Rittal – Das System.

Schneller – besser – überall.

Whitepaper –
Sicherheitsmanagement für
Rechenzentrumsinfrastrukturen

Bernd Hanstein

Inhaltsverzeichnis

Autor: Bernd Hanstein

Nach Abschluss des Diplomstudiengangs der Physik an der Justus-Liebig-Universität in Gießen im Jahr 1987 hat Bernd Hanstein in der Zentralen Forschung der Siemens AG auf dem Gebiet der Testverfahren für hochintegrierte Schaltungen gearbeitet. Anschließend war er in verschiedenen Positionen innerhalb der Siemens AG im Unternehmensbereich Öffentliche Netze für die Implementierung großer ITK-Projekte zuständig. Nach dem Wechsel zu Siemens VDO Automotive im Jahre 2002 war Bernd Hanstein als Hauptabteilungsleiter für den weltweiten Systemtest der Multimediageräte für Kraftfahrzeuge verantwortlich. Seit 2007 hat er die Leitung des IT-Produktmanagements bei Rittal in Herborn inne. Seine Schwerpunkte: IT-Komponenten, RiMatrix-Systemlösungen und Rechenzentrumstechnologie.

Abbildungsverzeichnis

Tabellenverzeichnis

Executive Summary

In einer vernetzten, digitalen Welt sind Rechenzentren essentielle Komponenten der Kommunikation; sie sind notwendig für die Bereitstellung von Daten und Diensten und finden sich daher in allen Bereichen gesellschaftlichen Lebens. Gerade auch innerhalb kritischer, versorgungsrelevanter Infrastrukturen stellen Rechenzentren das Zentrum der Kommunikation und Datenverarbeitung dar. Ein Ausfall hat daher drastische Folgen für die Allgemeinheit.

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) weist in dem Bericht „Die Lage der IT-Sicherheit in Deutschland 2015“ [Ref. 1] auf die Bedrohungen und Gefährdungspotentiale – auch anhand aktueller Beispiele – eindringlich hin. Dabei ist eine Zunahme von Cyber-Attacken festzustellen, die sich auch gegen staatliche Stellen richten und ebenso kritische Infrastrukturen zum Ziel haben. Den IT Grundschutz adressiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit einem ganzen Katalog an Maßnahmen [Ref. 2]. Doch ebenso gibt es im internationalen Kontext entsprechende Vorgehensweisen, wie z.B. in den Vereinigten Staaten durch das „Department of Homeland Security“ [Ref. 3].

Mit einer Gesetzesinitiative „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz“ [Ref. 4] hat die Bundesregierung gerade den besonderen Schutz kritischer Infrastrukturen adressiert und dabei die die Betreiber ebenso wie die Hersteller in die Pflicht genommen.

Diese Themen sind aber nicht nur für große Unternehmen und die Betreiber von kritischen Infrastrukturen interessant, sondern auch für Mittelständische Unternehmen werden solche Aspekte immer wichtiger, da mit dem Internet der Dinge (IoT) und Industrie 4.0 die Internet-Technologie bis zu den Maschinen an der Bandstraße vordringen wird [Ref. 5].

Damit einhergehend hat das BSI Empfehlungen formuliert [Ref. 6], wie kritische Software überprüft werden muss, um Schwachstellen zu detektieren und zu beheben. Für Rechenzentren kommt damit der Management-SW (DCIM-SW) eine besondere Bedeutung zu, da sie alle Komponenten der physischen Infrastruktur beobachtet und steuert:

- Die DCIM-SW und alle aktiven Komponenten müssen gehärtet sein.
- Rollen und Rechte müssen stringent vergeben und dokumentiert werden.
- Die Nutzung einer DCIM-SW ermöglicht die transparente Beobachtung und Steuerung des Rechenzentrums.
- Ereignisse können miteinander verknüpft, Meldungsketten generiert und Workflows vereinbart werden, so dass auf Bedrohungen und Störungen automatisiert reagiert werden kann.

Mit dem vorliegenden Whitepaper wird daher die Management Software eines Rechenzentrums in zweifacher Hinsicht beleuchtet:

- Wie sicher ist die DCIM-SW selbst im Zusammenspiel mit allen aktiven Komponenten einer physischen Rechenzentrumsinfrastruktur?

und

- Was kann eine DCIM-SW zur Sicherheit im Rechenzentrumsumfeld beitragen?

Einführung

Gefahrenvektoren in der physischen RZ-Infrastruktur

Rechenzentren, als Rückgrat einer zunehmend digitalen Gesellschaft, beherbergen eine große Zahl von Servern, Speichersystemen und aktiven Netzwerkkomponenten (Switches, Router). Um den reibungslosen Betrieb dieser aktiven IT Komponenten zu gewährleisten, ist eine entsprechende physische IT Infrastruktur vorzuhalten, durch die eine sichere Stromverteilung und Stromabsicherung ebenso zur Verfügung gestellt wird wie eine bedarfsgerechte Klimatisierung. Darüber hinaus muss das Rechenzentrum mit allen Komponenten gegenüber den klassischen Gefährdungspotentialen geschützt werden, wie z.B.:

- Feuer
- Rauch
- Wasser / Wasserdampf
- Staub
- Trümmerlasten
- Vandalismus
- Einbruch
- EMV (Einstrahlung, Abstrahlung)

Die erforderlichen Schutzmaßnahmen werden durch eine ganze Reihe von Produkten und Lösungen bereitgestellt, die sich an internationalen Standards und Normen orientieren, wie sie in einem separaten Whitepaper „Physische Sicherheit in der IT- und RZ-Technologie“ [Ref. 7] beschrieben sind.

