



BEST PRACTICES FÜR SICHERHEIT UND EFFIZIENZ IN DATENZENTREN.

Ein **WHITE PAPER** von BOON EDAM

**BOON EDAM**
YOUR **ENTRY** EXPERTS.

ÜBER STRATEGISCHE ANWENDUNG VON SICHERHEITSLÖSUNGEN ZUM SCHUTZ VON DATEN, ZUR EINHALTUNG VON COMPLIANCE UND ZUR VERBESSERUNG DER BETRIEBLICHEN EFFIZIENZ.

In der dynamischen Welt der Rechenzentren bestimmen drei zentrale Gebote die Strategien und Entscheidungen von Sicherheitsexperten:

1. **Schützen Sie sensible Vermögenswerte:**

Der Schutz von Rechenzentrumsressourcen geht über den Schutz von Daten hinaus und umfasst auch die physische Sicherheit von Personen, Eigentum und anderen Vermögenswerten innerhalb der Rechenzentrums Umgebung.

2. **Einhaltung gesetzlicher Vorschriften:**

Dies erfordert einen vielschichtigen Ansatz, der sicherstellt, dass Rechenzentren nicht nur die aktuellen Compliance-Standards erfüllen, sondern auch an sich entwickelnde regulatorische Rahmenbedingungen anpassbar bleiben.

3. **Steigende Kosten überwinden:**

Die steigenden Kosten für Energie, Land, Arbeitskräfte und die Lieferkette kritischer Infrastrukturen erfordern die Identifizierung und Beseitigung von Ineffizienzen, um die Verfügbarkeit von Diensten, wettbewerbsfähige Preise und nachhaltige Rentabilität sicherzustellen.

Durch die Konvergenz dieser Anforderungen unter einem einzigen Haushaltsposten wird die strategische Anwendung gesicherter Zugangslösungen von unschätzbarem Wert.

Über die verschiedenen Arten und Zugangsprozesse für Sicherheitseingänge in Rechenzentren.

Beim Übergang von der äußeren Zone einer Anlage zu ihrer kritischen Infrastruktur steigt die Effektivität der redundanten Absicherung von Zugangspunkten exponentiell an. Die Implementierung einer mehrschichtigen Sicherheitsstrategie, die mit zunehmender Nähe zu sensiblen Bereichen stärkere Sicherheitsmaßnahmen vorsieht, ist der optimale Ansatz, um sowohl die physischen als auch digitalen Vermögenswerte eines Rechenzentrums und seine Mitarbeiter zu schützen. Obwohl jedes Rechenzentrum und jeder Standort seine individuellen Besonderheiten aufweist, bietet die nachfolgende Übersicht eine solide Basis für eine robuste Strategie im Bereich der physischen Zugangssicherheit.

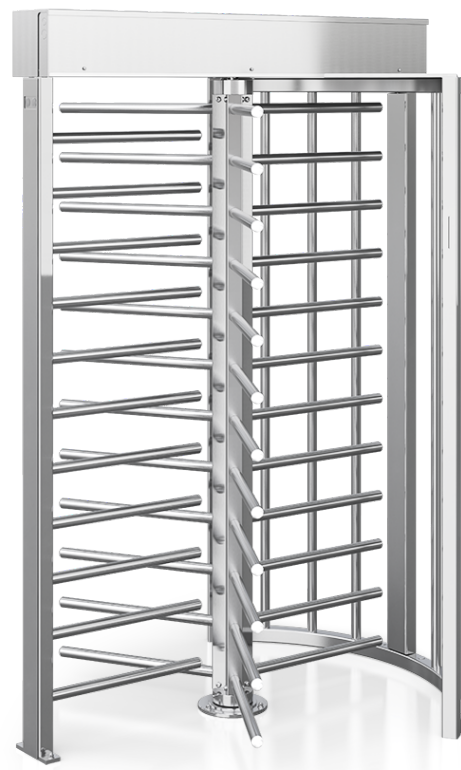
Wie allen Betreibern von Rechenzentren bewusst ist, verursacht Redundanz Kosten. Das Ziel besteht darin, Kunden und Besuchern einen möglichst reibungslosen Zugang zu ermöglichen, während gleichzeitig physische Sicherheitsebenen integriert werden, die aufeinander aufbauen. Beginnen wir damit, die verschiedenen Sicherheitsebenen klar zu definieren, um die aktuellen Abläufe zu optimieren und dadurch Arbeitseinsparungen zu realisieren.



