convergint | state • local education • defense

Leitfaden für bewährte Praktiken,

2024: SLED

Staatliche und lokale Behörden | Bildung | Verteidigung/Luft- und Raumfahrt

Die SLED-Vertikale, wie sie von Convergint definiert wird, umfasst die Bereiche staatliche und kommunale Verwaltung, Bildung sowie Luft- und Raumfahrt. Obwohl jeder dieser Teilbereiche sicherlich unterschiedlich ist, gibt es mehr Gemeinsamkeiten als Unterschiede, wenn es um die Sicherheit geht. Dies wird **durch die Herausforderung eskalierender physischer und Cyber-Risiken** veranschaulicht, die eine Priorisierung der Sicherheitsplanung und Verfahrensminderung für alle SLED-Einrichtungen erfordert.

Das engagierte SLED-Team von Convergint bietet **hochsichere Schutzstrategien, methodische Programmimplementierung und umfassende Lösungen**, die sowohl die Sicherheit als auch die Betriebseffizienz in diesem Sektor verbessern. Convergint verfügt über ein tiefes Verständnis der Bedrohungen in der Branche und der Anforderungen an die Einhaltung gesetzlicher Vorschriften und ist in der Lage, integrierte Systeme zu implementieren, die auch im Rahmen der Budgetplanung funktionieren.

SLED-Sicherheitsvorfälle und -Risiken

Die Sicherheitsverantwortlichen im SLED-Bereich konzentrieren sich vor allem darauf, **die Sicherheit der Öffentlichkeit zu gewährleisten und alle verfügbaren Mittel zu nutzen**, um Systeme einzurichten, die diese Aufgabe erleichtern.

Das größte Risiko besteht jedoch darin, bei der Sicherheitsplanung eine reaktionäre Haltung einzunehmen. Dieser notdürftige Ansatz, der sich mit dem Vorfall und nicht mit dem Gesamtbild befasst, ist viel zu verbreitet. So kann es beispielsweise in einer K-12-Schule zu einem Vorfall von Mobbing kommen, auf den mit zusätzlichen Kameras und Überwachungseinrichtungen reagiert wird. In einer Gemeindeverwaltung kann es zu einer Häufung von Diebstählen kommen, weshalb eine Zugangskontrolle installiert wird. Ein Vorfall mit einer Schießerei kann Anlass für eine Waffenerkennung sein.

Es ist wichtig, die Sicherheit nicht stückweise anzugehen, sondern sie ganzheitlich zu betrachten und sowohl kurz- als auch langfristige Ziele zu berücksichtigen. Die Umsetzung eines umfassenden Plans schließt viele einzelne Vorfälle aus, die zu einer Erosion der Marke, zu Problemen mit dem Ruf und zu rechtlichen Risiken führen.

Es ist auch hilfreich, die Dinge nach SLED-Teilbereichen aufzuschlüsseln, um wertvolle, auf das jeweilige Unternehmen zugeschnittene Erkenntnisse zu gewinnen.

Staatliche und lokale Behörden jetzt und in Zukunft

Für staatliche und kommunale Behörden hat die Gewährleistung der Sicherheit der Gemeinschaft und ihrer Mitarbeiter oberste Priorität. Neben den offensichtlichen Folgen müssen sie auch die Auswirkungen auf die öffentliche Wahrnehmung, die Einstellung und die Bindung von Mitarbeitern berücksichtigen. Die Kommunen sind mit einer Vielzahl von Sicherheitsrisiken konfrontiert, darunter:

- Verbrechen
- Sicherheit der Polizei und rechtliche Risiken

- Migranten und obdachlose Bevölkerungsgruppen
- Verkehr und Transitsicherheit

Doch es gibt noch andere Probleme. **Sachbeschädigung und Cyber-Bedrohungen sind nach wie vor kritische Risiken für Kommunen, die erhebliche Folgen für den Steuerzahler haben**. Alle Sicherheitsherausforderungen können durch eine schlechte Kommunikation innerhalb und zwischen den Behörden noch verschärft werden, was letztlich die Fähigkeit der Gemeinde beeinträchtigt, Vorfälle zu bewältigen und Finanzierungsressourcen voll auszuschöpfen.

