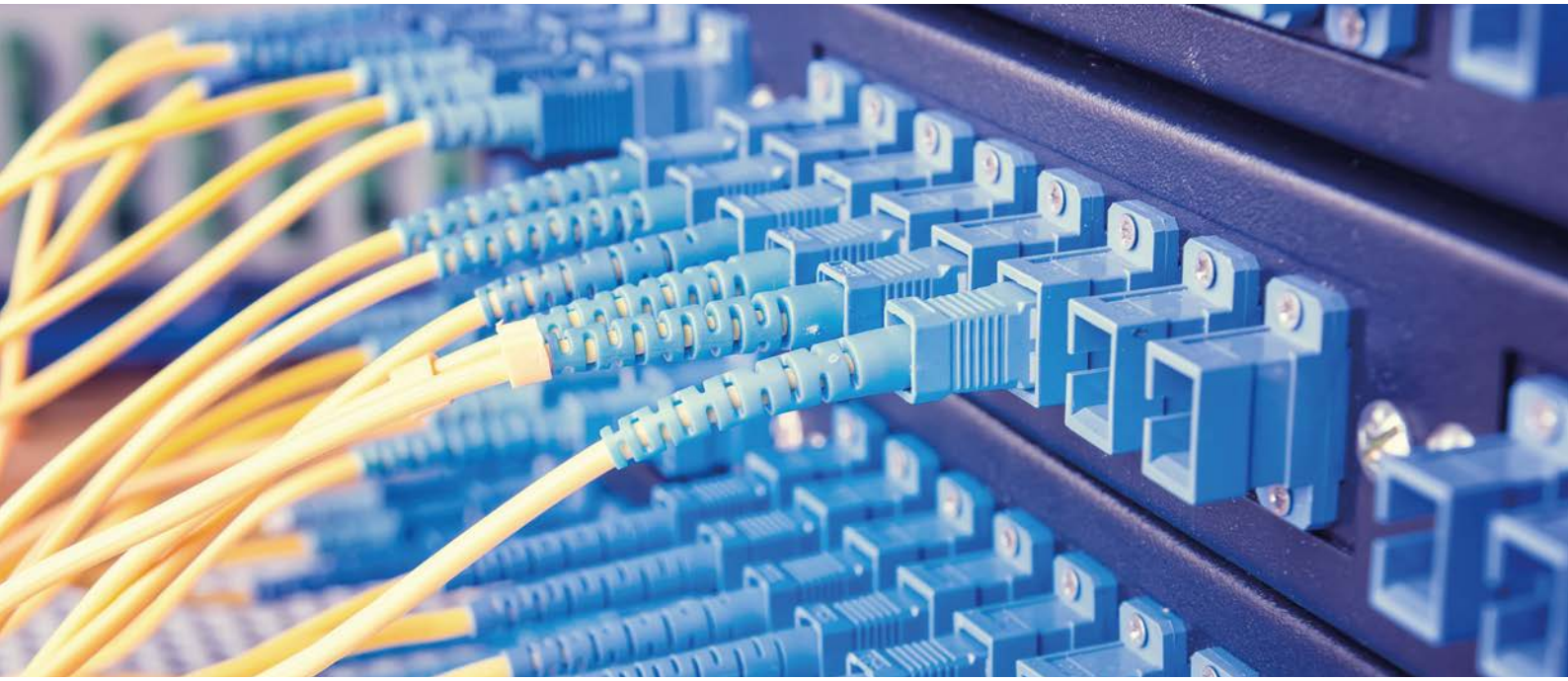

Hochverfügbarkeit oder die Suche nach den 100 Prozent Netzwerk-Sicherheit

circular Informationssysteme GmbH

Laut einer weltweit durchgeführten Studie betragen die Kosten für einen IT-Ausfall durchschnittlich 555.000 US-Dollar. Das kann neben Umsatz-Einbußen und Reputationsverlust im schlimmsten Fall den Ruin des Unternehmens bedeuten. Darum gilt für ein hochverfügbares IT-Netzwerk, Single Points of Failure (SPoF) in den einzelnen Netzwerk-Komponenten zu vermeiden, also die Schwachpunkte im System, die bei einer Fehlfunktion zum Ausfall führen. Sowohl aktive Komponenten (Firewall, Router, Switch etc.) als auch passive Komponenten (Patchpanel, Verkabelung, Stecker, Glas oder Kupfer etc.) sind in diesem Zusammenhang zu beachten. Das Thema „Hochverfügbarkeit" in einem lokalen (Local Area Network, LAN) oder weiter ausgelegten Netzwerk (Wide Area Network, WAN) sollte dabei nicht nur schichtweise, sondern im Ganzen betrachtet werden.

Ein Faktor ist entscheidend, um überhaupt eine der hohen Verfügbarkeitsklassen (ab 99,9 Prozent, was immerhin noch eine Ausfallzeit von acht Stunden und 45 Minuten im Jahr entspricht) erreichen zu können. Das Ziel muss sein, eine durchgehende, systemübergreifende Redundanz in Hardware, Software, Anwendungsmanagement etc. aufzubauen, also mindestens die doppelte Ausführung jeder Systemkomponente beziehungsweise jedes Daten-Transportwegs zu garantieren. Eine aktuelle ECC-Studie mit deutschen Unternehmen zeigt die Schäden, die durch den Komplettausfall von IT- und Netzwerkkomponenten entstehen können: Bei bis zu einem Tag Stillstand gehen bereits mehr als zwanzig Prozent der Befragten von einer Schadenshöhe von über 20.000 Euro aus *(siehe „https://de.statista.com/statistik/daten/studie/150900/umfrage/geschaetzte-schadenshoehe-im-betrieb-bei-it-ausfall-in-deutschland")*.