DIE UNTERSCHIEDE KENNEN PRODUKTE UND ZUGANGSPROZESS FÜR SICHERHEITSEINGÄNGE.

LAYER 1: DER ERSTE ZUGANG

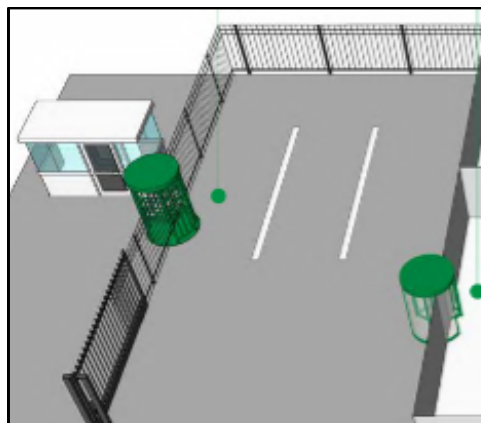
Physische Sicherheit beginnt damit, dass unbefugte Fußgänger und Fahrzeuge vollständig von der inneren Zaunlinie ferngehalten werden. Für diese erste Schicht sind Drehkreuze in voller Höhe ideal, da sie eine physische Abschreckung gegen Infiltration bieten. Bis vor Kurzem waren Drehkreuze in voller Höhe anfällig für **Piggybacking**, bei denen sich zwei Personen im selben Abteil hindurchquetschten. Die neue robuste, für den Außenbereich geeignete Sensortechnologie erkennt jetzt, wenn zwei Personen versuchen, das Drehkreuz mit einem Ausweis zu betreten, und verriegelt das Drehkreuz, um den Zutritt zu verhindern. Diese neuen Sensoren verfügen außerdem über eine „Walk-Away“-Erkennung, die das Drehkreuz verriegelt, wenn eine Person ihre Zugangsberechtigungsanzeige vorlegt, genehmigt wurde, das Drehkreuz entriegelt werden kann, das Drehkreuz betritt und sich dann zurückzieht, um einem anderen Unbefugten Zutritt zu gewähren Person, die eintreten soll. In Kombination mit einem Schaltausgang für abgeschlossene Drehungen kann diese Funktion mit Sicherheit die Aufstellung und Rückgabe bestimmen und dabei immer wissen, wer sich innerhalb der Umzäunung und des Gebäudes befindet und wer nicht.



Diese Boon Edam-Produkte eignen sich am besten für den Layer 1:

- **Turnlock 100 Fußgänger-Sicherheitsdrehkreuz**
Ein robustes Drehkreuz in voller Höhe, das für raue Außenumgebungen entwickelt wurde. *
- **Turnlock 150 Drehkreuz-Sicherheitstor**
Eine vielseitige Lösung, die Haltbarkeit mit Ästhetik verbindet, ideal für Innen- und Außenanwendungen. *

*Nur in den USA erhältlich



DIE UNTERSCHIEDE KENNEN PRODUKTE UND ZUGANGSPROZESS FÜR SICHERHEITSEINGÄNGE.