Bildung jetzt

Kohärente Planung

Wie bereits erwähnt, ist das größte Risiko für K-12-Schulen **nach wie vor das Fehlen einer kohärenten und ganzheitlichen Sicherheitsplanung**. Viel zu vielen Bezirken fehlt ein umfassender strategischer Masterplan, und sie kaufen willkürlich Sicherheitsausrüstungen, ohne zu bedenken, wie diese die vorhandenen Technologien ergänzen werden. Die fehlende Integration von Geräten und Ausrüstungen führt letztlich zu einem uneinheitlichen System, das nicht so funktioniert, wie es sollte.

Dieser bruchstückhafte Ansatz bei der Konzeption und Planung von Sicherheitssystemen wird häufig durch uneinheitliche und unzureichende staatliche und lokale Finanzmittel verursacht. K-12-Schulen sind insbesondere auf staatliche und bundesstaatliche Zuschüsse angewiesen, um Haushaltsdefizite auszugleichen, und die Finanzierungslücke vergrößert sich in der Regel im Laufe der Zeit, wodurch sich die Sicherheitsprobleme beschleunigen.

Kommunikation

Die Sicherheit im K-12-Bereich wird auch durch das Fehlen konsistenter und einheitlicher Notfallprotokolle und Formulierungen beeinträchtigt. Interessanterweise verwenden viele Bezirke im ganzen Land nach wie vor individuelle oder einzigartige Notfalleinsatzformulierungen für Vorfälle auf dem Schulgelände**. Dies kann zu Problemen führen, wenn mehrere Schulbezirke, die in den Zuständigkeitsbereich einer Strafverfolgungsbehörde fallen, unterschiedliche Notfallcodes verwenden oder wenn umgekehrt ein Bezirk während eines Notfalls von mehreren Zuständigkeitsbereichen betreut wird.** So könnte beispielsweise Distrikt A den "Code Red" für eine Abriegelung und den "Code Yellow" für eine gesicherte Umgrenzung verwenden, während Distrikt B den "Hard Lockdown" für eine Abriegelung und den "Soft Lockdown" für eine gesicherte Umgrenzung verwendet. Dies kann zu großer Verwirrung und einer verzögerten Reaktion bei einem kritischen Vorfall führen, bei dem die Zeit von entscheidender Bedeutung ist.

Die Kommunikationsprobleme werden noch verschärft, wenn benachbarte Bezirke und Ersthelfer bei der Auswahl und dem Kauf von Sicherheits- und Notfalleinrichtungen und -technologien nicht zusammenarbeiten. Oft wird den Distrikten die Fähigkeit einer Technologie verkauft, direkt mit

den Strafverfolgungsbehörden zu kommunizieren, um die Notfallmaßnahmen zu beschleunigen. Dies setzt jedoch voraus, dass die ersteintreffenden Behörden die Technologie gründlich verstehen und ihre Handhabung beherrschen. Wenn sich mehrere Schulbezirke, die einer einzigen Strafverfolgungsbehörde unterstehen, nicht für ein gemeinsames Produkt entscheiden, müssen die ersten Einsatzkräfte bei einem kritischen Vorfall mit mehreren Systemen arbeiten. Distrikt A könnte beispielsweise Technologie 1 verwenden, die Interoperabilität mit seiner Zentrale oder PSAP bietet. Der Disponent muss sich anmelden und über einen sicheren Kanal oder ein Portal direkt mit dem Bezirk kommunizieren. Distrikt B hingegen könnte ein anderes Technologiesystem verwenden, das völlig andere URL-Portal-Anmeldedaten erfordert, wobei die Benachrichtigung über einen anderen Kanal erfolgt. Dies birgt ein großes Potenzial für menschliche Fehler, die bei der Reaktion auf einen kritischen Vorfall auftreten können.

Cyber-Bedrohungen

Während die physische Sicherheit für K-12-Schulen nach wie vor ein Schwerpunkt ist, stellt die Cybersicherheit ein zunehmendes Sicherheitsrisiko im Bildungsbereich dar. Dazu gehören Ransomware, Datenschutzverletzungen, Social Engineering, Phishing und grundlegende Cybersicherheit. Da die Sicherheitstechnologie den Zugang zum Internet und den darin befindlichen elektronischen Systemen ermöglicht, ist der Bedarf an "Sicherheit der Sicherheit"-Geräten von entscheidender Bedeutung.

