

Vertrauen ist gut ...

Digitale Überwachung kann Risiken mindern
und Kosten einsparen

59 Prozent der Energieversorger betroffen

Doch der Wurm fand auch über seinen eigentlichen Zweck hinaus Einsatz: „Laut einer Studie von McAfee waren von Stuxnet 59 Prozent der deutschen Energieversorger betroffen“, so Sicherheitsexperte Bogs. Tückisch dabei ist die Raffinesse des Wurms. Industrielle Prozesse können sabotiert werden, ohne dass es im Kontrollzentrum überhaupt auffällt. Ein Virus wie dieses, eingespeist in das Atomkraftwerk in Lingen, könnte eine ungeahnte Kata-

Überwachung, besonders digitaler Natur, hat bei Unternehmern und Mitarbeitern gleichermaßen einen faden Beigeschmack. Besonders im Discount-Sektor wurden Negativschlagzeilen gemacht. Doch Kameratechnik alleine ist nur ein kleiner Teil der Möglichkeiten, um sich vor potentiellen

Gefahren zu schützen oder gerade im Speditionsbereich ökonomischer agieren zu können. Hier ist das Stichwort Telematik.

Derzeit ist aber ein anderes Thema im medialen Fokus. „Duqu“, ein Computerwurm der neuen Generation, aufwendig entwickelt und nur schwer in Systemen zu entdecken, zeigt auf, dass die digitale Überwachung insbesondere in der Schädlings- und Spionageabwehr gefragt ist. „In der Öffentlichkeit wird dieses Thema zwar behandelt, aber die potentiellen Gefahren werden von vielen Unternehmern nicht in dem Maße wahrgenommen, wie sie existent sind“, resümiert Uwe Bogs, Geschäftsführer der Bogs Consulting aus Osnabrück. Ganz unrecht dürfte er dabei nicht haben. Die Qualität des neuen Duqu-Wurms ist erschreckend hoch. Er arbeitet auf Basis des Stuxnet-Wurms, der im vergangenen Jahr Schlagzeilen machte. Dieser wird in Fachkreisen einer Kooperation zwischen der amerikanischen NSA und dem israelischen Mossad zugeschrieben, mit dem Zweck, die iranische Urananreicherung zu manipulieren. Reell ist das auch gelungen.

strophe auslösen. Dabei muss erwähnt werden, dass sich Stuxnet und auch Duqu nicht über das Internet verbreiten, sondern gezielt in Systeme durch externe Datenträgern eingespeist werden. Aus Spionage kann dabei schnell auch Sabotage werden. Zwar sind die großen Energieversorger eifrig damit beschäftigt, ihre Systeme abzusichern, doch bei Raffinerien und Gasspeichern sind diese Entwicklungen noch nicht flächendeckend zum Tragen gekommen. „Sobald die Möglichkeit besteht, mobile Endgeräte wie Smartphones, Notebook oder TabletPC ins Firmennetzwerk einzuloggen, besteht auch die Gefahr, Daten zu kopieren. Und da hört die Hoheit über Gut oder Böse auf. Die Sicherung des Firmennetzwerkes bedeutet auch immer die Sicherung der Existenz eines Unternehmens“, erklärt Dipl.-Ing. Rainer Hafemann, Geschäftsführer der z3 networks aus Weyhe. Erkennen, Abwehren und Lokalisieren interner Zugriffe sei dabei genauso wichtig wie die Kontrolle externer Angriffe. „Auch wenn man den Anwendern gewisse Rechte nimmt, so dass keine Software installiert werden kann, ist die ▶

IT und Software

SERIE

- 1: **Rechnungswesen und Personalwirtschaft** – Dezember/Januar
- 2: **Supply-Chain-Management** – Februar
- 3: **CRM** – März
- 4: **Business Intelligence** – April
- 5: **Document Management System** – Mai
- 6: **Outsourcing** – Juni
- 7: **Schutz der IT, Datenschutz, Internetschutz** – Juli/August
- 8: **Ihr Unternehmen im WEB 2.0** – September
- 9: **Logistik und Warenwirtschaftssysteme** – Oktober
- 10: **Digitale Überwachung** – November
- 11: **IT in Produktion** – Dezember

z3
NETWORKS
IT-SECURITY • WEB-HOSTING • OPEN SOURCE

Wissen Sie wer täglich Zugriff
auf Ihr Netzwerk hat?