LAYER 2: DER GEBÄUDEEINGANG

Sobald man sich innerhalb des Anlagenbereichs befindet, gelangt man in manchen Ausführungen über eine herkömmliche Schwingtür mit Kartenleser in den Empfangsbereich des Rechenzentrums und ist in der Regel mit einer Gegensprechanlage ausgestattet. Autorisierte Personen sollten entweder Mitarbeiter:in, Kunden oder bestätigte Auftragnehmer Besucher sein. Genehmigt, d. h. im Voraus registriert, aber nicht über einen Ausweis verfügen, muss man sich in der Regel mit einem Führerschein oder Reisepass registrieren. Dies ist der Punkt, an dem Sie eine Entscheidung treffen müssen. Wie soll das Kundenerlebnis aussehen? Wählen Sie eine Erkennungsstrategie, die Sensorschleusen nutzt, oder setzen Sie eine **Piggybacking**-Präventionsstrategie ein, die Sicherheitskarusselltüren nutzt?

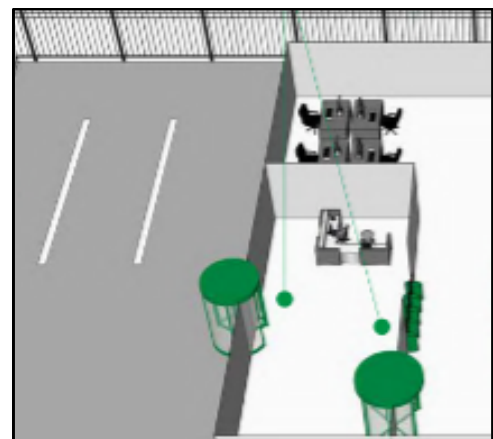
Schauen wir uns die Vor- und Nachteile an.

Sensorschleusen allein können ein **Tailgating** nicht verhindern. Daher müssen Sie sich bei der Durchsetzung von Richtlinien auf Governance und Arbeitskräfte verlassen. Eine Präventionsstrategie ist von entscheidender Bedeutung, wenn Governance mit Compliance- und Audit-Anforderungen verknüpft ist. Wenn Sie jedoch ein Colo (Co-Location) sind, der sich nicht an regulierte Kunden aus der Industrie richtet, dann bietet die Verwendung von Sensorschleusen ein großartiges Kundenerlebnis. Wenn Sie sich dafür entscheiden, die Compliance zu automatisieren und Ihr Personal stärker auf die Umsatzgenerierung durch Service-Level-Vereinbarungen zu konzentrieren, sind Sicherheits-Karusselltüren die richtige Wahl, da sie verhindern, dass Besucher an der Rezeption vorbeischlüpfen, Absprachen treffen und Kunden oder Auftragnehmern das gleichzeitige ungehinderte Kommen und Gehen ermöglichen. Darüber hinaus profitieren Sie weiterhin von allen Vorteilen der Luftfeuchtigkeits- und Staubfilterung sowie des Brute-Force-Schutzes, die Sie mit einer Erkennungsstrategie ohne den Einsatz einer wachsam Wachtruppe nicht erreichen können.



Diese Boon Edam-Produkte eignen sich am besten für den Layer 2 :

- **Tourlock 180 Hochsicherheits-Karusselltür** die ideale Lösung, wenn Sie unbefugten Zutritt verhindern und gleichzeitig hohe Verkehrsanforderungen an die Schrankbreite in der Industrie mit schwenkbaren Paneelen unterstützen müssen.
- **Lifeline Speedlane Swing Speed Gate** eine schlanke, funktionsreiche Sicherheitsbarriere, die als elegante Grenze zwischen öffentlichen und privaten Bereichen fungiert.



DIE UNTERSCHIEDE KENNEN PRODUKTE UND ZUGANGSPROZESS FÜR SICHERHEITSEINGÄNGE.