Ebenso wichtig ist die kontinuierliche und sichere Überwachung der Betriebsparameter eines Rechenzentrums, da Störungen in der physischen IT Infrastruktur ebenso die Funktion und damit das mit den Kunden vereinbarte Leistungsversprechen (SLAs) beeinträchtigen. Solche Störungen der Betriebsparameter können z.B. sein:

- Netzausfall des Energieversorgers
- Netzstörungen auf den Versorgungsleitungen
- Störungen im Stromverteilungspfad (Haupteinspeisung, Unterverteilung, Steckdosensysteme)
- Ausfall der Klimatisierung (Kälteerzeugung, Kältetransport, Kälteverteilung)
- Ausfall einzelner Sensoren / des Monitor-Systems (Temperaturüberschreitungen, Feuchtigkeit, Leckage, …)

Die Vielzahl der Komponenten einer physischen IT Infrastruktur, wie die große Anzahl der zu überwachenden Betriebsparameter macht eine automatisierte Überwachung und Auswertung der Daten notwendig.

Diese Aufgabe wird von der DCIM-SW (Data Centre Infrastructure Management) [Ref. 9] durchgeführt, da diese gesamte physische IT- Infrastruktur eines Rechenzentrums überwacht und steuert; dies umfasst z.B.:

- Stromversorgung und Zuverlässigkeit
- Kälteerzeugung und Verteilung
- Umgebungsparameter (Temperatur, Feuchte, …)
- Kapazitätsmanagement (Gewicht, HEs, Kühlung)
- Sicherheit im Rechenzentrum
- Effizienz und Energieverbrauch

Die einzelnen Parameter können in anwenderspezifischen Sichten in einem hierarchischen Dash-Board (Abbildung 1) dargestellt werden.

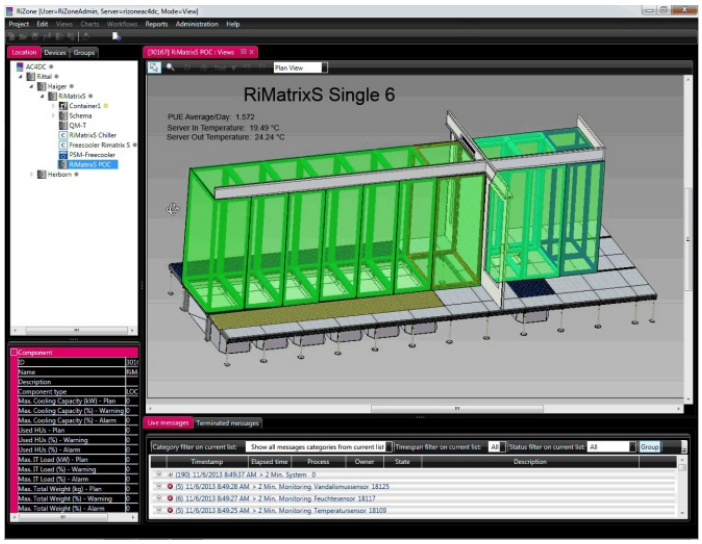


Abbildung 1: Dash-Board der DCIM-SW

Einzelne Ereignisse lassen sich dabei mit Workflows miteinander verknüpfen, so dass Alarmszenarien definiert und Reaktionen – auch automatisiert – eingeleitet werden können. Über entsprechende Schnittstellen können die erforderlichen Informationen und Alarme an übergeordnete Managementsysteme weitergeleitet werden.

Sicherheitsaspekte der DCIM-SW

Jedes Monitoring-System und auch jede DCIM-Lösung besteht aus mehreren Komponenten, wie aus der nachfolgenden Aufstellung und der Architekturdarstellung in Abbildung 2 ersichtlich wird:

- Applikationssoftware
- Datenbanksystem
- (ggf. virtualisiertes) Betriebssystem
- physischer Server

