ein Aspekt: Die Geschwindigkeit, mit der den Erwartungen des Marktes Rechnung getragen werden muss, der erhöhte Anspruch an die Informationssicherheit, die strengeren Auflagen der Behörden und der kulturelle Wandel sind die weiteren. Centris treibt und führt ihre digitale Transformation im Rahmen eines strategischen Programms über die gesamte Organisation.

*Als Provider der Swiss Health Platform ist Centris durchaus systemrelevant. Welchen Stellenwert nimmt das Risikomanagement bei Centris ein? Was sind die tragenden Pfeiler?*

Centris war schon immer um die Sicherheit ihrer Systeme besorgt. Schliesslich verantworten und verarbeiten wir Daten von diversen Kunden auf unserer Plattform. Sich an die sich ständig wandelnden Bedrohungslage anzupassen, hat bei uns deshalb oberste Priorität. Das Ziel ist es, umfassende Schutzmassnahmen zu bieten, die auch unvermeidbare Restrisiken abdecken. Unsere Risiko- und Sicherheitspolitik stützt sich auf ein Dispositiv zum Schutz der Unternehmenswerte und Geschäftsprozesse, einem Security Operations Center (SOC) zur Erkennung und Reaktion auf Bedrohungen, einer Business-Continuity-Lösung zur Überlebensfähigkeit und Weiterführung des Betriebs bei Ausfällen sowie – sofern nötig – einer Versicherungslösung, um Restrisiken zu minimieren.

*Fortsetzung:*
*Risikomanagement ist das A und O*

*Wurde die Pandemie in der bisherigen Risikobeurteilung berücksichtigt? Und wenn ja: Haben Sie Eintrittswahrscheinlichkeit und Auswirkungen richtig eingeschätzt?*

Ja, bereits bei der weltweiten Ausbreitung von «SARS» in den Jahren 2003/04 arbeiteten wir Notfallpläne aus. Das Risiko wurde seitdem immer wieder neu beurteilt im Hinblick auf die Intensivierung der Grippewellen. So konnten wir bei Ausbruch der Corona-Pandemie frühzeitig agieren und das Risiko auf Basis bereits bestehender Prozesse managen. Die Mitarbeitenden vertrauen darauf, dass ihr Arbeitgeber durch die Krise führt. Centris wird dieses Vertrauen hundertprozentig entgegengebracht.

*Wie hat das Pandemie-Krisenmanagement bei Centris genau funktioniert?*

Entsprechend unserer Vorkehrungen aus dem Business Continuity Management ist seit Februar bis heute eine interne Taskforce im Einsatz. Ihre tägliche Aufgabe ist es, die Situation und Entwicklungen sowie die Vorgaben des Bundes zu überwachen und der Geschäftsleitung entsprechende Schutzmassnahmen zur Umsetzung vorzuschlagen. Auch den Informationsfluss und die Kommunikation mit der Belegschaft und mit externen Anspruchsgruppen haben wir in dieser Zeit über verschiedene Kanäle und entsprechend der Situation intensiviert.

*Welches waren die Haupterkenntnisse?*

Es scheint, als hätte die Pandemie den Digitalisierungsprozess beschleunigt. Kurzum war es technisch möglich, dass über 90% der Belegschaft im Homeoffice arbeitet und gemeinsam mit den Mitarbeitenden unserer Kunden und Partner das Tages- und Projektgeschäft nahtlos weiterführt. Das hat das Vertrauen in die örtliche Unabhängigkeit, Eigenverantwortung und in die Zusammenarbeit generell gestärkt. Die raschen und überlegten Aktionen in der Krisenbewältigung haben bestätigt, dass unser Risikomanagement wirksam ist und einwandfrei funktioniert.

*Kennengelernt haben sich Centris und Funk bei der Bewertung der finanziellen Cyber-Restrisiken. Welcher Teil der Beratung war für Sie besonders wertvoll?*

Funk war in der Lage, das Cyber-Risiko in den Gesamtkontext unserer Unternehmensrisiken zu bringen und uns umfassend zu beraten. Im Ernstfall vertrauen wir darauf, dass Funk uns nicht nur im präventiven Bereich des Versicherungsmanagements, sondern auch bei der Schadensabwicklung professionell und im Interesse der Centris und ihren Kunden effektiv unterstützt.