LAYER 3: DIE KRITISCHE INFRASTRUKTUR (SERVERRÄUME)

Für den Schutz der sensibelsten Zonen in einem Rechenzentrum, wie Serverräume oder Technikräume, ist die strikte Durchsetzung der Ein-Personen-Regel in Hochsicherheitsportalen entscheidend. Dabei ist es von größter Wichtigkeit, dass stets die verifizierte, korrekte Person Zugang erhält, um die Compliance-Vorgaben einzuhalten. Ein zentrales Designelement dieser Hochsicherheitsportale ist die Verhinderung von Benutzersubstitutionen. Dies wird durch eine automatisierte, zwangsläufige Abfolge von Prozessen erreicht, die sicherstellt, dass bei der Identitätsprüfung keine Manipulationen oder Vertauschungen möglich sind. Es genügt nicht, lediglich die Anwesenheit einer einzelnen Person zu gewährleisten – es muss die richtige Person sein.

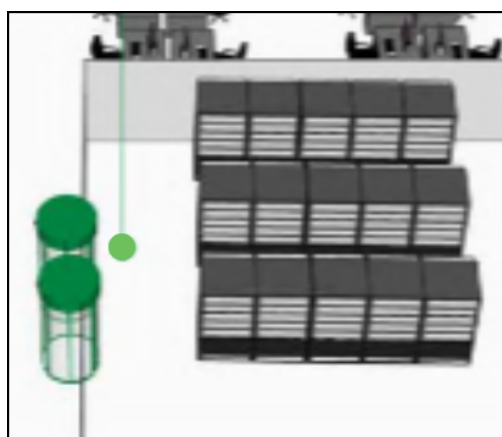
Sobald ein Nutzer seine Zugangsberechtigung präsentiert, öffnet sich die erste Tür des Portals. Beim Eintritt wird eine Kontrolle durchgeführt, um die Einhaltung der Ein-Personen-Regel zu bestätigen. Ist diese Kontrolle erfolgreich, schließt sich die erste Tür. Nachdem diese geschlossen ist, führt das Portal redundante Nachkontrollen durch. Erst wenn auch diese Kontrollen positiv sind, wird das biometrische Erfassungsgerät aktiviert. Auf diese Weise wird eine Substitution verhindert, indem die Funktionsbereitschaft des biometrischen Geräts verzögert und mit redundanten Kontrollen der Ein-Personen-Regel kombiniert wird.

Durch den Einsatz eines unbeaufsichtigten, gesicherten Zugangsportals mit Verriegelung, das dieselben hochentwickelten Stichprobenalgorithmen wie Sicherheitskarusselltüren verwendet, wird das Risiko neu bewertet, indem die Bedrohungsfläche durch Schichtung und fortlaufende Überprüfung an jedem Punkt drastisch reduziert wird. Der Vorteil dieser Algorithmen liegt darin, dass sie es ermöglichen, das Risikoniveau zu messen und vorherzusagen – eine Fähigkeit, die viele Rechenzentrumsbetreiber derzeit nicht nutzen. Zusätzlich bleibt das Verriegelungsportal auch während der Nutzung stets geschlossen, was die Gebäudeluftaufbereitung sowie die Feuchtigkeits- und Staubfilterung der Umgebungssysteme unterstützt. Diese Portale können zudem mit kugelsicherem Glas verstärkt werden.

In vielen Fällen müssen diese Hochsicherheitsportale in Brandschutzwände integriert werden. Dies lässt sich durch die direkte Montage an einer Brandschutztür realisieren. Halbportale, die an bestehenden Brandschutztüren angebracht werden, ermöglichen zudem die einfache Umwandlung einer Standardtür in einen Hochsicherheitseingang.

Diese Boon Edam-Produkte eignen sich am besten für den Layer 3

- **Circlelock Solo-Sicherheitsportal**
Das ultimative Sicherheitsportal mit einem Zugang.
- **Circlelock Combi**
Ein praktisches Halbportal, das an einer vorhandenen Schwingtür befestigt werden kann und eine gewöhnliche Tür in einen Hochsicherheitseingang verwandelt.





Das 3 Layer Sicherheitskonzept für Datacenter.