Hochverfügbare Netzwerke: Schicht für Schicht weniger Ausfallrisiko

Die Hochverfügbarkeit im LAN oder WAN ist eine sehr komplexe Angelegenheit, die verschiedene Bereiche in der Netzwerk-Architektur betrifft. Die folgenden Ausführungen orientieren sich am „Open Systems Interconnection"-Modell (OSI). Es besitzt einen hierarchischen Aufbau, der die Kommunikation zwischen den verschiedenen

Systemen, Geräten, Clients und Hosts über Protokolle strukturiert und regelt. Dabei sind sieben OSI-Schichten definiert. Im LAN- oder WAN-Umfeld kommen aber nur die ersten drei Layer in Betracht:

- *Layer 1 (Physical Layer)*
  Beschäftigt sich primär mit der physischen Infrastruktur und Hardware-Redundanz
- *Layer 2 (Data Link Layer)*
  Steht für die Sicherungsebene, die eine geschützte Übertragung der Daten gewährleisten soll
- *Layer 3 (Network Layer)*
  Ist die Vermittlungsschicht; sie schaltet Verbindungen über Leitungen frei oder vermittelt Datenpakete an den richtigen Empfänger

Die erste Schicht – doppelt hält besser

Die physikalische Schicht steht ganz am Anfang jedes modernen, hochverfügbaren IT-Netzwerks. Sie sorgt dafür, dass einzelne Datenpakete, Symbole oder Bits elektrisch, mechanisch, per Schall etc. übertragen werden können. Durch eine physikalische Redundanz versuchen Netzwerk-Experten, die Funktion aufrechtzuerhalten. Eine Möglichkeit bietet hier das Link-Aggregation-Verfahren, mit dem mehrere physische LAN-Schnittstellen zu einem logischen Kanal definiert werden und diesen damit hochverfügbar machen.