*Funk arbeitet im Cyber-Risikomanagement mit dem IT-Security-Unternehmen InfoGuard zusammen. Gab es für Sie durch diese Zusammenarbeit Synergien?*

Unbedingt. Die Partnerschaft mit dem Cyber Defence Center InfoGuard und Funk hat zu einem idealen Dreier-Konstrukt mit Centris geführt. So fliessen bei der regelmässigen Überprüfung unserer Haftungs- und Deckungsrisiken das Schadenspotential und die Konsequenzen eines Angriffs in die Risikobewertung mit ein und wirken auf die Weiterentwicklung unseres Cyber-Security-Dispositivs sowie den Cyber Security Service für die Kunden. Der Austausch ermöglicht zudem, dass wir unsere Lösung laufend verfeinern können.

*Welche Vorteile hat das für die Kunden von Centris?*

Unsere Kunden profitieren von dieser Resilienz, zum einen, weil sie Gewissheit haben, dass ihre uns anvertrauten Daten nachweislich und entsprechend der regulatorischen Anforderungen geschützt sind. Zum anderen können sie im Falle eines Schadens ihre Nachweis- und Meldepflicht gegenüber der FINMA erfüllen. Ausserdem gewinnen alle Parteien aus den Erfahrungswerten des Expertenkonstrukts, indem die neusten Erkenntnisse bezüglich Bedrohungen, auch aus anderen Branchen, direkt in die Prävention einfliessen und im Ernstfall auch kundenindividuelle Entscheidungen getroffen werden können. Centris unterstützt ihre Kunden auf Wunsch beim Aufbau ihrer Cyber-Security-Lösung oder übernimmt das Outsourcing.

*Das Arbeiten im Homeoffice hat sich über Nacht etabliert. Cyberkriminelle versuchen, diese neue Situation auszunutzen. Offenbar nimmt die Zahl der Angriffe auf Unternehmen klar zu. Können Sie das für Ihre Firma bestätigen?*

Die Zunahme der cyberkriminellen Aktivitäten ist uns aufgefallen. Unser SOC analysiert pro Monat mehrere hundert Offenses und klärt bestimmte Auffälligkeiten auch direkt mit Kunden und deren IT-Providern ab. Aufgrund der Homeoffice-Arbeitsplätze haben wir die Überwachung auf Stufe Client verschärft, die Reaktionsfähigkeit durch den Einsatz moderner Technologien verkürzt und die Mitarbeitenden entsprechend sensibilisiert.

Kontakt: Rolf Th. Jufer
Email: rolf.jufer@funk-gruppe.ch
Telefon: +41 58 311 05 74

## Cyber-Dienstleistungen von Funk im Überblick

### Funk CRC
**Cyber-Restrisiken berechnen**

Viele Unternehmen kennen die finanziellen Konsequenzen einer Cyber-Attacke nicht. Der Cyber Risk Calculator von Funk unterstützt Unternehmen dabei, die individuellen Restrisiken wie Betriebsunterbrechung, Datendiebstahl, Rechtsberatung etc. zu berechnen. Versuchen Sie es selbst - mit unserer Funk CRC Light-Version.

Funk Cyber Risk Calculator

### Funk CRD
**Cyber-Risiko-Dialog mit der Unternehmensleitung**

Die Experten der Funk Gruppe unterstützen das Management in der vertieften Interpretation und dem Finetuning der CRC-Ergebnisse. Die Erfahrung der letzten Jahre zeigt, dass der Zeitaufwand für diesen Prozess in engen Grenzen gehalten werden kann. Mit Funk CRC und Funk CRD erhalten Unternehmen eine erste wichtige Schadensindikation und können danach die weiteren Schritte konsequent angehen.

### Funk CyberSecure
**Kundenorientierter und passgenauer Versicherungsschutz**

Funk hat mit führenden Versicherern eine Spezialdeckung entwickelt, die sich den Herausforderungen der digitalen Welt stellt und sowohl kriminelle Handlungen im Cyberspace wie auch IT-Infrastrukturausfälle massgeschneidert deckt.

### Funk CyberAware
**Cyberfitness für Ihre Mitarbeitenden**

Das moderne und modular aufgebaute Sensibilisierungs- und Trainingsprogramm. Ideal auch für Betriebe mit Mitarbeitenden im Homeoffice. Mehr dazu lesen Sie in dieser Ausgabe.

