

**Multifocal-
Kameras:**
Schutzkonzept
für Neapels
Flughafen

S. 11

Datensicherheit
Übersicht durch
Berechtigungs-
management

S. 5

**Referenz-
projekte der
Sicherheit**

Mitherausgeber



Referenzen schaffen Vertrauen

Die beste Werbung, sagt man, sei die Zufriedenheit der Kunden. Das gilt für Projekte im Bereich Sicherheit ganz besonders. Denn hier geht es um Vertrauen. Und da hören Anwender besonders gern auf Kollegen, die gute Erfahrungen gemacht haben.

Der SecuMedia Verlag - seit 35 Jahren Mittler zwischen Anbietern und Anwendern von Sicherheit - bietet darum künftig regelmäßig eine Möglichkeit, interessante Projekte darzustellen, aus denen sich zweierlei Lehren ziehen lassen:

Erstens: Wer als Anbieter die Ausschreibung für ein prestigeträchtiges Projekt gewinnt, ist besonders gut, denn er hat sich in der Regel gegen viele interessierte Mitbewerber durchgesetzt.

Und zweitens stecken in jedem Fall Erfahrungen von Anwendern, die auch für andere Bedarfsträger nützlich sein können.

- Ein Flughafen verlangt von seiner neuen Videoüberwachungstechnik den totalen Überblick und zugleich höchste Auflösung.
- Wie und mit welchem Partner gewährleistet ein internationaler Handels- und Schifffahrtskonzern mit 2700 Nutzern in 40 Ländern sein existenziell wichtiges Berechtigungsmanagement?
- Eine Großstadt sucht ein System von Netzwerkkameras zur Verkehrssteuerung.
- Wem vertrauen große Hotels das Papier mit den sensiblen Daten der Gäste zur Vernichtung an?
- Welcher Anbieter kann eine umfassende Sicherheitslösung mit einer Brandmeldeanlage, Einbruchmeldeanlage, Videoüberwachung sowie Zutrittskontrolle für ein Industrieobjekt mit Hochregallager realisieren?
- Der Verlagskonzern Axel Springer sucht eine neue Lösung für komplexe Anforderungen an die Datensicherheit für 10000 Clients. Wer macht das Rennen um sein Vertrauen?
- Ein Sportartikelkonzern will die beste Lösung für Brandschutz und Sprachalarmierung in seiner innovativen Konzernzentrale.
- Und mit wem hat ein wichtiger Verband der Kreditwirtschaft seine neue biometrische Zeit- und Zutrittskontrolle realisiert?



Lauter faszinierende Geschichten, finde ich.

Ich wünsche Ihnen spannende Lektüre und eine glückliche Hand bei der Auswahl Ihres nächsten Projektpartners!

Ihr

Peter Hohl



Berechtigungsmanagement

Internationale Handelsgesellschaft baut auf 8MAN

Daten müssen sicher verwaltet und verwahrt werden. Hierfür vertraut die MPC Ferrostaal IT Services GmbH auf die Leistungen der Berechtigungsmanagement-Technologie 8MAN.

Seite 5

Datenschutz

Auf der sicheren Seite

Datensicherheit muss gelebt werden - Entscheidungen im Einkauf tragen einen entscheidenden Teil dazu bei. Die Hotels der gehobenen Klasse The Ritz-Carlton, Berlin und Berlin Marriott Hotel haben beim Kauf von Aktenvernichtern auf die Produkte von HSM gesetzt.

Seite 8

Malware-Abwehr

Kaspersky Lab liefert IT-Sicherheitslösung an Axel Springer

Um die IT-Infrastruktur von Axel Springer professionell vor Malware und sonstigen unerwünschten Eindringlingen zu schützen, stellt das Unternehmen seine IT-Security mit der Lösung von Kaspersky Lab neu auf.

Seite 10

Panomera-Kamera

Mehr Sicherheit am Flughafen Neapel

Der internationale Flughafen von Neapel, der Aeroporto di Napoli Capodichino, wird jährlich von sechs Millionen Fluggästen genutzt. Für mehr Sicherheit kommt mit dem Multifocal-Sensorsystem Panomera von Dallmeier neueste Kameratechnologie zum Einsatz.

Seite 11

Brandschutz

ESSER-Technik für das PumaVision Headquarter

Technik für Brandschutz und Sprachalarmierung der Marke ESSER schützen die neue Firmenzentrale des Sportartikelherstellers PUMA in Herzogenaurach.

Seite 12

IP-Video

Intelligente Steuerung des Stadtverkehrs

Die Stadt Maastricht will ihren Verkehrsfluss intelligenter und umweltschonender steuern. Dafür hat sie auf Basis eines Glasfasernetzes ein zentral verwaltetes System aus Netzwerk-Kameras des IP-Video-Spezialisten Axis Communications implementiert.

Seite 15

Gebäudeschutz

Ganzheitliches Sicherheitskonzept für ein Industriegebäude

Für das Unternehmen Betzold Lehrmittelverlag & Schulbedarf erstellte und realisierte Telenot eine umfassende Sicherheitslösung mit einer Brandmeldeanlage, Einbruchmeldeanlage, Videoüberwachung sowie Zutrittskontrolle.

Seite 16

Zutritt und Zeiterfassung

Sparkassenverband Bayern setzt auf Biometrie

Der Sparkassenverband Bayern steuert fortan mithilfe einer Biometrie-Lösung Zutritt und Zeiterfassung. Neben gesteigerter Betriebssicherheit und präziseren Workforce-Management-Prozessen konnte zudem der Administrationsaufwand reduziert werden.

Seite 18

Impressum

SecuMedia Verlags-GmbH

Postanschrift: Postfach 1234, 55205 Ingelheim (DE)
Hausanschrift: Lise-Meitner-Straße 4, 55435 Gau-Algesheim (DE)
Telefon +49 6725 9304-0, Fax +49 6725 5994
E-Mail: info@secumedia.de, Web: www.secumedia.de

Beteiligungsverhältnisse (Angabe gem. § 9, Abs. 4 Landesmedienges. RLP): Gesellschafter zu je 1/6 sind Gerlinde Hohl, Klaus-Peter Hohl, Peter Hohl (GF), Veronika Laufersweiler, Nina Malchus (GF), Steffi Petersen

Handelsregister AG Mainz HRB 22282

Herausgeber: Peter Hohl

Anzeigenleitung: Birgit Eckert, Andreas Hey
Tel. +49 6725 9304-20, E-Mail: anzeigenleitung@secumedia.de

Satz: BlackArt Werbestudio,
Stromberger Straße 47, 55413 Weiler bei Bingen

Druck: Bonifatius GmbH
Karl-Schurz-Straße 26, 33100 Paderborn

Bildnachweis Titelbild und S. 4: © CHW - Fotolia.com

Alle Rechte vorbehalten, auch die des auszugsweisen Nachdrucks, der Reproduktion durch Fotokopie, Mikrofilm und andere Verfahren, der Speicherung und Auswertung für Datenbanken und ähnliche Einrichtungen.



Datensicherheit

Internationale Handelsgesellschaft baut auf 8MAN

Die MPC Ferrostaal IT Services GmbH betreut alle Aufgaben der Informations- und Telekommunikationstechnik der traditionsreichen MPC Gruppe. Die Anfänge des Hamburger Dienstleistungs- und Handelskonzerns reichen bis ins Jahr 1846 zurück. Heute ist er unter anderem in Kapitalanlagen sowie in den Bereichen Schiffbau und Schifffahrt erfolgreich aktiv. Mit MPC Ferrostaal IT Services hat die MPC Gruppe ein solides Fundament für die Unternehmens-IT geschaffen, um Daten zu verwalten und sicher zu verwahren. Hierfür vertraut sie auf die Leistungen der Berechtigungsmanagement-Technologie 8MAN.