DIE OPTIMIERUNG VON PERSONAL DURCH DEN EINSATZ VON UNBEAUF SICHTIGTEN SICHERHEITSEINGÄNGEN.

Während die Abschreckung, Erkennung und Verhinderung unbefugten Zutritts die Hauptfunktionen gesicherter Zutrittslösungen sind, bieten Sicherheitszugänge eine Reihe weiterer wichtiger Vorteile in Bezug auf Kosteneinsparungen, Betriebseffizienz und Alarmmanagement.

SICHERER EINGANG MIT ENERGIEEFFIZIENZ

Power Usage Effectiveness (PUE) ist nicht die einzige Initiative zur betrieblichen Verbesserung, die Rechenzentren zur Verfügung steht. Angesichts der steigenden Energie- und Wasserressourcenkosten ist es eine einzigartige Herausforderung, einen Sicherheitseingang zu entwerfen, der immer offen und immer geschlossen ist und die Kosten für Luftaufbereitung und Filterung minimiert, ohne zu viel wertvollen Platz zu beanspruchen.

Herkömmliche Eingänge mit Dreh- und Schiebetüren erzeugen bei jedem Durchgang ein Loch in der Gebäudehülle, wodurch Außenluft eindringen und die kontrollierte Innenatmosphäre verdrängen kann. Tatsächlich entstehen bis zu 50 % des gesamten Energieverlusts in einem gut isolierten Gebäude durch und um Türen und Fenster herum, was teilweise darauf zurückzuführen ist, dass Rechenzentren nur nach den Mindestanforderungen von NFPA72 gebaut werden und selten über Fenster verfügen. Allerdings ist die Luftqualität von entscheidender Bedeutung, daher ist die Vermeidung von Luftverlusten und die Filterung sowohl betrieblich vorteilhaft als auch kosten- und energieeffizient. Sicherheitskarusselltüren und ineinandergreifende Portale sorgen für energieeffiziente Eingänge, die immer geschlossen sind, was die Effizienz steigert und die Kontaminationskontrolle im täglichen Gebrauch unterstützt. Piggybacking- und Tailgating-Präventionslösungen von Boon Edam verbrauchen 20 bis 50 % weniger Fläche und bieten eine überlegene Luftfilterleistung im Vergleich zu herkömmlichen Vorräumen.

„...Im Durchschnitt wird bei einer Karusselltür achtmal weniger Luft ausgetauscht als bei einer Schiebe- oder Schwingtür, was die Effizienz steigert und Verluste und Filtration reduziert.“



GESICHERTER ZUGANG FÜR COMPLIANCE

Über die Sicherheit hinaus stellen gesicherte Zugangslösungen den Beschäftigten die Infrastruktur und Tools zur Verfügung, die sie benötigen, um Zertifizierungen zu erfüllen und die absolute Einhaltung von Kundenaudits nachzuweisen.

Die Vorteile einer mehrschichtigen (1-3 Layer) Zugangsstrategie sind:

1. Automatisierung der Compliance für Ein- und Ausgangspunkte physischer Barrieren.
2. Effektive Aufrechterhaltung des kontinuierlichen Betriebs.
3. Optimaler Schutz von Kundendaten, Aktionäre und Versicherungspolizen.
4. Erstellen von unveränderliche, 90-Tage archivierte Aufzeichnungen und Alarmprotokolle für Kunden, Aktionäre, Versicherungen und Compliance-Audits.
5. Entwerfen Sie Leistungsfähigkeiten für Ein- und Ausgangspunkte, die Segmentierung, Redundanzen und Analysen nutzen, um Vertrauen aufzubauen.

