# Sicherheit

**Manche Dinge lassen sich nicht verhindern, andere schon. Wie? Experten wissen, worauf es heute ankommt.**

# Sicherheit in allen Lagen

*Sicherheit wird durch viele Faktoren bestimmt. Zu den wichtigsten zählen IT-Security, Objektschutz, Compliance, Produktivitätssicherung oder Finanzplanung. Setzt man rechtzeitig adäquate Maßnahmen, lassen sich viele Probleme verhindern.* VON HARALD HORNACEK

**Informations- und Kommunikationstechnologien (IKT)** sind wesentliche Innovationstreiber für den Wirtschaftsstandort Österreich, aber sie sind auch mit Gefahren verbunden. Für den Mobilfunkanbieter Hutchison Drei Austria geht es daher vor allem darum, Lösungen für Cybersecurity zu finden, bei denen neben Benutzerfreundlichkeit auch höchste Sicherheit im Vordergrund steht und die zu transparenten Kosten verfügbar sind. So bietet Drei mit der „3Cloud Business" ein Produkt mit entsprechenden Sicherheitsstandards wie ISO-Zertifizierung oder Georedundanz: Der Kunde erhält direkten Support durch Drei, Kundendaten verbleiben in Österreich und unterliegen dem österreichischen Datenschutzrecht. Zu „3Cloud Business" zählt unter anderem „3CloudTeam", die Online-Festplatte mit Gruppenfunktion, die Kunden und Mitarbeitern schnellen Austausch und sichere Ablage von Dokumenten ermöglicht. Und mit „3CloudBackup" gibt es eine automatische Datensicherung des PCs/Macs in der Wolke – Datenverlust ist somit ausgeschlossen.

**Mobile Device Management.** „Eine große Herausforderung ist die sichere Integration mobiler Arbeitsgeräte in die Unternehmens-IT-Infrastruktur", meint Drei-Sprecher Tom Tesch. Mit Mobile Device Management bietet Drei eine Lösung für Mobilgeräte und Schutz der darauf befindlichen Daten.
Auch T-Mobile verfügt über ein breites Portfolio von Mobile-Device-Management(MDM)-Lösungen, unabhängig davon, ob unterschiedliche mobile Betriebssysteme einheitlich verwaltet oder die Kommunikation zwischen Unternehmens-PCs und mobilen Endgeräten sicherer gestaltet werden soll. „Anhand einer genauen Ist-Analyse erarbeiten unsere Experten gemeinsam mit den Kunden die optimale MDM-Strategie. Unternehmen erhalten einen genauen Überblick darüber, wie ihre mobilen Endgeräte am besten und kostengünstigsten verwaltet und geschützt werden können", erklärt Maria Zesch, Bereichsleiterin Business bei T-Mobile. Und mit „BackUpPool pro" profitieren sie von professioneller, zuverlässiger und vollautomatischer Datensicherung: Die Daten werden täglich verschlüsselt auf einen Backup-Server in Österreich übertragen und dort komprimiert abgelegt. Damit können sie im Fall des Falles zuverlässig wiederhergestellt werden können.

**Cyberkriminalität.** Laut IBM Cyber Security Intelligence Index haben Cyberkriminelle allein im letzten Jahr weltweit über eine halbe Milliarde persönlicher Informationen gestohlen. Verkaufs- und Übernahmepläne, Protokolle, Strategiepapiere und geistiges Eigentum – all dies ist für Cyberkriminelle attraktiv. Für Unternehmen bedeutet das eine wachsende Herausforderung, sich vor kriminellen Attacken zu schützen. Oft sind mehrere Sicherheitslösungen im Einsatz – im Schnitt laut IBM 45 Anwendungen von 35 unterschiedlichen Anbietern. Die Abwehrmaßnahmen greifen allerdings nicht, wenn kein Gesamtüberblick der aktuellen Bedrohungslage besteht. Deshalb bietet IBM eine integrierte Lösung: So setzt das „Threat Protection System" bei der Abwehr von Advanced Persistent Threats (APTs) und anderen Cyberangriffen darauf, Gefahren zu eliminieren, noch bevor diese Schaden anrichten können. Dazu arbeitet es in drei integrierten Schritten: prevent, detect, respond – vorbeugen, erkennen, bekämpfen.