Von Stephan Brack, Berlin

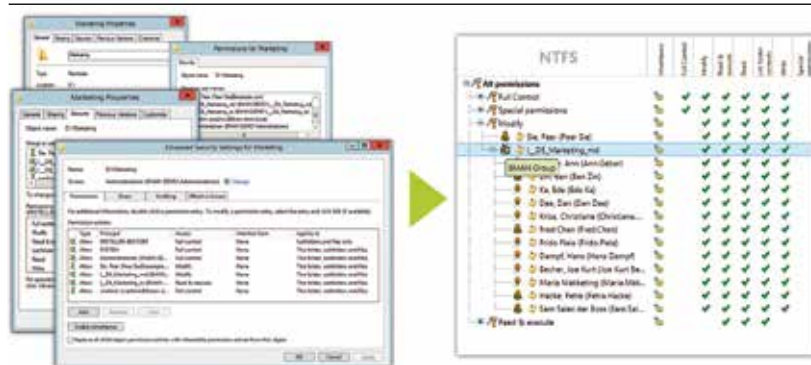
Als international agierender Konzern ist Datensicherheit für die MPC Gruppe von entscheidender Bedeutung. Ist diese nicht garantiert, könnten Verluste oder der Missbrauch von Daten entscheidende Folgen haben und beispielsweise empfindlich hohe Schadensersatzanforderungen nach sich ziehen. Zuständig für den Schutz der Daten ist die eigens gegründete MPC Ferrostaal IT Services GmbH. Als internes IT-Dienstleistungsunternehmen sichert sie sämtliche Daten vor äußeren und internen Angriffen ab. Die dynamische Entwicklung der MPC Gruppe in den vergangenen Jahren stellte auch die IT vor wachsende Herausforderungen. Unter dem Dach der MPC Holding finden sich heute der Asset- und Investmentmanager MPC Capital AG sowie verschiedene Unternehmen der Schifffahrtsbranche, die zuletzt Zuwachs durch die Übernahme der Reederei Ahrenkiel bekommen haben. Neben der MPC Capital AG gehören damit heute zum Beispiel

die MPC Marine GmbH oder die Ahrenkiel Steamship GmbH zur Unternehmensgruppe. In allen Leistungsspektren der MPC Gruppe müssen wertvolle Daten und kostbare Informationen verwaltet und gesichert werden.

Schutz der Unternehmensdaten

Diese unterschiedlichen Unternehmens- und Anspruchsgruppen, inklusive hoher Sach- und Vermögenswerte aus den Händen Dritter, fordern von der MPC Ferrostaal IT

Services einen lückenlosen Überblick über Verbleib und Verwaltung der Unternehmensdaten. Nur so kann der langfristige Unternehmenserfolg garantiert werden. Dennoch werden keine externen Dienstleister in das Datenmanagement mit einbezogen. Das IT-Dienstleistungsunternehmen sichert selbst sämtliche international benötigten digitalen Informationen sowohl vor äußeren wie auch vor inneren Diebstahl- und Missbrauchsversuchen ab und minimiert damit die Zugriffsmöglichkeiten – und somit auch die potenziellen Gefahren – von außen.



Berechtigungsmanagement-Technologie führt vom Datendurch-einander zum geordneten Überblick. Bilder: Protected Networks GmbH

Auch hochkomplexe Berechtigungsstrukturen müssen zu jeder Zeit schnell erfasst werden können.



Komplexe Voraussetzungen

Doch allein die Struktur der Holding stellt MPC Ferrostaal IT Services schon vor die ersten Herausforderungen: Mehr als 2700 Nutzer aus 40 Ländern müssen täglich je nach Bedarf auf Daten zugreifen und diese bearbeiten können. Es ist also ein stabiles System gefordert, das komplett durch die MPC Ferrostaal IT Services verwaltet wird. Sie kümmert sich um die Installation, das Management und die Instandhaltung der genutzten Computer, Notebooks und auch der Mobiltelefone. Verschiedene Abwehrmaßnahmen sorgen dafür, dass auch die eingesetzte Standardsoftware vor äußeren Zugriffen sicher ist und minimieren Datenverluste oder schützen vor deren Diebstahl und Missbrauch, zum Beispiel durch Hackerangriffe.

Solche strukturellen Voraussetzungen an einen effizienten Ablauf der IT verlangten bisher einen großen Aufwand. Ein Grund dafür war, dass MPC Ferrostaal IT Services vor der Einführung der Berechtigungsmanagement-Technologie 8MAN bei der Zusammenführung von IT-Strukturen und der Auflösung bestehender Datenorganisationen auf manuelle Sortierung vertraute.

Zuerst wurde der Status quo der Daten- und Zugriffsstruktur innerhalb der beteiligten Unternehmen festgestellt. Ein automatisierter Überblick war nicht möglich. Von Hand mussten vergangene Datenzugriffe sortiert und in Zweifelsfällen ehemalige IT-Administratoren befragt werden.

Schnelle und einfache Lösung

Ein Aufwand, dessen sich der IT-Dienstleister bewusst war: „Bislang gab es bei uns immer wieder Ansätze für ein transparentes Berechtigungssystem auf den Fileservern, mit denen wir allerdings nie zufrieden waren. Daher suchten wir eine Lösung, die schnell und einfach die grundlegenden Fragen, wer hat welche Berechtigung, wer hat Berechtigungen angefragt und wie ist die Berechtigungsstruktur aufgebaut, beantwortet und entsprechende Reports erstellt“, so John-Asmus Burmester, Geschäftsführer der MPC Ferrostaal IT Services. Denn genau solche Fehler im Berechtigungsmanagement bedeuten Schwachstellen. Dabei können sich IT-Administratoren bereits durch wenige Fragen Überblick verschaffen:

— Wer hat wann Zugriff auf welche Daten im Unternehmen?

— Wer hat darum gebeten, Zugriff auf bestimmte Daten zu erhalten?

— Wann hat er diesen Zugriff von wem bekommen?

— Wann müssen ihm diese Rechte wieder entzogen werden?

Durch die Antworten auf diese Fragen erhält der IT-Administrator eine Struktur, die ihm zeigt, an welchen Stellen unberechtigte Zugriffe auf Daten überhaupt möglich wären beziehungsweise wo die bestehende Berechtigungsstruktur nachjustiert werden sollte. Diese Fragen nicht zu stellen, kann fatale Folgen haben: Personen erhalten das Recht auf Daten zugreifen zu können, mit denen sie nicht arbeiten müssen und damit die Möglichkeit, diese zu missbrauchen. Manche Mitarbeiter sammeln Zugriffsrechte auf Daten im Laufe der Zeit, die ihnen oft gar nicht mehr entzogen werden. Reports über Datenzugriffe durchzuführen und überhaupt einen Status quo durch eine aussagefähige Datenstruktur ermöglichen zu können, bedeutet enorm großen Aufwand oder ist gar nicht erst möglich. Datenmissbrauch oder verlorenen Dokumenten sind so nicht nur Tür und Tor geöffnet – ihr Verbleib ist auch nicht mehr nachvollziehbar.

Burmester ist zufrieden damit, die Problematik mit der Berechtigungsmanagement-Technologie 8MAN aufgelöst zu haben: „8MAN schafft diese gewünschte transparente und standardisierte Umgebung. Jetzt ist es uns auch problemlos möglich, das Sicherheitsproblem der „Leichen unstrukturierter Berechtigungen“ aus dem Weg zu räumen.“ Gerade beim Wiederaufbau von Datenstrukturen sind solche Berechtigungsleichen an der Tagesordnung. Viele Firmen basieren auf einer hochkomplexen IT-Struktur, die zum Beispiel doppelt vergebene Zugriffsberechtigungen begünstigt. Bisher kostete schon das Feststellen des Status quo sehr viel Zeit, deren Länge bei komplexen Strukturen das vorab festgelegte Maß bei weitem überschreitet.