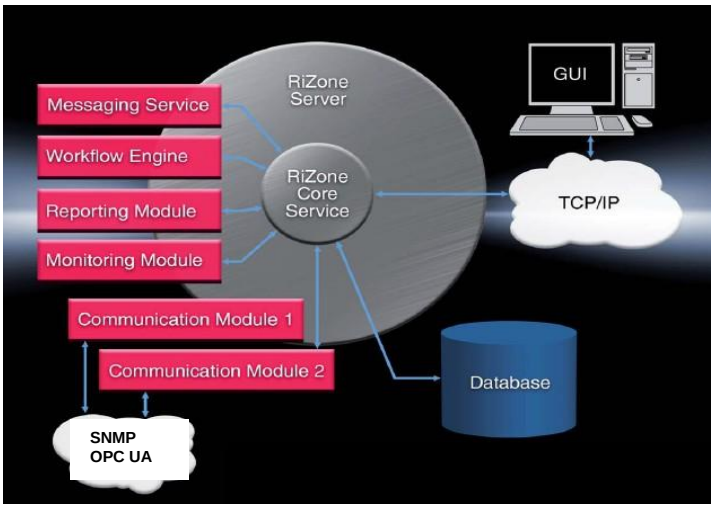


Abbildung 2: DCIM-Architektur

Damit wird verständlich, dass eine DCIM-Lösung ebenso wie jedes andere IT System Cyber-Angriffen ausgesetzt sein kann. Rechenzentren und damit auch deren Monitoring-Systeme oftmals Bestandteil einer kritischen Infrastruktur. Die Anzahl der Bedrohungen nimmt dabei zu, wie der Bericht des BSI [Ref. 1] zeigt, der jährlich veröffentlicht wird. In nachfolgender Tabelle 1 wird eine Übersicht der Aktivitäten dargestellt.

Gefährdung	2014	2015
Cloud Computing		→
Software-Schwachstellen	→	↑
Hardware-Schwachstellen		→
Nutzerverhalten und Herstellerverantwortung		↑
Kryptografie		→
Internet-Protokolle		↑
Mobilkommunikation		↑
Sicherheit von Apps		↑
Sicherheit von Industriellen Steuerungsanlagen		↑
Schadsoftware	↑	↑
Social Engineering	↑	→
Gezielte Angriffe - APT	→	↑
Spam	↑	↑
Botnetze	→	↑
Distributed Denial-of-Service (DDoS)-Angriffe	→	→
Drive-by-Exploits und Exploit-Kits	→	↑
Identitätsdiebstahl	↑	↑

Legende
Gefährdung 2015 (niedrig, durchschnittlich, hoch) ↓ → ↑

Tabelle 1: Gefährdungspotenziale (BSI 2015)

Gerade im Hinblick auf kritische Infrastrukturen sind sowohl vom Betreiber, wie auch vom Hersteller entsprechende Maßnahmen zu ergreifen, wie sie auch von der deutschen Gesetzgebung im „IT Sicherheitsgesetz“ [Ref. 4] zum Ausdruck gebracht worden sind. Vom BSI wurde dahingehend auch eine Empfehlung herausgegeben, wie Software-Lösungen zu überprüfen sind [Ref. 6], analog gibt es Empfehlungen vom „Department of Homeland Security“ in den Vereinigten Staaten [Ref. 3]. Eine Übersicht möglicher Schwachstellen wird z.B. vom Software Engineering Institute der Carnegie Mellon University [Ref. 8] herausgegeben.

In den nachfolgenden Kapiteln wird daher im Detail die Überprüfung der DCIM-Lösung beschrieben. Dabei ist darauf zu achten, dass nicht nur das DCIM-System alleine, sondern alle aktiven Komponenten der physischen IT Infrastruktur zu analysieren sind.

So ist es auch nicht ausreichend die Rechenzentrums-Infrastruktur durch eine Firewall zu schützen, vielmehr muss die Kombination der Schutzmaßnahmen dahingehend übergreifend optimiert werden, um eine zuverlässige Abwehr zu gewährleisten.

Schwachstellenanalyse DCIM

Das Ergebnis einer Schwachstellenanalyse der DCIM-SW RiZone ist abhängig davon, wie der Windows- Server konfiguriert wird. In der Bedienungsanleitung [Ref. 9] wird angegeben, welche Ports für den Betrieb benötigt werden:

- 161 (SNMP get/set)
- 162 (SNMP trap handler),
- 800 (certificate provider),
- 3389 (RDP)
- 4433 (https für Rollen und Rechte),
- 22222 & 22223 (Service-Port RiZone Core)

Die übrigen Ports können dann prinzipiell explizit dicht gemacht werden, um keinen Angriffspunkt zu bieten.

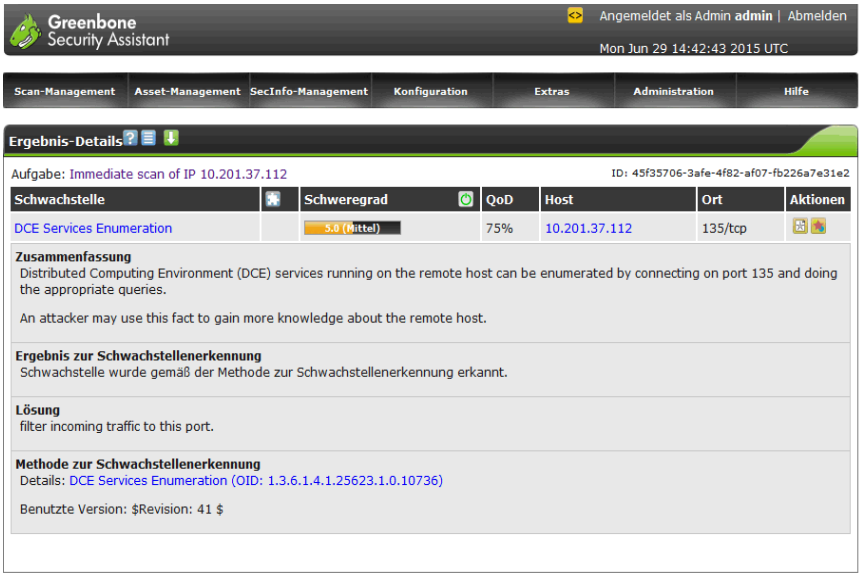


Abbildung 3: Bericht OpenVAS

Der Test der Härtung der DCIM-SW RiZone wurde mit Greenbone/OpenVAS [Ref. 9] mit den Betriebssystemen Windows Server 2008r2 und Windows Server 2012r2 durchgeführt.

