

FUNK JOURNAL

Facts zu Risiko-, Vorsorge- und Versicherungsmanagement



Happy End nach Grossschadenereignis

Im März 2018 zerstört ein riesiger Brand das gesamte Aussenlager und das Kühllager der Tobi Seeobst AG fast vollständig. Schon fünf Monate später steht alles wieder bereit für die Ernte 2018. Ein Krimi mit positivem Ende, dank des Anpackens aller Beteiligten.

Böses Erwachen nach Cyber-Angriff

Cyber-Kriminelle achten bei Angriffen nicht auf die Attraktivität eines Unternehmens. Sie suchen sich den Weg des geringsten Widerstands. Diese schmerzliche Erfahrung machte ein Schweizer Unternehmen im Sommer 2018.

Neue Funktionen im Kundenportal

Mit dem aktuellen Update führt Funk eine Vielzahl neuer Funktionalitäten ein und verbessert die Bestehenden. Bald folgt eine Reihe zusätzlicher Erweiterungen. Im Zentrum steht dabei die Funk App-Engine mit einer Vielzahl spezieller, auf die Kundenbedürfnisse zugeschnittenen Anwendungen.

Unmögliches wird gemeinsam möglich

Eigentlich nicht möglich: Grossbrand im März 2018, Aufrichte des Ersatzneubaus im August. Bereits im September findet die reiche Obsternte Platz im neuen, technisch modernisierten Kühllager. Nach einem Jahr lässt sich der Schadenfall zwar überblicken, vollständig abgeschlossen ist er dennoch nicht.



Benno Neff, CEO der Tobi Seeobst AG, und Theo Schmid, Leiter des Betriebs Egnach, besuchen am Freitagabend des 16. März 2018, gemeinsam eine Veranstaltung in Weinfeld, als kurz nach 23.30 Uhr das Handy klingelt: In Egnach ist ein Feuer ausgebrochen. Ruhig Blut, so schlimm wird es nicht sein, Menschen übertreiben in Stresssituationen gerne, geht es den beiden durch den Kopf. Auf der Rückfahrt sehen die Führungskräfte jedoch schon von weitem, dass ihre Hoffnung trügt. Der Nachthimmel glüht rot.

Kurz nach Mitternacht kämpfen die Einsatzkräfte mit über 30 Meter hohen Flammen. Mitarbeitende sind ebenfalls vor Ort, unterstützen organisatorisch, öffnen Türen. Das Aussenlager der 40'000 und je 300 Kilogramm Obst fassenden Kunststoffkisten brennt lichterloh. Trotz fünf Wasserleitungen gelingt es nicht, das Übergreifen auf das erst 2011 erstellte Kühllager zu vermeiden. Die SBB haben zwischenzeitlich den Bahnbetrieb auf der direkt am Betriebsareal vorbeiführenden Linie eingestellt und unterstützen die Feuerwehr mit einem Löschzug. Aber alles Wasser genügt

nicht: Es braucht zusätzlich Löschschaum, um weitere Gebäude zu sichern.

Die lange Nacht: Schon um zwei Uhr ist die Presse vor Ort, erste Zuschauer ebenso. Es gilt Fehlinformationen zu vermeiden und den Informationsfluss zu steuern. Denn eines stellt sich rasch heraus: Egal, welche Informationen oder Zahlen bekannt gegeben werden, sie finden sich innert Kürze in den Medien wieder – ob richtig oder falsch. Gut, dass auch der Pressesprecher der Kantonspolizei da ist, denn von Medienschaffenden sind teilweise Sensation und Emotionen gefragt – nein, ein trauriges Bild des CEO vor dem Feuer darf nicht sein – es gilt, das Richtige zu tun und Infos zu bündeln, zu koordinieren und zu kommunizieren. Auch der Verwaltungsrat will informiert sein, bevor alles durch die Medien geht. CEO und Betriebsleiter arbeiten die Nacht durch, sind an jedem Einsatzrapport dabei und rufen die Geschäftsleitung auf morgens sieben Uhr zusammen. Anschliessend findet die erste Pressekonferenz statt. Alle «funktionieren» – mit hohem Adrenalinspiegel. Zum Glück hat es keine Verletzten gegeben.