Berechtigungsmanagement automatisiert die Ordnung

MPC Ferrostaal IT Services führte bisher fünf IT-Konsolidierungsaufträge mithilfe von 8MAN durch. Das Programm wird im

übergreifenden Active Directory für die Windows-Server der einzelnen Unternehmen der Gruppe sowie für die zentralen Dateiserver für unternehmensübergreifende Projekte innerhalb der Firmengruppe eingesetzt. Die Verantwortlichen betonen vor allem, dass der Status quo dank der Digitalisierung sehr viel einfacher festgestellt werden konnte. Auch in anderen Bereichen konnte der Aufwand verringert werden, da komplexe Strukturen vorab aufgelöst wurden. Etwa halb so lange braucht es nun, um IT-Strukturen von Unternehmen auf internationaler Ebene zusammenzuführen.

Björn Pursche, Teamleiter MPC Ferrostaal IT Benutzerservice: „Was uns nachhaltig überzeugt hat, war der pragmatische Ansatz von 8MAN für ein ganzheitliches und sicheres System.“ Mit 8MAN benötigen sie 30 Minuten weniger pro Berechtigungsvergabe. Mitarbeiter konnten in 15 bis 30 Minuten eingearbeitet werden. Auch die finale Implementierung war weniger zeitintensiv und bereits nach eineinhalb Tagen abgeschlossen.

Überblick über alle Systemlandschaften

8MAN ermöglicht die Visualisierung von Berechtigungen, ist für Administration und Delegation verantwortlich und sorgt für das gesetzlich relevante Dokumentieren aller Zugriffsrechte. Die Technologie zeigt die Berechtigungen aller Nutzer auf File- und Exchange Servern, im Active Directory, auf SharePoint und VMware vSphere an. Innerhalb weniger Stunden kann 8MAN in nahezu jede Microsoft Systemlandschaft und in VMware vSphere implementiert werden und liefert demnächst auch aus SAP-Systemen sofort Ergebnisse. Auch spontane Abrufe von Reporten werden so möglich. Externe Systeme lassen sich auch über Zeitgrenzen hinweg schnell und einfach einbauen. ■

Kontakt:
Protected Networks GmbH
Alt-Moabit 73
10555 Berlin
www.8man.com

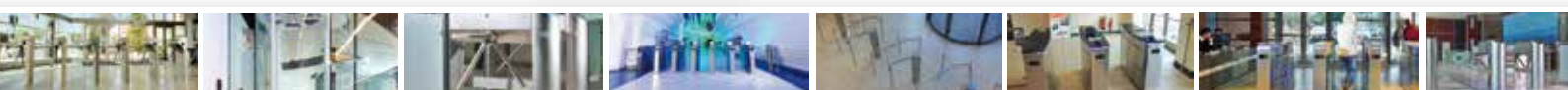
Werra Entrance Control
- effizient und sicher!

www.werra.de

Personenvereinzlung mit Werra Entrance Control

- elegante Anlagen für kontrolliert reibungslose Zutritte

Das neue Werra Entrance Control Portfolio der Perimeter Protection Group umfasst unterschiedliche Anlagen zur Regulierung, Steuerung oder strikten Vereinzlung von Personen. Darüber hinaus bietet Werra Entrance Control Lösungen, die der Fluchtwegverordnung gerecht werden. Von der Anbindung an Ihre Zutrittskontrolle oder Ihr Gebäudemanagement bis hin zu ganzheitlichen Lösungen erfüllen die Werra Entrance Control Vereinzlungsanlagen Ihre Anforderungen an eine geregelte Personenkontrolle.





Marriott Hotel in Berlin am Potsdamer Platz: gehobenes Angebot an prominenter Adresse.

Aktenvernichter von HSM

Auf der sicheren Seite

Datensicherheit muss gelebt werden – Entscheidungen im Einkauf tragen einen entscheidenden Teil dazu bei. Die Hotels der gehobenen Klasse The Ritz-Carlton, Berlin und Berlin Marriott Hotel am Potsdamer Platz haben daher beim Kauf von Aktenvernichtern auf die Erfahrungen und das Know-how ihrer Lieferanten Horn&Görwitz sowie HSM gesetzt.

Von Stefan Syndikus, Wiesbaden

Wie können wir die Arbeit in unseren Büros noch effizienter, nachhaltiger machen? Auch in einem Hotelbetrieb macht der sichere Umgang mit Informationen einen wichtigen Teil der täglichen Arbeit aus. Effizienz ist eine wesentliche Voraussetzung für den wirtschaftlichen Erfolg: Reservierungen, Angebote, Stornierungen, Rechnungen und Schriftverkehr mit Lieferanten. Hunderte Papiere werden von den Mitarbeitern täglich erstellt, gelesen, ausgedruckt – und nach ihrer Verwendung in den Papierkorb geworfen. All diese Papiere enthalten jedoch auch sensible Informationen: etwa Kundennamen, Kreditkartendaten oder Preise. Solche Daten müssen vor dem Zugriff Fremder geschützt werden. Nicht zuletzt fordern dies die gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes. Unternehmen müssen Datenträger so vernichten, dass die Reproduktion je nach Inhalt unmöglich oder weitestgehend erschwert wird.

„Überviele Jahre hinweg hatten wir mit einem speziellen Dienstleister zusammengearbeitet, der für uns die Vernichtung und Entsorgung unserer Papiere übernommen hatte“, erklärt der Cheftechniker vom Berlin

Marriott Hotel, Claudio Trübenbach. Die Mitarbeiter sammelten alle Papierdokumente in Tonnen, die der Dienstleister bereitgestellt hatte. Sie wurden auch von ihm abgeholt und in einer eigenen Schredderanlage vernichtet, sodass die Informationen nicht wiederhergestellt werden konnten. „Doch diese Organisation hat uns in der Praxis Aufwand verursacht“, sagt der technische Leiter. So mussten die Restpapiere in den Räumen der Verwaltung zwischengelagert werden, die Fahrer waren nicht immer die gleichen, sodass

sich neue Mitarbeiter immer wieder durchfragen mussten, um den Weg zu den Papiertonnen zu finden, was wiederum Sicherheitsfragen aufwarf. Es gab mithin einige Gründe, über eine neue Organisation dieses Prozesses nachzudenken.

Der Hersteller von Aktenvernichtern HSM und der langjährige Lieferant Horn&Görwitz rieten dem Hotel zu einem anderen Weg: Und zwar Aktenvernichter selbst zu kaufen und direkt dort aufzustellen, wo das Altpapier anfällt – also in den Büroetagen – und dabei sogar noch Kosten zu sparen. Statt einen Spezialisten zu beauftragen, werden nun die Papiere selbst geschreddert. Holger Müller, Gebietsverkaufsleiter von HSM, hat mit dem technischen Leiter der Hotels ein Lastenheft erstellt und die Anforderungen an die Aktenvernichtung aufgenommen: Papiervolumen, Papierstärke, Sicherheitsstufe nach Schutzklasse und -stufe entsprechend der neuen DIN 66399, erforderliches Auffangvolumen. „So ist dann die Wahl auf das leistungsstärkste Wechselstromgerät aus unserem Portfolio gefallen, den ‚Securio P44‘, der neben Papier auch optische, magnetische und elektronische Datenträger vernichten



Der Aktenvernichter „HSM SECURIO P44“ vernichtet neben Papier auch optische, magnetische und elektronische Datenträger.

kann“, erklärt Maximilian Görwitz vom Lieferanten Horn&Görwitz.

Sechs Aktenvernichter dieser Reihe verrichten im The Ritz-Carlton, Berlin und Berlin Marriott Hotel in den Druckerräumen nun ihren Dienst. Auf jedem Gang im Verwaltungstrakt – und an den Rezeptionen – steht ein Gerät gut erreichbar für die Mitarbeiter bereit. Wird der Auffangbehälter des Aktenvernichters voll, muss ihn der Mitarbeiter in den Presscontainer der Berliner Entsorgungsbetriebe entleeren. Die Bereitstellung dieses Containers und seine Abholung sind für das Hotel kostenlos. Die Entsorgungsbetriebe der Stadt Berlin führen das Papier später unter dem Aktionsmotto „Papier sammeln macht Schule!“ der Wiederverwendung zu und lassen daraus Schulhefte herstellen.