Die Sicherung Ihres Netzwerkes
bedeutet die Sicherung Ihrer Existenz.
Erkennen, abwehren und lokalisieren
interner Angriffe. Schützen Sie sich rechtzeitig.

» z3 networks | Hauptstraße 42 | 28844 Weyhe | Tel. (0421) 8091732 | www.z3networks.de/netzwerkschutz | info@z3networks.de

... wegweisende
Erfahrung
und Kompetenz

Gefahr bestenfalls nur ein bisschen geringer geworden“, so Hafemann weiter. Ein Network Access Control System kann hierbei ein Teilaspekt sein, damit in einem Firmennetzwerk nur Geräte Zugriff auf Ressourcen haben, die hierfür zugelassen sind und einen definierten Sicherheitsstandard besitzen. Das Ganze funktioniert allerdings nur in einer ganzheitlichen Betrachtung der Unternehmensprozesse, fügt Bogs an.

Staatstrojaner nicht das einzige Übel

Auch der sogenannte Staatstrojaner zeigt in der aktuellen Berichterstattung, dass es selbst staatlicherseits Bedrohungen für Netzwerke gibt. Dieses Problem sieht Bogs allerdings nur marginal: „Es hat in den letzten drei Jahren im Rahmen von Ermittlungen, zum Beispiel gegen Terroristen und Drogenhändler, circa 100 Einsätze von Trojanern seitens staatlicher Stellen gegeben. Hier müssen zwar Fragen in Bezug auf den Rechtsrahmen gestellt werden. Die allgemeine Aufregung, als ob alle 83 Millionen Bundesbürger nun mit Staatstrojanern überzogen würden, halte ich aber für übertrieben.“

Imposanter sei da schon das Problem mit der Malware: „Im gleichen Zeitraum hat sich die Anzahl von krimineller Schadsoftware von etwa 15 Millionen auf rund 150 Millionen erhöht. Täglich sind wir alle – das betrifft in Deutschland etwa 56 Millionen Rechner – mehr als 60.000 neu hinzukommenden Trojanern und circa 15.000 anderen Schädlingen wie Viren, Würmern, Dos-Attacken etc. seitens der organisierten Kriminalität ausgesetzt.“ Ein moderner Trojaner nistet sich heute völlig selbstständig und ohne Zutun des Nutzers in jedes System ein: „Der Besuch einer präpa-



rierten Webseite (auch die seriösen sind betroffen), das Anschließen eines USB-Sticks oder der bloße Erhalt einer Mail reichen da zum Beispiel schon aus. Und ein Virens Scanner allein reicht da auch noch lange nicht, um sich vor so etwas zu schützen“, erläutert Computertexperte Bogs.

Cyberkriminalität kostet die Wirtschaft Milliarden

Fast die Hälfte aller Computerbenutzer in Deutschland hat laut BITKOM bereits Schaden durch Cyberkriminalität erlitten. Allein beim Online Banking betrug die Steigerung laut BKA im letzten Jahr 80 Prozent. Von sieben Millionen Nutzern wurden die Zugangsdaten ausspioniert. Der von der Cyberkriminalität verursachte Schaden in der deutschen Wirtschaft erreichte 2010 laut dem BSI (Bundesamt für Sicherheit in der Informationstechnik) eine „hohe zweistellige Milliardensumme“. Die Gefahr sind dabei

oftmals die Mitarbeiter: „Mit scheinbar nützlichen Werkzeugen wie Toolbars, mit Sozialen Netzwerken, über Online-Shops und mit Bonusprogrammen macht sich jeder Nutzer für Fremde freiwillig vollständig gläsern. Weit mehr, als eine Behörde mit einer angeordneten Trojaneraktion herausfinden könnte. Doppelt schlimmer wird es dann, wenn diese Daten dann, wie zum Beispiel bei Sony, Westermann oder Schlecker, wiederum von Kriminellen abgegriffen werden“, so Bogs. Dabei liegt der Schaden nicht zwingend nur im Datenschutz. Es passiert schon mal, dass in einem Unternehmen die gesamten Gehaltszahlungen ins baltische Ausland überwiesen werden. Darüber sprechen wollen betroffene Unternehmen nur selten. „Nicht ohne Grund sprechen wir Sicherheitsleute von der ‚silent Epidemy‘ – es findet statt, aber niemand nimmt es wahr. Die Kriminellen haben kein Interesse an Öffentlichkeit, die Geschädigten schämen sich oder haben Angst vor Imageverlust“, zeigt Bogs die Problematik auf. Hinzu komme das seltsame psychologische Phänomen, dass jeder glaube,

BOGS CONSULTING
unabhängig · effektiv · sicher

Die TITANIC war sicher!?