# Funk CyberAware macht Mitarbeitende Cyber fit

Das schwächste Glied in jedem Cyberabwehrdispositiv ist der Mensch. Die einfachsten Einfalltore für Cyberkriminelle bleiben Unwissenheit, Nachlässigkeit oder Neugier des Anwenders. Homeoffice öffnet neue Lücken in den IT-Systemen der Unternehmen.

Mit Funk CyberAware können Unternehmen ihre Mitarbeitenden nachhaltig und kontinuierlich zu Informationssicherheitsthemen sensibilisieren – und das mit minimalem internem Aufwand. Die Experten von Funk stellen verschiedene Lösungen bereit, um die Mitarbeitenden für die digitale private und berufliche Welt fit zu halten. Von grundlegenden Informationen zur Passwortsicherheit bis hin zur koordinierten Phishing-Angriffssimulation mit anschliessender Schulung.

«Unternehmen können das Risiko eines Phishing-Angriffs minimieren, indem Sie ihre Mitarbeitenden regelmässig in Security-Awareness-Trainings schulen.»

Stefan Brändli, Funk RiskLab

Funk CyberAware deckt die ganze Bandbreite ab. Für Unternehmen stehen standardisierte oder individualisierte Schulungssequenzen bereit. Funk stellt deren Administration und Koordination sicher. Die Inhalte variieren dabei nicht nur im Detail- und Verständnisgrad, sondern auch in der Präsentation und der Didaktik. Spielerische Elemente, Quizze und Videos bringen eine Lockerheit, ohne dabei den Lerneffekt zu beeinträchtigen. Der Wissensstand der Mitarbeitenden kann dabei getrackt und in Reports aufbereitet werden. Damit lassen sich Stärken und Schwächen der Belegschaft ermitteln und dann gezielt angehen – und dies ohne grossen Aufwand seitens des Arbeitgebers.

## Das Funk CyberAware-Angebot im Überblick

Funk CyberAware beinhaltet zwei Schulungsangebote: Basic und Advanced. Das Basic-Paket besteht aus einer von Funk-Spezialisten modellierten Zusammenstellung von Schulungsinhalten (Best Practice). Sie vermitteln den Mitarbeitenden die notwendigen Grundkenntnisse für ein sicheres digitales Arbeiten.

Das Advanced-Paket ist auf die individuellen Bedürfnisse des Unternehmens zugeschnitten und eignet sich für spezielle Branchen und/oder komplexe Unternehmensstrukturen. Zu beiden Produkten kann zusätzlich ein Attack-Paket gebucht werden. Dabei wird ein Phishing-Angriff geplant und simuliert. Damit lässt sich die Cyber-Fitness der Mitarbeitenden ideal und realitätsnah überprüfen. Alle Pakete beinhalten ein strukturiertes Reporting, welches Unternehmensintern weiterverwendet werden kann.

## Angebot auch im Jahresabonnement

Cyber-Risiken sind hochdynamisch und entwickeln sich rasant. «Ein» Training ist «kein» Training. Nur wenn die Schulungsinhalte periodisch aktualisiert werden und die Trainings regelmässig erfolgen, kann eine höhere Cyber-Security gewährleistet werden. Darum bietet Funk die Trainingsmodule auch im Abonnement an. Ihr Unternehmen delegiert dieses wichtige Projekt an die Spezialisten von Funk. So bleibt Ihnen mehr Zeit für Ihre Kernkompetenzen.

## Leistungsstarke Cyberversicherungen bald nur noch mit Cybertrainingsnachweis

Versicherungsunternehmen prüfen Cyber-Risiken immer detaillierter und stellen immer höhere Anforderungen an die Cyberfitness ihrer Kunden. Dabei erwarten sie vermehrt jährliche Mitarbeiterschulungen und Trainingsberichte zur Wahrung der Obliegenheiten eines Versicherungsvertrags. Funk CyberAware unterstützt Unternehmen somit auch auf dem Weg, eine leistungsstarke Versicherungslösung abzuschliessen und zu halten.

