Risiko, Widerstandsfähigkeit und Sicherheit für Behörden und Städte

Bewährte Verfahren und Technologien zur Aufrechterhaltung des Geschäftsbetriebs

Alcatel·Lucent Enterprise

Inhaltsverzeichnis

Sicherheit und Widerstandsfähigkeit haben oberste Priorität

Behörden und Städte auf der ganzen Welt sehen sich heute mit einer Polykrise konfrontiert, d. h. mit einer Kombination aus Cyber- und physischen Risiken, die Bürger, wichtige Dienste und sensible Daten bedroht.

In der heutigen Welt erwarten die Bürger Dienstleistungen, die über sichere Websites angeboten werden, und sind darauf angewiesen. Aber auch die Arbeitnehmer erwarten, dass sie je nach ihren Bedürfnissen und Vorlieben von zu Hause aus oder im Büro arbeiten können. Diese neuen Anforderungen sowie die exponentielle Ausbreitung von Geräten des Internets der Dinge (IoT) dehnen die Netzwerkgrenzen aus. Und das zu einer Zeit, in der geopolitische Spannungen und politische Polarisierung das Risiko von Cyberangriffen erhöhen.

Darüber hinaus hat das Dark Web einen rentablen Markt für den anonymen Verkauf sensibler Regierungsdaten geschaffen, was Behördensysteme zu sehr attraktiven Zielen für Informationsdiebstahl macht. Außerdem bietet es einen Online-Hafen für die Koordinierung von Angriffen auf Regierungen.

Vandalismus, Terrorismus, Unruhen und Kriminalität nehmen ebenfalls zu und stellen eine immer größere Bedrohung für die zivile und militärische Infrastruktur und die Aufrechterhaltung des Geschäftsbetriebs dar. Hinzu kommen Unwetter und Naturkatastrophen, die es sehr schwierig, wenn nicht gar unmöglich machen, öffentliche Dienste zu gewährleisten und die Bürger zu schützen, wenn es am nötigsten ist. Und in Zeiten, in denen die weltweite Inflation die Etats belastet, ist der Bedarf an Digitalisierungsinitiativen, die die betriebliche Flexibilität, Effizienz und Produktivität steigern, so groß wie nie zuvor.

Diese Risiken machen es für Behörden und Städte schwieriger denn je, die immer strengeren Vorschriften zur Datenhoheit und zum Datenschutz einzuhalten. Infolgedessen drohen Geldstrafen und Klagen wegen Rechtsverletzungen.

Angesichts dieser neuen Realität können sich die Behörden und Städte nicht mehr auf ihre bisherigen Strategien für Sicherheit und Widerstandsfähigkeit verlassen. Zur Eindämmung dieser Risiken müssen sie entschlossene, proaktive Schritte unternehmen, um ihre allgemeine Sicherheitslage zu verbessern. Es bedarf eines neuen und innovativen Ansatzes, der stärker auf die wichtigsten Bedrohungen von heute ausgerichtet ist. Durch mehr Sicherheit werden Behörden und Städte besser in der Lage sein, ihre Bürger und Abläufe zu schützen und ihre Widerstandsfähigkeit zu stärken, damit sie unter allen Umständen die Aufrechterhaltung ihres Betriebs gewährleisten können.

Die Risiken sind allgegenwärtig

Leider schieben Behörden und Städte Maßnahmen zur Risikominderung nur allzu oft auf die lange Bank, vor allem, wenn sich brisante Geschehnisse nur an weit entfernten Orten ereignen. Tatsache ist jedoch, dass jede staatliche Einrichtung ein potenzielles Ziel für Angriffe ist.

Aktuelle Faktenlage

- Die Zahl der Cyberangriffe auf staatliche Einrichtungen ist in der zweiten Jahreshälfte 2022 [1] um 95 Prozent gestiegen.
- Der Angriff auf die Regierung von Costa Rica wurde als einer der kostspieligsten Angriffe des Jahres angesehen[2], und Ransomware war die bevorzugte Methode für Angriffe auf öffentliche Dienste[3].
- Es wird geschätzt, dass bis 2025 30 Prozent der kritischen Infrastrukturorganisationen von einer Sicherheitsverletzung betroffen sein werden[4].

Mit der wachsenden Stadtbevölkerung[5] nehmen auch die Risiken für Behörden und Bürger zu. Die Vereinten Nationen raten den staatlichen Stellen, sich dafür einzusetzen, dass Städte und Gemeinden inklusiver, sicherer, widerstandsfähiger und nachhaltiger werden, wie es im Ziel 11[6] formuliert ist.

---

[1] Cyberattacks against governments jumped 95% in last half of 2022, CloudSek says. CSO Vereinigte Staaten, Januar 2023.

[2] The 13 Costliest Cyberattacks of 2022: Looking Back. Security Intelligence, Dezember 2022.

[3] Grundsatzdokument: Nationale Cyberstrategie 2022. U.K Cabinet Office, Dezember 2022.

[4] Gartner Predicts 30% of Critical Infrastructure Organizations Will Experience a Security Breach by 2025. Gartner, Dezember 2021.

[5] Urban Development. Weltbank, April 2023.

[6] Ziel 11: Städte und Siedlungen inklusiv, sicher, widerstandsfähig und nachhaltig gestalten. Vereinte Nationen.

In Anbetracht all dieser Faktoren wird deutlich, dass Behörden und Städte ihr Augenmerk verstärkt auf Risiken, Widerstandsfähigkeit und Sicherheit richten müssen, damit folgende Punkte gewährleistet sind:

- **Sicherstellung der kontinuierlichen Verfügbarkeit wichtiger Dienste und des Schutzes sensibler Daten**, insbesondere in unerwarteten Krisenzeiten
- **Minimierung der Kosten für Risikoversicherungen** durch Implementierung des richtigen Schutzes für jede Art von Cyber- und physischen Risiken, denen sie ausgesetzt sind
- **Verringerung der finanziellen Verluste** aufgrund von Cyber- und physischen Angriffen, Klagen durch Bürger und Geldstrafen für Datenschutzverletzungen und Nichteinhaltung von Vorschriften
- **Aufrechterhaltung des guten Rufs und des Vertrauens der Bürger**, die beide durch Verspätungen und Ausfälle von Diensten beschädigt werden oder ganz verloren gehen können
- **Schutz der Bürger** durch Bereitstellung wichtiger Informationen zu den Themen Gesundheit, Sicherheit und Schutzmaßnahmen

Die Digitalisierung ist mit Vorteilen und Risiken verbunden

In der heutigen digitalen Welt sind Menschen, Objekte und Prozesse vernetzt. Dank dieser Vernetzung eröffnen sich den Behörden und Städten folgende Möglichkeiten:

- Nutzung der IoT-Technologie und der damit verbundenen Informationen
- Automatisierung von Arbeitsabläufen zur Steigerung der Effizienz und Verkürzung der Reaktionszeiten für Bürger
- Verwendung präziser Echtzeitdaten, um die Transparenz zu erhöhen und fundierte Entscheidungen zu treffen
- Implementierung intelligenter Gebäudeanwendungen, die einen nachhaltigeren, kostengünstigeren und widerstandsfähigeren Betrieb ermöglichen

Diese Verbesserungen sind zwar für Behörden und Städte unerlässlich, um ihre Ziele zu erreichen, doch bringen die neuen Technologien auch eine Reihe neuer Cyber- und physischer Risiken mit sich, die es zu bewältigen gilt.

Neue Denkanstöße zum Thema Sicherheitsrisiken

Durch die Digitalisierung lassen sich Sicherheitsrisiken leichter ausnutzen, und Bedrohungen können sich schnell über vernetzte Systeme, Geräte und Anwendungen ausbreiten:

- Ein Ausfall in einem System kann sich auf alle Systeme ausweiten
- Hacker können Verbindungen zwischen Infrastrukturen zur Ausdehnung ihrer Reichweite missbrauchen
- Viren können sich über die Verbindungen in der gesamten Einrichtung verbreiten

Die Digitalisierung verschärft auch die Schnittstelle zwischen Cyber- und physischen Risiken. Angreifer können sich beispielsweise aus der Ferne in Rechenzentren von Behörden einhacken oder sich physischen Zugang verschaffen, indem sie ein elektronisches Türschloss knacken. In ähnlicher Weise können Sicherheitskameras durch einen Cyberangriff oder einen physischen Angriff deaktiviert, abgeschaltet oder wieder mit zuvor aufgezeichneten Videofeeds verbunden werden, sodass sie in allen Fällen keinerlei Schutz mehr bieten.

Die Konvergenz zwischen IT und Betriebstechnologien (OT) schafft neue Möglichkeiten für Angriffe. Jetzt können Hacker einen IoT-Sensor angreifen, um Zugang zum Netzwerk und den damit verbundenen hochwertigen Systemen und Informationsressourcen zu erhalten. Umgekehrt können sie sich direkt in das Netzwerk einhacken und es als Einfallstor für Angriffe auf wichtige Gebäudesysteme wie Aufzüge, Rauchmelder, Feuermelder und Sprinkleranlagen nutzen.

Hinzu kommen neue Technologien, die sowohl für als auch gegen öffentliche Einrichtungen eingesetzt werden können. Nehmen wir als Beispiel die künstliche Intelligenz (KI). KI hilft, Cyber- und physischen Bedrohungen vorzubeugen, sie zu bekämpfen und die Reaktion darauf zu beschleunigen, aber sie ermöglicht es auch böswilligen Akteuren, Passwörter für Behördensysteme zu knacken. Eine ähnliche Situation ist in Zukunft beim Quantencomputing zu erwarten, das einerseits Regierungen und Behörden bei der Lösung komplexer Probleme helfen wird, andererseits aber auch die Entschlüsselung sensibler Informationen erleichtert.

Individuelle Aspekte und Herausforderungen

Die spezifischen Risiken, die mit der Digitalisierung einhergehen, hängen von den eingesetzten Technologien ab. Moderne Netzwerke und Kommunikationstechnologien bergen drei Hauptrisiken:

- **Ausfälle**: Hardware- und Softwarefehler und -ausfälle können jederzeit und ohne Vorwarnung auftreten. Brände, Überschwemmungen, extreme Witterungsbedingungen und andere unvorhersehbare Faktoren können ebenfalls zu Ausfällen führen, während Stromausfälle die Qualität und Stabilität der Stromversorgung beeinträchtigen können, was zu Störungen und Versagen führt.
- **Cyberangriffe**: Vertrauliche Daten können verloren gehen oder gestohlen werden, und Netzwerke und Systeme können beschädigt werden, wodurch Behördendienste und -tätigkeiten verlangsamt oder ganz eingestellt werden. Ransomware-Angriffe können ganze Netzwerke und Systeme in Geiselhaft nehmen und den Zugriff auf Daten und wichtige Funktionen unmöglich machen.
- **Veralterung**: Technologieanbieter können den Support für Hard- und Software einstellen, und Engpässe in der Lieferkette können es logistisch unmöglich oder zu teuer machen, Lösungen weiter zu nutzen. Auch Änderungen der gesetzlichen Vorschriften können dazu führen, dass technologische Lösungen nicht mehr zeitgemäß sind.

Jedes dieser Risiken kann andere Risiken nach sich ziehen. Ein technischer Ausfall oder eine veraltete Technologie kann die Tür für Cyberangriffe öffnen. Und Cyberangriffe können einen technischen Ausfall verursachen oder deutlich machen, dass die Technologie veraltet ist.

Zusammengenommen bedeuten diese Risiken, dass Regierungen und Städte ihre Präventions-, Schutz- und Reaktionsmaßnahmen verbessern müssen, um Bedrohungen auszuschalten. Untätigkeit kann nicht mehr hingenommen werden. Sich weiterhin auf veraltete und isolierte Netzwerke und Kommunikationstechnologien zu verlassen, während sich die Risiken weiter vervielfachen, ist aus keiner Perspektive ein gangbarer Weg.

Ein ganzheitlicher Ansatz und ein standardisierter Prozess

Jede Behörde und Stadt muss einen strategischen und taktischen Ansatz für Sicherheit und Widerstandsfähigkeit entwickeln, der auf ihr individuelles Risikoprofil, ihre geografische Lage, ihre Aufgabe, ihr Budget und andere Anforderungen zugeschnitten ist. Auch wenn die Ergebnisse ihrer Maßnahmen unterschiedlich ausfallen werden, sind ein standardisierter Ansatz und der Austausch bewährter Verfahren für bessere Ergebnisse von Nutzen.

Ein ganzheitlicher Ansatz zur Risikominderung ermöglicht es Behörden und Städten, die Sicherheit und Widerstandsfähigkeit in drei Schlüsselbereichen ihres Aufgabenbereichs zu erhöhen, darunter:

- **Bürger**: Schutz der persönlichen Sicherheit und der Daten vor allen Bedrohungen
- **Betrieb**: Aufrechterhaltung von Funktionen, Transaktionen und Diensten in jeder Situation
- **Gebäude**: Erhöhung der Intelligenz und Sicherheit von Arbeitsplätzen und Räumen in Behörden

Vier Schritte zur Erhöhung der Sicherheit und Widerstandsfähigkeit

Mit Blick auf die oben genannten Bereiche können die folgenden Schritte Behörden und Städten helfen, ihr Risikoprofil zu bestimmen und die geeigneten Netz- und Kommunikationslösungen für ihre jeweilige Situation auszuwählen.

1. **Evaluieren**: Ermitteln Sie die Cyber- und physischen Risiken, die gefährdeten Bereiche und die möglichen Folgen sowie die verschiedenen Möglichkeiten, in jeder Situation Angriffen vorzubeugen, sich zu schützen und darauf zu reagieren. Beginnen Sie mit einer Prüfung und bewerten Sie dann die Risiken und das Verlustpotenzial bei jedem festgestellten Sicherheitsrisiko. Dies hilft, die geeigneten Maßnahmen und Lösungen für jede Situation zu finden.

   Die Evaluierung ist zwar der erste Schritt, aber sie ist keine einmalige Angelegenheit. Um der sich schnell verändernden Bedrohungslandschaft zu begegnen, ist es wichtig, die Risiken regelmäßig neu zu analysieren und Cyber- und physische Ressourcen kontinuierlich auf neue Sicherheitsrisiken zu überwachen.
2. **Vorbeugen**: Wählen Sie Lösungen, mit denen Sie Cyber- und physische Risiken vermeiden oder eindämmen können. Nachfolgend finden Sie einige Beispiele:
   - Aus der Cyberperspektive sollten Sie nach Lösungen mit integrierten Sicherheitsfunktionen suchen, die nicht separat erworben oder verlängert werden müssen. Lösungen sollten die Sicherheit in jedem Schritt der Produktdefinition, -entwicklung und -bereitstellung berücksichtigen und zu einer Zero-Trust-Architektur und -Technologieumgebung beitragen. Sie sollten auch die automatische Sicherung und Wiederherstellung unterstützen und Informationen für Prüfungszwecke bereitstellen.
   - In physischer Hinsicht sollten Lösungen gefunden werden, die die Transparenz erhöhen und den Zugriff auf die Vermögenswerte erschweren. Lösungen für die Videoüberwachung, die Zugangskontrolle, das Asset-Tracking, die Erkennung von Einbrüchen und Alarmen, standortbezogene Dienste und Gesichtserkennung sind allesamt gute Beispiele.
3. **Schützen**: Entscheiden Sie sich für Lösungen, die einen Schutz vor Cyber- und physischen Risiken bieten. Nachfolgend finden Sie einige Beispiele:
   - Auf der Cyberseite sollten Sie sicherstellen, dass die Lösungen nach Sicherheitsstandards zertifiziert sind, native Verschlüsselungsfunktionen und fortschrittliche Authentifizierungsmechanismen enthalten und der Verbreitung von Cyberangriffen und Viren entgegenwirken.
   - Um den physischen Schutz zu verbessern, sollten Sie über die Videoüberwachung hinaus auch die Rolle von Kommunikation, Warnungen und Benachrichtigungen sowie Lösungen zum Schutz von Mitarbeitern an abgelegenen Orten berücksichtigen.
4. **Reagieren**: Wählen Sie Lösungen, die eine effiziente Wiederherstellung ermöglichen, z. B. im Falle eines Sicherheitsverstoßes:
   - Cyberlösungen sollten von einem Product Security Incident Response Team unterstützt werden, einen Prüfpfad und Wiederherstellungsverfahren bieten und die Wiederherstellung von Daten unterstützen.
   - Physische Lösungen müssen Befehls- und Kontrolloperationen (C2) und geschäftskritische Kommunikation unterstützen.

RRS-Framework für den öffentlichen Sektor, Regierungen und Städte

	1 Evaluieren	2 Vorbeugen	3 Schützen	4 Reagieren
Sicherheit	✓	✓	✓	
Widerstandsfähigkeit	✓	✓		✓
Cyberbereich	• Ermittlung von Risiken • Beurteilung • Kartierung von Vermögenswerten • Bewertung • Dauerüberwachung	• Integrierte Sicherheit • Risikobewertung/Prüfung • Beratung vor dem Verkauf • Schulung für Nutzer • Betrugserkennung • Backup-Verfahren • Einrichtung von Prüfpfaden • Robuste Geräte für schwierige Umgebungen • Redundanz	• Sicherheitszertifikate • Verschlüsselung • Authentifizierung	• PSIRT/CERT • Prüfpfad • Incident Management • Wiederherstellungsverfahren • Wiederherstellen
Physischer Bereich	• Ermittlung von Risiken • Beurteilung • Bewertung • Dauerüberwachung	• Videoüberwachung • Zugriffssteuerung • Asset-Tracking • Erkennung und Alarm • Standortbasierte Dienste • Gesichtserkennung • Redundanz	• Videoüberwachung • Kommunikation • Warnung und Benachrichtigung • Schutz dezentral arbeitender Mitarbeiter	• Kontrolle und Steuerung • Geschäftskritische Kommunikation

Angesichts der Risiken sind Widerstandsfähigkeit und flexible Reaktionsmechanismen der Schlüssel zum Erfolg

„ Widerstandsfähigkeit ist mehr als nur die Fähigkeit, sich schnell zu erholen. In der Wirtschaft bedeutet Widerstandsfähigkeit, Widrigkeiten und Schocks zu bewältigen und sich ständig anzupassen, um zu wachsen. Wirklich widerstandsfähige Unternehmen erholen sich nicht nur schneller, sondern gedeihen auch in feindlichen Umgebungen... Agilität ermöglicht es Unternehmen, gezielt auf jede Krise zu reagieren, anstatt unflexible Universallösungen anzuwenden."

— McKinsey & Company

Stärkung der Sicherheit und Widerstandsfähigkeit

Behörden und Städte, die den im vorherigen Abschnitt empfohlenen ganzheitlichen Ansatz und Prozess verfolgen, haben neue Möglichkeiten, Netzwerk- und Kommunikationslösungen zu nutzen, um die Sicherheit und Widerstandsfähigkeit von Bürgern, Betriebsabläufen, Gebäuden und Räumen zu erhöhen.

Schutz der Sicherheit der Bürger

Dank modernster Videoüberwachungslösungen können Behörden und Sicherheitskräfte Ereignisse und Notfälle direkt in Echtzeit verfolgen und sich so ein besseres Bild von der Lage machen. Sie können dann eine Plattform für die Orchestrierung der öffentlichen Sicherheit und das Management von Arbeitsabläufen nutzen, um dieses Wissen zu teilen und die Gegenmaßnahmen zu koordinieren. Teams aus verschiedenen Abteilungen, Behörden und Standorten können durch die optimale Kombination von Sprach-, Video- und Textkommunikation zeitnahe kontextbezogene Informationen und Erkenntnisse austauschen und so effizientere, effektivere und gemeinschaftliche Entscheidungen treffen.

Massenbenachrichtigungssysteme können Menschen und Prozesse schnell auf Notfälle aufmerksam machen, sodass sie schneller angemessen reagieren können. Anrufe von Mitarbeitern im Außendienst werden vorrangig an die Kontaktzentren der Behörden weitergeleitet, und die Funktion zur Aufrechterhaltung der Leitung sorgt dafür, dass die Ansprechpartner im Kontaktzentrum für Mitarbeiter und Bürger unter allen Umständen erreichbar bleiben. Kommunikationslösungen für Alleinarbeiter, Totmann-Situationen und Kontaktverfolgung beschleunigen die Reaktionen weiter und erhöhen das Bewusstsein für potenzielle Gefahrensituationen.

Zur Vorbeugung von Notfällen und zur Beschleunigung von Reaktionen können KI-Lösungen, die mit mehreren Datenquellen verbunden sind, zur Identifizierung von Risiken und potenziell problematischen Ereignissen sowie zur Automatisierung von Arbeitsabläufen eingesetzt werden.

Erhöhung der Zuverlässigkeit bei allen Vorgängen

Ein sicheres und stabiles Unternehmensnetzwerk unterstützt die geschäftskritische Kommunikation sowie die IoT-, Cyber- und physischen Sicherheitstechnologien, die für einen zuverlässigen Betrieb unerlässlich sind.

Die idealen Netzwerklösungen umfassen Funktionen, die für den Schutz des Zugangs zum Netzwerk und der darin enthaltenen Informationen entscheidend sind, wie z. B:

- **Abgesicherter Quellcode und abgesicherte Software auf Netzwerk-Switches**: Der Quellcode wird absichtlich variiert, um es potenziellen Angreifern zu erschweren, Sicherheitslücken auszunutzen. Darüber hinaus werden der Code und die Software von unabhängiger Seite überprüft und validiert, um ihre Integrität und Sicherheit zu gewährleisten.
- **Makro- und Mikrosegmentierung**: Im Zusammenhang mit Zero Trust wird der Segmentierung sowohl auf der Makro- als auch auf der Mikroebene besondere Aufmerksamkeit geschenkt. Bei der Makrosegmentierung wird das Netzwerk in verschiedene Zonen unterteilt, die auf Faktoren wie Funktion, Anwendung oder Benutzergruppe basieren, um kritische Anlagen und Ressourcen vom Rest des Netzwerks zu isolieren. Die Mikrosegmentierung verfolgt einen differenzierteren Ansatz und segmentiert das Netzwerk auf Benutzer- oder Geräteebene, um eine präzisere Kontrolle über den Netzwerkzugang und die Durchsetzung von Sicherheitsrichtlinien zu ermöglichen.
- **Autonomer Betrieb**: Durch die automatische Zuordnung von Anlagen und Ressourcen zu Makrosegmenten und die Anwendung von Richtlinien auf Benutzer- und Geräteebene lässt sich das Risiko menschlicher Fehler – eine häufige Ursache von Verletzungen der Cybersicherheit – verringern.
- **Robuste Geräte**: Netzwerkgeräte können schwierigen Bedingungen wie extremen Temperaturen und starken Vibrationen standhalten. Die Geräte unterstützen eine redundante Stromversorgung aus zwei Quellen, damit auch bei Stromausfällen ein kontinuierlicher Betrieb gewährleistet ist. Eine hohe mittlere Betriebsdauer zwischen Ausfällen (MTBF) kann die Zuverlässigkeit gewährleisten und unerwartete Ausfallzeiten und Störungen aufgrund von Pannen und Ausfällen minimieren.

Behörden und Städte erhalten außerdem die Flexibilität, Netzwerk- und Kommunikationslösungen sowohl vor Ort als auch in öffentlichen und privaten Cloud-Umgebungen einzusetzen. Diese Bereitstellungsoptionen ermöglichen geografische und räumliche Redundanzstrategien, die für die Aufrechterhaltung des Geschäftsbetriebs bei Ausfällen und Notfällen selbst an entfernten Standorten von entscheidender Bedeutung sind.

Erhöhung der Sicherheit in Gebäuden und Räumen

Ein sicheres Multiservice-Netz ist erforderlich, um die Anwendungen und Prozesse zu unterstützen, die zum Schutz vor Risiken und zur Aufrechterhaltung der Serviceverfügbarkeit zu jeder Zeit benötigt werden. Um die wachsende Zahl der mit dem Wi-Fi-Netz verbundenen drahtlosen Geräte zu unterstützen, benötigen Behörden und Städte außerdem ein robustes und zuverlässiges drahtloses Netzwerk, das reibungslos funktioniert, ohne dass es zu Überlastungen kommt, die seine Effizienz beeinträchtigen könnten.

Die gleichen modernen Videoüberwachungslösungen, die dem Schutz der Bürger dienen, tragen auch zur Sicherheit von Gebäuden und Räumen der öffentlichen Hand bei. Ergänzt werden diese Lösungen durch Asset-Tracking, das das Auffinden von Personen und wichtigen Gegenständen bei unerwarteten Ereignissen und Notfällen beschleunigt und erleichtert.

Behörden und Städte verfügen nun auch über die notwendigen Automatisierungsmöglichkeiten, um IoT-Lösungen für Sicherheitsanwendungen wie Zugangskontrolle und Asset-Tracking effizient implementieren und verwalten zu können. Sie können eine große Anzahl neuer IoT-Geräte mit gerätespezifischen Fingerabdruck-Verfahren sowie durch die Klassifizierung und Containerisierung von Geräten sicher und automatisch einbinden. Dadurch besteht keine Gefahr, dass abgelenktes IT-Personal versehentlich Sicherheitsrisiken schafft.

Ein Partner zur Unterstützung Ihrer Strategien

Da die Risiken für Behörden und Städte immer weiter zunehmen, steigt auch der Bedarf an einem kompetenten Technologiepartner.

Alcatel-Lucent Enterprise, ein Technologie-Innovator seit mehr als 100 Jahren, hat ein RRS-Framework (Risk, Resilience and Security) entwickelt, das auf die Anforderungen von Behörden und Städten abgestimmt ist. Das RRS-Framework umfasst die Prozesse, bewährten Verfahren und Lösungen, die Behörden und Städte benötigen, um Cyber- und physische Risiken zu antizipieren, zu überwachen, zu vermeiden und ihnen entgegenzuwirken.

Das ALE-Team aus hochqualifizierten Behördenexperten arbeitet mit Behörden- und Stadtverantwortlichen zusammen, um sie bei folgenden Aspekten zu unterstützen:

- Ermittlung ihrer individuellen Risiken und Auswahl der richtigen Lösungen zur Bewältigung dieser Risiken
- Überbrückung der Kluft zwischen Cyber- und physischer Sicherheit und Widerstandsfähigkeit
- Ausarbeitung von Argumenten für die Genehmigung des Etats

Flexible, vollständig konforme Lösungen

ALE integriert bereits in der Anfangsphase der Entwicklung Sicherheitsfunktionen in seine Netzwerk- und Kommunikationslösungen. Die Lösungen zeichnen sich durch folgende Merkmale aus, um ein Höchstmaß an Sicherheit und Widerstandsfähigkeit zu gewährleisten:

- Sie sind mit Sicherheitsmaßnahmen ausgestattet, denen Regierungen und Verteidigungsorganisationen auf der ganzen Welt vertrauen
- Sie werden mithilfe spezieller, sicherheitsspezifischer Verfahren getestet, z. B. mit Penetrationstests
- Sie halten globale, branchenspezifische und regionale Datensicherheits- und Datenschutzstandards ein, einschließlich der wichtigsten Sicherheitsstandards der Branche, wie Common Criteria EAL2+
- Sie können in einer beliebigen Kombination aus lokalen und Cloud-Modellen eingesetzt werden, um auch die komplexesten Anforderungen zu erfüllen
- Sie unterstützen offene Standards, um die Komplexität der Integration und Inkompatibilitäten zwischen Lösungen und Anbietern zu verringern

Zusätzlich zu den herkömmlichen Kaufmodellen bietet ALE Abonnementpläne an, mit denen Kunden Zugang zu den neuesten Technologien und Sicherheitsfunktionen erhalten und gleichzeitig ihr Budget nicht sprengen müssen. Darüber hinaus steht ein umfassendes Angebot an Dienstleistungen zur Verfügung, um Behörden und Städte in jeder Phase ihrer Entwicklung zu unterstützen.

Erfahrung + Kompetenz

Die Experten und Lösungen von ALE genießen das Vertrauen von Behörden und städtischen Einrichtungen auf der ganzen Welt. Dazu zählen beispielsweise:

- Metz Eurometropolis in Frankreich, wo ALE dem Ballungsraum geholfen hat, die Aufrechterhaltung kritischer Dienste und der Kommunikation zu gewährleisten, Notdienste schnell verfügbar zu machen und Nutzer und vernetzte Objekte auf sichere Weise gebäudeübergreifend zu verbinden.
- Die schottische Regierung, wo ALE-Lösungen eine konsistente, sichere und zuverlässige Infrastruktur und Netzwerkzugangskontrolle sowie eine verbesserte Datensicherheit für mehr als 40 Regierungsbehörden gewährleisten.
- Das US-Verteidigungsministerium, wo robuste, moderne Lösungen einsatzkritische Kommunikation und Anwendungen zuverlässig unterstützen und dabei alle Anforderungen in Bezug auf Umwelteinflüsse und Erschütterungen sowie die Anforderungen des Trade Agreement Act (TAA) und der Verteidigungszertifizierung erfüllen.
- Die Gwinnett County Public Schools in den USA, wo ALE-Lösungen die physische Sicherheit, Videoüberwachung, E-911, sichere Datenverarbeitung und vieles mehr in einem großen Schulbezirk unterstützen, in dem Sicherheit an erster Stelle steht.

Weitere Informationen

Wenn Sie erfahren möchten, wie Alcatel-Lucent Enterprise Ihrem Unternehmen helfen kann, Risiken zu minimieren und die Sicherheit und Widerstandsfähigkeit zu erhöhen, besuchen Sie die Website oder kontaktieren Sie uns noch heute.

DID23061901DE (Dezember 2023)

Alcatel·Lucent Enterprise