Überlassen Sie die Sicherheit nicht einfach anderen. Denn als Kapitän sind SIE für ALLES verantwortlich.

Offt wird die IT-Sicherheit allein den Mitarbeitern oder "irgendwelchen" Dienstleistern überlassen - ohne Einblick oder Kontrolle der Unternehmensleitung, die dafür haftet. Wir sorgen für ein Sicherheitsmanagement nach DIN / ISO 27001, dass SIE steuern.

Navigieren Sie zu:

www.bogs-consulting.de

Zur Umschiffung und Abwehr von Gefahren empfehlen wir außerdem:

SOPHOS

F-Secure

PANDA

es könne immer nur die anderen treffen, nie einen selbst. Im Ergebnis fühlt sich die Mehrheit aller Computernutzer in Deutschland daher wohl laut einer Forsa-Umfrage „sicher“ bis „ziemlich sicher“.

Mitarbeiter kontrollieren

Ohne Frage sind die Mitarbeiter gerade in wissenslastigen Betrieben, die eine hohe Patentquote aufweisen, ein großer Verwundungspunkt. Überwachung hat dabei zwar einen negativen Beigeschmack, findet dennoch Rechtfertigung, erläutert Uli Kramer, Sales Manager von InnoTec DATA aus Bad Zwischenahn: „Inventurdifferenzen, Kassendifferenzen, Warenschwund, Tankbetrug an Tankstellen und andere negative betriebliche Begebenheiten rechtfertigen eine offene, oder in speziellen Fällen auch verdeckte Videoüberwachung. Aufgrund einer steigenden Kriminalitätsrate ist es oftmals auch ratsam, sein Privathaus mit einer zumindest leichten Form der Videoüberwachung auszustatten.“

Datenschutzbeauftragter nötig

Doch häufig wird die Videoanlage in Betrieb genommen, ohne die entsprechenden Regelungen des BDSG zu beachten, das den Einsatz einer Videoüberwachung in einem eigenen Paragraphen behandelt (§ 6b BDSG). Demgemäß ist die Verhältnismäßigkeit zwischen dem berechtigten Interesse des Betreibers und den schutzwürdigen Interessen der Betroffenen besonders zu beachten. Diese Abwägung muss im Rahmen einer Vorabkontrolle durch den Datenschutzbeauftragten durchgeführt und dokumentiert werden. Das bedeutet aber, dass bei Einsatz einer Videoüberwachung grundsätzlich ein Datenschutzbeauftragter im Unternehmen zu bestellen ist. Im Übrigen ist es unerheblich, ob es sich um analoge oder digitale Kameras beziehungsweise um Systeme mit oder ohne Aufzeichnungsfunktion handelt. Bereits das Erheben von Daten wird durch das BDSG geregelt und nicht erst eine weitere Verarbeitung sowie die Speicherung von Daten. Verstöße gegen diese Regelung gelten als unbefugte Verarbeitung und können nach § 43 Abs. 1 BDSG mit bis zu 300.000 Euro geahndet werden. Erfahrungsgemäß prüft die Aufsichtsbehörde bei Besuchen die Einhaltung der datenschutzrechtlichen Voraussetzungen der Videoüberwachung besonders genau.

Kosten

Die Kosten für eine Überwachung sind individuell: „Soll die Überwachung nur der Abschreckung dienen, ist dem Unternehmer sicherlich schnell mit einigen Kamera-Dummys geholfen, die aber auch meist in kurzer Zeit als solche entlarvt werden. An dieser Stelle gilt wie so oft der Grundsatz ‚Qualität kostet mehr, zahlt sich aber aus‘. Sicherlich gibt es Systeme bereits ab 200 Euro zu erwerben. Da gerade in diesem sensiblen Umfeld die Zuverlässigkeit und Qualität eine wichtige Rolle spielt, sind diese Systeme für den professionellen Einsatz jedoch nicht geeignet“, erklärt Fachmann Kramer. Je nach Anzahl der Kameras und Größe des Videoservers, der die Daten speichert, ist im Regelfall ein fünf- bis sechsstelliger Betrag als Investition zu kalkulieren. Dazu kommen natürlich monatliche Kosten für Energie, Verschleiß und Auswertung.

Kurze Amortisierungszeit

Korrumpierte oder diebische Mitarbeiter zu entlarven, bewahrt Unternehmer vor mittelfristigen Folgeschäden. Denn sobald ein Mitarbeiter beginnt, sich am Firmeneigentum zu bereichern, und dabei nicht ertappt wird, sinkt seine Hemmschwelle. Die Schadenssummen werden automatisch höher. Der Einsatz von Videoüberwachung gereicht da zum Vorteil: „Häufig reicht allein die Ankündigung des Einsatzes von Videotechnik zur Reduzierung der Unregelmäßigkeiten. Konkrete Zahlen zum Erfolg können wir aufgrund der Vertraulichkeit dieser Daten und Fakten leider nicht nennen. Richtig ist aber, dass Systeme zur Videoüberwachung sich in wenigen Monaten amortisieren können“, erklärt Sicherheitsexperte Kramer.

Telematik

Doch digitale Überwachung trägt nicht nur dazu bei, das Unternehmen vor Schäden zu bewahren. Andersherum kann durch Überwachungsinstrumente wie beispielsweise durch Telematik kosteneffizienter gearbeitet werden. Telematiksysteme finden überall dort Anwendung, wo es einen Fuhrpark gibt. Dies sind zum Beispiel Speditionen im klassischen Sinne. „Immer mehr hält die Telematik aber auch Einzug in andere Betriebe mit Fuhrparks. Pflegedienste, Handwerksunternehmen, Baumaschinenverleiher, Bäcker, etc“, erläutert Uli Kramer die wachsenden Geschäftszweige seines Unternehmens. ▶

RAKERS

Computer und Software



Neue Str. 9 - Lingen
Tel. 0591 - 91233 - 0
rakers-computer.de

sage

Personalwirtschaft

- ⇒ Personalabrechnung
- ⇒ Steuerprüfung - Revision
- ⇒ Personalmanagement
- ⇒ Bewerbermanagement
- ⇒ Bewerbung-Online
- ⇒ Weiterbildungsmanagement
- ⇒ Personalkostenplanung
- ⇒ Reisekosten - Reiseplanung
- ⇒ Zeitmanagement

sp heißt jetzt sage

reflex[®]

plus

Innovative Software-Lösungen

Die vollintegrierte ERP-Lösung
für Ihr Unternehmen!



"Unsere Lösungen setzen Ihre vorhandenen Ressourcen effizient ein, um die Steuerung Ihrer Geschäftsprozesse zu optimieren."

Ralf Ebken, Geschäftsführer

BT

// it-service gmbh

Königstr. 3, 26180 Rastede

www.bt-its.de 04402 98201-40

Telematik ist ein Kunstwort, das sich aus den Begriffen Telekommunikation und Informatik zusammensetzt. Telematik ist also das Mittel der Verknüpfung von Systemen mittels Telekommunikation. Häufig wird die Telematik durch GPS Ortungsfunktionen unterstützt. Eines der verbreitetsten Anwendungsgebiete ist der Einsatz in Fahrzeugen, wie man ihn beispielsweise aus dem Paketdienst kennt. Hier werden über mobile Geräte Informationen zwischen den Fahrzeugen wie zum Beispiel LKW und einer zentralen Anwendung ausgetauscht. Daneben gibt es mit den Bereichen Sicherheit, Gebäudeautomatisierung oder Gesundheit zahlreiche weitere Einsatzumfelder.

Vorteile

Der Einsatz eines solchen Systems kann dabei auch die Qualitätskontrolle verbessern: „Transparenz und totale Sichtbarkeit der Waren und Lieferkette sind möglich. Die Kontrolle von Vorschriften wie zum Beispiel das Erstellen von Kühlkettennachweisen sind weitere interessante Aspekte beim Einsatz von Telematik“, ergänzt Kramer.

Immer wichtiger werde die Sicherung von Warenketten. „Oft verschwinden ganze Ladungen. Diese mögen versichert sein, aber Schaden entsteht auch dadurch, dass Kundenmärkte nicht bedient werden und Fristen nicht eingehalten werden können“, erklärt Kramer. „Ebenfalls ist es so, dass der Fuhrpark sowie die Mitarbeiter der Garant für das Fortbestehen der Firma sind. Alles gehört zu einem großen Körper. Genauso wie man sich von einem Arzt auf seinen aktuellen Gesundheitszustand checken lässt, überprüft man an dieser Stelle sein Firmenkapital auf mögliche Schwachstellen, die es aus unserer Erfahrung heraus immer gibt. Wenn man diese dann kennt, kann man diese entsprechend optimie-

ren. Für den Unternehmer heißt das letzten Endes im Klartext, dass er Geld einspart. Eingespartes Geld bedeutet Wachstum und ein gesünderes Unternehmen“, so Sicherheitsexperte Kramer.

„Geo-Fences“ einrichten

Mobile Objekte wie LKW, PKW oder Baumaschinen lassen sich durch entsprechende Technologien überwachen. „Im Falle der genannten Objekte können beispielsweise sogenannte ‚Geo-Fences‘ eingerichtet werden. Ein Geo-Fence beschreibt ein geografisches Gebiet, das man frei definieren kann. Verlässt ein mobiles Objekt einen definierten Bereich, wird dieses Ereignis gemeldet“, erklärt Kramer die praktische Anwendung. Dieses Verfahren kann natürlich auch auf Personen oder Tieren angewendet werden. In diesem Fall liegt der Vorteil zum Beispiel im einfachen Auffinden von vermissten Personen oder Tieren.

Zukunftsfähigkeit

„Wo Anfangs nur LKW-Flotten mit Telematik ausgerüstet wurden, ist heute der Trend zu erkennen, die Technologie bis auf die unterste Warenebene zum Einsatz zu bringen. Warenpaletten oder Luxusgüter werden hierfür zunehmend mit sehr kleinen Telematikeinheiten ausgestattet. In Verbindung mit speziellen Langzeit-Batterietechnologien und einem intelligenten Power-Management der mobilen Geräte ist es möglich, ‚Objekte‘ über einen Zeitraum von mehreren Jahren wartungsfrei orten zu können“, zeigt Kramer die Richtung des Einsatzes auf.

Daneben sei das Thema der durchgängigen Verfolgung entlang der kompletten Supply Chain (Lieferkette) ein sehr aktuelles: „Derzeit ist die Durchgängigkeit gerade im

Niedriges Sicherheitsniveau Thema muss „Chefsache“ sein



EXPERTENTIPP

Uwe Bogs,
BOGS CONSULTING,
Unternehmensberatung
für IT-Sicherheit und
Informationsschutz,
Osnabrück

Die IT-Sicherheitslage in deutschen Unternehmen ist so kritisch wie nie zuvor. Darin sind sich alle Experten einig. Mit hergebrachten Sicherheitsarchitekturen, die noch vor wenigen Jahren einen wirksamen Schutz boten, kommt heute kein Unternehmen mehr den gestiegenen Bedrohungen und Anforderungen wirksam bei.

Vielmehr sind heute viele verschiedene Maßnahmen organisatorischer und technischer Art notwendig, um ein Unternehmen angemessen vor Schaden zu schützen und dem Datenschutz gerecht zu werden. Oft fehlen aber internes Know-how und/oder die Kapazitäten, viele Systemhäuser besitzen keine fundierten Kenntnisse in der IT-Sicherheit. Das führt zu einem niedrigeren Sicherheitsniveau und zu höheren Kosten.

Angesichts der persönlichen strafrechtlichen Verantwortung und zivilrechtlichen Haftung der Geschäftsführung bei Sicherheitsvorfällen muss die Sicherheit im Unternehmen zwingend eine „Chefsache“ sein. Dabei ist die Beauftragung eines neutralen Sicherheitsspezialisten eine lohnende Investition. Durch zusätzlichen Sachverstand von Spezialisten können existenzbedrohende Risiken gemindert und teure Schäden vermieden werden.

Luft- und Seetransport noch nicht gegeben“, so Uli Kramer von der InnoTec DATA aus Bad Zwischenahn. ■



Produktionsleitstände
Etikettierung • Scanning
RFID • Lager • MDE
Kommissionierung
Transport-Steuerung
SCADA • Zeiterfassung
Kamera-Überwachung
BDE • Bildverarbeitung
Chargen-Rückverfolgung

Vernetzen.



Synchronisieren.



Automatisieren.



Computer und Software für die Industrie.



Telematik in der Praxis

Kombi Fracht-Geschäftsführer Hans Risch von Technik überzeugt

WEM: Herr Risch, wo finden Telematik-Systeme bei Ihnen Anwendung und seit wann nutzen Sie die Technik?

Hans Risch: Die Telematik-Systeme finden in allen unseren 140 Lkw Anwendung. Seit Ende 2009 arbeiten wir mit einem speziell entwickelten System.