Kontakt: Stefan Brändli
E-Mail: stefan.braendli@funk-gruppe.ch
Telefon: +41 58 311 05 79

### CyberAware Basic

- Vorgefertigte «Best Practice» Schulungssequenzen
- Administration und Koordination der Schulungen durch Funk
- Reporting

### CyberAware Advanced

- Auf den Kunden zugeschnittene Schulungssequenzen
- Administration und Koordination der Schulungen durch Funk
- Reporting

### CyberAware Attack

- Simulierter Phishing-Angriff mit anschliessenden zielgerichteten Schulungssequenzen
- Administration, Koordination und Durchführung des Angriffs durch Funk
- Reporting

# China: Kulturelle Unterschiede mit Konsequenzen

Wer viel in China unterwegs ist oder mit chinesischen Partnern zusammenarbeitet, kennt das schon: Immer wieder gibt es ungewohnte, gar überraschende Situationen.

Sprachhürden aber auch eine uns wenig vertraute Kultur sind meist die Gründe für solche Situationen. Oft erleben wir die Kommunikation als verklausuliert und wenig direkt – gerade etwa im Vergleich zu den als sehr direkt geltenden Amerikanern. Mimik, Gestik und Körpersprache können für Menschen aus dem Westen schwierig zu deuten sein. Missverständnisse sind die Folge. Wichtig ist es für die Menschen in China, dass niemand das Gesicht verliert. Fehler werden nur ungern zugegeben. Direkte Kritik hilft kaum weiter.

### Funk in China

Der chinesische Versicherungsmarkt ist für Funk sehr wichtig. Seit 2019 hat Funk in Shanghai eine Vertretung. Diese Repräsentanz steht Funk als interkulturelle Schnittstelle zur Verfügung, dies in enger Zusammenarbeit mit dem Funk Allianz Partner in China.

## Implikationen für die Versicherungswirtschaft

Funk hat umfassende Erfahrungen darin gesammelt, versicherungstechnische Implikationen mit kulturell kundiger Kommunikation zu lösen. So hat etwa ein typisches chinesisches KMU lediglich eine Sachversicherung und sonst keine weiteren Policen. Die umfassenden Schweizer Rundumlösungen entsprechen oft nicht dem chinesischen Ansatz. Hier ist es wichtig, nichtversicherte Risiken transparent und wertungsfrei aufzuzeigen.

Die von der Schweizer Muttergesellschaft gewünschte Integration in die internationalen Versicherungslösungen wird oft mit konkurrenzlos günstigen lokalen Lösungen argumentativ blockiert. Wer Optionen objektiv und umfassend vergleichen will, kontaktiert den Funk Alliance Partner. Ein weiteres Beispiel: Oft werden Bauversicherungen über den Rahmenvertrag des Generalunternehmers abgeschlossen. Die Generalunternehmer haben in China eine starke Position. Für Funk Kunden sind die Folgen drastisch: Die Deckung ist intransparent, die Unsicherheit im Schadenfall hoch. Funk unterstützt die Kunden darin, dass die Deckungen direkt platziert werden.

Der chinesische Staat schützt die lokale Versicherungsindustrie. So sind grenzüberschreitende Deckungen nicht erlaubt. Funk hat kompetente und markterfahrene Partner vor Ort. Gemeinsam gelingt es, die Deckungen möglichst umfassend zu gestalten. Die neueren Versicherungsbranchen (früher D&O, heute vor allem Cyber) sind in China nicht weit verbreitet, das Risikobewusstsein in China ist noch gering und die Versicherer haben nur rudimentäre Wordings. Funk arbeitet intensiv mit den Kollegen vor Ort zusammen. So lassen sich die Kunden in China überzeugen und eine lokale Police erzielen, die sämtliche wichtigen Deckungen beinhaltet.

Kontakt: Armin Gutmann
Telefon: +41 58 311 05 41
E-Mail: armin.gutmann@funk-gruppe.ch

# Kundenzufriedenheit 2020: Wow!

Die Resultate der im Sommer durchgeführten Befragung übertreffen die hohen Werte zur Kundenzufriedenheit aus früheren Jahren deutlich.

## Befragung durch unabhängige Spezialisten

Eine repräsentative Auswahl von Funk-Kunden wurde in den Monaten August und September in einer Online-Befragung um ihre Meinung gebeten. Value-Quest, ein unabhängiges, auf Umfragen spezialisiertes Unternehmen, unterstützte Funk und stellte sicher, dass die Daten vertraulich behandelt sowie objektiv ausgewertet wurden.