Die Umstellung auf das Schreddern im eigenen Haus musste zugleich hohe Anforderungen an die Nachhaltigkeit erfüllen, denn das Berlin Marriott Hotel strebt die Zertifizierung nach ISO 14001 (Umweltmanagement) an. Unter dem Motto „Marriott going Green“ setzt das Hotel in sämtlichen Bereichen auf moderne Technik, Energieeinsparung, Abfallvermeidung und Recycling.



Claudio Trübenbach, Cheftechniker des Marriott, Maximilian Görwitz von Horn&Görwitz und Holger Müller (v.l.n.r.), der Gebietsverkaufsleiter von HSM: Datenschutzauflagen des Gesetzes erfüllen und zugleich kostengünstig Akten vernichten.

Inzwischen wurde die Beleuchtung auf LED und Energiesparleuchten umgestellt. Der größte Papierverbraucher in der Hotel-Verwaltung, die Abteilung „Reaktiver Verkauf“, ist zu einem „papierlosen Büro“ geworden. Sämtliche Häuser der Marriott-Gruppe weltweit verwenden ausschließlich Papier, Flipcharts und Blöcke aus zertifizierter Forstwirtschaft, selbst die Stifte bestehen aus wiederverwertbaren und biologisch abbaubaren Materialien. Und die neuen Aktenvernichter? Sie arbeiten

energiesparend, bei Nichtbenutzung schalten sie nach zwei Minuten automatisch in einen „Schlafmodus“ und nach einer Stunde komplett ab, sodass sie dann gar keinen Strom mehr verbrauchen. ■

Kontakt:
HSM GmbH + Co. KG
Austraße 1-9
88699 Frickingen
Tel. +49 7554 2100-0
Internet: www.hsm.eu
E-Mail: info@hsm.eu

Gratis: Online-Lexikon, News und Hintergrundwissen

Gratis: Die Plattform

SecuPedia ist ein Online-Lexikon, das mit mehr als 2000 Sicherheitsbegriffen das gesamte Wissen zum Thema Sicherheit und IT-Sicherheit sammelt und gratis zur Verfügung stellt. Mehr als 100 Autoren bringen ihr Fachwissen auf dieser Plattform ein.

Grundlage ist das seit mehr als 25 Jahren bekannte „Sicherheits-Jahrbuch“, das nun als Onlineversion freien Zugriff erlaubt. Alle Artikel sind redaktionell geprüft.

Gratis: Der Newsletter

Monatliche Infos rund um die SecuPedia Plattform und das Thema Sicherheit: Kurz-Nachrichten aus der Branche und redaktionell hochwertige Artikel. Gratis-Angebote, Produkt-Proben, Verlosungen und Einladungen zu Events.

Anmeldung unter: www.secumedia.com/newsletter-secupedia

Sponsored by





Geschützt vernetzt

Kaspersky Lab liefert IT-Sicherheitslösung an Axel Springer

Als eines der größten Medienhäuser Europas hat Axel Springer ein klares Ziel: der führende digitale Verlag zu werden. Im Zeitalter der Digitalisierung und der Kommunikation über das Internet steigen allerdings die Gefahren aus dem Netz. Um die IT-Infrastruktur von Axel Springer professionell vor Malware und sonstigen unerwünschten Eindringlingen zu schützen, stellt das Unternehmen seine IT-Security mit der Lösung von Kaspersky Lab neu auf.

Stefan Rojacher, Ingolstadt

Im Jahr 1946 wurde der Verlag von Axel Springer und seinem Vater Hinrich in Hamburg gegründet. Seit dieser Zeit hat sich das Unternehmen kontinuierlich vergrößert. Mit 12800 Mitarbeitern, über 230 Online-Angeboten, 300 Apps und 220 Printtiteln ist der Konzern heute maßgeblich an der Gestaltung der internationalen Medienlandschaft beteiligt. Weltweit ist die Axel Springer SE mit Tochtergesellschaften, Joint Ventures und Lizenzen in mehr als 40 Ländern tätig.

Als Medienunternehmen dieser Größe besitzt Axel Springer ein riesiges Netzwerk an sensiblen Daten und Informationen, die nicht in falsche Hände geraten dürfen. Entsprechend hoch ist natürlich der Stellenwert von IT-Sicherheit.

Aktuell besteht die IT-Infrastruktur der Axel Springer SE aus rund 10000 Clients, davon befinden sich etwa 6000 Clients am Konzernsitz in Berlin und 3000 Clients im Verlagshaus in Hamburg. Alle Anwender arbeiten mit Apple-Rechnern, die teilweise mit Microsoft-Windows-Betriebssystem laufen. Hier ist also eine Sicherheitslösung wichtig, welche die heterogene IT-Infrastruktur beider Standorte überwachen und koordinieren kann.

Kaspersky punktet bei OS X

Bisher nutzte das Verlagshaus für die Absicherung der Clients eine andere Security-Lösung. Allerdings waren hier Performance und Erfolgsquote nicht mehr zufriedenstellend. „Bei der Suche einer Alternative waren uns Benutzerfreundlichkeit für den Endanwender, Performance und Erfolgsquote bei Virenerkennung und -beseitigung besonders wichtig“, erklärt Harald Monihart, Teamleitung Client DevOps bei Axel Springer SE. Vor allem in den OS X-bezogenen, internen Tests konnte Kaspersky punkten und so die Konkurrenz aus dem Rennen werfen.

Nach einer etwa achtwöchigen Testphase mit einem Demosetup-Server und 25 OS X-Clients wurde der Produktivserver im Februar 2014 installiert. Innerhalb von sechs Wochen fand der Rollout von 4500 OS X-Clients statt. Die Fehlerquote war mit 1,17 Prozent sehr gering und die Installation erfolgte vollkommen im Hintergrund, ohne dass Arbeitsprozesse durch einen Neustart oder Interaktionen mit den Anwendern gestört wurden. Lediglich ein Workshop-Tag war notwendig, um IT-Administrator und Anwender in das System einzuweisen. Diese Aufgabe übernahm der

Kaspersky Business-Partner save IT first GbR.

Im Juli 2014 fand der Rollout wie geplant auch auf den Windows-Clients statt. Heute werden 34 Standorte, die hauptsächlich in Deutschland liegen, durch die zentrale Verwaltung mit dem Kaspersky Security Center 10 betreut.

Fazit

Nach dem Wechsel zu Kaspersky sind nun weitaus mehr Clients mit aktuellen Datenbanken versorgt und es kommt deutlich seltener zu Performancestörungen. Außerdem arbeitet der Anti-Virus-Schutz wie gewünscht so unauffällig, dass Anwender durch ihn nicht gestört werden. Für Harald Monihart ist die Umstellung sehr positiv verlaufen: „Wir schätzen das ausgeprägte Fachwissen und die hohe Zuverlässigkeit der Kaspersky Lab-Mitarbeiter. Insgesamt gesehen, sind wir überaus zufrieden mit der freundlichen Zusammenarbeit.“ ■

Kontakt:

*Kaspersky Labs GmbH
Despag-Straße 3, D-85055 Ingolstadt
salesdach@kaspersky.de
www.kaspersky.de*

Dallmeier:

Panomera-Kameras sorgen für mehr Sicherheit am Flughafen Neapel

Der internationale Flughafen von Neapel, der Aeroporto di Napoli Capodichino, wird jährlich von sechs Millionen Fluggästen genutzt. Für mehr Sicherheit sowohl auf dem Rollfeld als auch auf dem Flughafen-Vorplatz kommt mit dem Multifocal-Sensorsystem Panomera von Dallmeier neueste Kameratechnologie zum Einsatz.

Von Roland Meier, Regensburg

Der Aeroporto di Napoli Capodichino bietet Verbindungen zu 50 nationalen und internationalen Zielflughäfen. Der Flughafen wird von der GESAC SPA, die zur Gruppe F2I Aeroporti gehört, betrieben. Die GESAC ist stets bestrebt, effiziente Lösungen zu finden und die Anforderungen der Passagiere und des Flughafenpersonals bestmöglich zu erfüllen. Dies gilt insbesondere auch für die Punkte Personensicherheit und Umweltschutz.