Bildung in der Zukunft

Kohärente Planung

K-12-Schulen im ganzen Land **erkennen** allmählich**, wie wichtig es ist, ihre Sicherheitssysteme und -abläufe** auf der Grundlage komplexer Sicherheitsbewertungen, Sicherheitsrisikobewertungen für Unternehmen oder strategischer Masterpläne auszubauen. Die Identifizierung der Bedürfnisse, Schwachstellen, Vermögenswerte, Lücken und Bedrohungen eines Bezirks ist von entscheidender Bedeutung, aber die Implementierung von mehrschichtigen Sicherheitsstrategien, die sich auf die Fähigkeit konzentrieren, diese Schwachstellen und Bedrohungen abzuschrecken, zu erkennen, zu verzögern und abzuwehren, ist von größter Bedeutung. Und ein methodischer Ansatz kann die Fähigkeit eines Distrikts sicherstellen um sowohl kurz- als auch langfristige Sicherheitsziele zu erreichen.

Da eine angemessene Finanzierung für die Unterstützung dieses Ansatzes unerlässlich ist, profitieren K-12-Schulen von der Zusammenarbeit mit vertrauenswürdigen Partnern, die die internen Ressourcen für die Erstellung von Zuschüssen ergänzen. Das SLED-Team von Convergint bietet umfassende Unterstützung bei der Vergabe von Zuschüssen und der Finanzierung. Dazu gehört auch professionelle Hilfe bei der Erstellung und Verfeinerung von Förderanträgen.

Mehrschichtige Sicherheit

Die Partner Alliance for Safer Schools (PASS K-12) bietet Leitlinien und bewährte Verfahren für die Sicherheit an Schulen.

Viele Schulen folgen diesen Empfehlungen und verfolgen bereits ein mehrschichtiges Sicherheitskonzept, das sich in den kommenden Jahren noch weiter durchsetzen dürfte.

Die Verstärkung von fünf physikalischen Schichten kann ein breites Spektrum von Bedrohungen abdecken, da jede aufeinanderfolgende Schicht spezifische Komponenten zur Abschreckung, Erkennung/Verzögerung und Reaktion auf feindliche Verhaltensweisen bereitstellt, falls andere Schichten umgangen oder durchbrochen werden.

Jede Schicht umfasst grundlegende Schutzkomponenten der Sicherheit:

- Richtlinien und Verfahren
- Menschen (Rollen und Ausbildung)
- Architektur
- Kommunikation
- Zugangskontrolle
- Video-Überwachung
- Erkennung und Alarm

Und innerhalb jeder Schicht gibt es verschiedene Sicherheitsstufen. Einfach ausgedrückt**, bietet die erste Ebene einen guten Basisschutz, während die letzte Ebene den umfassendsten Ansatz für die Sicherheit von K-12 verspricht**. Viele Schulen sind nicht in der Lage, Maßnahmen zu implementieren, die über die erste und zweite Stufe hinausgehen, oder haben keinen Bedarf dafür.

Convergint bietet Schuladministratoren Tools, mit denen sie und unter Berücksichtigung der verfügbaren Ressourcen und Finanzmittel maßgeschneiderte Sicherheitspläne entwickeln, die bewährte Praktiken und Verfahren beinhalten. Denken Sie daran, dass ein mehrstufiges Sicherheitskonzept zwar kostspielig sein kann, die PASS-Richtlinien jedoch auch kostengünstige Empfehlungen und praktische Überlegungen enthalten.

Kommunikation

K-12-Schulen profitieren von der Einführung einheitlicher und konsistenter Notfallprotokolle, die sich an bewährten Verfahren der Branche orientieren, wie z. B. dem Standard Response Protocol (SRP) der I Love U Guys Foundation. Dieses SRP, das bereits von 36.000 Schulen im ganzen Land angenommen wurde, verwendet eine gemeinsame Terminologie und Formulierung, die für Ersthelfer, Schulen und Gemeinden einheitlich ist. Dadurch können die Ersthelfer bei einem Vorfall die Situation besser verstehen und mit mehr Klarheit bewältigen. Es wird erwartet, dass sich weitere Schulsysteme anschließen werden, sobald sich dies herumspricht. Wenn sich ein Vorfall weiterentwickelt, werden möglicherweise auch benachbarte Bezirke aufgefordert, verstärkte Maßnahmen zu ergreifen.

