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.