Der sprichwörtliche Tobi-Biss: nicht nur für Früchte

Weiterhin zählen Reaktion und Organisation: Am GL-Meeting kommen die vielen Facetten des Wie-weiter zum Vorschein. Nachdem die Einsatzkräfte die Brandnacht, in der man sich etwas hilflos gefühlt hat, dominierten, ändert sich nun die Verantwortung. Es gilt, den Notfallbetrieb aufrecht zu erhalten, die Brandstelle zu übernehmen und alle Personen vom einsturzgefährdeten Verbindungsdach fernzuhalten. Wichtige vermeintliche Kleinigkeiten sind festzulegen, wie z.B. der Einsatz einer Hundepatrouille oder die Sperrung des angrenzenden Velowegs. Denn zwischenzeitlich hat sich die Tobi Seeobst AG zu einer Art Sehenswürdigkeit entwickelt. Vor allem gilt es, Prioritäten zu setzen: Wohin soll die reiche Ernte der Region? Wie funktioniert der Betrieb weiter? Wer räumt auf? Wie schnell ist ein Wiederaufbau vor Ort und auch kühltechnisch zeitgerecht möglich? Wo steht das Ausbauprojekt im Schwesterbetrieb Bischofszell? Wo ist, nach der mageren Ernte

(Fortsetzung: *Unmögliches wird gemeinsam möglich*)

2017, genügend gleichwertig gutes Obst für die Lieferverpflichtungen verfügbar? Besteht Ersatz für die zerstörten Kisten bis zur neuen Ernte? Dieses Meeting ist das wichtigste überhaupt, denn hier wird das gesamte weitere Vorgehen geplant und damit die Basis gelegt, notwendige Schritte schnell mit den erforderlichen Partnern anzugehen.

Am Samstag geht's nonstop weiter: Positive, proaktive Kommunikation ist das A und O, um Ängste von Belegschaft, Kunden und Produzenten sowie Mietern zu minimieren. Mittags sind Vertreter von Mobiliar und Funk vor Ort, es geht um Schadensermittlung, erste Zusagen und nicht zuletzt um die beruhigende Gewissheit, über ausreichenden Versicherungsschutz zu verfügen. Denn die erste Schätzung eines Gesamtschadens in der Grössenordnung von 15 Mio. Franken sollte sich bewahrheiten. Dass auch die Lager der eingemieteten Firmen voll mitversichert sind, vereinfacht das Ganze. Daneben laufen weitere Interviews. Am Sonntag ist es deutlich ruhiger. Umso grösser die Überraschung, als nach der 45-minütigen Kaderbesprechung zum Thema «Sofortmassnahmen und next» am Montagmorgen wieder reihenweise Journalisten, frisch erholt vom Wochenende, anstehen. Diese erhalten die aktuellen Informationen.

Bewährte Partnerschaften zählen

Alle Partner sind sich dem Ernst der Lage bewusst und legen sich ins Zeug. Wiederum zählt die positive Grundhaltung: Vom mittlerweile 76-jährigen Ingenieur, der den 2011 gebauten Stahlbau plante und so eine Baueingabe zwölf Tage nach Brandausbruch ermöglicht, bis zum Verzicht der Nachbarschaft auf Einsprachen, damit der raschstmöglichen Baubewilligung der Gemeinde nichts im Wege steht. Der Einsatz der Entsorgungsfirmen, des Stahlbauers,

des Lieferanten der grossen Kühlaggregate, bis zum über die Schmerzgrenze hinaus arbeitenden Elektrikers – allen Akteuren sei herzlich gedankt. Nur so war ein Neubau in weniger als fünf Monaten möglich.

Partnerschaftlich verläuft auch die versicherungsseitige Abwicklung mit dem Schadenexperten der Mobiliar, Fredy Niedermann. Man kennt sich von früheren Ereignissen und als gelernter Meisterlandwirt ist der sympathische Berner Seeländer hier genau der Richtige. Es gibt kein Feilschen um Details, gemeinsam blickt man aufs grosse Ganze. Speditiv erfolgen Freigaben für Ersatzbeschaffungen. Die Fairness ist gegenseitig: Im Gesamtinteresse verzichtet auch die Tobi Seeobst AG auf die Geltendmachung der eigenen Arbeitsstunden. Angesichts der zeitlichen Verhältnisse hat «pingelig sein» keinen Platz. Funk bietet Unterstützung im Schadenprozess und muss nicht wie bei anderen Grossschäden Diskussionen mit dem Versicherer um Deckung und Obliegenheiten führen. Denn die Brandursache ist klar: Es war Brandstiftung durch Jugendliche. Funk weiss das kundengerechte Verhalten der Mobiliar zu schätzen.

Happy End mit Pendenzen

Für Benno Neff ist das Aufrichtefest im August 2018 ein Höhepunkt und zugleich Bestätigung seiner stets positiven Kommunikation. Die 350 geladenen Gäste – Einsatzkräfte, Handwerker und die Egnacher Belegschaft – kommen gerne und verbringen einen vergnügten langen Abend.

Neben eindrücklichen Erlebnissen bleibt für alle Beteiligten eine Reihe von Erkenntnissen. Dazu einige Beispiele: Kunststoffkisten brennen unerwartet schnell und sie schmelzen zu einer lavaähnlichen Masse, die so heiss wird, dass sie sich mit dem Teerbelag vermischt. Die so entstehende, 30 bis 70 Zentimeter dicke und feste Schicht zwischen dem schwarz verbrannten Kunststoff an der Oberfläche und dem Teergemisch auf

dem Boden ist ein Klumpen aus buntem, kaum beschädigtem Kunststoff. Die Aufräumarbeiten müssen sehr schnell erfolgen, denn die 1'900 Tonnen Obst und Gemüse bilden einen Saft, der die Bodenplatte zerfrisst. Und ohne solide Bodenplatte dauert ein Wiederaufbau deutlich länger. Weitere Erkenntnisse: Wasser als Löschmittel hat seine Grenzen und grosse Mengen von Löschschaum verursachen sowohl Zusatzkosten für die Wasserreinigung wie auch Umweltschäden durch Tenside auf dem benachbarten Bauland. Ein Brandschaden kann also auch zu Haftpflichtfällen führen, auch dann wenn selbst keine Mitschuld besteht.

Ebenso sind aus versicherungstechnischer Sicht Lehren zu ziehen: Dieser an sich klassische Brandfall zeigt die Wichtigkeit einer ausreichenden Pauschale für Zusatzkosten. Eine fundierte Bedarfsermittlung, basierend auf Szenarien, zeigt Schadenpotenziale auf und führt so zur Diskussion ausreichender Versicherungssummen und Sublimiten – auch in der Haftpflicht- oder Betriebsunterbrechungsversicherung. Dieser Fall zeigt: Man denkt spontan an die in der Schadenpraxis oft überraschend hohen Aufräumungs- und Entsorgungskosten und zu wenig an die anderen gut zwanzig Kostenarten. Im vorliegenden Fall ist der Einschluss «Mehrkosten aufgrund behördlicher Verfügung» von Bedeutung. Denn aufgrund der seit 2011 geänderten Vorschriften war die Kühltechnologie (damals waren Ammoniak und Glykol noch zulässig) von Gesetzes wegen anzupassen. Die Mehrkosten dafür betrugen rund eine Million Franken – kein Problem, wenn auch diese genügend versichert sind. So sind der CEO der Tobi Seeobst AG und der Schadenexperte der Mobiliar zufrieden, auch die Berater von Funk atmen tief durch.

Kontakt: Claudio Mazzariello
E-Mail: claudio.mazzariello@funk-gruppe.ch
Telefon: +41 58 311 04 42

Titelbild, Fotograf: Ralph Ribi/St.Galler Tagblatt



Weg des geringsten Widerstands gesucht und gefunden

Ein Funk Kunde machte 2018 eine unangenehme Erfahrung mit Cyber-Kriminellen. Die Anatomie eines zielgerichteten Cyber-Angriffs.

Der Sommer 2018 ging als Anomalie in die europäische Wetteraufzeichnung ein. Einem etablierten, mittelständischen Unternehmen in der deutschsprachigen Schweiz wird diese Phase des Jahres nicht nur aufgrund der andauernden überdurchschnittlichen Temperaturen in Erinnerung bleiben, denn die zweite Anomalie trat in den IT-Systemen des besagten Unternehmens auf. Ein zielgerichteter Cyber-Angriff führte zu einem Umdenken der Führungskräfte und zur nachhaltigen Umstellung der IT-Sicherheitsorganisation.

An einem Mittwoch im Juli 2018 fiel dem IT-Support eine Unregelmässigkeit in der Auslastung der Server auf. «Wir stellten eine deutliche Zunahme von Aktivitäten auf unseren Servern fest, was jedoch keine Auswirkungen auf Verfügbarkeit der IT-Systeme hatte» so der CFO des betroffenen Unternehmens. Stunden später fiel der Mail-Server kurzfristig aus. Auch dann erwartete niemand das Schlimmste. Am Donnerstagmorgen kam jedoch das böse Erwachen. «Der IT-Support musste feststellen, dass die Dateien auf 17 der insgesamt 22 Server vollständig verschlüsselt waren» erinnert sich der CFO. Der Angriff war besonders heimtückisch, denn neben den Core-Applikationen wurden teilweise auch die Dateien der Backup-Applikationen verschlüsselt. Dies verunmöglichte eine sofortige Wiederherstellung der Daten. In den verschlüsselten Dateien war die Forderung der Cyber-Kriminellen enthalten. Das Unternehmen sollte 24 Bitcoins für die Entschlüsselung der Daten und damit für die sofortige Fortführung der Geschäftstätigkeiten bezahlen.

Angriff war kein Zufall

Drei Indizien deuteten auf einen zielgerichteten und von langer Hand geplanten Cyber-Angriff hin. Erstens begann dieser just dann, als sich der IT-Leiter in den Sommerferien befand. Zweitens sollte das Datensicherungskonzept nach der Ferienabwesenheit des IT-Leiters vollständig überarbeitet werden. Drittens wurden die Konfigurationen der Backups so verändert, dass die Spezialisten im Nachgang nur eine unvollständige Datensicherung vorfanden.

Das Führungsteam war am Anfang davon überzeugt, kein Lösegeld zu bezahlen und meldete den Vorfall den zuständigen Behörden. Währenddessen wurde die Krisen-

organisation hochgefahren. Ein IT-Service- sowie ein IT-Security-Provider spannten mit dem Unternehmen zusammen und bildeten einen Krisenstab. Der IT-Security-Provider startete seine Arbeiten am Freitag und isolierte zuerst das Unternehmensnetzwerk von der Aussenwelt, um allfällige Datenabflüsse zu unterbinden.

Kommunikation im Fokus

Inzwischen begannen die Aufräumarbeiten. Am Wochenende wurden alle Laptops und Clients mit einem DeepScan überprüft und von jeglichen Schadprogrammen bereinigt. Um die vitalen Kommunikationsfunktionen wiederherzustellen, wurde bis Montag ein Notserver beschafft und konfiguriert. Nun konnte das Unternehmen zumindest wieder in gewohnter Art mit seinen Kunden kommunizieren. Der Datenserver konnte ebenfalls wieder zur Verfügung gestellt werden. Demgegenüber lief die Produktion langsam leer, da die Arbeitsvorbereitung nur mittels spezifischer Applikationen erfolgen konnte. Der CFO erinnert sich an die neuen Herausforderungen: «Die Anspannung war auch bei unseren Mitarbeitenden zu spüren, die während dieser Phase ihre Gleitzeiten abbauten. Während der Sommerzeit waren zudem viele Mitarbeiter in den Ferien. Da auch die Lohnzahlung in der besagten Woche anstand, vereinbarten wir mit unserer Geschäftsbank, die gleichen Zahlungen zu veranlassen wie im vergangenen Monat. Die interne und externe Kommunikation war zudem besonders wichtig, um Mitarbeitenden und Kunden Sicherheit zu vermitteln.»

«Als die ernüchternde Erkenntnis vorlag, dass unsere Backups teilweise nicht verwendbar waren und der IT-Security Provider auch keine passende Decryptor-Software finden konnte, mussten wir umdenken» beschreibt die Führungskraft die unbequeme Ausgangslage. Die Rekonstruktion hätte zu viel Zeit in Anspruch genommen und die Reputation hätte Schaden genommen. Der Krisenstab kam zu der Entscheidung, einen spezialisierten amerikanischen Unterhändler für die Verhandlungen mit den Cyber-Erpressern zu mandatieren.

Nachdem die Formalitäten mit dem Unterhändler geregelt waren und eine Anzahlung für das Lösegeld und die Verhandlungskosten geleistet wurde, nahm dieser am Freitag die Verhandlungen mit den



Cyber-Kriminellen im DarkNet auf. Tatsächlich gelang es dem Unterhändler, das Lösegeld von 24 auf 12 Bitcoins zu reduzieren und am Montag in den Besitz des Schlüssels zu gelangen. Für die rasche Entschlüsselung wurde Tag und Nacht gearbeitet, trotzdem nahm dies zusätzliche 48 Stunden in Anspruch, sodass die Geschäftstätigkeit erst am Donnerstag wieder vollständig hergestellt wurde.

Es kann jeden treffen

«Rückblickend betrachtet haben wir bei den IT-Sicherheitsmassnahmen zu stark auf die klassischen Methoden vertraut. Das Ausmass einer professionellen Attacke konnten wir nicht abschätzen. «Die 'business first'-Einstellung» führte zu einer offenen IT-Architektur und machte es den Angreifern zu einfach, unsere IT-Systeme zu kompromittieren. Wir sind stets davon ausgegangen, dass unser Unternehmen zu uninteressant für Cyber-Kriminelle ist. Doch die Angreifer achten nicht auf die Attraktivität des Ziels. Im Gegenteil, sie suchen sich den Weg des geringsten Widerstands. Ich bin überzeugt, dass 99 von 100 Unternehmen die Möglichkeiten von Hackern unterschätzen. Der Vorfall hat uns die Augen geöffnet, seitdem ist IT-Security mindestens genauso wichtig wie das Tagesgeschäft.»

Der zweiwöchige Ausfall der IT-Systeme kostete das Unternehmen umgerechnet rund 400'000 Schweizer Franken. Neben den rund 10'000 verlorenen produktiven Stunden, dem Lösegeld, den Beratungskosten und den Kosten für den Notserver, investierte das Unternehmen im Nachgang rund 200'000 Schweizer Franken in ein Security Operation Center (SOC) und weitere IT-Security-Massnahmen. Glück im Unglück hatte das Unternehmen im Nachhinein dann trotzdem noch, denn das Lösegeld und die Beratungskosten der involvierten Parteien waren im Rahmen einer Kidnap & Ransom-Versicherung abgedeckt.

Kontakt: Max Keller
E-Mail: max.keller@funk-gruppe.ch
Telefon: +41 58 311 05 51

Funk Global Risk Consensus

Ein neutraler Blick auf die wichtigsten Risiken 2019

Jedes Jahr führen namhafte Unternehmen und Institute Umfragen und Analysen durch, um die Stimmungen im wirtschaftlichen Umfeld zu untersuchen. Ein spezieller Fokus wird dabei auf diejenigen Risiken gelegt, mit denen Unternehmen aktuell konfrontiert sind. Zudem werden Risiken identifiziert, die im folgenden Geschäftsjahr als besonders besorgniserregend eingestuft werden. Aus den Antworten werden meist die Top-10 Risiken ermittelt.

Die Resultate der einzelnen Studien sind jedoch mit Vorsicht zu geniessen, da sie tendenziell durch voreingenommene Fragestellungen und Auswertungen beeinflusst werden können. Sie stimmen dann vor allem mit den Marketing- und Verkaufsstrategien der Auftragsfirma überein. Um den Marktteilnehmern einen neutralen Überblick zu verschaffen, ist es sinnvoll, die mögliche Befangenheit der Studien zu eliminieren. Hier setzt der Funk Global Risk Consensus an.

Für den Funk Global Risk Consensus werden sechs jährlich wiederkehrende Studien und Risikoreporte konsolidiert und ausgewertet. Dies stellt sicher, dass auch in den kommenden Jahren eine verlässliche und vergleichbare Datenbasis vorliegt. Die Studienauswahl umfasst Arbeiten von Rück- und Direktversicherern, Beratungsgesellschaften, wissenschaftlichen Instituten und dem World Economic Forum (WEF). Die getroffene Auswahl garantiert Vielfältigkeit und ermöglicht eine ausgewogene Auswertung.

Die ersten beiden Plätze für das Jahr 2019 nehmen Cyber-Risiken und politische Risiken ein. Diese wurden in den Studien am häufigsten gelistet und als besonders kritisch eingestuft. Auf den Plätzen drei, vier und fünf folgen der Fachkräftemangel, Naturkatastrophen und von Menschen verursachte Katastrophen.

Die gelisteten Risiken sind dabei als Risikokategorie zu verstehen. Cyber-Risiken beinhalten neben IT- und Telekommunikations-Ausfällen, die durch eigene Mitarbeitende und Dritte verursacht werden, auch gezielte und ungezielte Cyber-Angriffe. In die Kategorie politische Risiken fallen all jene Risiken, die durch Entscheidungen von Regierungen entstehen, durch politische Prozesse ausgelöst oder durch Interessengruppen provoziert werden. Von Menschen verursachte Katastrophen sind Risiken, die ihre Ursprünge im Nichteinhalten von Normen, Nachlässigkeit, Fahrlässigkeit oder aber auch Absicht (wie z.B. Terroranschläge) haben.

Unternehmen schätzen eine fundierte und neutrale Basis für ihre eigene Risikobeurteilung. Der Funk Global Risk Consensus bietet diese Grundlage. Die unternehmensspezifischen Konsequenzen lassen sich sodann direkt in der Risiko- und Versicherungsstrategie umsetzen.

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



1. Cyberrisiken



2. Politische Risiken



3. Fachkräftemangel



4. Naturkatastrophen



5. Von Menschen verursachte Katastrophen

AI-Bescheinigung bei grenzüberschreitender Tätigkeit zwischen EU- und EFTA-Ländern

Bei einer grenzüberschreitenden Beschäftigung müssen Mitarbeitende mittels AI-Bescheinigung nachweisen, dass sie dem Sozialversicherungssystem eines bestimmten Mitgliedstaates unterstellt sind. Dies gilt für jede grenzüberschreitende Tätigkeit, sei diese auch noch so minim. Selbst stundenweise Aufenthalte wie z.B. für Meetings, Schulungen, VR-/GL-Sitzungen, Workshops, Auftritte oder gar das Tanken eines Geschäftsfahrzeugs fallen darunter. Seit Anfang 2019 haben die Kontrollen der ausländischen Behörden massiv zugenommen. Ohne Bescheinigung kann der Zutritt zu einem Firmen- oder Messegelände verweigert werden und es drohen zum Teil prohibitive Bussen. Toleranz ist nicht vorgesehen. Diese Verschärfung betrifft sehr viel mehr Mitarbeitende, als allgemein angenommen wird. Die Entsendebescheinigung kann online bei der jeweiligen Ausgleichskasse beantragt werden.

Buchtipp: Reanimation der Arbeitsmotivation

Was tun, wenn die Arbeitsmotivation von Mitarbeitenden so weit abgesunken ist, dass sich diese für eine gewisse Zeit mit einer Krankenschreibung aus dem Arbeitsprozess abmelden? Das eBook von Dr. Hildegard Nibel, Arbeitspsychologin und Senior Consultant HR Risk Management bei Funk, liefert Vorgesetzten und HR-Verantwortlichen eine Fülle von einfach handhabbaren Ideen und Massnahmen, um Mitarbeitende in den Arbeitsprozess zurückzuführen und Präventionsmassnahmen zu optimieren. Der Leitfaden dient zudem als HR-Controlling-Instrument, das die Auswirkungen des Personalmanagements anhand von harten Daten widerspiegelt und mit Fallbeispielen praktisch veranschaulicht.

(ISBN 978-3-939255-82-6)

Funk Kundenportal erhält neue Funktionen

Erweiterter Funktionsumfang bietet zusätzlichen Mehrwert



Absenzmanagement

Das neueste Update des Funk Kundenportals bringt eine Vielzahl neuer Funktionalitäten und Verbesserungen. Das elektronische Erfassen und Übermitteln von Schadenfällen an Funk ist die wichtigste Neuerung. Es lassen sich komplexe Motorfahrzeug- und Haftpflichtschäden sowie allgemeine, kleinere Schäden erfassen. Einfache Schadenfälle können mit einer (universellen) standardisierten Eingabemaske mit lediglich fünf Mussfeldern schnell und unkompliziert eingereicht werden. Darüber hinaus lassen sich Unfall- und Krankheitsmeldungen im Rahmen der datenschutzrechtlichen Bestimmungen übermitteln. Die Anzeige der Erfassungsmasken ist für alle Endgeräte wie z.B. Mobile- und Tablet-Geräte optimiert.