Die zweite Schicht – die richtige Weichenstellung entscheidet

Im Data-Link-Layer beziehungsweise in der Sicherungsschicht geht es um das Thema „Switching". Layer-2-Switches funktionieren wie mechanische Weichen, sind hardwarebasiert (dadurch sehr schnell) und verbinden verschiedene Netzwerk-Komponenten über die entsprechenden angesteuerten Ports miteinander. Die Switches entscheiden über den Weg, den ein Datenframe durch das Netzwerk nimmt. Sie bestehen aus Ziel- und Quell-Adressen (MAC-Adressen), aus Steuer-Informationen zur Datenfluss-Steuerung, Nutzdaten des Pakets der Vermittlungsschicht und Prüfsummen zur Gewährleistung der Daten-Integrität. Auch in dieser Schicht ist auf Redundanz zu achten.

Die dritte Schicht – alles eine Frage der Route

Netzwerke unterscheiden sich in den Bereichen „Core" (Backbone), „Distribution" und „Access". Im Access-Bereich, der noch zu Layer 2 gehört, existiert eine hohe Portdichte. An diesen Ports hängen die verschiedenen Arbeitsplätze, die aber meist nicht redundant angebunden sind, da der Ausfall eines Rechners die Funktionsweise des Netzwerks nicht beeinträchtigt. Allerdings kann der Ausfall eines Servers schwerwiegende Folgen haben. Deshalb sind sie beispielsweise über ein Port-Bündelungsverfahren oder Link Bundling stets redundant aufgebaut.

Entscheidend für Layer 3 beziehungsweise die Vermittlungsschicht ist das IP-basierte Routing: Wenn ein Client oder Computer-Programm eines Endgeräts ein Datenpaket an eine bestimmte IP-Adresse versenden will, wird es zunächst an einen Router übermittelt. Dieser prüft dann, ob er eine Route kennt, die zu dieser IP-Adresse führt. Meist gibt es in dieser Schicht auch eine Default-Route ins Internet.

Redundancy-Protokoll – nur ein Geräte-Setup ist hochverfügbar

Das Routing-Verfahren lässt sich um Redundancy-Protokolle erweitern. Sind Übertragungsrouten überlastet oder fehlerhaft, ermitteln sie einen Alternativweg, der durch eine entsprechende Netz-Infrastruktur und redundante Komponenten bereits angelegt ist.

Technisch funktionieren Redundancy-Protokolle nach folgendem Schema: Jedes der beiden gedoppelten Geräte erhält eine eigene IP-Adresse. Eine dritte virtuelle IP-Adresse dient als Gateway für das Datenpaket. Sie entscheidet in einem Fail-Over-Szenario, an welches Gerät das Paket schließlich geht. Dabei gibt es zwei Device-Setups: Es existieren ein aktives und ein passives Gerät, wobei letzteres nur bei Ausfall des bisher aktiven Geräts einspringt.

In der zweiten Variante sind beide Geräte aus Load-Balancing-Gründen aktiv und teilen sich damit die Paket-Übermittlung untereinander auf. Dieses Konzept ist technisch und finanziell sinnvoll, da so die relativ teuren Switch-Ports und deren verfügbare Bandbreite effizient sowie ressourcenschonend genutzt werden können. Allerdings hat diese Variante den Nachteil, dass sich im schlechtesten Fall die Last des Traffic-Aufkommens von einem einzelnen Gerät nicht mehr abfangen lässt. Diese „Überbuchung" kann zu Betriebs-Einschränkungen beispielsweise bei der Bereitstellung von Bandbreite bis hin zum Ausfall eines Dienstes führen. Aus der Hochverfügbarkeitsperspektive ist deshalb das erste Setup zu empfehlen.