WEM: Welchen Vorteil sehen Sie in dieser Technik?

Hans Risch: Vorteile dieser Technik sind Transparenz im Fuhrpark über Standort, Kraftstoffverbrauch, Geschwindigkeit, Lenkzeiten und das Bremsverhalten. Darüber hinaus ermöglicht das System eine Kommunikation per GPS.

WEM: Wie sieht die Fehleranfälligkeit in der Praxis aus?

Hans Risch: In den Anfängen war die Fehleranfälligkeit relativ hoch. Dies ist größtenteils zurückzuführen auf technische Pannen beziehungsweise Bedienfehler.

WEM: Lassen sich durch Telematik konkrete Einsparungen erzielen?

Hans Risch: Es lassen sich auf jeden Fall Einsparungen erzielen, die sich allerdings zur Zeit noch nicht kostenrelevant auswirken, da die Entwicklungen noch nicht abgeschlossen sind. Unsere Erwartungshaltung liegt hier bei circa drei Prozent der Fuhrparkkosten.

WEM: Wie hoch waren bei Ihnen die Investition für ein Telematik-System?



Hans Risch, geschäftsführenden Gesellschafter der Kombi Fracht GmbH, Groß Ippener

Hans Risch: Pro Lkw liegt die Investition für ein System bei etwa 800 Euro im Jahr.

WEM: Und wie nehmen Ihre Fahrer die Systeme auf?

Hans Risch: Die Fahrer nehmen die Systeme sehr unterschiedlich auf. Wir müssen viele Schulungen vornehmen. Die größte Blockade ist das Gefühl der Überwachung, weil wir seit einiger Zeit die Fahrerkarten täglich auslesen lassen. Hier hilft nur ständige Information.

WEM: Wie kompliziert ist die Implementierung im laufenden Betrieb?

Hans Risch: Die Implementierung in den laufenden Betrieb ist kontinuierlich und in der Praxis mittlerweile sehr gut. Die Schulungen für Fahrer und Auswerter sind notwendig und müssen regelmäßig wiederholt werden. ■

WEM: Vielen Dank für das Gespräch!

Anzeige

IT ist unsere Leidenschaft!

OMG...makes IT work!

Der Kunde hat höchste Priorität – Diese Maxime verfolgt die Geschäftsführung von OMG schon seit der Gründung 1997. Nicht nur als Systemintegrator, sondern auch als IT-Dienstleister hat sich so das Unternehmen einen Namen im gesamten Raum Weser-Ems gemacht. Inzwischen agiert die Firma als Bindeglied zwischen Kommunen, Unternehmen und ihren weltweiten Handels- und Kontaktpartnern.

Die Leistungen, die das Unternehmen bereitstellt, basieren grundlegend auf den Bereichen der:

- Server- und Clientsysteme,
- Internet- und Netzwerkservices,
- Festverbindungen und VPN,
- Printing-Lösungen
- Telekommunikationssysteme

Auch in den Bereichen Webservice, Webauftritte, professionelles eCommerce oder Online-/Offline-Marketing stellt die OMG-Gruppe eine Fülle von Leistungen bereit, aus der sich der Kunde nach Bedarf bedienen kann. Zusammen mit den zwei Tochtergesellschaften – der ActiView und der emsnet GmbH – ist das Unternehmen in der Lage, individuelle IT-Landschaften ganz nach den Wünschen seiner Kunden zu entwickeln und zu betreiben. Die Kunden bekommen somit die gesamte Bandbreite der IT aus einer Hand.

Thilko Cullmann: Geschäftsführer der OMG.de GmbH

Der entscheidende Vorteil hierbei: Es gibt einen Ansprechpartner für alle Belange.

Zur Optimierung des Workflows arbeitet die Geschäftsführung eng mit dem Außendienst zusammen, als Garant für eine gezieltere Koordination und schnellere Umsetzung von Projekten. Der stetige Lernprozess, der hierbei das Unternehmen begleitet, dient als Erfahrungspool für die jeweiligen Kunden des Unternehmens. Diese können sich zudem nach Abschluss von Projekten auf ein umfassendes Supportpaket verlassen. Von der Instandhaltung bis zum Support vor Ort, die OMG unterstützt aktiv den Workflow seiner Kunden. ■



KONTAKT



OMG.de GmbH
Tannenbergstraße 29 · 26603 Aurich
Tel: 04941 604450 · info@omg.de

omg.de
www.omg.de