„...Die Fähigkeit zur Einhaltung des Gramm-Leach-Bliley-Act (GLBA), der 2022 Safeguards Rule Compliance, FISMA, ISO 27001, HITRUST, PCI DSS, SOC 1, SOC 2, SOC 3 und ITAR gehört dazu Ihrer automatisierten Implementierungsstrategie für physische Sicherheit zur Kundenakquise und -bindung.“



ABGESICHERTER ZUGANG FÜR ALARMMANAGEMENT

Die raumhohen Drehkreuze, Sicherheitskaruselltüren und Sicherheitsportale von Boon Edam verhindern alle diese Sicherheitsverletzungen und eliminieren daher alle von ihnen an herkömmlichen Türen erzeugten Alarme.

Zu den Compliance-Vorteilen gehören:

1. Automatisierte Benachrichtigungen für Nutzer werden lokal an Ein- und Ausgangspunkten generiert und lösen alle Benutzerschnittstellen- und Fehlerprobleme ohne Alarme.
2. Richtlinien und Verfahren werden automatisch und ohne Alarme durchgesetzt.
3. 100 % Eliminierung von DHOs (Door Held Open) für die Compliance-Berichterstattung.
4. DFO (Door Forced Open)-Alarme treten nur auf, wenn das System einem Brute-Force-Angriff ausgesetzt ist.

Am wichtigsten ist, dass gesicherte Zugangslösungen konsequent die Einhaltung von Vorschriften erzwingen und den Problemlösungsprozess automatisieren. Dadurch müssen die Mitarbeitenden keine Abhilfemaßnahmen wie Fehlalarmreaktionen und manuelle Eingangskontrollen durchführen, sondern können sich auf kundenorientierte Aufgaben konzentrieren, die Umsatz generieren.

Durch die Tailgating- und Piggybacking-Lösungen von Boon Edam können die Alarme „Door Forced Open“ (DFO) und „Door Held Open“ (DHO) praktisch zu 100 % eliminiert werden.

GESICHERTER ZUGANG FÜR EINE EFFIZIENTE ARBEITSALLOKATION

Viele Rechenzentren beschäftigen im Rahmen ihrer Sicherheitsstrategie Wachpersonal. Während Wachen eine starke physische Abschreckung darstellen, stellt der wachsende Fachkräftemangel die Suche nach zuverlässigem Personal vor eine Herausforderung. Wie in anderen Branchen wird auch von den Beschäftigten in so einem Fall mehr verlangt, um den zu geringen Personalstamm auszugleichen. Das daraus resultierende Ungleichgewicht zwischen Angebot und Nachfrage von Sicherheitsdiensten hat die Art und Weise, wie Rechenzentren ihre verfügbaren Ressourcen nutzen, nachhaltig verändert.

Sicherheitseingänge schließen erfolgreich die Lücke zwischen Arbeitskräfteangebot und -nachfrage, indem sie Lösungen anbieten, die unabhängig von oder gemeinsam mit Sicherheitspersonal arbeiten. Diese Lösungen verringern die Kostenstruktur des Sicherheitsapparates, indem sie eine technologiebasierte Alternative bieten. Geben Sie Ihren Mitarbeitern die richtigen Werkzeuge für den Job.

Nehmen wir zum Beispiel einen bemannten Sicherheitseingang, bei dem Wachdienste die Mitarbeiter:in kontrollieren und mögliche Durchgriffsversuche verhindern müssen. Berücksichtigen Sie das Gehalt, die Sozialleistungen usw. des Wachpersonals und multiplizieren Sie dies dann mit allen anderen Eingängen zu Einrichtungen, die diese Lösung nutzen. Die Kosten summieren sich schnell. Stellen Sie sich nun ein raumhohe Sicherheitskarusselltür oder ein Hochsicherheitsschleuse vor, die am selben Eingang installiert ist. Auch diese Lösungen können Mitarbeiter einchecken und Fälle von Tailgating und Piggybacking verhindern, wobei der damit verbundene Aufwand und das Risiko weitaus geringer sind.

„...Anstatt mehrere Beschäftigte für die Aufrechterhaltung sicherer Eingänge einzusetzen, können sich Unternehmen jetzt auf unbemannte Sicherheitseingänge verlassen, die rund um die Uhr funktionieren.“



RAGINGWIRE DATACENTER: EINE CASE STUDY

Herausforderung: In den Co-location-Rechenzentren von RagingWire in Virginia und Kalifornien ist die Kontrolle des Zugangs und die Verhinderung unbefugten Zutritts von entscheidender Bedeutung, während gleichzeitig autorisiertem Personal rund um die Uhr unbeaufsichtigter Zugang ermöglicht wird. RagingWire bietet Rechenzentrumsdienste für einige der anspruchsvollsten Hyperscale-Cloud- und Enterprise-Unternehmen und gilt unter anderem aufgrund seines Engagements für die Sicherung der geschäftskritischen Geräte und Daten seiner Kunden als erste Wahl.

Lösung: Boon Edam lieferte Tourlock-Sicherheitskarusselltüren, um das ausgeklügelte, mehrschichtige Sicherheitssystem von RagingWire zu unterstützen. Die Sicherheitskarusselltüren ermöglichen einen effizienten Durchgang für die Änderungskontrolle der Kunden, während sie gleichzeitig das tailgating und piggybacking sowohl beim Eintritt als auch beim Austritt verhindern. Die Türsysteme erkennen solche Verstöße und verhindern unbefugtes Passieren, was die Strategie der mehrschichtigen Sicherheit von RagingWire unterstützt.



PHYSISCHE SICHERHEIT IST CYBERSECURITY.

Schließlich ist es zum Schutz von Rechenzentren und ihren kritischen Daten unerlässlich, Cybersicherheit und physische Sicherheit als Hand in Hand zu betrachten, um kritische Daten zu schützen. Durch die Installation von Sicherheitseingängen kann sichergestellt werden, dass nur Personen, die das Gebäude betreten, autorisierte Mitarbeitenden oder autorisierte Besucher sind, wodurch ein Höchstmaß an Sicherheit für Einrichtungen gewährleistet wird, in denen sensible Daten aufbewahrt werden.

Denken Sie bei der Risikominimierung bei Ihrer Planung der physischen Sicherheit und Cybersicherheit daran, dass Sicherheitseingänge Ihre Haftung verringern, indem sie einen plausiblen Grad an Anstrengungen zur Verhinderung von Infiltration nachweisen.

Sie schützen die persönliche Sicherheit von Mitarbeitenden, Besuchern und allen anderen Personen in Ihrer Einrichtung sowie die IT- und Computersysteme und Daten Ihrer Organisation. Darüber hinaus können Sicherheitseingänge dazu beitragen, die Kosten für Sicherheitspersonal und Fehlalarmmanagement zu senken und gleichzeitig die Einhaltung verschiedener von der Regierung und der Industrie auferlegter Vorschriften sowie interner Sicherheitsrichtlinien zu gewährleisten.

WIR AGIEREN GLOBAL.

Boon Edam produziert seit mehr als 150 Jahren hochwertige, ästhetische Sicherheitseingangslösungen in den Niederlanden, den USA und China. Wir sind stolz darauf, dass wir mit unseren Tochtergesellschaften jeden Winkel der Erde abdecken. Zudem arbeitet unsere globale Exportabteilung nicht nur mit Distributoren zusammen, sondern ist auch für den direkten Vertrieb und Service auf diesen Gebieten verantwortlich. Durch dieses breite Netz erreichen wir eine starke globale Präsenz und haben ein besseres Verständnis der lokalen Marktbedürfnisse für Eingangslösungen und der Bedürfnisse unserer Kunden.

Sie suchen Ihren Experten für Boon Edam in Ihrer Nähe? Besuchen Sie uns auf:

www.boonedam.de/kontakt



Boon Edam GmbH
T +49 (0) 211 416118 90
E de.info@boonedam.com
I www.boonedam.com


BOON EDAM
YOUR ENTRY EXPERTS.