OpenVAS [Ref. 9] ist ein Werkzeug, welches es gestattet, eine umfangreiche Analyse auf eventuelle Schwachstellen eines IP-basierten Systems durchzuführen, wie es bei einem DCIM- bzw. Monitoring-System der IT-Infrastruktur der Fall ist. Dabei können verschiedene Prüftiefen definiert werden, so dass die Identifikation und Eingrenzung potentieller Schwachstellen erleichtert wird. Herzstück des Werkzeugs ist dabei ein NVT-Scanner (Network Vulnerability Test), der - mit aktuellen Pattern versorgt - das Netzwerk auf potentielle Schwachstellen absucht. Die detektierten Schwachstellen können dann kategorisiert und mit Prioritäten versehen werden, so dass Abstellmaßnahmen definiert und umgesetzt werden können.

Bei der Überprüfung der DCIM-SW RiZone mit Hilfe von OpenVAS – wie in Abbildung 3 dargestellt – wurden Gefährdungen detektiert. Diese Gefährdungsstellen sind auf das Betriebssystem zurückzuführen. Mit Hilfe der Windows-Firewall lassen sich diese Schwachstellen komplett eliminieren.

Überprüfung der aktiven IT Infrastruktur-Komponenten

In einem typischen Rechenzentrum (Abbildung 4) finden sich eine Vielzahl aktiver Komponenten der IT Infrastruktur, die über IP-Schnittstellen verfügen und in das Netzwerk eingebunden sind. Für diese Komponenten gelten die gleichen Bedrohungspotenziale wie sie zuvor für die DCIM-SW beschrieben wurden.

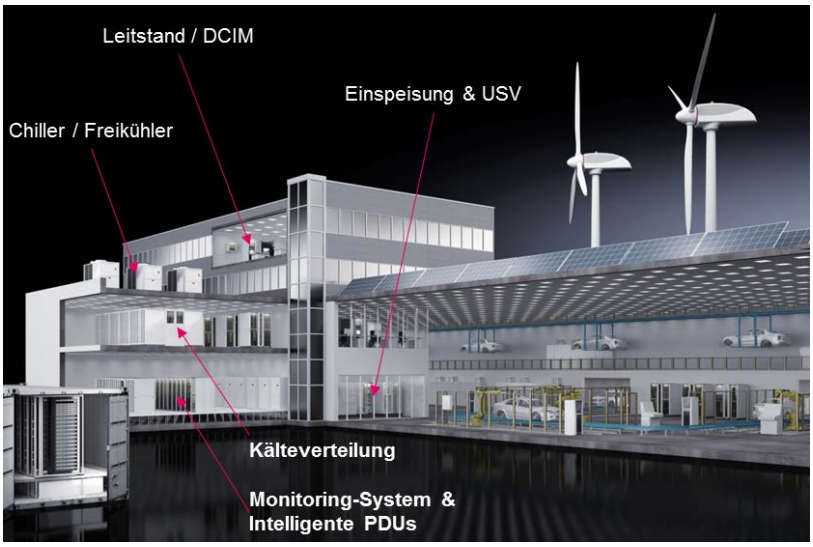
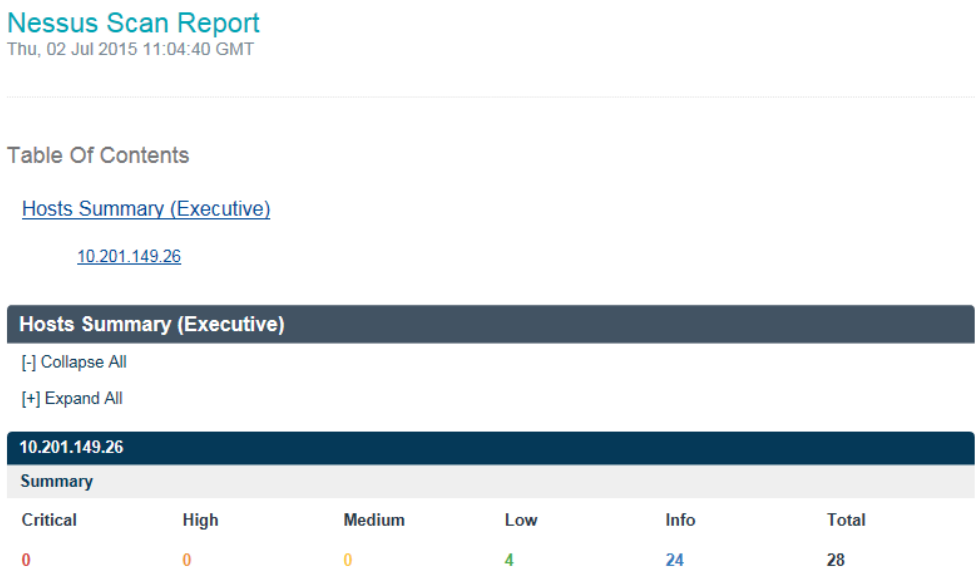


Abbildung 4: Aktive Komponenten der IT Infrastruktur

Der nachfolgende, beispielhafte Test des Monitoring Systems CMC (Abbildung 5) wurde mit der Software Nessus V.6.4.1 der Firma tenable network secruity [Ref. 11] durchgeführt.