Cyber-Bedrohungen

Als Reaktion auf die Cyber-Bedrohung **werden die Schulbezirke wahrscheinlich mehr Ressourcen** für die Sensibilisierung, Schulung und Härtung der Ausrüstung **bereitstellen**. Letzteres sollte mit der Evaluierung von Kameras und anderen physischen Sicherheitsgeräten beginnen, die möglicherweise fehlerhafte Anmeldedaten, veraltete Firmware oder gefährliche Sichtbarkeit bei offenen Zugängen/Gästen aufweisen.

Luftfahrt jetzt

Flughäfen haben mit einem Anstieg von Sicherheitsverletzungen zu kämpfen. Dies kann zur Schließung des Flughafens und zu Geldstrafen seitens der FAA und TSA führen, was sehr kostspielig sein kann. Infolgedessen verstärken die Einrichtungen die Einbruchserkennung mit Kameras, Radar, Lidar und Zaunerkennungstechnologien. KI spielt eine Rolle beim Fehlalarmmanagement.

Auch das Bewusstsein für die Bedrohung durch Insider ist gestiegen, was die TSA dazu veranlasst hat Screening-Verpflichtungen für Mitarbeiter und spezielle Schulungen einführen. Dazu gehören auch Cyber-Schulungen und Protokolle, um bewährte Praktiken und den Schutz von Geräten mit Hilfe spezieller Software zu verstärken.

Luftfahrt in der Zukunft

In der Luftfahrt wird es in Zukunft wahrscheinlich eine Vielzahl von Technologien zur Optimierung der Sicherheit geben, darunter PSIM und modernere Beschallungssysteme. Zusätzlich zu den Anforderungen des Risikomanagements besteht auch die Notwendigkeit, die betriebliche Effizienz zu verbessern. Lidar-/Sensortechnologien können beispielsweise sowohl die Sicherheit als auch die Steuerung des Verkehrsflusses (von Bordstein zu Bordstein oder von Bordstein zu Bordstein) unterstützen und eine Einnahmequelle darstellen.

Die Kosten von physischen oder Cyber-Angriffen

SLED-Einrichtungen können **infolge eines physischen oder Cyberangriffs** erhebliche Verluste erleiden, von denen die wichtigsten sind:

1. **Menschliches Leben**
   Das bedrohlichste Ergebnis eines physischen Angriffs ist natürlich der Verlust von Menschenleben. Bedauerlicherweise gibt es dafür zu viele Beispiele im öffentlichen Raum, um sie zu nennen.

2. **Reputation/Vertrauen**
   Schulen und öffentliche Einrichtungen leben vom Vertrauen der Gemeinschaft. Wird der Eindruck erweckt, dass sie auf einen Sicherheitsvorfall nicht vorbereitet sind, kann dies ihren Ruf erheblich beeinträchtigen. Dies könnte die Bürger dazu veranlassen, die Schule zu wechseln, jemanden aus dem Amt zu wählen oder sogar umzuziehen.

Bedrohlichste zukünftige Risiken

Bei der Bewältigung physischer Bedrohungen müssen alle SLED-Einrichtungen genau darauf achten, dass die Lösungen nicht zu weiteren Problemen wie Cyberrisiken führen. Insbesondere müssen Schutzvorkehrungen getroffen werden, damit die physische Sicherheitsausrüstung nicht zu einem Vektor für Cyber-Bedrohungen wird. Vielen öffentlichen Einrichtungen, Schulbezirken, Campus-Sicherheitsdiensten und Kommunalverwaltungen fehlt es an Personal für die Verwaltung und Wartung von Systemen zum Schutz vor Cyber- und anderen Risiken. Sie müssen sich daher auf die Sicherheitsvorkehrungen von Anbietern verlassen. Letztendlich minimiert die Verstärkung und Vereinfachung der Lösung für den Benutzer die Auswirkungen auf den täglichen Betrieb und optimiert den Schutz.