## Betreuung und Beratung mit den höchsten Werten

Top-Werte in der Umfrage erhielten die Betreuung und Beratung sowie die Beratungsqualität. Auch die Unterstützung und Abwicklung bei Schadenereignissen wird von den Kunden besonders geschätzt und ausgezeichnet bewertet.

**68** Net Promoter Score

## Höchste Bereitschaft für Weiterempfehlung

Ausserordentlich positiv war auch der Umfang der Weiterempfehlung. Der in früheren Umfragen bereits hohe Wert kletterte in der Umfrage 2020 auf einen Spitzenwert. Mit grosser Wahrscheinlichkeit werden Sie zu diesem Thema noch persönlich angesprochen.

## Potential

Natürlich sehen Kunden noch Potential. Trotz hohen Investitionen in unser digitales Angebot erwarten einige Kunden diesbezüglich noch mehr von uns. Dabei geht es teilweise um die Portal-Reaktionszeiten, eine breitere Palette von Lösungen (Applikationen) im Kundenportal oder um punktuell höhere Convenience. Glücklicherweise sind das Bereiche, in die Funk in den nächsten Jahren bewusst investieren wird.

## Interessante Zusatzinformationen

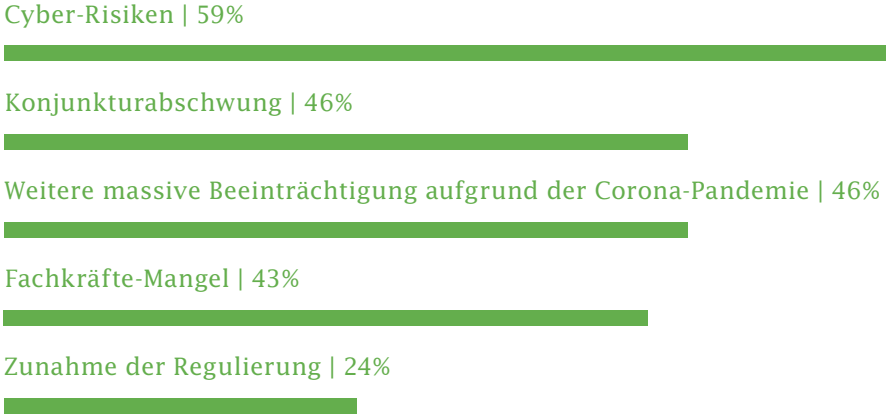
Die Funk-Kunden sehen Cyber-Risiken, den Corona-bedingten Konjunkturabschwung und den Fachkräftemangel als Hauptrisiken der nächsten Jahre. Von den angebotenen Zusatzdienstleistungen wurden das Cyber-Security-Training und das Risikomanagement mit deutlichem Abstand als besonders interessant bewertet.

## Herzlichen Dank!

Das ganze Funk-Team bedankt sich herzlich bei allen Kunden, die sich für diese Umfrage Zeit genommen haben. Die top Bewertung setzt weitere Energie frei, damit Funk auch in Zukunft Ihre beste Empfehlung sein wird!

Kontakt: Rolf Th. Jufer
E-Mail: rolf.jufer@funk-gruppe.ch
Telefon: +41 58 311 05 74

## Wo sehen Sie in den nächsten 2-3 Jahren die grössten Risiken für Ihr Unternehmen?




Sicherheit für Unternehmen seit 1879.
Die beste Empfehlung. Funk.

Funk Insurance Brokers AG
info@funk-gruppe.ch
www.funk-gruppe.ch

Funk Basel
Wartenbergstrasse 40
CH-4052 Basel
T +41 58 311 01 00

Funk Bern
Feldstrasse 42
CH-3073 Gümligen
T +41 58 311 02 00

Funk Luzern
Seidenhofstrasse 14
CH-6002 Luzern
T +41 58 311 03 00

Funk St.Gallen
Davidstrasse 38
CH-9001 St.Gallen
T +41 58 311 04 00

Funk Vaduz
Städtle 36
LI-9490 Vaduz
T +423 262 99 00

Funk Zürich
Hagenholzstrasse 56
CH-8050 Zürich
T +41 58 311 05 00

Folgen Sie uns auf: