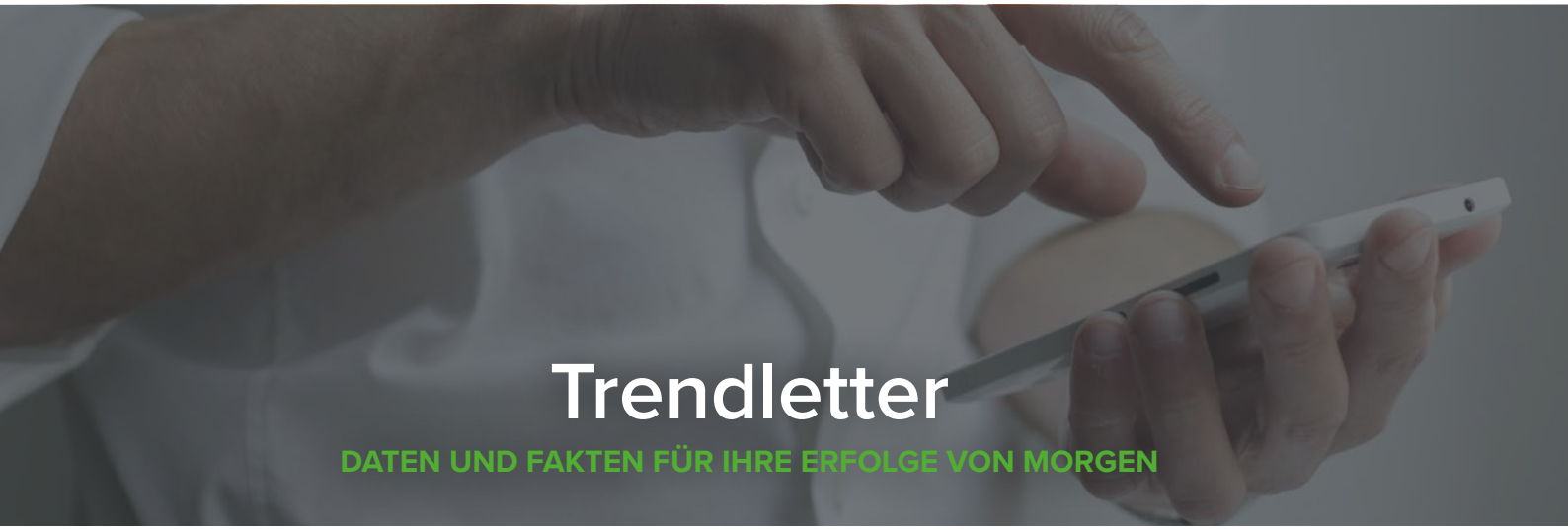
COMPDATA
Spezialisiert auf IT. Und Sie.

AUSGABE 2B | 2022



Trendletter

DATEN UND FAKTEN FÜR IHRE ERFOLGE VON MORGEN

Starke Version: ATOSS Time Control App

Leistungsstarke Prozesse und moderne Technologie – ATOSS Time Control ist die ideale Zeitwirtschaft für Bäckereien. Für die Zukunft des Mobile Workforce Managements bringt die neugestaltete ATOSS App großartige Funktionen mit. Das entlastet die Personalabteilung, schafft schnell Überblick und steigert die Zufriedenheit der Mitarbeiter.

Die Highlights der neuen App:

- Arbeitszeiten schnell erfassen und in Echtzeit übertragen
- Mobiles Stempeln für Mitarbeiter und Team-Stempelung für Teamleiter
- Saldenstände, Stempelsätze und Fehlzeiten einfach einsehen
- Personaleinsatzpläne und Schichtangebote jederzeit abfragen
- Kurzfristige Änderungen einfach umsetzen
- Sicherer Login mit biometrischem Verfahren oder PIN
- Anträge stellen, bearbeiten und einsehen
- An- und Abwesenheiten der Teams auf einem Blick

INTERESSANTE SCHWERPUNKTE FÜR SIE

1 Cyber-Abwehr sicher aufstellen

Beim IT-Security-Kongress kamen zahlreiche Experten der IT-Sicherheit zusammen und zeigten, worauf es bei Cyber-Sicherheit in Zukunft ankommt.

SEITE 2 →

2 IT-Risiken versichern

Gibt es einen Komplettschutz gegen Internetkriminalität? Warum zu einem runden Gesamtkonzept eine Risikoabsicherung gehört und worauf Sie bei Cyber-Versicherungen achten sollten.

SEITE 3 →

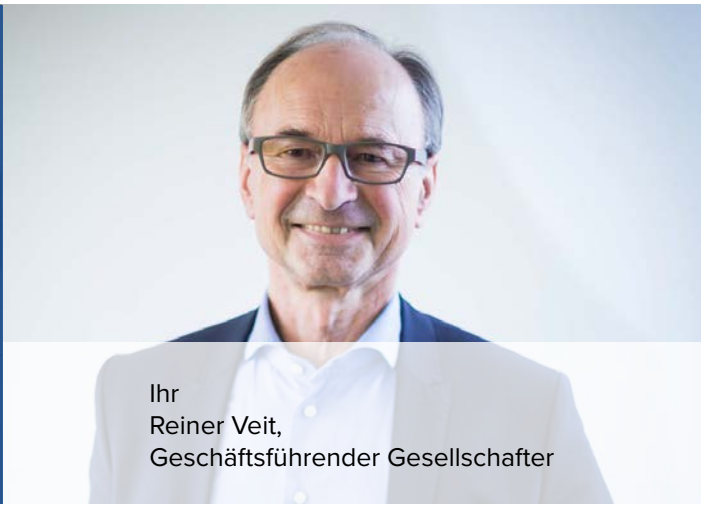
3 Das sagen unsere Kunden

Die Bäckerei Lohner entschied sich für ATOSS Time Control, um den rund 2.000 Mitarbeitern eine übersichtliche und benutzerfreundliche Zeiterfassung zu bieten.

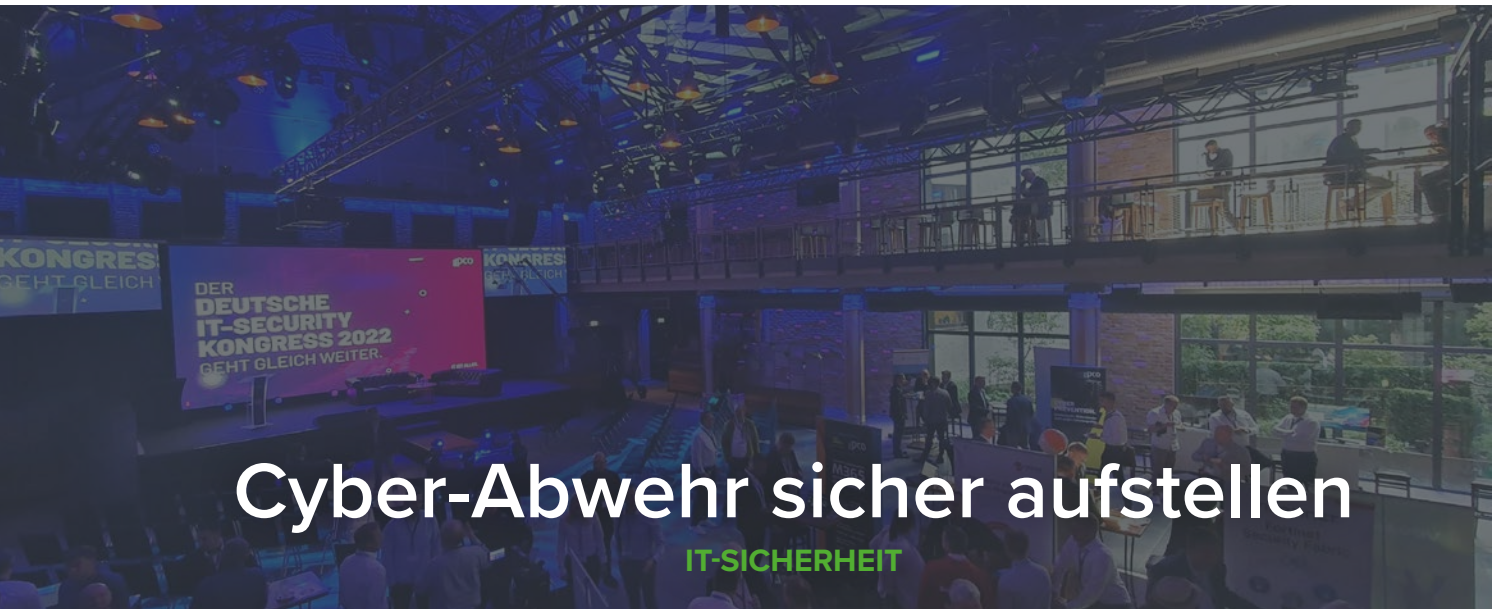
SEITE 4 →

Auf ein Wort

Nahezu jeder Bäckereibetrieb setzt digitale Lösungen ein, Nachholbedarf besteht bei der Integration. Verschiedene Software-Anwendungen als eigenständige Inseln zu nutzen, hat den Nachteil, dass Daten nicht vernetzt sind. Das reduziert die Effizienz, erhöht den Aufwand und erzeugt Fehlerquellen.
Ziel der Digitalisierung ist es, mit vernetzten Daten automatisierte Prozesse zu schaffen. Erst dann wird Zeit und Geld gespart. Das gilt für das Buchen von Bankumsätzen genauso wie für Warenwirtschaft oder Personaldaten. Eine jährliche Bestandsaufnahme hilft, Optimierungsansätze zu definieren. Sprechen Sie uns an!



Ihr
Reiner Veit,
Geschäftsführender Gesellschafter



Cyber-Abwehr sicher aufstellen

IT-SICHERHEIT

Über moderne Methoden der Cyber-Abwehr informierten am 29. September 2022 die klügsten Köpfe der IT-Security beim deutschen IT-Security-Kongress in Osnabrück.

Beim IT-Security-Kongress 2022 kamen zahlreiche Experten der IT-Sicherheit, internationale Hersteller und bekannte Sprecher in einem einzigartigen Format zusammen. Professionelle Vorbereitung, eine tolle Location und innovative Lösungen zeichnen diesen Kongress aus.

Auch CompData war Teil der Veranstaltung. Im Impulsvortrag informierte Marco Fischer, Leiter der IT-Security-Abteilung bei CompData, worauf es in Zukunft bei der IT-Sicherheit ankommt. Cyber-Angriffe sind heute so vielfältig wie die digitale Welt selbst. In dem sehr dynamischen Umfeld spielen die rechtzeitige Erkennung von Gefahren und die passende Abwehr wichtige Rollen.

Die Dauer eines Datenverlusts entscheidet schlimmstenfalls über den Fortbestand eines Unternehmens. IT-Abteilungen benötigen für Sicherheitsvorfälle einen Notfallplan für die Systemwiederherstellung. Reaktionsschnelle ist essenziell. Nur wenn die richtige Expertise zur richtigen Zeit am richtigen Ort ist, kann die Cyber-Abwehr zügig und erfolgreich arbeiten. Genau diesen Hintergrund nehmen acht Partner der CompassGruppe für das Projekt „DIRT“ zum Anlass.

DIRT Deutsches Incident Response Team

Spezialeinheit Cyber-Sicherheit

Incident Response ist die Reaktion eines Unternehmens auf einen IT-Sicherheitsvorfall. Die IT-Abteilungen von Bäckereien sind nach einem Angriff oft überfordert und haben nicht die Erfahrung, solche Vorfälle zu bewältigen.
Als externe Unterstützung zur Wiederherstellung der IT-Systeme schließen sich aktuell acht Mitglieder der CompassGruppe zusammen als DIRT-Spezialeinheit. Die erfahrenen IT-Security-Experten unterstützen nach einem Cyber-Angriff – reaktionsschnell, bundesweit und direkt vor Ort. Die Planung der Einsatztruppe befindet sich in der finalen Entwicklungsphase. Weitere Infos folgen.
CompData ist Mitglied der CompassGruppe, die seit 35 Jahren als Zusammenschluss mittelständischer IT-Spezialisten im Markt erfolgreich ist.

IT-Risiken versichern

IT-SICHERHEIT

Zu einem aktiven Risikomanagement zählen die technische IT-Sicherheit, Präventionsmaßnahmen und das Notfallmanagement. Für ein rundes Gesamtkonzept kann das Restrisiko finanziell abgesichert werden. Lesen Sie hier, was es zu beachten gibt.

Viele Bäckereien fragen uns „Was könnten Hacker mit unseren Daten anfangen? Interessieren sie sich für unser Unternehmen?“ Die Antwort lautet: Ja. Auch wenn Daten nicht rentabel scheinen, das Lösegeld bei erfolgreicher Verschlüsselung ist es in jedem Fall.

Das CompData IT-Securtiy-Portfolio bedient alle Anforderungen an die technische IT-Sicherheit – inklusive Notfallmanagement und Präventionsmaßnahmen. Warum wir uns zusätzlich Gedanken über eine Cyber-Versicherung gemacht haben? Das Stichwort lautet: Risikoabwägung.

Alle bekannte Risiken auszuschalten, ist nicht möglich. Menschliche Fehler, Lücken in einer Software – es kann immer gelingen, dass Angreifer in das Netzwerk gelangen und Schaden anrichten. Die Folge sind Lösegeldforderungen und Kosten für die Aufarbeitung des Vorfalls. Öffentliche Schadensmeldungen bekannter Unternehmen lassen die Alarmglocken schrillen.

Von Datendiebstahl, Erpressung und Fake President Fraud ist die Rede. Betriebsunterbrechung, Instandsetzung der Systeme, Schadensbewältigung sind die Folgen, die zu Existenzgefährdung und Reputationsschaden führen können.

Schadensabdeckung prüfen

Wie bei allen Versicherungen ist es unterschiedlich, welche Schäden Deckungsinhalte der Cyber-Versicherung sind. Wichtig ist die Kombination aus verschiedenen Risiken innerhalb und außerhalb des Unternehmens. Dazu zählen Datenschutz- sowie IT-Risiken. Leistungen aus klassischen Eigenschadenversicherung sowie die Abdeckung von Haftungsansprüchen sollten zu einem passenden Paket kombinierbar sein. Dabei sind immer die technischen Gegebenheiten im Unternehmen einbezogen werden.

Beispiele für Schäden durch Cyber-Angriffe

- Datenzugriff: Trojaner über E-Mail Anhänge verschlüsseln Daten
- Betriebsstillstand: Kosten für Unterbrechung und Wiederherstellung der Systeme durch Angriff
- Zahlungsmittelschaden: Verlust von Kreditkartendaten
- Vertrauensschaden: Diebstahl von Firmenvermögen durch Überweisung auf Privat- oder Auslandskonto
- Fake President Fraud: Gehackte E-Mail der Geschäftsführung weist Überweisung hoher Geldsumme an
- Cyber-Forderung: Daten werden durch Angriff verschlüsselt oder zerstört, Lösegeldforderung folgt
- Cyber-Haftpflicht: Eine infizierte Datei wird zum Download angeboten und steckt andere Systeme an

Das sagen unsere Kunden

„Die Bäckereierfahrung von CompData und das Verständnis für unsere täglichen Arbeitsabläufe haben uns überzeugt. Das Team von CompData kennt verschiedenste Schichtmodelle, den Umgang mit Abschnittszeiten – es gab keinen Punkt, wo wir für die Umsetzung bei Null anfangen mussten. Wir gewinnen durch Time Control unter anderem bis zu 25 % Arbeitszeit.“

Johannes Eiffler,
IT-Leiter bei Lohner‘s

Ziel war es, ein zukunftssicheres System für die Zeiterfassung und Zutrittskontrolle für alle Mitarbeiter im Verkauf, in der Verwaltung und in der Produktion mit kompletter Lohnvorbereitung und Übergabe an den Lohn zu installieren.

Neue Schnittstelle: OPTIback & RechnungsManager

WARENWIRTSCHAFT UND EINGANGSRECHNUNGSMANAGEMENT

In Bäckereien werden täglich eine Vielzahl an Wareneingängen bearbeitet. Die Verwaltung der zugehörigen Dokumente, der Lieferscheine und Rechnungen, bindet viel Arbeitszeit. Für schnellere Abläufe und eine automatisierte Datenverarbeitung wurde eine komplett neue Schnittstelle geschaffen – die Verbindung der Warenwirtschaft OPTIback mit dem RechnungsManager.

Der Wareneingangslieferschein wird von OPTIback bearbeitet, im Hintergrund verarbeitet und dem Kreditor als Lieferschein zugeordnet. Eine Schnittstellendatei mit den buchungsrelevanten Daten wird ebenfalls bereitgestellt und zu einer Kontierung zusammengefasst. Im Rahmen des finalen Rechnungsworkflows wird dem User die Kontierung vorgeschlagen und gegen die Rechnungspositionen geprüft. Abweichungen werden grafisch dargestellt. Die Kontierung bleibt zu jeder Zeit anpassbar und wird im Anschluss an das Buchhaltungssystem übergeben.

Sie haben Fragen? Gerne informieren wir Sie.
+49 (0)7431 950-555
vertrieb@compdata.de

10,7 Mrd.

Zahl des Monats

Milliardenschäden durch Datendiebstahl
Eine Bitkom-Studie erfasste Anfang des Jahres erneut Milliardenschäden durch Datendiebstahl in Unternehmen in Deutschland. Nach der Selbsteinschätzung der befragten Unternehmen entfielen 10,7 Milliarden Euro der hochgerechneten Gesamtschadenssumme in Höhe von 202,7 Milliarden Euro in den letzten 12 Monaten auf Kosten für Erpressung mit gestohlenen oder verschlüsselten Daten.

Herausgeber
CompData Computer GmbH

Adressdaten
Eschachstr. 9 | 72459 Albstadt
+49 (0)7431 950-0
info@compdata.de
www.compdata.de

Verantwortlich für den Inhalt
Reiner Veit,
Geschäftsführender Gesellschafter

Konzeption, Redaktion und Grafik
kommunikation.pur GmbH
Sendlinger Str. 31 | 80331 München
www.kommunikationpur.com