Sicherheitstechnische Gegenmaßnahmen

Viele öffentliche Räume sind von Natur aus offen, so dass sich dort häufig Personen aufhalten, die nicht unbedingt "eingeladen" sind. Diese Einrichtungen beherbergen neben Mitarbeitern, der allgemeinen Öffentlichkeit und Studenten oft auch Besucher. Auch wenn der offene Zugang scheinbar im Widerspruch zur Sicherheit steht**, können beide Aspekte nebeneinander bestehen, wenn die Sicherheitstechnologie vollständig in eine nahtlose Plattform integriert ist**, die eine optimale Reaktion und forensische Berichterstattung unterstützt.

Convergint geht diese Herausforderung mit einem beratenden Ansatz zur Systembewertung und Bedarfsermittlung an. Dabei konzentrieren wir uns darauf, die größten Lücken und/oder den größten Bedarf des Kunden zu ermitteln, wobei wir unsere eigenen Richtlinien und branchenübliche Best Practices wie PASS für sicherere Schulen nutzen. Wir stellen die passenden technologischen Alternativen zusammen und nutzen unsere Erfahrung, um den pragmatischsten Ansatz zu finden, um mit einem bestimmten Sicherheitssystem von Punkt A nach Punkt B zu gelangen.

Das SLED-Team von Convergint erkennt leicht Lücken in der Risikoexposition und weiß, wie man geeignete Lösungen findet. Und da wir nicht auf Partner angewiesen sind, erhalten unsere Kunden Optionen, die auf ihre Bedürfnisse zugeschnitten sind. Insbesondere werden unsere Lösungen durch Prozessempfehlungen ergänzt, wie die folgenden Beispiele zeigen:

Beispiel 1

Herausforderung: Verbrechensverhütung

Ausrüstungsempfehlung: LPRs, Kameras,

Einzelheiten: Convergint empfiehlt, in den Anträgen auf Geschäftslizenzen die Verpflichtung des Eigentümers zu vermerken, bei Ermittlungen mit der Polizei zusammenzuarbeiten oder seine Kameras zu vernetzen. Dies wird zu einer schnelleren Reaktion, zur Aufklärung von Verbrechen und zur Situationserkennung beitragen.

Beispiel 2

Herausforderung: Sicherheit der Beamten,

Öffentlichkeitsarbeit/Wahrnehmungsmanagement Ausrüstungsempfehlung:

Am Körper getragene Kameras

Einzelheiten: Convergint empfiehlt, dass alle Polizeibeamten Körperkameras tragen, um sicherzustellen, dass sie in der Lage sind, die Details eines Vorfalls aus der Perspektive des Beamten wiederzugeben. Dadurch wird die Wahrscheinlichkeit einer falschen Beschwerde gegen einen Polizeibeamten gesenkt.

Beispiel 3

Herausforderung: Lock-up Management

Ausstattungsempfehlung: Überwachungskameras, Zugangskontrolle und Panikalarm

Einzelheiten: Convergint empfiehlt die Zugangskontrolle in Haftanstalten, um den internen Aufseher zu alarmieren, damit er den Gefangenen in den erforderlichen Abständen kontrolliert. Die Ausweise der Zugangskontrolle überprüfen die Einlasskontrollen. Das VMS kann in die Zugangskontrolle integriert werden, um die Check-Ins einzusehen und sicherzustellen, dass sowohl die Gefangenen als auch die Wärter geschützt sind.

Verbesserung der Effektivität des Sicherheitspersonals/ Kostenreduzierung

Effektivität der Arbeitskräfte

Sicherheitsausrüstungen können ein Multiplikator sein, der die Gesamtwirksamkeit des Sicherheitsplans erhöht, aber sie können auch zu einer zusätzlichen Komplexität führen, die von den Ressourcen des Kunden nicht ohne weiteres aufgefangen werden kann. In der Folge erfordert jede Ausrüstung eine gründliche Evaluierung. Wenn beispielsweise mehr Kameras installiert werden, kann man davon ausgehen, dass weniger Wachpersonal vor Ort ist, was die Effizienz erhöht. Allerdings erfordern zu viele Kameras komplexere Überwachungsmaßnahmen, wie z. B. ein voll besetztes Command-and-Control-Center.

Keines der Geräte in einem Sicherheitsplan sollte als eigenständige Anlage betrachtet werden. Ein Vape-Detektionssystem in Schultoiletten oder ein Schützen-Detektionssystem in einer öffentlichen Einrichtung mag wie eine überzeugende Lösung für ein sehr dringendes Problem aussehen, **aber es wird ohne Wartung, Prüfung, Überwachung und Integration** in das Gesamtsystem **nicht optimal wirksam sein**. Die Integration ist besonders wichtig. Wenn eine Behörde über ein Videoüberwachungs-, ein Alarm- und ein Zutrittskontrollsystem verfügt, diese aber nicht in ein einziges System integriert sind, muss das Sicherheitspersonal an drei verschiedenen Arbeitsplätzen arbeiten, nur um die Systeme zu überwachen. Das ist eindeutig ineffektiv.

Kostenreduzierung

Der ROI einer jeden Technologieinvestition hängt von den anfänglichen Investitionskosten und den laufenden Betriebskosten ab. Es ist wichtig, nicht nur die Anfangsinvestitionen zu berücksichtigen, sondern auch die Zeit und die Ressourcen, die für die Verwaltung und Wartung dieser Systeme erforderlich sind. Die Personalausstattung ist ein entscheidender Faktor in dieser Gleichung.

Bei jeder Entscheidung über eine Technologieinvestition müssen sowohl die finanziellen Aspekte als auch die allgemeinen Geschäftsziele berücksichtigt werden. Öffentliche Einrichtungen konzentrieren sich im Allgemeinen mehr auf die Verringerung von Sicherheitsvorfällen als auf die Maximierung des Gewinns, aber auch andere geschäftliche Anforderungen spielen eine Rolle. Alle müssen geprüft werden, um eine bessere Rentabilität der Investition in Sicherheitstechnologie zu erreichen. Zum Beispiel: Gegensprechanlage/Massenkommunikation Sicherheitsvorfälle zu verwalten, sondern erleichtern auch die Übertragung von Kommunikationsmöglichkeiten für die Besucherverwaltung. Die Vorteile gehen über die Sicherheit hinaus.

Verwaltung des Sicherheitsbudgets

Die Budgetierung ist für öffentliche Einrichtungen oft eine Herausforderung, und Zuschüsse sind eine hervorragende Lösung für die Finanzierung wichtiger Sicherheitsausgaben. Dennoch sind viele SLED-Kunden mit dem Prozess der Identifizierung von Finanzierungsmöglichkeiten und dem Durchlaufen der entsprechenden Schritte überfordert. Convergint hat daher ein Team für Zuschüsse und Finanzierungen eingerichtet, das unsere Kunden bei der Beschaffung von Mitteln für Sicherheitsinvestitionen unterstützt.

Darüber hinaus können wir das Argument unterstützen, dass finanzielle und/oder personelle Ressourcen von anderen Abteilungen bereitgestellt werden müssen, um erfolgreiche Sicherheitsprogramme zu gewährleisten. Abteilungsübergreifende Finanzmittel können Zuschüsse ergänzen, und engagierte Mitarbeiter können den Unterschied ausmachen, wenn es um die Genehmigung von Zuschüssen geht. Gut integrierte Organisationen werden von den Entscheidungsträgern für Zuschüsse gut aufgenommen.

Wenn der Kunde in der Lage ist, die Anforderungen anderer Unternehmensbereiche über die Sicherheit hinaus zu erfüllen, ist es wahrscheinlicher, dass er die notwendige abteilungsübergreifende Unterstützung erhält. Damit ist der Grundstein für künftige Beziehungen, wiederkehrende Verpflichtungen und einen proaktiveren Ansatz bei Sicherheitsinvestitionen gelegt.

Vertragsfahrzeuge als Option

Staatliche, städtische, kommunale, K-12-Schulen und höhere Bildungseinrichtungen können die Vorteile von Contract Vehicles nutzen, um die neueste innovative Technologie zu wettbewerbsfähigen Preisen zu erwerben und so die allgemeine Sicherheit zu erhöhen. Die richtigen Produkte und sorgfältig konzipierten Systeme können die Effizienz steigern und den Betrieb verbessern.

Contract Vehicles erleichtern den Beschaffungs- und Budgetierungsprozess durch im Voraus ausgehandelte Preise für wettbewerbsfähige Angebote, die durch Ausschreibungsverträge gesichert werden. **Ein Contract Vehicle ist im Wesentlichen eine rationalisierte Methode, die sowohl staatliche als auch kommunale Behörden für den Kauf von Waren und Dienstleistungen nutzen, von iPads bis hin zu Aufzügen**. Die kooperativen Beschaffungsverträge von Convergint gewährleisten, dass wir unseren Kunden wettbewerbsfähige Preise bieten können.

Durch die Nutzung der kollektiven Kaufkraft mehrerer Organisationen können die Agenturen wettbewerbsfähige Preise für Produkte und Dienstleistungen erzielen. Darüber hinaus ermöglicht die Bündelung der Anforderungen aller Kunden die Standardisierung von Produkten und Dienstleistungen, was zu einer größeren Konsistenz und Effizienz bei der Beschaffung führt. Die Verwaltungskosten werden durch die Aufteilung des Aufwands auf mehrere Stellen gesenkt. Convergint verfügt über eine Vielzahl von Vertragsinstrumenten, die alle einen effizienten Einkauf ermöglichen.

Einsatz von Sicherheitstechnologie zur Verbesserung der Wettbewerbsfähigkeit von Unternehmen oder Marken

Sicherheit betrifft nicht nur eine Seite der Bilanz. Sicherheit ist ein Verkaufsargument. Sicherere öffentliche Räume fördern die Marke und den Ruf der Stadt. Dies wiederum zieht Unternehmen, Einwohner und Besucher an. Auch für die Schulen ist dies von Nutzen. **Hochschulen und Universitäten nutzen das Thema Sicherheit als wichtigstes Verkaufsargument bei der Anwerbung von Studenten und der Unterstützung durch deren Eltern**. Das Fazit: Ein gut gemachtes Sicherheitsprogramm kann das Kundenerlebnis erheblich verbessern und sich anschließend für die Förderung der angestrebten Geschäftsergebnisse eignen.

Zusammenfassung der Empfehlungen, 2024

SLED-Sicherheitsentscheider sind ständig bestrebt, kurz- und langfristige Ziele zu erreichen, und überlegen daher, welche Lösungen in ihren aktuellen Plan unter Einhaltung der geplanten Budgets integriert werden können. Es ist wichtig, das Ziel vor Augen zu haben. **Wir raten ihnen** daher **dringend, einen Schritt zurückzutreten und mit einem Partner zusammenzuarbeiten, der sich in diesem Bereich auskennt**. Ein ganzheitlicher 5-Jahres- oder sogar 10-Jahres-Sicherheitsplan ist von unschätzbarem Wert, selbst wenn einige der in diesem Plan enthaltenen Punkte nie umgesetzt werden. Alle Herausforderungen müssen berücksichtigt werden, um alle potenziellen Lösungen aufzudecken. Ein strategischer Fahrplan beseitigt die Risiken, die mit einer reaktionären Reaktion verbunden sind, und sorgt stattdessen für einen maßvolleren Ansatz beim Bedrohungsmanagement. Der erste Schritt zum Erfolg ist eine umfassende Sicherheitsbewertung. Dies ist kein großer Budgetposten und bringt letztlich zahllose Vorteile, angefangen bei einer besseren Kontrolle der größten Risiken für SLED-Kunden: reaktionäre Planung und das Versäumnis, echte Integration für beste Ergebnisse zu erreichen.

Das SLED-Team von Convergint ist bereit, seinen Kunden zu helfen, von umfassenden ESRM-Standortbewertungen (Enterprise Security Risk Management) über kreative und technologisch leistungsstarke Lösungen bis hin zu Zuschüssen und Finanzierungshilfen. Unser Erfolg wird durch den Erfolg unserer Kunden belegt.