IT- und Netzwerk-Sicherheit

Netzwerke bestehen aus verschiedenen Komponenten wie Switch, Router, Load Balancer, Firewall und Intrusion Prevention System (IPS) sowie Intrusion Detection System (IDS) und können unterschiedlich aufgebaut sein. Im Hinblick auf das Thema „Hochverfügbarkeit" spielt dabei der Schutz des Netzwerks eine entscheidende Rolle. Hier beschäftigt sich die Netzwerk-Sicherheit grundsätzlich mit allen Maßnahmen zur Planung, Ausführung und Überwachung der Sicherheit in Netzwerken, was sowohl technologische Maßnahmen, die redundant vorliegen sollten, als auch organisatorische Schritte umfasst, wie etwa Mitarbeiterschulungen und Compliance-Regeln.

Ein Teil ist die Identifikation und Abwehr der verschiedenen Angriffe auf die eingesetzten Komponenten/Protokolle. Beispiele dafür sind etwa Man-in-the-Middle-Angriffe, die die Kommunikation zwischen Client und Zielsystem mitlesen oder beispielsweise durch falsche Routen (Route Poisoning) Verkehr umleiten und kompromittieren, oder Tunneling, mit dem sich Firewalls umgehen lassen. Um eine unerlaubte Ressourcen-Nutzung zu erkennen und zu verhindern, werden Maßnahmen zur Authentifizierung, Autorisierung und Identifikation eingesetzt.

Firewalls sind obligatorisch

Laut einer globalen Studie kosten Cybersicherheitsvorfälle große Unternehmen durchschnittlich über eine halbe Million US-Dollar, kleine und mittelständische Firmen müssen im Schnitt mit rund 38.000 US-Dollar rechnen *(siehe „http://media.kas-*

persky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf"). Deshalb sollte das Primärziel jedes IT-Verantwortlichen sein, das eigene Netzwerk möglichst sicher gegen externe und interne Cyber-Bedrohungen abzuschotten. Eine der immer noch entscheidenden State-of-the-Art-Sicherheitsmaßnahmen für Netzwerke sind Firewalls, die es hardwarebasiert in der Vermittlungsschicht und softwarebasiert in der Anwendungsschicht gibt.

Firewalls zählen heute wie Daten-Backup-Systeme zum Sicherheitsstandard jedes Unternehmens, so eine aktuelle Studie *(siehe „https://www.bundesdruckerei.de/digitalisierung/system/files_force/bundesdruckerei_studie_zu_it-sicherheit_und_digitalisierung.pdf")*. Doch im Dark Net finden sich immer neue Gefahren, wie etwa Baukästen für Spionage-Software oder Advanced Persistent Threats (APT), die in komplexen, mehrstufigen Attacken ins Netzwerk eindringen und oft erst zu spät oder gar nicht bemerkt werden. Ziel dieser Angriffe sind meist unternehmenskritische Informationen.

Heute benötigt es jedoch eine modernere Netzwerk-Architektur, da sich die Anforderungen an Firewalls durch die Zunahme von mobilen Endgeräten, Anwendungen, Homeoffice etc. geändert haben. Erlaubt ein Unternehmen unter anderem das Surfen im Internet, lässt sich dafür über herkömmliche Firewalls nur eine pauschale Freigabe erteilen. Deshalb stellt der Aus- und Eingang zum Internet, der bei den meisten Netzwerken über Port 80 oder bei verschlüsselten Webseiten über Port 443 erfolgt, einen besonders beliebten Angriffspunkt für Schadsoftware und Hacker dar. Hat ein Anwender, der immer noch das größte Sicherheitsrisiko für ein Netzwerk darstellt, beispielsweise versehentlich einen Trojaner, Wurm etc. installiert, versucht das Schadprogramm, die erbeuteten Informationen gegebenenfalls über diese beiden Ports aus dem Netzwerk zu schleusen.

Dagegen findet bei den Next-Generation-Firewalls eine tiefergehende Analyse des Traffics beziehungsweise der Datenpakete statt. Zu den herkömmlichen Funktionalitäten kommen IDS, IPS, QoS-Maßnahmen (Quality of Service), Applikationskontrollen, SSL- und SSH-Inspection, Deep Packet Inspection, reputationsbasierte Malware-Abwehr und Application Awareness etc. hinzu. Dabei werden unter anderem Datenpakete und Verbindungen genauer geprüft, etwa daraufhin, welche Anwendungen sowie Dienste sich dahinter verbergen und angesteuert werden.