Zusätzlich zu einer Schadenerfassung im autorisierten Bereich des Kundenportals können Personen neu auch ohne Portalzugang einen Schadenfall anlegen und einreichen. Über eine innovative Link-Engine können berechtigte Portalbenutzer einen verschlüsselten, temporären Internet-Link auf ein Schadenerfassungsformular generieren und der betroffenen Person direkt via E-Mail oder SMS zusenden. Klickt der Empfänger diesen Link an, öffnet sich die entsprechende Erfassungsseite. Nach Ablauf der definierten Gültigkeitsdauer verfällt der temporäre Link und kann nicht mehr verwendet werden. Der autorisierte Portalbenutzer behält dabei aber immer den Überblick über die Erfassungen. Ein Anwendungsbeispiel: Ein Lieferwagenfahrer verursacht bei einer Auslieferung einen Schaden am Fahrzeug. Der Flottenmanager kann nun dem Fahrer einen Link zur Erfassung des Schadenfalls zustellen und behält selbst den Überblick, ob die Erfassung stattgefunden hat.

Geschäftsrelevante Dokumente können neu per Drag&Drop ins Portal hochgeladen werden und das mühselige Herunterladen einzelner Dateien entfällt mit der neuen Massen-Download-Funktionalität. Diese lässt den Download mehrerer markierter Dokumente in einem Durchgang zu.



Link sharing

Performance-Optimierungen und visuelle Korrekturen runden die neueste Version des Funk Kundenportals ab.

Funk Apps – ein Ausblick

Funk treibt die laufende Freigabe weiterer Versicherungsbranchen für die Schadenerfassung konsequent und mit höchster Priorität voran. Parallel läuft bereits die Umsetzung und Implementierung einer zukünftigen Erweiterung – der Funk App-Engine. Diese Engine umfasst im Endausbau diverse Funk Apps, die wiederum massgeschneidert auf die unterschiedlichsten Bedürfnisse der Kunden ausgerichtet sind. Darunter findet sich z.B. eine App für das betriebliche Absenzenmanagement inkl. intelligenter Auswertungsmöglichkeiten und Echtzeit-Benachrichtigungen. Mit Hilfe der Cyber Risk Calculator-App kann der Kunde sein versicherbares Cyber-Risiko berechnen. Nebenbei bietet die Schendashboard-App Unterstützung bei der mehrdimensionalen Analyse des eigenen Schadenportfolios, um daraus entsprechende innerbetriebliche Massnahmen zur Reduktion gewisser Schadensmuster oder -häufigkeiten abzuleiten.

In Analogie dazu fließen derzeit grosse Anstrengungen und Ressourcen in die Entwicklung einer Risikomanagement-App. Diese RM-Applikation zielt auf den ganzheitlichen Risikomanagement-Ansatz und auf die Verschmelzung des Risiko- mit dem Versicherungsmanagement ab. Mit Hilfe dieser Verknüpfung lassen sich Benchmarks für Kunden aus gleichen Industrien herstellen und wichtigste Branchenrisiken sowie ideale Strategien für den Risikotransfer oder die Risikoreduktion ermitteln. Auch diese App wird einfach und intuitiv zu bedienen sein.

Kontakt: Matthias Meier
Email: matthias.meier@funk-gruppe.ch
Telefon: +41 58 311 05 14

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
F +41 58 311 01 10

Funk Bern
Feldstrasse 42
CH-3073 Bern-Gümligen
T +41 58 311 02 00
F +41 58 311 02 20

Funk Luzern
Seidenhofstrasse 14
CH-6002 Luzern
T +41 58 311 03 00
F +41 58 311 03 30

Funk St.Gallen
Davidstrasse 38
CH-9001 St.Gallen
T +41 58 311 04 00
F +41 58 311 04 40

Funk Vaduz
Städtle 36
LI-9490 Vaduz
T +423 262 99 00
F +423 262 99 02

Funk Zürich
Hagenholzstrasse 56
CH-8050 Zürich
T +41 58 311 05 00
F +41 58 311 05 50

Folgen Sie uns auf:

