

Überwachung von physikalischen Gefahren in Datacentern

Von Christian Cowan
Chris Gaskins

White Paper Nr. 102

APC[®]
Legendary Reliability[®]

Zusammenfassung

Traditionelle Methoden zur Überwachung der Datencenterumgebung sind heute nicht mehr ausreichend. Moderne Technologien, wie Blade-Server, stellen neue Anforderungen an die Kühlungssysteme, und Regelwerke, wie der Sarbanes-Oxley Act, erhöhen die Anforderungen an den Datenschutz. Mit dieser Entwicklung geht die Notwendigkeit einer strengeren Überwachung der physikalischen Umgebung im Datacenter einher. Trotz vorhandener Prozesse zur Überwachung von physikalischen Komponenten, wie USV-Systemen, Klimaanlage in Computerräumen und Feuerlöschsystemen, gibt es verteilte physikalische Risiken, die häufig nicht beachtet werden. Dieses Dokument beschreibt diese Gefahren und zeigt Ansätze zur Implementierung von Überwachungskomponenten auf. Zudem werden Best-Practice-Hinweise gegeben, wie die gesammelten Daten zur Reduzierung von Ausfallzeiten genutzt werden können.

Einführung

Die heute gängigen Verfahren zur Überwachung der Datencenterumgebung stammen aus den Zeiten der zentralisierten Mainframe-Konzepte und beinhalten Praktiken wie das Mitführen eines Thermometers und das Vertrauen darauf, dass die IT-Mitarbeiter die richtige Raumumgebung „im Blut haben“. Die Weiterentwicklung der Datencenter auf der Basis verteilter Verarbeitung und von Servertechnologien, die neue Anforderungen an die Stromversorgung und Kühlung stellen, erfordert jedoch eine strengere Überwachung der Umgebung.

Steigende Leistungsdichte und dynamische Leistungsschwankungen sind die beiden Hauptursachen, die Änderungen in der Methodik der Überwachung von IT-Umgebungen erforderlich machen. Blade-Server haben eine enorme Erhöhung der Leistungsdichten und eine drastische Änderung der Leistungs- und Stromdynamik ihrer Umgebungen bewirkt. Energieverwaltungssysteme haben die Fähigkeit von Servern und Kommunikationsgeräten zur variablen Leistungsaufnahme (und daher auch Wärmeabgabe) auf der Grundlage der Auslastung vorangetrieben. Dieses Thema wird im APC White Paper Nr. 43, „Dynamische Leistungsschwankungen in Datencentern und Netzwerkräumen“, erläutert.

Ausgefeilte Überwachungs- und Warnfunktionen in physikalischen Systemen, wie USV-Systeme, Klimaanlage im Computerraum sowie Feuerlöschsysteme, sind zwar inzwischen die Regel, jedoch werden andere Aspekte der physikalischen Umgebung häufig nicht beachtet. Die Überwachung von Geräten allein reicht nicht aus. Die Umgebung muss als Ganzes betrachtet und auf proaktive Weise im Hinblick auf Bedrohungen und unbefugtes Eindringen überwacht werden. Zu diesen Bedrohungen zählen extreme Server-Eingangstemperaturen, Wasserlecks sowie der Zugang nicht autorisierter Personen zum Datencenter oder Fehlverhalten von Mitarbeitern im Datencenter.

Entfernte Netzwerkstandorte, wie Niederlassungen, Datenräume und lokale Point-of-Sale-Stellen unterstreichen noch die Notwendigkeit der automatisierten Überwachung in Fällen, in denen es nicht möglich oder nicht zuverlässig genug ist, Umgebungsbedingungen wie Temperatur und Luftfeuchtigkeit von Personen vor Ort überprüfen zu lassen. Im Zuge der Einführung von nicht besetzten Netzwerk-Außenstellen müssen IT-Administratoren über zuverlässige Systeme verfügen, um über alle Vorkommnisse informiert zu werden.

Moderne Technologien ermöglichen eine detaillierte Konfiguration der Überwachungssysteme, die den besonderen Umgebungs- und Sicherheitsanforderungen des Datencenters entspricht. Dabei kann jedes Rack als kleines „Datencenter“ betrachtet werden, mit eigenen Anforderungen und einer Überwachungsstrategie, die mehrere Datenerfassungspunkte beinhalten kann.¹

¹ Das APC White Paper Nr. 100, „Management Strategy for Network-Critical Physical Infrastructure“ (Management-Strategie für die physikalische Infrastruktur hochverfügbarer Netzwerke), befasst sich mit dem Problem der Integration einer großen Anzahl von Rack-basierten Überwachungspunkten in ein bestehendes Enterprise Management System (EMS) oder ein Building Management System (BMS).

In diesem Dokument werden die physikalischen Bedrohungen erläutert, die durch verteilte Überwachungsstrategien verringert werden können. Zudem werden Richtlinien und Best-Practice-Hinweise für die Implementierung von Sensoren im Datacenter gegeben. Erläutert wird außerdem die Verwendung von Entwicklungstools für Datacenter, die dazu beitragen, den Spezifikations- und Entwicklungsprozess für diese verteilten Überwachungssysteme zu vereinfachen.

Was sind verteilte physikalische Bedrohungen?

Dieses Dokument befasst sich mit einer Untergruppe der Bedrohungen, den *verteilten physikalischen Bedrohungen*, die von besonderem Interesse sind, da ihre Abwehr eine gezielte und sachkundige Planung erfordert. Zur Definition dieser Untergruppe ist eine kurze Darstellung der Bandbreite der für Datacenter möglichen Bedrohungen hilfreich.

Die Bedrohungen für Datacenter können in zwei große Kategorien unterteilt werden, je nachdem, ob sie sich auf den Bereich der IT-Software und Netzwerke (**digitale** Bedrohungen) oder auf den Bereich der physikalisch unterstützenden Infrastruktur des Datacenters beziehen (**physikalische** Bedrohungen).

Digitale Bedrohungen

Digitale Bedrohungen sind u. a. Hacker, Viren, Netzwerkengpässe und andere unbeabsichtigte oder böswillige Angriffe auf die Datensicherheit oder den Datenfluss. Digitale Bedrohungen finden große Aufmerksamkeit in der Branche und in der Presse, und die meisten Datacenter verfügen über robuste und gut gewartete Systeme, wie z. B. Firewalls und Anti-Virenprogramme, um diese Bedrohungen abzuwehren. Die grundlegenden Schutzmaßnahmen gegen digitale Bedrohungen werden im APC White Paper Nr. 101, „Grundprinzipien der Netzwerksicherheit“, erläutert. *Digitale Bedrohungen sind jedoch nicht Thema des vorliegenden Dokuments.*

Physikalische Bedrohungen

Zu den physikalischen Bedrohungen für IT-Geräte zählen Stromversorgungs- und Kühlprobleme, menschliches Versagen oder Böswilligkeit, Brände, Leckagen und die Luftqualität. Einige dieser Bedrohungen, darunter die Bedrohungen im Hinblick auf die Stromversorgung, Kühlung und Brandgefahr, werden routinemäßig von den in die Stromversorgungs-, Kühl- und Feuerlöschsysteme integrierten Funktionen überwacht. Zum Beispiel überwachen USV-Systeme die Stromqualität, die Belastung und den Akku-Ladezustand, PDUs überwachen die Stromkreisbelastungen, Kühleinheiten überwachen die Eingangs- und Ausgangstemperaturen sowie den Filterstatus, und die baurechtlich vorgeschriebenen Feuerlöschsysteme überwachen die Rauch- oder Wärmeentwicklung. Diese Überwachungsaktivitäten erfolgen in der Regel nach genau definierten, automatisierten Protokollen, die auf Softwaresystemen beruhen, die die verfügbaren Informationen sammeln, protokollieren, auswerten und anzeigen. Bedrohungen, die auf diese Weise angezeigt werden, d. h. durch werkseitig in die Systeme integrierte Funktionen, erfordern vom Benutzer keine speziellen Kenntnisse oder Planungen für eine effiziente Steuerung, vorausgesetzt, die Überwachungs- und Informationssysteme sind in einem technisch einwandfreien Zustand. *Diese automatisch überwachten physikalischen Bedrohungen sind zwar ein wesentlicher Bestandteil eines umfassenden Verwaltungssystems, sie sind jedoch nicht Thema des vorliegenden Dokuments.*

Mit zu den schwerwiegendsten physikalischen Bedrohungen gehören jedoch solche, die sich der Benutzer nicht mithilfe von bereits vorhandenen, werkseitig integrierten Funktionen anzeigen lassen kann. Die Bedrohung durch zu geringe Luftfeuchtigkeit kann beispielsweise überall im Datacenter vorhanden sein. Die Anzahl und Positionierung von Luftfeuchtigkeitssensoren ist daher ein wichtiger Aspekt für den Umgang mit dieser Bedrohung. Bedrohungen dieser Art können **über das gesamte Datacenter verteilt sein und je nach Raumaufteilung und Gerätepositionierung an den unterschiedlichsten Stellen auftreten**. Die verteilten physikalischen Bedrohungen, die in diesem Dokument behandelt werden, fallen in folgende allgemeine Kategorien:

- Gefährdung von IT-Geräten durch die Luftqualität (Temperatur, Luftfeuchtigkeit)
- Flüssigkeitslecks
- Menschliche Anwesenheit oder ungewöhnliche Aktivitäten
- Gefährdung von Personen durch die Luftqualität (Fremdstoffe in der Luft)
- Rauch und Feuer aufgrund von Gefahren im Datacenter²

² Die grundlegenden Maßnahmen zur Rauch-/Feuererkennung, die baurechtlich vorgeschrieben sind, werden in den entsprechenden Rechts- und Sicherheitsvorschriften behandelt und sind nicht Thema dieses Dokuments. Das vorliegende Dokument befasst sich mit *ergänzenden* Maßnahmen zur Rauchererkennung, die die besonderen Gegebenheiten in einem Datacenter berücksichtigen und über die baurechtlich vorgeschriebenen Maßnahmen hinausgehen.

Abbildung 1 veranschaulicht den Unterschied zwischen digitalen und physikalischen Bedrohungen und zeigt die weitere Unterteilung in physikalische Bedrohungen, die mithilfe von werkseitig in Geräte integrierten Funktionen zur Überwachung der Stromversorgung/Kühlung bewältigt werden können, und den verteilten physikalischen Bedrohungen, die Analysen, Entscheidungen und Planungen erfordern, um die Art, Positionierung und Anzahl der Überwachungssensoren zu bestimmen. Diese verteilten physikalischen Bedrohungen sind Thema des vorliegenden Dokuments. Es sind auch diejenigen physikalischen Bedrohungen, die leicht aufgrund mangelnder Kenntnisse und Erfahrungen bei der Entwicklung einer effizienten Überwachungsstrategie vernachlässigt werden.

Abbildung 1 – Bedrohungen im Datacenter

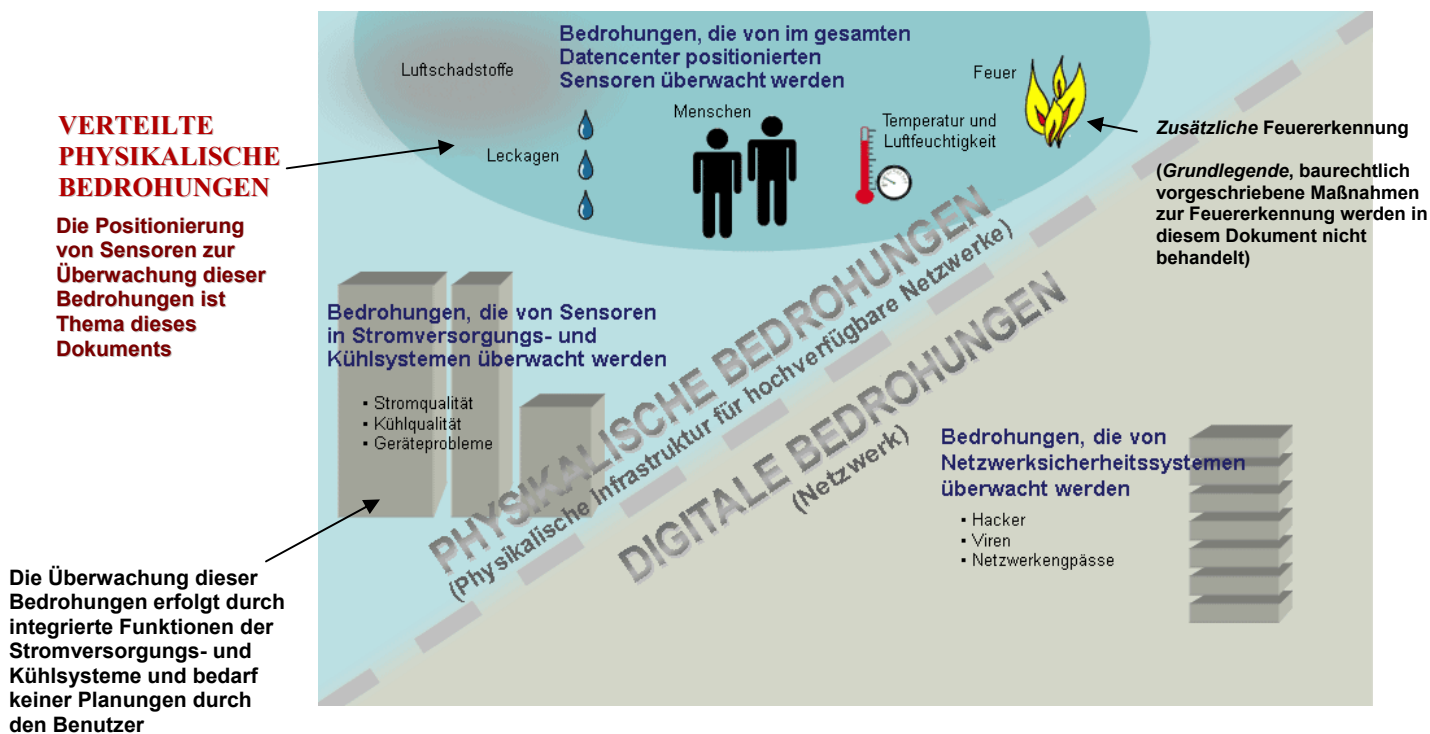


Tabelle 1 gibt einen Überblick über die verteilten physikalische Bedrohungen, ihre Auswirkung im Datacenter und die verschiedenen Arten von Sensoren für ihre Überwachung.

Tabelle 1 – Verteilte physikalische Bedrohungen





Bedrohung	Definition	Auswirkung im Datacenter	Sensorart
Lufttemperatur	Lufttemperatur in Räumen, Racks und Geräten	Geräteausfall und geringere Lebensdauer von Geräten durch höhere Temperaturen als spezifiziert und/oder drastische Temperaturschwankungen	Temperatursensoren
Luftfeuchtigkeit	Die relative Luftfeuchtigkeit im Raum und in Racks bei einer bestimmten Temperatur	Geräteausfall durch die Entstehung elektrostatischer Entladung an Stellen mit geringer Luftfeuchtigkeit Bildung von Kondenswasser an Stellen mit hoher Luftfeuchtigkeit	Luftfeuchtigkeitssensoren
Flüssigkeitslecks	Wasser- oder Kühlmittellecks	Flüssigkeitsschäden an Böden, Kabeln und Geräten Hinweis auf CRAC-Probleme	Kabelsensoren zur Leckageerkennung Punktsensoren zur Leckageerkennung
Menschliches Versagen und Mitarbeiterzugang	Unbeabsichtigtes Fehlverhalten von Mitarbeitern Nicht autorisierter und/oder erzwungener Zugang zum Datacenter mit böswilliger Absicht	Geräteschaden und Datenverlust Geräteausfallzeiten Diebstahl und Sabotage von Geräten	Digitale Videokameras Bewegungssensoren Rack-Schließschalter Raum-Schließschalter Glasbruchsensoren Vibrationssensoren
Rauch/Feuer	Von elektrischen Anlagen ausgehende Feuer/Materialbrand	Geräteausfall Inventar- und Datenverlust	Ergänzende Rauchsensoren
Gefährliche Luftschadstoffe	In der Luft enthaltene chemische Stoffe, wie z. B. Wasserstoff von Batterien, und Partikel, wie z. B. Staub	Gefahrensituation für Mitarbeiter und/oder unzuverlässiger USV-Betrieb und -Ausfall durch die Freisetzung von Wasserstoff Geräteausfall durch Anstieg der elektrostatischen Entladung und Verstopfung von Filtern/Lüftern durch Staubansammlungen	Chemie-/Wasserstoff-sensoren Staubsensoren

Die Positionierung von Sensoren


Zur frühzeitigen Warnung vor Problemen durch die oben beschriebenen Bedrohungen können verschiedene Arten von Sensoren verwendet werden. Während die konkrete Art und Anzahl der Sensoren abhängig von Budget, Bedrohungsrisiko und den durch eine Sicherheitsverletzung verursachten Geschäftsschaden variieren kann, gibt es eine kleine Gruppe von Sensoren, die für die meisten Datacenter sinnvoll sind.

Tabelle 2 enthält Richtlinien für diese empfohlene grundlegende Gruppe von Sensoren.

Tabelle 2 – Richtlinien für grundlegende Sensoren



Sensorart	Position	Empfohlene Vorgehensweise	Anmerkungen	Industrierichtlinien	Beispiel
Temperatursensoren	Rack	Am oberen, mittleren und unteren Teil der Vordertür aller IT-Racks zur Überwachung der Eingangstemperatur der Geräte in einem Rack	In Schaltschränken oder anderen offenen Rack-Umgebungen sollte die Temperaturüberwachung möglichst nahe an den Geräteeingängen erfolgen	ASHRAE-Richtlinien ³	
Luftfeuchtigkeits-sensoren	Rackreihe	Ein Sensor pro kaltem Gang, an der Vorderseite eines Racks in der Mitte der Rackreihe	Da CRAC-Einheiten (Präzisionsklimaanlagen) die Luftfeuchtigkeitswerte messen, muss die Position eines Luftfeuchtigkeitssensors in einer Rackreihe evtl. korrigiert werden, wenn er sich zu nahe an einem CRAC-Ausgang befindet	ASHRAE-Richtlinien	
Kabelsensoren zur Leckageerkennung Punktsensoren zur Leckageerkennung	Raum	Positionierung von Kabelsensoren zur Leckageerkennung um jedes CRAC-System, um Einheiten zur Kühlungsverteilung, unter Zwischenböden und allen weiteren Leckagequellen (wie z. B. Rohrleitungen)	Punktsensoren zur Leckageerkennung zur Verhinderung des Überlaufens von Auffangwannen, zur Überwachung in kleineren Räumen/Schränken und an allen niedrigen Stellen	Kein Industriestandard	
Digitale Videokameras	Raum und Rackreihe	Strategische Positionierung entsprechend der Raumaufteilung des Datacenters unter Erfassung der Zugangs- und Ausgangspunkte und mit guter Sicht auf alle warmen und kalten Gänge; sicherstellen, dass das gesamte erforderliche Sichtfeld abgedeckt ist	Überwachung und Aufzeichnung des autorisierten Zugangs und des nicht autorisierten Zugangs sowie des Zugangs außerhalb der Arbeitszeit durch Videoüberwachungssoftware	Kein Industriestandard	

³ ASHRAE TC9.9 Mission Critical Facilities, „Thermal Guidelines for Data Processing Environments,“ 2004.

Raum-Schalter	Raum	Ein elektronischer Schalter an jeder Zugangstür zur Überwachung des Raumzutritts und zur Beschränkung des Zugangs auf bestimmte Personen zu bestimmten Zeiten	Die Integration von Raum-Schaltern in das Anlagensystem kann wünschenswert sein und lässt sich durch eine Kommunikationsschnittstelle erreichen	HIPPA und Sarbanes-Oxley ⁴	
----------------------	------	---	---	---------------------------------------	---

Zusätzlich zu den in **Tabelle 2** aufgeführten grundlegenden Sensoren können je nach Raumkonfiguration, Bedrohungsstufe und Verfügbarkeitsanforderungen optional weitere Sensoren sinnvoll sein. **Tabelle 3** führt diese zusätzlichen Sensoren zusammen mit Best-Practice-Richtlinien auf.





Tabelle 3 – Richtlinien für zusätzliche, situationsabhängige Sensoren

Sensorart	Standort	Empfohlene Vorgehensweise	Anmerkungen	Industri-richtlinien	Beispiel
Ergänzende Rauchsensoren	Rack	VESD-Detektoren (Very Early Smoke Detection) auf Rack-Ebene zur frühzeitigen Warnung bei Problemen in hochkritischen Bereichen oder Bereichen ohne eigene Rauchsensoren ⁵	Wenn ergänzende Rack-Rauchmelder das Budget überschreiten, kann durch die Positionierung eines VESD-Detektors am Eingang jeder CRAC-Einheit ein bestimmtes Maß an Frühwarnung erreicht werden	Kein Industriestandard	
Chemie-/Wasserstoffsensoren	Raum	Bei Verwendung von VRLA-Batterien im Datacenter müssen keine Wasserstoffsensoren im Raum positioniert werden, da bei diesen Batterien im Normalbetrieb kein Wasserstoff freigesetzt wird (wie dies bei Nasszellenbatterien der Fall ist)	Nasszellenbatterien in einem separaten Batterieraum unterliegen besonderen Vorschriften	IEEE/ASHRAE-Handbuchentwurf ⁶	

⁴ Hierzu Fiona Williams, Leiterin Sicherheit bei den Deloitte & Touche Sicherheitsdiensten: „Die physikalische Sicherheit fällt unter die Anforderungen des Sarbanes-Oxley Acts. Sie ist wesentlicher Bestandteil des infosec-Programms sowie allgemeiner Computerkontrollen. Relevant sind hier die Abschnitte 302 und 404, in denen die Unternehmensführung verpflichtet wird, das effektive Funktionieren der internen Kontrollen zu überprüfen und sicherzustellen.“
<http://www.csoonline.com/read/100103/counsel.html> (aufgerufen am 20. April 2006)

⁵ Setzt das Vorhandensein eines separaten Feuermeldesystems voraus, um den baurechtlichen Vorschriften zu entsprechen.

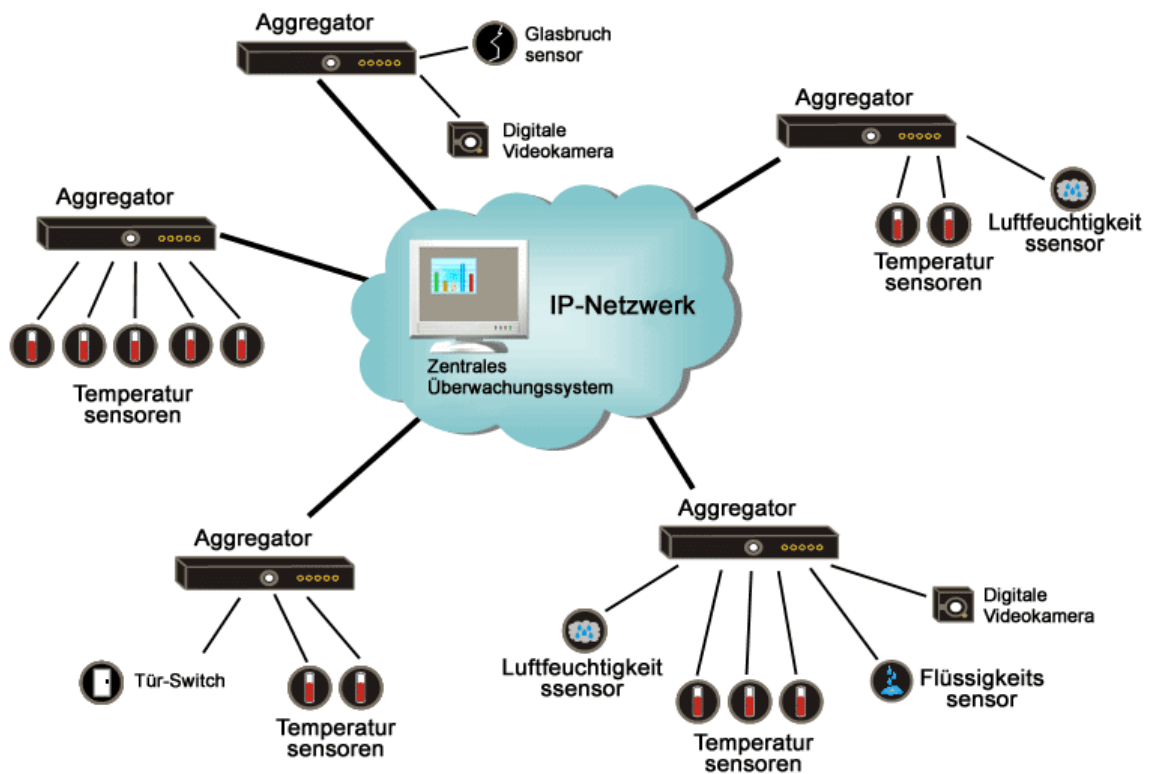
⁶ IEEE/ASHRAE, „Guide for the Ventilation and Thermal Management of Stationary Battery Installations“, Handbuchentwurf, verfügbar Ende 2006

Sensorart	Standort	Empfohlene Vorgehensweise	Anmerkungen	Industri-richtlinien	Beispiel
Bewegungssensoren	Raum und Rackreihe	Werden verwendet, wenn Budgetbeschränkungen die Installation einer digitalen Kamera nicht erlauben, was die empfohlene Vorgehensweise wäre (siehe Tabelle 2)	Bewegungssensoren sind für die Überwachung menschlicher Aktivitäten eine kostengünstigere Alternative zu digitalen Videokameras	Kein Industriestandard	
Rack-Switches	Rack	In Datacentern mit hohem Verkehrsaufkommen elektronische Switches an der vorderen und hinteren Tür jedes Racks, um den Zugang zu überwachen und den Zugang zu wichtigen Komponenten auf bestimmte Personen zu bestimmten Zeiten zu beschränken	Die Integration von Rack-Switches in das Anlagensystem kann wünschenswert sein und lässt sich durch eine Kommunikationsschnittstelle erreichen	HIPPA und Sarbanes-Oxley	
Vibrationssensoren	Rack	In Datacentern mit hohem Verkehrsaufkommen Vibrationssensoren in jedem Rack zur Erkennung von nicht autorisierter Installation oder der Entfernung von wichtigen Geräten	Vibrationssensoren in jedem Rack können auch verwendet werden, um zu erkennen, ob Racks bewegt wurden	Kein Industriestandard	
Glasbruchsensoren	Raum	Glasbruchsensoren auf jedem Fenster des Datacenters (sowohl bei Außenfenstern als auch bei Innenfenstern zu einem Gang oder einem anderen Raum)	Die Verwendung zusammen mit Videoüberwachungskameras wird empfohlen	Kein Industriestandard	

Sammeln von Sensordaten

Nach der Auswahl und Positionierung der Sensoren besteht der nächste Schritt darin, die von den Sensoren erfassten Daten zu sammeln und zu analysieren. Anstatt alle Sensordaten direkt an eine zentrale Sammelstelle zu senden, empfiehlt es sich in der Regel, über das gesamte Datacenter verteilte Sammelstellen mit Warn- und Benachrichtigungsfunktionen an jedem Sammelpunkt zu verwenden. Dadurch wird nicht nur das Risiko des Ausfalls einer einzigen zentralen Sammelstelle vermieden, sondern auch die Überwachung von Remote-Server-Räumen und Telekommunikationsschränken unterstützt.⁷ Die Sammelstellen kommunizieren über das IP-Netzwerk mit einem zentralen Überwachungssystem (**Abbildung 2**).

Abbildung 2 – Sammeln der Sensordaten



⁷ Diese Architektur mit mehreren Sammelstellen, von denen jeder über Warn- und Benachrichtigungsfunktionen für die von ihm unterstützten Sensoren verfügt, wird manchmal auch als „verteilte Intelligenz an der Grenze“ bezeichnet.

Einzelne Sensoren stellen in der Regel keine einzelne Verbindung zum IP-Netzwerk her. Vielmehr interpretieren die Aggregatoren (Sammelstellen) die Sensordaten und senden Warnungen an das zentrale System und/oder direkt an die Benachrichtigungsliste (siehe nächster Abschnitt). Diese verteilte Überwachungsarchitektur vermindert auf drastische Weise die Anzahl der erforderlichen Netzwerkanschlüsse und reduziert die Gesamtsystemkosten und die Verwaltungslast. Sammelstellen werden meist physikalischen Bereichen im Datacenter zugeordnet und verbinden Sensoren eines begrenzten Bereichs miteinander, um die Sensorverkabelung überschaubar zu halten.

„Intelligente“ Maßnahmen

Sensoren liefern die Grunddaten. Genau so wichtig ist jedoch die Interpretation dieser Daten für die Ausgabe von Warnungen und Benachrichtigen und für Korrekturmaßnahmen. Durch immer ausgefeiltere Überwachungsstrategien und die stark zunehmende Verbreitung von Sensoren im gut überwachten Datacenter ist die „intelligente“ Verarbeitung dieser potenziell großen Datenmenge von entscheidender Wichtigkeit. Die effektivste und effizienteste Methode zum Sammeln und Analysieren von Sensordaten und zum Auslösen entsprechender Maßnahmen besteht in der Verwendung von so genannten Sammelstellen, wie im vorherigen Abschnitt beschrieben.

Es ist wichtig, dass die Daten gefiltert, ins Verhältnis gesetzt und ausgewertet werden können, um die beste Vorgehensweise zu bestimmen, wenn außergewöhnliche Ereignisse auftreten. Effiziente Maßnahmen zu ergreifen, bedeutet, Warnungen mit den richtigen Informationen auf dem richtigen Weg an die richtigen Personen auszugeben. Es gibt drei Möglichkeiten, Maßnahmen zu ergreifen:

- **Warnmeldungen** aufgrund außergewöhnlicher Bedingungen, die bestimmte Geräte, Racks oder das gesamte Datacenter gefährden könnten
- Automatische **Maßnahmen** auf der Grundlage definierter Warnungen und Schwellenwerte
- **Analysen und Berichte** zur Unterstützung von Verbesserungen, Optimierungen und Fehler-/Ausfallmessungen

Warnmeldungen

Zum Einstellen von Warnungen müssen drei Werte festgelegt werden: **Alarmgrenzwerte**, die angeben, bei welchem Wert bzw. Welchen Werten eine Alarmmeldung ausgelöst werden soll. Die **Meldemethode**, die angibt, wie und an wen die Alarmmeldung gesendet werden soll. Und die **Eskalationsmethodik**, durch die festgelegt wird, ob für bestimmte Arten von Alarmmeldungen eine andere Eskalationsstufe zur Lösung erforderlich ist.

Alarmgrenzwerte: Für jeden Sensor müssen angemessene Betriebsbedingungen festgelegt und Grenzwerte konfiguriert werden, bei deren Erreichung Warnmeldungen ausgegeben werden, wenn die Messwerte diese Betriebsbedingungen übersteigen. Im Idealfall sollte das Überwachungssystem so flexible sein, dass mehrere Grenzwerte pro Sensor konfiguriert werden können, um Alarmmeldungen für unterschiedliche Stufen (Informell, Warnung, kritisch, schwerwiegende Fehler und Ausfall) zu ermöglichen. Zusätzlich zu Grenzwerten mit nur einem Wert sollten Auslösebedingungen festgelegt werden, wie z. B. Grenzwertüberschreitungen während einer definierten Zeitspanne, die Steigerungsrate und die Abnahmerate. Im Hinblick auf die Temperatur gibt die Warnmeldung über die Änderungsrate einen schnelleren Hinweis auf eine Fehlfunktion als eine Momentaufnahme des Temperaturwerts.

Grenzwerte müssen sorgfältig festgelegt werden, um maximalen Nutzen sicherzustellen. Es können verschiedene Grenzwerte festgelegt werden, die entsprechend der Schwere einer Störung verschiedene Alarmmeldungen auslösen. Zum Beispiel könnte beim Erreichen des Luftfeuchtigkeitsgrenzwerts eine E-Mail an den IT-Administrator gesendet werden, ein Rauchsensor dagegen würde einen automatischen Anruf bei der Feuerwehr auslösen. Analog dazu werden verschiedenen Grenzwertstufen unterschiedliche Eskalationspfade zugeordnet. Beim nicht autorisierten Zugang zu einem Rack könnte beispielsweise eine Eskalation an den IT-Administrator erfolgen, beim erzwungenen Zugang dagegen eine Eskalation an den IT-Leiter.

Grenzwerte sollten global auf Standardwerte eingestellt und dann entsprechend den IT-Gerätespezifikationen und dem Sensormontageort im Verhältnis zum Gerätestandort individuell angepasst werden (zum Beispiel sollte ein Sensor, der sich in der Nähe der Stromversorgung eines Servers befindet, bei einem höheren Wert eine Alarmmeldung ausgeben als ein Sensor, der sich in der Nähe des Lufteinlasses eines Servers befindet). **Tabelle 4** listet empfohlene Standardgrenzwerte für Temperatur und Luftfeuchtigkeit gemäß ASHRAE TC9.9 auf. Es ist wichtig, zusätzlich zu diesen Grenzwerten die Temperaturänderungsrate zu überwachen. Eine Temperaturänderung von 5,6 °C innerhalb von 5 Minuten weist mit großer Wahrscheinlichkeit auf einen CRAC (Präzisionsklimaanlagen)-Ausfall hin.

Tabelle 4 – Empfohlene Grenzwerte für Temperatur- und Luftfeuchtigkeitssensoren⁸

Sensor	Oberer Grenzwert	Unterer Grenzwert
Lufttemperatursensor	25 °C	20 °C
Luftfeuchtigkeitssensor	55 % relative Luftfeuchtigkeit	40 % relative Luftfeuchtigkeit

⁸ ASHRAE TC9.9 – Empfehlungen für Umgebungen der Klasse 1, für die die strengsten Kontrollmaßnahmen gelten und die für Datacenter mit betriebskritischen Abläufen am besten geeignet sind.

Meldemethoden – Warnmeldungen können auf unterschiedliche Weise erfolgen, wie z. B. per E-Mail, SMS-Textnachricht, SNMP-Traps und HTTP-Post. Es ist wichtig, dass die Warnsysteme flexibel und anpassbar sind, damit die richtige Informationsmenge erfolgreich an den vorgesehenen Empfänger übermittelt wird. Warnmeldungen sollten Angaben enthalten, wie z. B. den benutzerdefinierten Namen des Sensors, die Sensorposition sowie Datum und Uhrzeit des Alarms.

Alarmeskalation – Einige Alarme erfordern möglicherweise sofortige Maßnahmen. Ein intelligentes Überwachungssystem sollte fähig sein, bestimmte Alarme auf höhere Zuständigkeitsstufen zu eskalieren, wenn ein Problem nicht innerhalb einer definierten Zeitspanne gelöst wird. Die Alarmeskalation hilft sicherzustellen, dass Probleme rechtzeitig behoben werden, ehe aus kleinen Problemen große werden.

Nachfolgend einige Beispiele für sinnvolle und weniger sinnvolle Warnungen:

Grenzwertüberschreitung bei Temperatursensor Nr. 48 – Nicht sehr sinnvoll, weil die Position von Sensor Nr. 48 nicht angegeben wird

Überhitzungsgefahr bei Webserver X – Ist nützlicher, da der betreffende Server angegeben wird.

Türsensor wurde aktiviert – Nicht sehr sinnvoll, da nicht angegeben wird, um welche Tür es sich handelt

Tür X an Standort Y wurde geöffnet und ein Bild der Person beim Öffnen der Tür aufgezeichnet – Sehr nützlich, da die Meldung die Angabe der Tür, ihres Standorts und ein Foto des Zwischenfalls umfasst

Maßnahmen auf der Grundlage der Daten

Das Sammeln von Sensordaten ist nur der erste Schritt, und wenn ein Datacenter-Manager nur auf manuelle Maßnahmen setzt, können die Daten nicht maximal genutzt werden. Es gibt Systeme, die auf der Grundlage von benutzerdefinierten Alarmen und Grenzwerten automatisch Maßnahmen auslösen. Zur Implementierung dieser „intelligenten“ Automatisierung muss Folgendes geklärt werden:

Alarmmaßnahmen – Welche automatisierten Maßnahmen sollen entsprechend der Sicherheitsstufe eines Alarms ergriffen werden? Diese automatisierten Maßnahmen könnten persönliche Benachrichtigungen sein, oder Korrekturmaßnahmen, wie z. B. die Aktivierung von Trockenkontakt-Schnittstellen zum Ein- und Ausschalten von Geräten wie Lüftern oder Pumpen.

Kontinuierliche Sichtbarkeit von Sensordaten in Echtzeit – Die Möglichkeit zur Anzeige individueller Sensordaten als Momentaufnahme ist eine grundlegende Anforderung. Die Möglichkeit zur Anzeige individueller *Sensortrends* in Echtzeit bietet jedoch ein viel besseres Bild der Situation. Die Interpretation dieser Trends ermöglicht es Administratoren, breitere Probleme zu erkennen und Daten mehrerer Sensoren zu korrelieren.

Warnsysteme sollten mehr bieten als Benachrichtigungen bei Grenzwertverletzungen. Bei einigen Überwachungssystemen können Administratoren beispielsweise den Warnungen zusätzliche Daten hinzufügen. Diese zusätzlichen Daten können Video- oder Audio-Aufnahmen, Diagramme und Karten sein. Ein funktionsstarkes Warnsystem dieser Art ermöglicht Administratoren informiertere Entscheidungen aufgrund der Kontextdaten, die der Warnung hinzugefügt wurden. In einigen Fällen müssen aus einem zu großen Informationsumfang die nützlichen Informationen herausgefiltert werden. Zum Beispiel wäre es in einem Datacenter mit hohem Verkehrsaufkommen extrem störend, wenn bei jeder Bewegung im Datacenter eine Warnung ausgegeben würde. Es kann Fälle geben, in denen bestimmte Informationen im Interesse der Sicherheit verdeckt oder „ausgeblendet“ werden. In einem Video, das auch eine Tastatur zeigt, könnten beispielsweise Personen bei der Passworteingabe ausgeblendet werden.

Nachfolgend einige Beispiele für „intelligente“ Interpretation und Maßnahmen:

- Automatische Aktivierung eines Lüfters oder einer CRAC (Präzisionsklimaanlagen)-Einheit bei einer Temperaturgrenzwertverletzung
- Gewährung von ferngesteuertem Zugang zu bestimmten Racks mit elektronischen Türschlössern in Abhängigkeit davon, welche Person über die Echtzeit-Videoüberwachung zu sehen ist
- Automatische Aktivierung einer Pumpe, wenn in einem entfernten Datacenter Wasser festgestellt wird
- Automatisches Starten der Video-Aufzeichnung und Ausgabe eines Alarms an den Sicherheitsdienst, wenn nach der normalen Arbeitszeit eine Bewegung im Datacenter festgestellt wird
- Benachrichtigung des Sicherheitsdienstes und Ausgabe eines hörbaren Alarms, wenn außerhalb der normalen Arbeitszeit ein Glasbruch festgestellt wird
- Ausgabe eines Alarms an den Administrator mit dem Hinweis, dass die Tür kontrolliert werden soll, wenn ein Tür-Schließschalter meldet, dass eine Rack-Tür bereits länger als 30 Minuten offen steht (was darauf hinweist, dass die Tür nicht ordnungsgemäß geschlossen wurde)

Analysen und Berichte

Intelligente Überwachungssysteme sollten nicht nur kurzfristige Trends von Sensordaten, sondern auch langfristige historische Daten bieten. Hochwertige Überwachungssysteme sollten über Zugang zu Sensormesswerten von Wochen, Monaten oder sogar Jahren verfügen und die Möglichkeit bieten, Diagramme und Berichte auf der Grundlage dieser Daten zu erstellen. Die Diagramme sollten zu Vergleichs- und Analysezwecken mehrere Arten von Sensoren in einem Bericht darstellen können. Die Berichte sollten niedrige, hohe und mittlere Sensormesswerte im ausgewählten Zeitrahmen von verschiedenen Sensorgruppen bereitstellen können.

Langfristige historische Sensordaten können auf verschiedene Weise verwendet werden, beispielsweise um anschaulich darzustellen, dass das Datencenter am Rande seiner Kapazität arbeitet, und zwar nicht im Hinblick auf den physikalischen Platzbedarf, sondern aufgrund unzureichender Kühlung. Solche Informationen könnten für die Extrapolation von zukünftigen Trends verwendet werden, wenn dem Datencenter immer mehr Komponenten hinzugefügt werden, und könnten helfen, vorherzusagen, wann das Datencenter seine maximale Kapazität erreichen wird. Langfristige Trendanalysen könnten auf Rack-Ebene verwendet werden, um die Wärmeerzeugung der Komponenten verschiedener Hersteller in verschiedenen Racks zu vergleichen und auf diese Weise Entscheidungskriterien für zukünftige Käufe zu gewinnen.

Die vom Überwachungssystem erfassten Sensormesswerte sollten in Industriestandardformate exportiert werden können, damit die Daten in handelsüblichen sowie benutzerdefinierten Bericht- und Analyseprogrammen verwendet werden können.

Planungsmethode

Die Spezifizierung und Planung eines Systems zur Überwachung von Bedrohungen erscheint möglicherweise kompliziert, kann jedoch mithilfe von Entwicklungstools für Datencenter, wie z. B. InfraStruXure Designer von APC, automatisiert werden. Solche Entwicklungstools können auf der Grundlage einer einfachen Liste mit Eckdaten, die vom Benutzer eingegeben wird, automatisch die geeignete Anzahl von Sensoren und Sammelstellen ermitteln. Zusammenfassende Berichte stellen Teilleisten und Anleitungen für die Installation der empfohlenen Sensoren bereit. Diese Entwicklungstools für Datencenter nutzen Algorithmen und anerkannte Regeln auf der Grundlage von Bewährten Methoden sowie Industriestandards und geben anhand von Dichte, Raumaufteilung, Raumzugangsrichtlinien und benutzerspezifischen Überwachungsanforderungen Empfehlungen für bestimmte Konfigurationen.

Zum Beispiel könnten die folgenden benutzerspezifischen Eckdaten die Planung des Überwachungssystems nach Verkehrsaufkommen und Zugang beeinflussen:

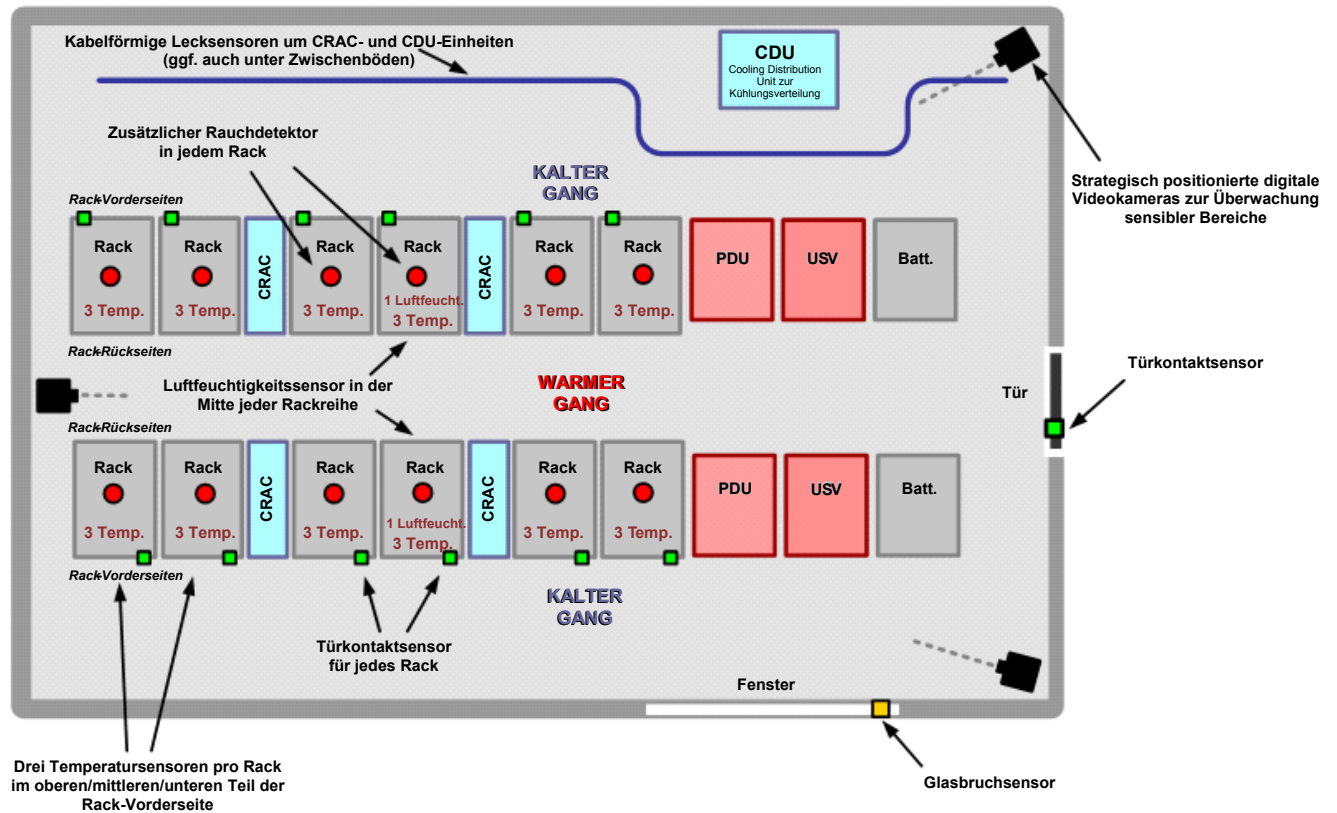
Hohes Verkehrsaufkommen/Zugang – Wenn im Datencenter viele Personen verkehren, von denen jede unterschiedliche Anwendungen und Aufgaben im Datencenter hat, würde das Entwicklungstool Rack-Schließschalter an jedem Rack vorschlagen, um den Zugang zu bestimmten Racks auf die Personen zu beschränken, die ihn benötigen.

Wenig Verkehrsaufkommen/Zugang – Wenn im Datencenter nur wenige ausgewählte Personen verkehren, von denen jede für alle Datencenter-Funktionen verantwortlich ist, würde das Entwicklungstool keine Rack-Schließschalter vorschlagen, um den Zugang zu einzelnen Racks zu steuern. In diesem Fall würde ein Raumtür-Schließschalter ausreichen, um den Zugang zu dem Raum auf autorisierte Mitarbeiter zu beschränken.

Beispiel für die Positionierung von Sensoren

Abbildung 3 veranschaulicht anhand der schematischen Darstellung eines Datacenters die mögliche Positionierung von Überwachungskomponenten gemäß den in diesem Dokument beschriebenen Best Practices.

Abbildung 3 – Beispiel für die Sensorpositionierung



Schlussfolgerung

Der Schutz gegen verteilte physikalische Bedrohungen ist wesentlicher Bestandteil einer umfassenden Sicherheitsstrategie. Während die Positionierung und Konzeption von Überwachungskomponenten Analysen, Entscheidungen und Planungen erfordern, sind für eine effiziente Sensorimplementierung Best Practices und Entwicklungstools verfügbar.

Zusätzlich zur geeigneten Art, Position und Anzahl von Sensoren werden Softwaresysteme benötigt, um die gesammelten Daten zu verwalten und Protokolle, Trendanalysen, intelligente Warnmeldungen sowie automatisierte Korrekturmaßnahmen zu ermöglichen.

Durch die Kenntnis der Methoden zur Überwachung von physikalischen Bedrohungen kann der IT-Administrator kritische Sicherheitslücken im Datacenter schließen und die physikalische Sicherheit anpassen, wenn sich die Infrastruktur und Verfügbarkeitsziele des Datacenters ändern.

Über die Autoren

Christian Cowan ist bei APC als Produktlinienmanager für Umgebungs- und Sicherheitsprodukte tätig. Er verfügt über fünfzehn Jahre Erfahrung im IT- und NCPI-Bereich und ist Mitglied des IEEE. Cowan erwarb an der Villanova University einen Bachelor- und an der University of Rhode Island einen Master-Abschluss in Elektrotechnik.

Chris Gaskins ist seit 15 Jahren in der Hightech-Branche tätig und arbeitete in den Bereichen Engineering, Produktmanagement und Support. Er verfügt u. a. über Erfahrungen mit PC-basierten Servern, System-Management, Netzwerkmanagement sowie digitaler und physikalischer Sicherheit. Gegenwärtig arbeitet er bei APC als Produktlinienmanager für Umgebungs- und Sicherheitsprodukte, darunter auch die Produkte der NetBotz-Familie. Davor war er Vice President of Engineering bei AppGate, Inc. wo er ein Ingenieurs-Team für die Entwicklung von VPN-Systemen auf Anwendungsebene leitete. Er verfügt über einen Bachelor-Abschluss in Informatik, den er am Berry College in Rome, Georgia, erworben hat.