Nessus Scan Report
Thu, 02 Jul 2015 11:04:40 GMT

Table Of Contents

Hosts Summary (Executive)

10.201.149.26

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

10.201.149.26

Summary

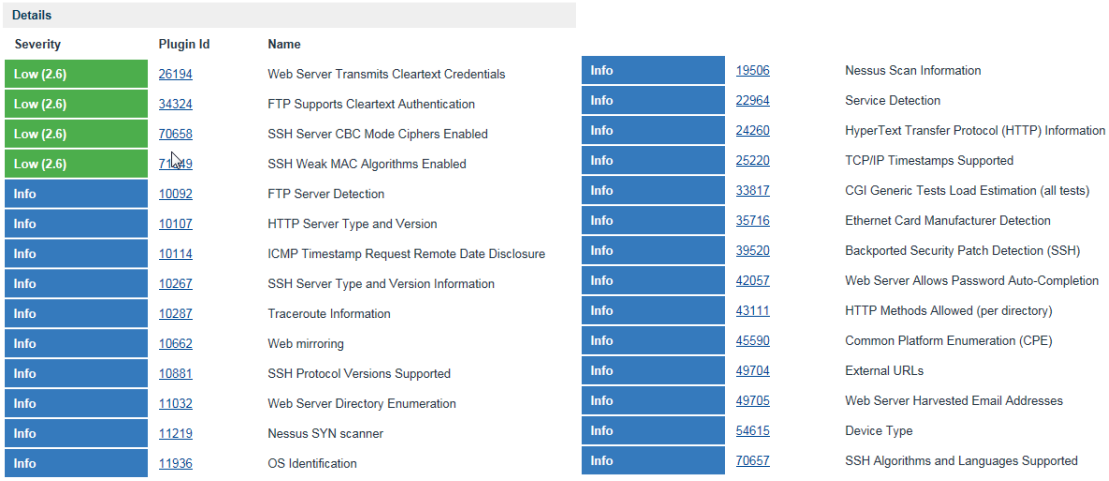
Critical	High	Medium	Low	Info	Total
0	0	0	4	24	28

Abbildung 5: Nessus-Bericht für das Monitoring-System CMC

Nessus [Ref. 11] ist ein Web-basierter NVT-Schwachstellen-Scanner, der aus einem HTTP-Server und einem Web-Client besteht. Das LDAP-Protokoll wird unterstützt, so dass sich der Nessus-Server im Netzwerk authentisieren kann.

Untersuchungen können auf IPv4 bzw. IPv6 Adressen (CIDR Annotation zur effizienteren Nutzung des Adressraums) durchgeführt werden. Die Ergebnisse einer Analyse können exportiert oder auf einem Dash-Board (siehe z.B. Abbildung 5) visualisiert werden.

Nessus identifiziert Schwachstellen und Sicherheitslücken durch ein sogenanntes „Vulnerability-Scannen“ der Netzwerkkomponenten, Applikationen, Datenbanken und Betriebssystemen. Das Scan-Ergebnis liefert Hinweise auf Schwachstellen und Abstellmaßnahmen, so dass gezielt die betroffenen Schnittstellen gesichert werden können oder eine entsprechende Maßnahme im Kundennetzwerk des Rechenzentrums vorgenommen werden muss (siehe z.B. Abbildung 6).



Details

Severity	Plugin Id	Name
Low (2.6)	26194	Web Server Transmits Cleartext Credentials
Low (2.6)	34324	FTP Supports Cleartext Authentication
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10092	FTP Server Detection
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10662	Web mirroring
Info	10881	SSH Protocol Versions Supported
Info	11032	Web Server Directory Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	33817	CGI Generic Tests Load Estimation (all tests)
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	42057	Web Server Allows Password Auto-Completion
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	49704	External URLs
Info	49705	Web Server Harvested Email Addresses
Info	54615	Device Type
Info	70657	SSH Algorithms and Languages Supported

Abbildung 6: Nessus-Detailbericht

Die gleichen Überprüfungen / Härtungen müssen für alle aktiven Komponenten in der physischen Infrastruktur durchgeführt werden.

DCIM – Ein essentieller Baustein der RZ-Sicherheit

Rollen und Rechte

Eine DCIM-Lösung ist ein mächtiges Werkzeug, welches nicht nur das Beobachten, sondern auch das Steuern der physischen IT Infrastruktur unterstützt. So ist z.B. möglich, einzelne Töpfe eines Steckdosensystems aus der Ferne zu schalten, oder aber auch die Betriebsparameter eines Chillers zu ändern. Derartige Eingriffe in die IT Infrastruktur dürfen nur von autorisiertem Fachpersonal vorgenommen werden. Daher ist die stringente Umsetzung der Rollen und Zugriffsrechte im DCIM-/Monitoring-System essentiell:

- Beobachten
- Auswerten
- Ändern
- Administrative Rechte

Die Rollen und Verantwortlichkeiten sind im Betriebs- und Notfallhandbuch des RZs entsprechend zu dokumentieren. Im Falle einer Auditierung sind diese Maßnahmen nachzuweisen.

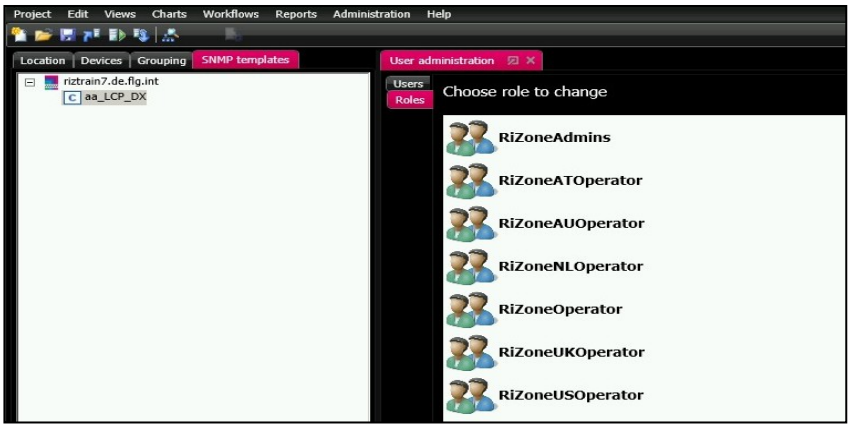


Abbildung 7: Rollen- und Rechtevergabe im DCIM-Tool

Visualisierung der Ereignisse

Das DCIM-System ist in der Lage alle Ereignisse und deren zugehörigen Betriebsparameter aufzuzeichnen und in eine (SQL-) Datenbank abzulegen. Entscheidend ist dabei die

Zuordnung der aktiven Komponenten zu der Topologie des Rechenzentrums (Platzierung im Schrank, Schrankreihe, Raum, Etage, Gebäude, Ort, Land), so dass ein direkter Bezug zwischen einem Ereignis und der Position der betroffenen Komponente in einer hierarchischen Darstellung erzeugt werden kann.

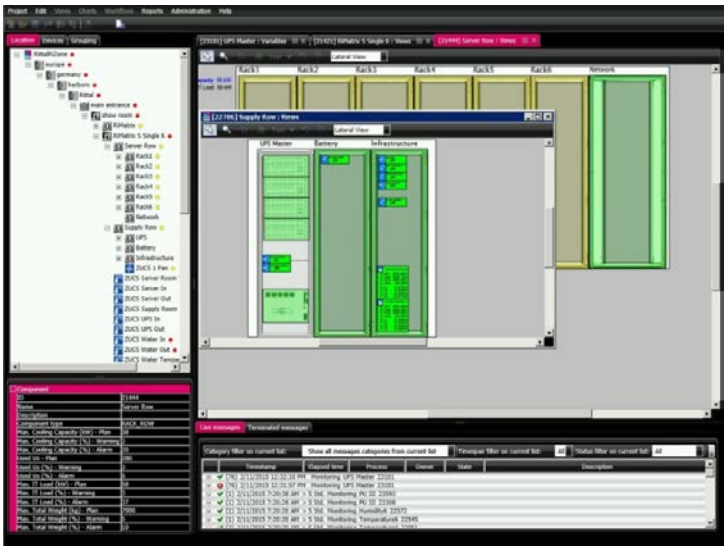


Abbildung 8: On-line Monitoring im DCIM-Tool

Dabei erlauben es die zuvor vereinbarten Rollen und Rechte spezifische Sichten zu definieren, die dem jeweiligen Benutzerkreis zugeordnet werden können.

Monitoring und Trendanalyse

Alle Werte, die eingelesen oder berechnet werden, können in beliebiger Zusammenstellung in Diagrammen dargestellt und mit historischen Werten aus der (SQL-) Datenbank verglichen werden. Das DCIM-System unterstützt bei der Berechnung von Formeln, die es erlauben, die gemessenen Werte miteinander zu verknüpfen und Berechnungen durchzuführen, wie z.B. zur Berechnung des PUEs.

Abbildung 9: Trendanalysen im DCIM-Tool

Darauf aufbauend können Berichte automatisiert generiert werden, um z.B. die Entwicklung der Stromkosten zu dokumentieren. Basierend auf den Rollen und Rechten, können diese Funktionen für die jeweiligen Benutzergruppen zugeschnitten werden.

Alarmmanagement & Workflows

Durch die Workflow-Engine der DCIM-SW können automatisierte Überwachungs- und Steuerszenarien abgebildet werden, diese basieren auf den zuvor definierten Schwellwerten für Warnungen und Alarmen.

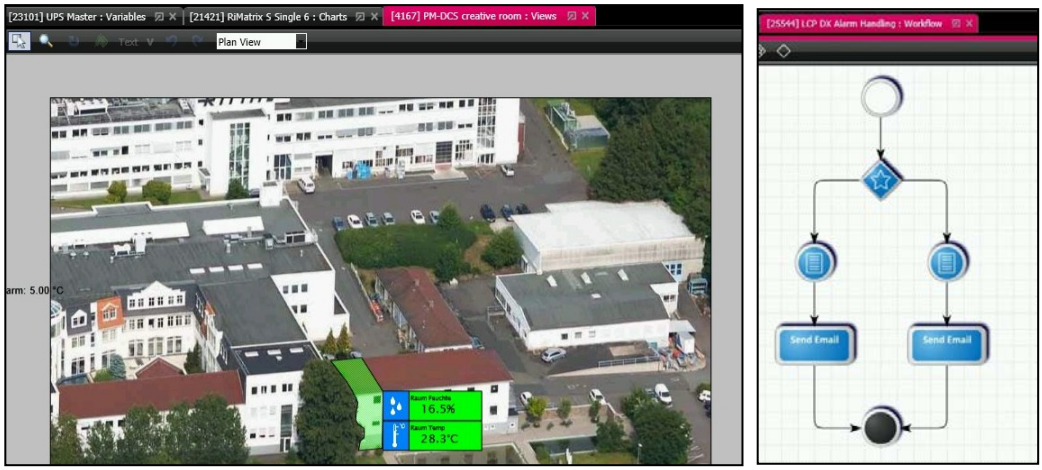


Abbildung 10: Workflows und Alarmszenarien im DCIM-Tool

Die Möglichkeit, Ereignisse miteinander zu verknüpfen, gibt dem Anwender eine Sicht auf das Rechenzentrum, die bei isolierter Betrachtung der Einzelkomponenten nicht möglich ist. Alarme werden dabei schematischen oder photographischen Darstellungen überlagert. Die komplette Übersicht wird individuell für jeden Anwendungsfall gestaltet.

Darüber hinaus können Meldungen (Warnungen, Alarme) gezielt bearbeitet werden. In der Historie ist dokumentiert, wer wann welches Ereignis bearbeitet hat.

Einbindung in Management-Systeme

Die Möglichkeit, Daten der DCIM-SW in ein Managementtool für Server, Betriebssystem, Virtualisierung und Applikation zu senden (Abbildung 11), gestattet dem Rechenzentrums-Betreiber die Realisierung eines einheitlichen Dash-Boards.

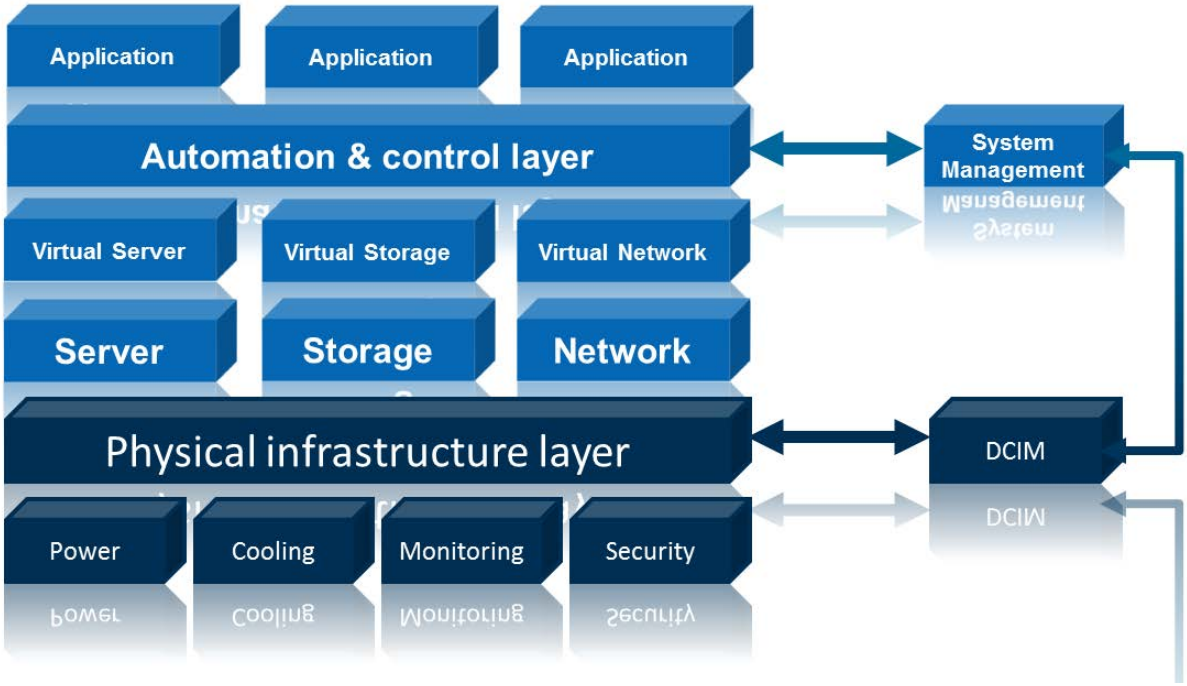


Abbildung 11: Zusammenspiel im Kontext der Virtualisierung

Die Protokolle SNMP und OPC-UA werden dabei unterstützt, so dass auch die Einbindung in eine GLT / BMS möglich.

Literatur

Ref. 1 Bundesamt für Sicherheit in der Informationstechnik (BSI), “Die Lage der IT-Sicherheit in Deutschland 2015“, Link: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf

Ref. 2 Bundesamt für Sicherheit in der Informationstechnik (BSI), “IT Grundschutz“, Link: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

Ref. 3 Department of Homeland Security, Critical Infrastructure Vulnerability Assessment, Link: http://www.dhs.gov/critical-infrastructure-vulnerability-assessments

Ref. 4 Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31, ausgegeben zu Bonn am 24. Juli 2015, „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)“, Link: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__//*[@attr_id='bgbl115s1324.pdf']__1440083508634

Ref. 5 Bundesministerium für Bildung und Forschung, Plattform Industrie 4.0, Whitepaper: Zukunftsbild „Industrie 4.0“; Link: http://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/zukunftsbild-industrie-4-0.pdf

Ref. 6 Bundesamt für Sicherheit in der Informationstechnik (BSI), Open Vulnerability Assessment System (OpenVAS), Link: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Tools/OpenVAS/OpenVAS.html

Ref. 7 Rittal Whitepaper: „Physische Sicherheit in der IT- und RZ-Technologie“

Ref. 8 Übersicht möglicher Schwachstellen: “Vulnerability Notes Database“, Carnegie Mellon University, Software Engineering Institute, Link: https://www.kb.cert.org/vuls/

Ref. 9 Rittal „RiZone Bedienungsanleitung“, Link: http://www.rittal.de/downloads/rimatrix5/software/V3_6/Manual_Rizone_Appendix36_V10_en.pdf

Ref. 10 OpenVAS, Link: http://www.openvas.org/index.html

Ref. 11 tenable network security, Link:

http://www.tenable.com/products/nessus-vulnerability-scanner

Ref. 12 Namenskonvention für Schwachstellen in IT-Systemen, Link: https://cve.mitre.org/cve/cna.html

Abkürzungsverzeichnis

APT	Advanced Persistent Threads (ausgefeilter, andauernder, zielgerichteter Angriff auf kritische IT-Infrastrukturen)
BMS	Building Management System
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBC	Cipher Block Chaining Mode (Verschlüsselung eines Klartext-Blocks)
CIDR	Classless Inter-Domain Routing
CMC	Computer Multi Control (Basiseinheit Monitoring-System)
CPE	Common Platform Enumeration (einheitliche Namenskonvention zur Bezeichnung von Schwachstellen in IT-Systemen
CVE	Common Vulnerabilities and Exposures (einheitliche Namenskonvention für Sicherheitslücken in IT-Systemen)
DCE	Distributed Computing Environment
DCIM	Data Centre Infrastructure Management
DDoS	Distributed Denial of Service
DoS	Denial of Service (Ausfall eines Dienstes aufgrund einer Ressourcen-Überlastung)
EMV	Elektromagnetische Verträglichkeit
FTP	File Transfer Protocol
GLT	Gebäudeleittechnik
GUI	Graphical User Interface
HE	Höheneinheit
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol (Protokoll zum Austausch von Informations- und Fehlermeldungen)
IoT	Internet of Things (Internet der Dinge)
IPv4	Internet Protocol Version 4 (Verwendung von 32-Bit Adressen)
IPv6	Internet Protocol Version 6 (Verwendung von 128-Bit Adressen)
IT	Informationstechnologie
LDAP	Lightweight Directory Access Protocol (Verzeichnisdienst zur Autorisierung)
NVT	Network Vulnerability Test (Schadensanfälligkeit eines Netzwerks)
OLE	Object Linking and Embedding
OPC UA	Open Platform Communications Unified Architecture
OS	Operating System (Betriebssystem)

PUE	Power Usage Effectiveness
RDP	Remote Desktop Protocol
RZ	Rechenzentrum
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SSH	Secure Shell (verschlüsseltes Netzwerkprotokoll)
SSL	Secure Sockets Layer (Verschlüsselungsprotokoll zur Datenübertragung)
SQL	Structured Query Language
SW	Software
SYN	SYN-Flood (Denial of Service Attacke) auf eine nicht vollständig aufgebaute TCP-Verbindung
TCP/IP	Transmission Control Protocol / Internet Protocol
URL	Uniform Resource Locator (IT-Ressource und zugehörige Zugriffsmethode)
VAS	Vulnerability Assessment System

Rittal – Das System.

Schneller – besser – überall.

- Schaltschränke
- Stromverteilung
- Klimatisierung
- IT-Infrastruktur
- Software & Service

RITTAL GmbH & Co. KG
Auf dem Stützelberg · D-35726 Herborn
Phone + 49(0)2772 505-0 · Fax + 49(0)2772 505-2319
E-Mail: info@rittal.de · www.rittal.de · www.rimatrix5.de