Innovative Multifocal-Sensortechnologie

Auf der Messe „Sicurezza“ 2010 in Mailand haben die Sicherheitsverantwortlichen der GESAC zum ersten Mal das Multifocal-Sensorsystem Panomera von Dallmeier gesehen und waren von der Leistungsfähigkeit dieser innovativen Videotechnologie überzeugt. Im Gegensatz zu herkömmlichen Videokameras, die über ein einziges Objektiv verfügen, beruht die Multifocal-Sensortechnologie auf einer Multisensor-Plattform mit mehreren Objektiven und jeweils unterschiedlichen Brennweiten. Das System ermöglicht so die Überwachung weitreichender Areale bei maximaler Auflösung, und dies alles von einem einzigen Installationsstandort aus. Dabei wird der gesamte zu überwachende Bereich dauerhaft aufge-

zeichnet, noch im Nachhinein kann auf Details zurückgegriffen werden - ohne dass das Übersichtsbild während einer Detailaufnahme verloren geht. Die Aufzeichnung beruht auf der Blade-Technik DIS-2/M NSU von Dallmeier. Jede Blade-Einheit verfügt über eine redundante Festplatte.

Sicherheit für Flugfeld und Flughafenvorplatz

Für die GESAC waren vor allem zwei Bereiche des Flughafengeländes wichtig: Der Flughafen-Vorplatz (Projekt „Panomera Forecourt“) sowie das Rollfeld (Projekt „Panomera Airfield“).

Auf dem Vorplatz und dem Eingangsbereich zum Flughafen überwacht Panomera die Verkehrsströme von Fahrzeugen und Fußgängern zwischen dem mehrstöckigen Parkhaus, dem Terminal 1 und dem Straßen- und Wegenetz des Flughafens für die Zufahrt bzw. den Zugang in beide Richtungen.

Die Panomera-Kameras für das Projekt Airfield zur Überwachung der Verkehrsströme von Fahr- und Flugzeugen auf dem gesamten Flugfeld inklusive Vorfelder (Ramps und Aprons), Anschlussbereiche sowie Start- und Landebahnen wurden in beträchtlicher Höhe auf ca. 13 m in der Nähe des Dachs



Panomera-Kameras am Tower zur Überwachung des Flugfeldes (Bild: Dallmeier/Flughafen Neapel)

des APRON-Towers installiert: Mit drei halbkreisförmig angeordneten Systemen wird so ein Überblick von 228° erreicht. Die Workstation Panomera Viewer wurde im Inneren des APRON-Towers eingerichtet, um den Sicherheitsbeauftragten eine durchgängige Panorama-Ansicht des gesamten Flugfeldes zu ermöglichen. „Mit der Panomera-Technologie können weit entfernte Objekte in der gleichen Qualität erfasst werden wie Objekte im Vordergrund. Die unglaublich hohe Auflösung über den gesamten Aufnahmebereich hinweg und die intuitive Bedienung des Systems haben maßgeblich dazu beigetragen, dass wir uns für Dallmeier entschieden haben“, so Giuseppe Musto, verantwortlich für die Abteilung Technologische Innovation und Systemkontrolle bei GESAC. ■

www.dallmeier.com

www.panomera.com

Roland Meier ist Head of Panomera Multifocal Sensor Systems bei der Dallmeier electronic GmbH & Co. KG in Regensburg. Kontakt: info@dallmeier.com

Brandschutz und Sprachalarmierung:

ESSER-Technik für das PumaVision Headquarter

Technik für Brandschutz und Sprachalarmierung der Marke ESSER schützen die neue Firmenzentrale des Sportartikelherstellers PUMA in Herzogenaurach.

Von Kurt Sikora, Ingolstadt

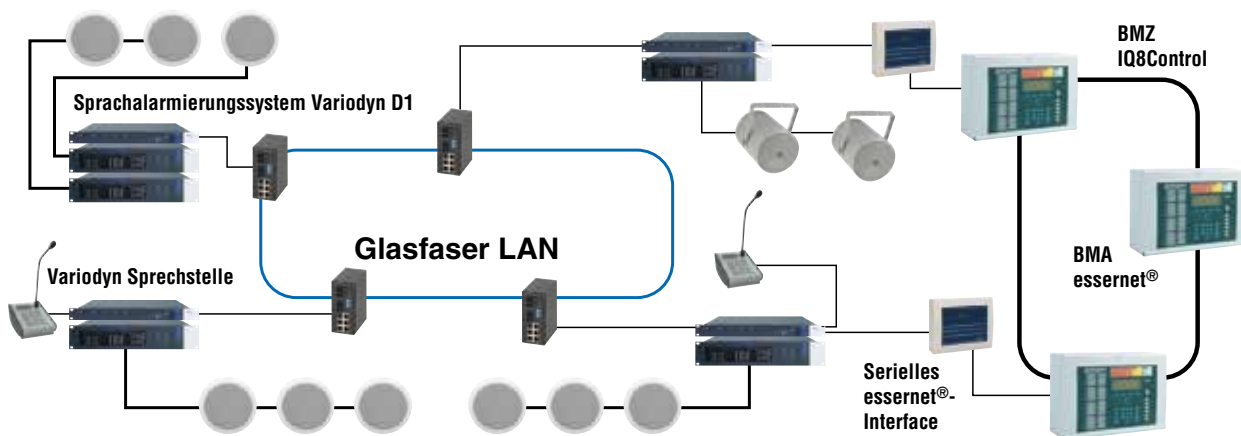
Mit der Fertigstellung seiner neuen, eindrucksvollen Firmenzentrale stärkt der Sportartikelhersteller PUMA seinen Standort im fränkischen Herzogenaurach. Nach zweijähriger Bauzeit hatte das Sportlifestyle-Unternehmen seit der Eröffnung seines Factory Outlets 2002 und nach dem Erweiterungsbau 2005 sein drittes Investitionsvorhaben in Herzogenaurach abgeschlossen. Die neue Firmenzentrale an der Flughafenstraße wurde auf einer Gesamtfläche von 50.000 Quadratmetern errichtet und bietet rund 700 Mitarbeitern Platz. Die

Neubauten sind so angeordnet, dass in der Mitte eine große Freifläche entstand, die Plaza; neben dem siebenstöckigen Verwaltungszentrum mit über 100 Büroeinheiten wurde ein neuer Concept- und Factory Outlet Store mit eigenem Restaurant sowie ein Brand-Center errichtet, das als firmeneigenes Kongresszentrum über eine 1.500 Personen fassende Multimediahalle und zahlreiche Veranstaltungsräume verfügt, in denen das Unternehmen auf insgesamt 10.000 Quadratmetern seine Kundenpräsentationen durchführt.

Durch den Einsatz innovativer und erneuerbarer Energien geht PUMA beim Umweltschutz neue Wege. So befindet sich auf dem Dach des PUMA Stores eine große Photovoltaikanlage, zudem sind Solarmodule in der Fassade integriert. Die Warmwassererzeugung erfolgt teils durch Solarkollektoren, eine Zisterne ermöglicht die Verwendung von Regenwasser in den Waschräumen. Mit Hilfe von moderner Betonkerntemperierung lassen sich die Gebäude umweltverträglich über Wärmepumpen grunderwärmen und -kühlen. Darüber hinaus wird

Die neue Firmenzentrale von PUMA in Herzogenaurach
Foto: PUMA





Die schematische Darstellung zeigt, wie die Gewerke Brandmeldetechnik und Sprachalarmierung untereinander vernetzt sind. Novar: „Eine redundante Auslegung der Datenanbindung - wie in diesem Fall - kann nur von sehr wenigen Herstellern umgesetzt werden.“ Grafik: Novar GmbH

die Unternehmenszentrale über Fernwärmeleitungen mit Biogas versorgt. Die Verlegung von insgesamt 200.000 Meter Datenkabel und 600.000 Meter Stromleitungen im gesamten Objekt lässt auf die Dimensionen des Baukomplexes und die installierte Technik schließen. Die Gesamtkosten beliefen sich auf rund 50 Millionen Euro.

Jochen Zeitz, bis 2012 Vorstandsvorsitzender der PUMA AG: „Die PUMA Plaza dient nicht nur der Stärkung unserer Markenpräsenz, sondern auch dem Ausbau unseres deutschen Standortes in Herzogenaurach. Die Entstehung moderner Büroflächen und damit attraktiver Arbeitsbedingungen fördert die Unternehmenskultur und unterstreicht auch unsere Rolle als einer der führenden Arbeitgeber in der Region.“

Vernetzte Sicherheit

Viel Wert wurde auch auf die Sicherheit der Mitarbeiter und Einrichtungen im neuen Gebäude gelegt, die vor allem durch den Einsatz von moderner Brandmelde- und Überwachungstechnik zum Ausdruck kommt. Dazu zählt zum Beispiel die komplexe Vernetzung des hochwertigen Brandmeldesystems und der professionellen Sprachalarmierungsanlage der Marke ESSER.

Projektspezifische Anforderungen

Die Gesamtplanung der sicherheitstechnischen Einrichtungen übernahm die Haustechnik Projekt GmbH mit Sitz in Nürnberg, die fachgerechte Installation wurde von dem Errichterunternehmen ADT mit Sitz in Erlangen durchgeführt. Unterstützung bei den umfangreichen Arbeiten leisteten Stefan Kihselewski und Dieter Schmitz, die den Bereich Sprachalarmierung bei der Novar GmbH in Neuss seit einiger Zeit personell verstärken. Beide sind bei der Planung von Detaillösungen, der Projektierung der Lautsprecher beziehungsweise bei der technischen Umsetzung der komplexen Anforderungen einbezogen worden. Einer der Aspekte, die berücksichtigt werden mussten, war die Anforderung an eine gezielte Abschaltung der Musikanlage im Eventbereich im Fall eines Alarms, um zu verhindern, dass durch die Beschallung die Alarmsignale übertönt werden.

Als technischer Berater der Novar GmbH in der Verkaufsregion Süd freue ich mich über die erfolgreiche Umsetzung und sehe dem zukünftig stark steigenden kombinierten Einsatz von Brandmeldetechnik und Sprachalarmierungsanlage optimistisch entgegen. Das Prestigeobjekt stellt einmal mehr unter

Beweis, dass es sich lohnt, die Gewerke stets im Gesamtzusammenhang zu betrachten. Nicht nur aufgrund der neuen Vorschriftenlage wird der Umstand zunehmend wichtiger. Die Brandmeldetechnik wurde hier mit einer redundanten Datenanbindung an das Sprachalarmierungssystem gekoppelt. Auf diese Weise wird eine sehr große Flexibilität und höchster Komfort bei optimaler Sicherheit erreicht. ■

www.esser-systems.com

Kurt Sikora ist als Technischer Verkaufsberater der Novar GmbH zuständig für die Kundenbetreuung in der Vertriebsregion Süd hinsichtlich der Produktlinie Brandmeldetechnik der Marke ESSER.

Kontakt: Kurt.sikora@honeywell.com

Sind Sie verantwortlich für die IT-Sicherheit? Dann lernen Sie <kes> jetzt noch besser kennen!

<kes> liefert zweimonatlich alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

In jeder Ausgabe finden Sie wichtiges Know-how, Hinweise zu Risiken und Strategien, Lösungsvorschläge und Anwenderberichte zu den Themen:

Internet/Intranet-Sicherheit, Zutrittskontrolle, Virenabwehr, Verschlüsselung, Risikomanagement, Abhör- und Manipulationsschutz, Sicherheitsplanung, Elektronische Signatur und PKI, IT-Recht, BSI-Forum

<kes> ist die Fachzeitschrift zum Thema Informationssicherheit - eine Garantie für Zuverlässigkeit.

Neben den regulären Ausgaben können Sie von den <kes>-specials profitieren, die zu Veranstaltungen oder besonderen Themen erscheinen.

Jetzt Probeheft anfordern!



<kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung Kurzmeldungen, ein Verzeichnis relevanter Veranstaltungen, außerdem aktuelle Artikel zum Probelesen und den SecuPedia Newsletter.

www.kes.info

PROBEHEFT-ANFORDERUNG

ja, bitte schicken Sie mir gratis und unverbindlich

- ein Exemplar <kes> - Die Zeitschrift für Informations-Sicherheit
- ein Exemplar <kes> Special „Kliniken und Praxen“
- ein Exemplar <kes> Special „Mobile Security“
- ein Exemplar <kes> Special „Wirtschaftsspionage“

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.
Anforderung per Mail an: vertrieb@secumedia.com

Datum

Zeichen

Unterschrift

FAX an +49 6725 5994

Lieferung bitte an

SecuMedia Verlags-GmbH
Leser-Service
Postfach 12 34
55205 Ingelheim

Telefon Durchwahl

IP-Video:

Intelligente Steuerung des Stadtverkehrs

Die Stadt Maastricht will ihren Verkehrsfluss intelligenter und umweltschonender steuern. Dafür hat sie auf Basis eines Glasfasernetzes ein zentral verwaltetes System aus Netzwerk-Kameras des IP-Video-Spezialisten Axis Communications implementiert.

Von Jochen Sauer, Ismaning

Maastricht in den Niederlanden zieht jährlich tausende Touristen in sein historisches Zentrum. Das enge Straßennetz muss so zusätzlichen Belastungen Stand halten. Maastricht hat deshalb die Ampeln an wichtigen Verkehrsknotenpunkten mit Netzwerk-Kameras ausgerüstet. Zusammen mit der Firma Arkasis B.V. hat die Stadt das Kontrollsystem entwickelt und installiert. So kann sich die Stadt einen optimalen Eindruck vom Verkehrsaufkommen verschaffen und Gefahrensituationen vorbeugen. Damit hat das zuständige Maastrichter Team für dynamisches Verkehrsmanagement immer einen Überblick über die aktuelle Verkehrslage. Die an den Maastrichter Ampeln aufgenommenen Kamerabilder werden auf einem speziellen Server im Rechenzentrum des Rathauses zentral verarbeitet. Die Bilder können in der Leitstelle, an den Arbeitsplätzen

oder über iPads eingesehen werden. Darüber hinaus ist es möglich, diese externen Parteien wie der Polizei oder den Bürgern zugänglich zu machen.

Mit dem zentralen Kontrollsystem verfügt Maastricht über eine komplett integrierte Lösung zur Echtzeit-Darstellung. Der Verkehr kann auf Basis dieser Daten gesteuert werden. Das neue System ist ausreichend flexibel und skalierbar, um auch zusätzliche Anwendungen zu realisieren. Beispiele hierfür sind die Anzeige des Fortschritts des groß angelegten Bauprojekts für den A2-Tunnel auf einer öffentlichen Website, die Herstellung von Zeitraffer-Filmen oder die Installation einer speziellen Zähl-Software (Cognimatics-Software), mit welcher der ein- und ausgehende Fahrradverkehr rund um das historische Zentrum von Maastricht analysiert wird.



Von der Zentrale im Rathaus haben die Sicherheitsverantwortlichen Tag und Nacht Zugriff auf die Video-Bilder.

Eine Herausforderung für die Videoüberwachung von öffentlichen Plätzen ist dabei, farbige Bilder in jeder Situation liefern zu können, die zudem die gewünschte Auflösung für die entsprechenden Anforderungen wie die Identifizierung von Personen, Fahrzeugen oder Gegenständen zulässt. Herkömmliche Kameras mit Tag- und Nachtfunktionalität schalten in der Dunkelheit in den Schwarz-Weiß-Modus. Dies ist jedoch ein Problem, wenn die Plätze nicht die ganze Nacht beleuchtet sind. Infrarot- oder Wärmebildkameras liefern bei Dunkelheit nur ein Schwarz-Weiß- bzw. ein Fehlfarbenbild. Das wiederum ist schlecht für das Erkennen von Personen oder



Um dem Platzproblem entgegenzuwirken, versucht Maastricht, das Radfahren in der Stadt so angenehm wie möglich zu machen. Mittels Netzwerk-Kamera und einer speziellen Zähl-Software wird nun der Fahrradverkehr auf einer zentralen Route analysiert und gezählt, um so Optimierungspotenzial zu erkennen. Bilder: AXIS

Gegenständen. Eine gute Alternative bietet hier die Axis Lightfinder-Technologie, die auch in Maastricht Anwendung findet. Damit können auch bei sehr schlechten Lichtverhältnissen Farbbilder aufgenommen werden. ■

Jochen Sauer ist Business Development Manager A&E bei Axis Communications in Ismaning.