Vor allem die applikationsspezifischen Abwehrmaßnahmen kümmern sich um die steigende Anzahl von Angriffen auf den Ebenen vier bis sieben des OSI-Stacks. Der Aspekt „QoS" kommt besonders bei verstärkt genutzten Applikationen wie VoIP oder Video-Konferenzsystemen zum Tragen. Deren ausfallsicherer Betrieb kann beispielsweise durch Maßnahmen wie Bandbreiten-Regulierung oder der Priorisierung der Applikationen bei der Bandbreiten-Bereitstellung zentral gemanagt werden.

Mit Next-Generation-Firewalls lassen sich Internet-Anwendungen managen,

erlauben und sperren, wie etwa die Facebook-Nutzung oder ein Freeware-Download. Dadurch werden das Herunterladen von Schadprogrammen oder der Aufbau einer unsicheren Schatten-IT an der eigenen IT-Abteilung vorbei verhindert.

Im Zusammenhang mit Next-Generation-Firewalls steht ebenfalls das Thema „Unified Threat Management" (UTM). UTM-Lösungen lassen sich als Firewall-Appliances definieren und stehen für ein multifunktionales Sicherheitskonzept, mit dem sich unternehmensspezifische Sicherheitsstrategien im Unternehmensnetz durchsetzen lassen. Ein Vorteil ist, dass Sicherheitstechniken und -funktionen, die bisher auf verschiedene Systeme verteilt waren, nun in einer Lösung vereint vorliegen. Damit sollen Angriffe, Datendiebstähle, Spams, Viren und Würmer, trojanische Pferde und andere Attacken kontrollierbar werden.

Zu den UTM-Features und -Schutzmechanismen gehören unter anderem die Content- und Spam-Filterung, Applikations- und Web-Kontrolle sowie Einbruchserkennung und Antiviren-Aktivitäten. Zudem lässt sich ein Security- und Policy-Management für Gruppen oder Anwender definieren. UTM-Lösungen sollen vor allem die Netzwerksicherheit zentral steuerbar machen und die Applikations-Schicht vor den Next-Generation-Bedrohungen schützen, ohne die Performance oder das Netzwerk zu belasten.

Mit Systemen für das Security Information and Event Management (SIEM) lässt sich der Traffic in Echtzeit überwachen. SIEM-Appliances wie etwa IBM QRadar oder Splunk sammeln und indexieren dabei Logs oder Ereignisse beziehungsweise Events, korrelieren diese und werten sie aus. Damit lassen sich anomales Anwenderverhalten, Eindringlinge und komplex vorgehende Malware auch innerhalb des Netzwerks identifizieren und gegebenenfalls sofort Gegenmaßnahmen einleiten.

Die Informationen betreffen das Zugangsmanagement, das Schwachstellen-Management und Compliance-Tools, Betriebssysteme, Datenbanken und Logfile-Analysen. Aus den gesammelten Ereignis-, Bedrohungs- und Risiko-Daten lassen sich Maßnahmen für die adaptive Verwaltung von Sicherheitsrisiken ableiten. Sie basieren auf unternehmensspezifischen Anforderungen – also auf klaren und umfassenden Definitionen, welche Ereignisse sicherheitsrelevant sind und wie mit welcher Priorität darauf zu reagieren ist. Das Ziel ist, anhand eines Regelwerks kontinuierlich die Standards für Sicherheit, Compliance und Qualität des IT-Betriebs zu verbessern.