FOTO: GETTY IMAGES

Der Schutz umfasst Personen, Daten, Applikationen und Infrastruktur. Auch im Bereich Forensik bietet IBM intelligente Lösungen: Mit „Security QRadar Incident Forensics“ können die Vorgehensweise eines Angreifers Schritt für Schritt zurückverfolgt sowie schnell und einfach umfassende Untersuchungen von mutmaßlichen Verletzungen der Netzsicherheit durchgeführt werden. So lässt sich die Ursache eines Angriffes feststellen, ein nochmaliges Auftreten verhindern bzw. der Verursacher blockieren.

**Finanzsicherheit.** Finanzplanung und Liquiditätsmanagement gelten laut Umfragen als zentrale Themen der meisten Großbetriebe. Das sieht man auch bei der Raiffeisen Bank International (RBI) so und hat deshalb eine Reihe unterstützender Maßnahmen entwickelt. Zu den wichtigsten Herausforderungen zählt die oftmals fehlende Übersicht über tagesaktuelle Kontostände, wodurch mancherorts Liquidität ungenützt bleibt und anderswo Konten überzogen werden. Auch eine unzureichende Steuerung der Zahlungsströme oder eine restriktivere Kreditvergabe der Banken als noch vor der Finanzkrise erfordern neue Wege in der Finanzplanung. Ausnützen des niedrigen Zinsniveaus in der Eurozone sowie richtiges Debitorenmanagement und Mahnwesen sind daher Teil eines zukunftsorientierten Financial Management.
Mit „CMI@Web“ der RBI erhalten Unternehmen eine komplette Übersicht über die gesamte Konzernliquidität sowie die Möglichkeit der zentralen Abwicklung von Zahlungen. Diese internationale, bankübergreifende E-Banking-Lösung wird mittels verschlüsselter Internetverbindung für die Abwicklung des weltweiten Zahlungsverkehrs eingesetzt. Damit können Informationen global gehaltener Konten in einem standardisierten Format abgerufen sowie der gesamte Zahlungsverkehr

*Compliance ist nicht nur Sache der Mitarbeiter sondern zuallererst der Manager.*
**Bettina Knötzl, Wolf Theiss**

*Unsere Experten erarbeiten gemeinsam mit den Kunden die optimale MDM-Strategie.*
**Maria Zesch, T-Mobile**

gesteuert werden. Darüber hinaus bietet die RBI die gesamte Palette an automatisierten Cash-Pooling-Lösungen national und grenzüberschreitend an. „Dadurch wird die Liquidität des Konzerns zentralisiert und das Zinsergebnis optimiert“, erklärt RBI-Sprecherin Ingrid Krenn-Ditz. Mit dem „Cash-Management-Konto“ gibt es fixe Stückpreise für Zahlungsverkehrstransaktionen, eine übersichtliche Monatsrechnung sowie eine geldmarktnahe Kontokorrentverzinsung. Und: Im Zuge der Liquiditätsplanung kann auch der Einsatz von Forderungsverkauf und Factoring zur Optimierung des Working Capitals und der Liquidität beitragen.

**Managerhaftung und Compliance.** Ein robustes Compliance System (CS) ist heute ein absolutes Muss für Großbetriebe. Fehlt es, kann dies zur Haftung von Unternehmen, Managern sowie Mitgliedern des Aufsichtsrats führen. Eine große Herausforderung stellt dabei die Wahl des „richtigen“ Compliance Officers (CO) dar. „Im Idealfall sollte dieser das Unternehmen gut kennen, natürliche Autorität ausstrahlen und beim Top-Management Gehör finden“, erklärt Bettina Knötzl, Partner bei Wolf Theiss Rechtsanwälte und Head of Litigation & Dispute Resolution. Diese Person zu finden, sei oft schwierig. Und: „Das robusteste CS scheitert, wenn das Management nicht voll dahinter steht. Compliance ist nicht nur Sache der Mitarbeiter, sondern zuallererst der Manager.“ Knötzl betont auch, dass das Investment in ein CS als Prävention zu sehen sei: „If you think compliance is expensive – try non-compliance!“ Eine präzise, maßgeschneiderte Vorgangsweise spare Ressourcen. „Das CS kann oft auf einem guten Fundament aufbauen, vorhandene Bausteine müssen nur gesucht und zusammengetragen werden“, weiß Knötzl. Außerdem verhalten sich Mitarbeiter überwiegend ohnehin regelkonform. „Mit einem CS zielen wir nur darauf ab, die Werte und Regeln bewusster und strukturierter zu vermitteln“, so Knötzl, „wobei der Spaßfaktor nicht unterschätzt werden darf. Mit Humor lässt sich das Thema leichter verbreiten, wobei eine

FOTOS: BEIGESTELLT (2)

*Die Projekte werden laufend größer und komplexer und damit auch kostenintensiver.*
**Franz Amesberger, TCI Consult**

Botschaft wichtig ist: Compliance schützt uns alle und bewahrt den guten Ruf des Unternehmens. Jeder Mitarbeiter profitiert vom Zurückdrängen der Risiken von Non-Compliance."

**Komplexe Projekte.** Franz Amesberger, Geschäftsführer der TCI Consult, erklärt die aktuellen Trends im Bereich Business Intelligence wie folgt: „Die Projekte werden laufend größer und komplexer, somit auch kostenintensiver, die dreistellige Millionengrenze ist rasch erreicht." Wesentliches zu erkennen und die Anstrengungen darauf zu fokussieren, seien zwei Hauptfaktoren für erfolgreiches Projektmanagement. Eine weitere Herausforderung liege in der knappen Durchlaufzeit. Die sogenannte „Time to Market" werde immer kürzer, das bringe zusätzliche Risiken mit sich und erfordere die Berücksichtigung von Fallback-Strategien. „Zugleich gilt es, die für den Projekterfolg essenzielle Kommunikation mit den beteiligten Stakeholdern gut zu organisieren, um die teils sehr großen Einheiten eines Konzerns gesamthaft mit auf die Reise zu nehmen", weiß Amesberger. Die Rolle der TCI Consult definiert er so: „Wir sind Integratoren von fachlichen Anforderungen mit Technologie und Organisation und beziehen während der gesamten Projektzeit die internen wie externen Teams intensiv mit ein. Dazu gehört auch die Wahrung der Interessen des Auftraggebers gegenüber Vendoren und Systemintegratoren. Das kann viel Geld sparen!" Es gehe nicht nur darum, Lösungen hervorzubringen und zu implementieren, sondern sie den beteiligten Mitarbeitern näherzubringen. Ziel sei, mit Informationsqualität die Leistungsfähigkeit der Organisation und damit den Unternehmenswert zu steigern sowie eine „Corporate Intelligence" zu schaffen: „Wir sehen unsere Aufgabe darin, den tatsächlichen Bedarf einer Organisation zu ermitteln und die Gesamtheit der Werte, auf deren Basis das Unternehmen gesteuert wird, zu unterstützen. Das ist ‚Value Driven Information Management'. Wir setzen dabei Methoden und Tools ein, durch die wir treffsicher die relevanten Informationen bestimmen können, denn nur 25 bis 30 Prozent der zur Verfügung stehenden Informationen sind auch wirklich relevant!"

**Gebäude- und Objektschutz.** Bleibt ein wesentlicher Punkt, der gerne übersehen wird: Der Schutz von Gebäuden und Betriebsobjekten. „Selbst ein ausgefeiltes Sicherheitskonzept reduziert lediglich das Restrisiko. Daher ist es extrem wichtig, mit dem Risiko- und Krisenmanagement sehr eng zusammenzuarbeiten, um Leben und Sachwerte zu schützen. Das ist die Voraussetzung für ein integriertes Sicherheitskonzept", betont Helmuth Hochegger, Leiter der zur Simacek-Gruppe zugehörigen SIM.GUARD Security Services. Ihre Leistung für Unternehmen definiert er wir folgt: „Bestimmen, analysieren, bewerten – und daraus gemeinsam entsprechende Maßnahmen entwickeln. Aber auch Genehmigungen einholen und mit Empathie sowie Fingerspitzengefühl und Diskretion das Konzept umsetzen." Dabei gebe es keine Standardlösung, denn jedes Sicherheitsthema müsse individuell auf die jeweilige Situation zugeschnitten und auch im Umsetzungsprozess laufend evaluiert werden.
Höchste Anforderungen werden dabei an die Mitarbeiter gestellt. „Hervorragend ausgebildetes Personal zu bekommen ist schon eine Herausforderung an sich, es ist aber praktisch unerlässlich, selbst aus- und weiterzubilden", weiß Hochegger aus Erfahrung. Prävention werde in Österreich erst allmählich anerkannt und entsprechende Sicherheitsmaßnahmen oft als reiner Kostenfaktor gesehen. „Das subjektive Sicherheitsempfinden muss sensibilisiert und geschärft werden und die Bewusstseinsbildung bezüglich sicherheitsrelevanter Maßnahmen und deren Bedeutung im Anlassfall muss gesteigert werden", ist Hochegger überzeugt. ■

*Selbst bereits hervorragend geschultes Personal wird permanent weitergebildet.*
**Helmut Hochegger, SIM.GUARD**

FOTOS: BEIGESTELLT (2)