Kontakt zum Autor:
Jochen.Sauer@axis.com
www.axis.com

Telenot:

Ganzheitliches Sicherheitskonzept für ein Industriegebäude

Für das Unternehmen Betzold Lehrmittelverlag & Schulbedarf erstellte und realisierte Telenot eine umfassende Sicherheitslösung mit einer Brandmeldeanlage, Einbruchmeldeanlage, Videoüberwachung sowie Zutrittskontrolle. Insbesondere das Hochregallager, der Versand und der Serverraum gehören bei Betzold zu den am wichtigsten zu schützenden Bereichen und wurden daher mit spezieller Sicherheitstechnik ausgestattet.

Von Alexander Kurz, Aalen

Jeder dritte Brand führt in Industrieunternehmen zu einem Schaden von mehr als 500.000 Euro. Mit den hohen Kosten sind auch Produktions- und Lieferausfälle sowie die Abwanderung von Kunden verbunden. Bis zu 30 Prozent der betroffenen mittelständischen Unternehmen gehen kurz nach einem Brand insolvent. Doch soweit muss es nicht kommen. Industriell genutzte Gebäude lassen sich effektiv mit einem Sicherheitskonzept vor Brand und Einbruch schützen. Ein Beispiel, wie Schwachstellen und Betriebsräume abgesichert werden können, bietet das Sicherheitskonzept für die Arnulf Betzold GmbH in Ellwangen, das Telenot für den deutschen Marktführer für den Versand von Lehrmitteln, Bildungsmedien und Schulausstattung entwickelt und realisiert hat.

Brand frühzeitig erkennen

Telenot passte die Brandmeldeanlage den räumlichen Gegebenheiten und den betrieblichen Anforderungen an. In allen Bereichen, die nicht zum Hochregallager-Bereich gehören, sind rund 100 optische Rauchmelder eingebaut. Diese erkennen mittels Streulichtverfahren bereits erste Rauchpartikel, wie sie beispielsweise bei Schwelbränden

entstehen. Zusätzlich befinden sich an allen Fluchtwegen Handfeuermelder. Bei einem Brand werden die Mitarbeiter über Warntonsirenen und Blitzleuchten alarmiert und können das Gebäude schnellstmöglich über die Fluchtwege verlassen.

Als weitere Maßnahme, mögliche Schadensereignisse zu begrenzen, wurde vom Versicherer eine Sprinkleranlage gefordert. Diese koppelte Telenot mit der Brandmeldeanlage. Sollte eine Störung der Brandmelde- oder der Sprinkleranlage auftreten, wird dies per Überwachter Übertragung direkt an einen Wachdienst gemeldet. Bei Alarm wird zudem die Feuerwehr-Leitstelle informiert. Über ein Schlüsseldepot



Optische Rauchmelder alarmieren bei einem Brand.

mit Freischaltelement ist der Zugang zum Objekt für die Feuerwehr sichergestellt. Zur Orientierung und Bedienung der Anlage nutzen die Einsatzkräfte das Feuerwehr-Informations- und Bediensystem im Gebäude.

Türen und Rolltore gesichert

Doch nicht nur die Brandgefahr ist für Industrieunternehmen eine ernstzunehmende Bedrohung. Immer häufiger sind sie auch das Ziel von Einbrechern. Besondere Schwachstellen und damit attraktive „Anziehungspunkte“ für Täter sind Türen und Rolltore. Um einen Einbruchversuch bei Betzold möglichst frühzeitig erkennen zu können, sicherte Telenot die Bereiche Hochregallager und Versand nach außen ab. Der Versandbereich des Unternehmens mit Ladebuchten für LKW, Rolltoren und zusätzlichen



Die Installation der Brandmeldezentrale, für die ein separater E30 Brandschutzraum gefordert war, erfolgte innerhalb eines entsprechend geschützten Bereichs im EDV-Raum. Bilder: Telenot Electronic GmbH



Der Versandbereich wird mit Tür- und Rolltorkontakten geschützt.

Personaltüren ist mit Tür- und Rolltorkontakten gesichert. Diese Kontakte sind so angebracht, dass schon der Versuch, ein Tor aufzuhebeln, erkannt und Alarm ausgelöst wird. Zusätzlich sind die Innenbereiche mit Bewegungsmeldern ausgestattet. Dadurch werden auch Eindringlinge erkannt, die sich auf anderen Wegen Zugang zum Gebäude verschafft haben.

Die Bedienung eines modernen Gefahrenmeldesystems muss sich in den betrieblichen Ablauf eingliedern und fast „automatisch“ funktionieren. Gleichzeitig muss die Zutrittskontrolle den kontrollierten Personalverkehr im Objekt ermöglichen. Telenot installierte hierfür Zutrittskontrollleser. Über diese erfolgt die Scharfschaltung der Einbruchmeldeanlage an der Personaleingangstür. Ist die Anlage scharf geschaltet, wird die Tür mit einem Sperrelement und einem selbstverriegelnden Panikschloss ge-

sichert. Die Tür kann somit nur bei unscharfer Anlage geöffnet werden, das Risiko eines Fehlalarms ist auf ein Minimum reduziert. Über das Schloss und den Leser wird in unscharfem Zustand der Anlage die Zutrittskontrolle geregelt. Mehr als 100 Mitarbeiter erhalten per Transponderchip Zugang zum Gebäude. Geht ein Chip verloren, muss nicht das komplette Türschloss ausgetauscht werden, sondern der verloren gegangene Chip wird gesperrt und der betroffene Mitarbeiter erhält einen neuen. Die Leser eignen sich auch, um den Zutritt zu Bereichen im Inneren des Objektes zu kontrollieren. So werden damit etwa bestimmte Räume geschützt, in denen sensible Daten oder Wertsachen hinterlegt sind.

Besonderer Schutz des EDV-Bereichs

Ein Industriebetrieb im Logistikbereich mit einem Lager von rund 12.500 Paletten, tausenden Lieferungen am Tag und einer Vielzahl sensibler Kundendaten ist auf eine zuverlässig geschützte Datentechnik angewiesen. Verständlich, dass der EDV-Bereich besonders geschützt und nur für einen kleinen Personenkreis zugänglich ist. Der Zutritt zum Serverraum, in dem sich zudem die Einbruchmelderzentrale und das Zutrittskontrollsystem befinden, wird über einen Zutrittskontrollleser in Verbindung mit einem Elektrotüröffner gesteuert. Ein DUAL-Bewegungsmelder



Für Sicherheit am Personaleingang wurden cryplock-Zutrittskontrollleser neben den Türen angebracht. Auch die Einbruchmeldeanlage lässt sich an diesen Lesern scharfschalten.

überwacht den Raum bei scharfgeschalteter Einbruchmeldeanlage. Bei einem Alarm wird der Wachdienst über eine Übertragungseinrichtung verständigt. Das Besondere: Fällt der ISDN-Übertragungsweg aus, übermittelt das System den Alarm automatisch über den redundanten Übertragungsweg per GSM.

Für erhöhte Sicherheit wurde die Einbruch- und Brandmeldeanlage im Außenbereich und Hochregallager durch Netzwerkkameras für die Videoüberwachung ergänzt. Zum Einsatz kommen Tag-/Nachtkameras und reine Nachtkameras. Die Tag-/Nachtkameras besitzen zwei Objektive, eines für Farbbilder bei Tag, eines für Schwarzweiß-Bilder bei Nacht. Reine Nachtkameras sind ebenfalls installiert. Der Wachdienst kontrolliert die Kameras von der Leitstelle aus, ohne vor Ort sein zu müssen.