Empfehlungen für ein modernes, hochverfügbares Netzwerk

Um ein möglichst hohes Maß an Hochverfügbarkeit und Netzwerk-Sicherheit zu schaffen, sollten grundsätzlich alle Komponenten im Netzwerk redundant aufgebaut sein. So lassen sich mögliche SPoF weitestgehend ausschließen. Damit Unternehmen auf heutige sowie künftige Herausforderungen angemessen reagieren können, müssen Netzwerke der nächsten Generation Aspekte wie Flexibilität, Netzwerk-Intelligenz und eine verteilte Steuerung in sich vereinen. Sich stetig verändernde IT-Landschaften und geschäftliche Anforderungen verlangen dabei dynamische und schnell anpassbare Systeme.

Durch die Fokussierung auf ein eventuell Cloud-optimiertes, skalierbares und adaptives Netzwerk können Netzwerk-Betreiber die Einschränkungen bewältigen, mit denen sie konfrontiert werden. Cloud-Services ermöglichen eine flexible Nutzung der IT-Ressourcen. Gleichzeitig stellen sie aber auch ein Sicherheitsrisiko dar, weil die Netzwerk-Sicherheit in fremde Hände gegeben wird. Wenn man jedoch von Anfang an den Sicherheitsaspekt berücksichtigt – und hier die Sicherheit des Dienstes und der Verwaltung –, können sich deutsche Unternehmen für Cloud-Dienste entscheiden, die sich in die bestehende IT-Landschaft integrieren lassen. Zudem sollten sie zumindest kritische Unternehmensdaten auf dem eigenen Firmenserver belassen und nur Cloud-Provider wählen, die den deutschen Datenschutz-Richtlinien unterliegen.

Ein anderer wichtiger Punkt ist die Einbindung sowohl lokaler als auch auswärts tätiger Mitarbeiter. Dank moderner und zentraler Netzwerksystem-Lösungen lassen sie sich zuverlässig in das Netzwerk integrieren. Die Systeme sind schnell und einfach an aktuelle sowie kommende Business Cases anpassbar. So können Mitarbeiter unternehmensweit auf dieselben Geschäftsanwendungen und -dienste zugreifen – mobil oder stationär. Weitere Vorteile sind:

- Nahtlose und sichere Vernetzung von Mitarbeitern, Kunden und Informationen
- Bestmögliche Nutzung qualitativer Echtzeit-Anwendungen wie ERP-, Audio- oder Video-Systeme
- Zugriff auf Dateien und Ressourcen – jederzeit und von überall
- Senkung der Betriebskosten
- Unterstützung nachhaltiger Geschäfts-, IT- und Netzwerkprozesse

Fazit

Die wichtigsten Bestandteile eines modernen, hochverfügbaren Netzwerks sind diese:

- Redundant aufgebaute Netzwerk-Komponenten
- Mindestens zweistufiger Firewall-Cluster von verschiedenen Herstellern (Diversivität)
- Redundant ausgelegte Internet- oder WAN-Verbindung
- UTM- und SIEM-Appliances für die Identifikation von Anomalien im Netzwerk
- Monitoring-Lösungen, um Netzwerke und Dienste zu überwachen, zu überprüfen und sich per Alerts automatisiert einen Ausfall anzeigen zu lassen (etwa ob ein Webserver oder eine Datenbank überhaupt noch verfügbar ist)
- Reporting-Lösungen, um über einen längeren Zeitraum beurteilen zu können, ob die bisherige Netzwerk-Infrastruktur oder die Bandbreite noch ausreicht oder ob skaliert werden muss
- Quality-of-Service-Funktionen und -Vorgaben: Dadurch lassen sich beispielsweise Applikationen (wie etwa die Bandbreiten-Nutzung) priorisieren und gegebenenfalls einschränken
- Out-of-Band-Management: ein Managementnetz getrennt vom Datennetz
- Policy based Routing/Forwarding: Damit können Daten bestimmt werden, die nicht innerhalb des normalen Datenstromes geroutet werden, sondern einen gesonderten Weg nehmen, etwa über eine zweite Internet-Anbindung

circular Informationssysteme GmbH
info@circular.de