Zuverlässige Planung gemäß Richtlinien

Bei dem Sicherheitskonzept für Betzold galt es, eine Vielzahl an gesetzlichen, baurechtlichen und versicherungstechnischen Sicherheitsauflagen einzuhalten. „Das dazu notwendige Wissen ist in den meisten kleinen und mittelständischen Unternehmen verständlicherweise nicht vorhanden“, so Ulrich Betzold, Geschäftsführer des Betzold Lehrmittelverlags. Aufgrund der zertifizierten Fachkompetenz und des bundesweiten Service- und Dienstleistungs-Netzwerkes hat er sich daher für Sicherheitslösungen von Telenot entschieden. Betzold: „Wir wurden fachlich kompetent beraten. Die Absprachen mit den Architekten, Behörden und Versicherungen sowie der Feuerwehr, der VdS Schadenverhütung und anderen Gewerken erfolgten zu unserer vollsten Zufriedenheit.“ ■

Alexander Kurz ist technischer Mitarbeiter der Telenot Electronic GmbH, Aalen, www.telenot.de.

Zutritt und Zeiterfassung:

Sparkassenverband Bayern setzt auf Biometrie

Der Sparkassenverband Bayern steuert fortan mithilfe einer Biometrie-Lösung Zutritt und Zeiterfassung. Neben gesteigerter Betriebssicherheit und präziseren Workforce-Management-Prozessen konnte zudem der Administrationsaufwand reduziert werden. Mitarbeiter müssen sich künftig nicht mehr um verlorene oder defekte Unternehmensausweise kümmern – das Buchen der Arbeitszeiten sowie der Zugang zum Arbeitsplatz erfolgt mittels berührungsloser 3D-Fingererkennung.

Von Hans-Peter Eckstein, Stuttgart

Bedingt durch steigende kriminelle Handlungen sind Unternehmen heute mehr denn je gefordert, ihre Firmengebäude zuverlässig abzusichern. So geht eine aktuelle Studie der NIFIS davon aus, dass die Nachfrage nach IT- und Informationssicherheit bis 2020 deutlich zunehmen wird [1]. Auch beim Sparkassenverband Bayern (SVB) verstärkte sich das Sicherheitsbewusstsein immer mehr. Dementsprechend war es erforderlich und vom SVB ausdrücklich gewünscht, das bisherige Ausweissystem durch eine innovative Lösung zu ersetzen. Das neue System sollte Nutzern hohen Komfort bieten und dem Verband helfen, noch effizienter zu arbeiten.

Sicherheitsansprüche bringen Altsystem an Grenzen

Mit den bisherigen Terminals für Zutritt und Zeiterfassung arbeitete der SVB bereits seit mehreren Jahrzehnten. Die einst von Interflex installierte Infrastruktur arbeitete zuverlässig, stieß jedoch aufgrund der gestiegenen Sicherheitsanforde-



Für ein Höchstmaß an Sicherheit und Komfort bei Zutrittskontrolle und Zeiterfassung: Biometrische Lösung von Interflex mit 3D-Fingerprint-Terminal des Interflex-Implementierungspartners TBS. Bild: TBS/Interflex

rungen an ihre Grenzen. Ein sicherer Zutritt musste jedoch weiterhin an allen Eingängen gewährleistet werden.

Mit der Interflex-Software war der Verband stets zufrieden, daher sollten nur die Hardwarekomponenten ausgetauscht werden. Nach diversen Gesprächen mit den Sicherheitsexperten von Interflex war die Entscheidung für ein biometrisches System mit berührungsloser

3D-Fingererkennung gefallen. Die physiologischen Merkmale von Personen sorgen für eine eindeutige Identifikation – unabhängig von Unternehmensausweisen oder Passwörtern. Wolfgang Pinsel, stellvertretender Bereichsleiter beim SVB: „Mit der Einführung des biometrischen Systems wollten wir eine Vorreiterrolle einnehmen, da diese Lösungen zunehmend an Bedeutung gewinnen. Zudem versprechen sie ein hohes Maß an Sicherheit und Anwenderkomfort.“ Wichtig war, dass es sich um ein System handelt, in dem Daten mehrfach verschlüsselt sind und keine Fingerabdrücke reproduziert werden können. Unberechtigte Personen haben somit keine Möglichkeit, ins Unternehmen zu gelangen.

Weiche Migration sichert reibungslosen Geschäftsbetrieb

Der SVB setzte die neue Generation der dreidimensionalen und berührungslosen 3D-Fingerabdruck-Terminals des Interflex-Implementierungspartners TBS ein. Die Schweizer Firma entwickelte das biometrische Sub-System, das höhere Sicherheit, bessere Erkennungsleistung und mehr Fingerdetails verspricht. In der ersten Phase der Implementierung wurde die Zeitwirtschaft umgestellt. Erst nach vollkommener Funktionsfähigkeit in beiden Unternehmensgebäuden widmete sich der Verband der Einführung der Zutrittskontrolle. Die biometrische Lösung ließ sich einfach montieren und integrierte sich nahtlos in das bereits bestehende Netzwerk.

www.interflex.de

Hans-Peter Eckstein ist Manager Marketing Communications bei der Interflex Datensysteme GmbH & Co. KG, Stuttgart.

Kontakt: interflex.pr@allegion.com

Literatur

[1] Studie: „Investitionen in IT-Sicherheit verdoppeln sich bis 2020“, Nationale Initiative für Informations- und Internet-Sicherheit (NIFIS)

WIK-Leser kennen alle relevanten Informationen

Wik

Zeitschrift
für die Sicherheit
der Wirtschaft

WIK liefert 6 Mal im Jahr aktuelle Informationen und Basiswissen zum Thema Sicherheit. Sie wird seit über 30 Jahren von einer unabhängigen und hochqualifizierten Fachredaktion zusammengestellt. Unsere Redakteure bereiten in jeder Ausgabe für Sie wichtiges Know-how auf, führen Interviews mit relevanten Vertretern der Branche, geben Hinweise zu Risiken, machen Lösungsvorschläge und zeigen praxisnahe Strategien und Anwendungsbeispiele. Dazu erhalten Sie regelmäßig: Einkaufsführer für den Sicherheitsverantwortlichen, Produktneuheiten, einen Branchenüberblick und Informationen aus den Sicherheitsverbänden.

Wik-Leser erfahren mehr:

- Aktuelle Beurteilung der Sicherheitslage
- Sicherheitstechnik: Ideen und Produkte
- Lösungen für den Unternehmensschutz
- Infos über und für Sicherheitsdienstleister
- Praxis und Anwenderbeispiele
- Checklisten, Marktübersichten
- ASW - Informationen



Web: www.wik.info

E-Mail: vertrieb@secumedia.de

Fax: +49 6725 5994

Sie haben Fragen? Ihr telefonischer Ansprechpartner im SecuMedia Verlag: Heidrun Jung, Tel. +49 6725 9304-0

Probeheft-Anforderung

Fax an +49 6725 5994

Per Fax oder per Post im Fensterumschlag an:

SecuMedia Verlags-GmbH
Abonnenten-Service
Postfach 1234
55205 Ingelheim

ja, bitte schicken Sie mir gratis und unverbindlich ein Exemplar der WIK - Zeitschrift für die Sicherheit der Wirtschaft.

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.

Das Abonnement beinhaltet ein Passwort zur Nutzung des Abo-Bereichs auf www.wik.info und den Bezug des WIK/secupedia Newsletters.

Absender

Telefon Durchwahl



„Intelligente Sicherheit,
flexibel einsetzbar.
Und das bei niedrigem
Einrichtungsaufwand.“

Thorsten Körting, Planer



**FlexES Guard –
das Gefahrenmanagementsystem
für alle Objektgrößen.**

- Kosteneffizienter und flexibler Einsatz
- Innovatives Datenbankkonzept
- Hohe Ausfallsicherheit



Jetzt den Film
ansehen!