neustifter.systems

IT-Infrastruktur

Wie Sie Ihr Firmen-Netzwerk strategisch aufstellen – übersichtlich und widerstandsfähig

Vorwort

Der wirtschaftliche Erfolg Ihres Unternehmens ist eng mit der konstanten Verfügbarkeit Ihrer Firmen-IT verknüpft. Eine solide IT-Infrastruktur ist für die Stabilität und Entwicklung Ihres Unternehmens unerlässlich.

Das Problem: Mit Firewall, Antiviren-Software und regelmäßigen Updates wähnen viele Firmen ihr Netzwerk in Sicherheit. Doch zu einem grundlegenden IT-Sicherheitskonzept zählt auch die Inventarisierung, Dokumentation und Segmentierung Ihrer IT-Infrastruktur. Dieser Dreiklang erleichtert die Verwaltung und Entwicklung Ihrer EDV-Landschaft um ein Vielfaches. Hinzu kommt, dass er Ihren Betrieb widerstandsfähig aufstellt – gegen Energieschwankungen sowie Angriffe auf Systeme und Daten, von innen und außen.

Im Folgenden erfahren Sie:

- Was diese Begriffe konkret für Ihr Unternehmen und Netzwerk bedeuten,
- Welche Chancen und Herausforderungen damit verbunden sind,
- Was Sie bei Erneuerung bzw. Erweiterung Ihrer Server-Landschaft beachten sollten.

Für individuelle Fragen und Beratungen zur passenden Strategie für Ihr Firmen-Netzwerk stehen wir Ihnen gerne zur Verfügung.

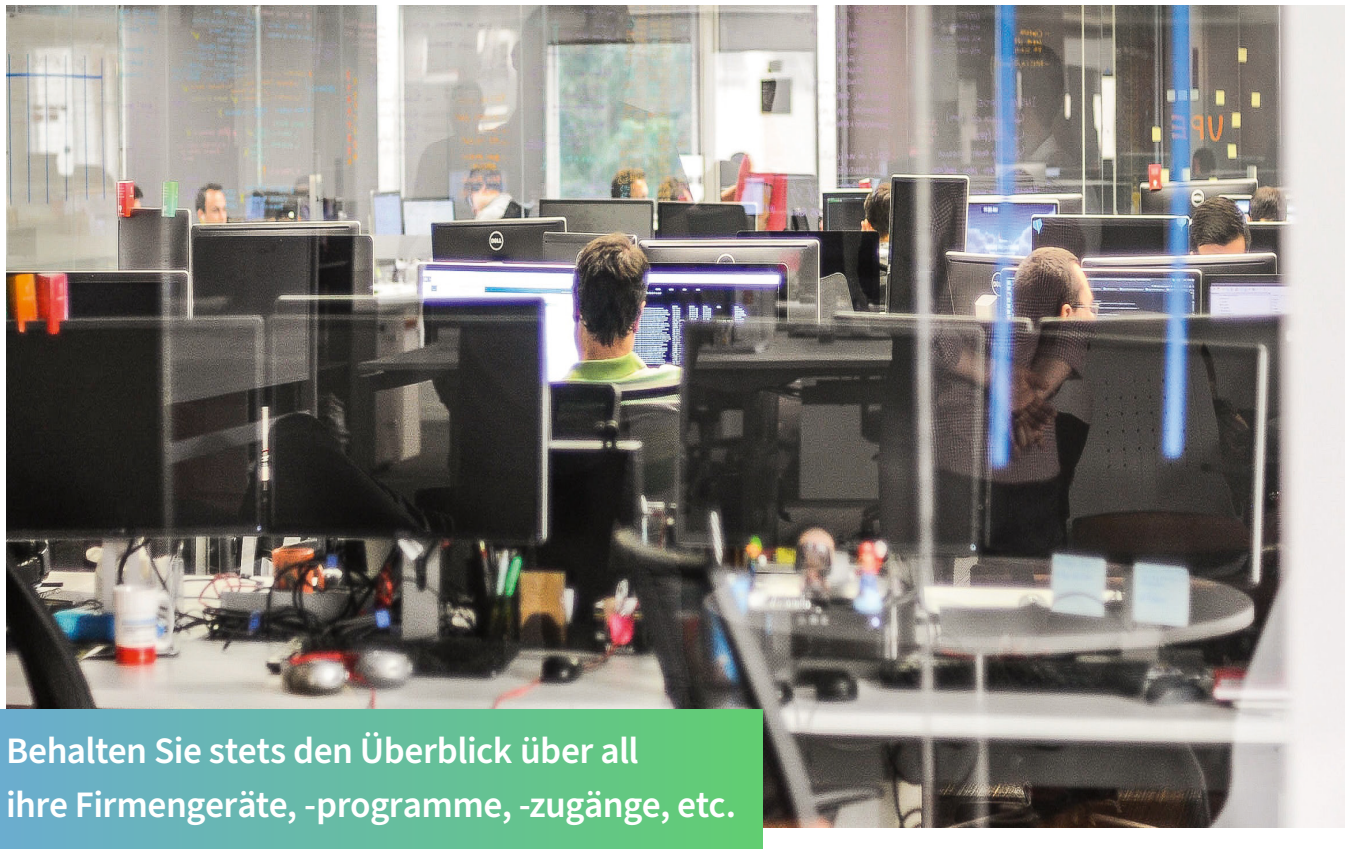
Inhaltsverzeichnis

1. Was ist eine Netzwerkdokumentation?

Eine Netzwerkdokumentation ist die Aufzeichnung des technischen Ist-Zustands Ihres Unternehmensnetzwerks – vollständig, übersichtlich, aktuell.

Diese IT-Dokumentation enthält in Tabellen, Dokumenten und Grafiken alle wichtigen Informationen über die gesamte Netzwerkinfrastruktur Ihrer Firma – angefangen bei der Hardware und ihren Standorten, über Softwareanwendungen, Internet- und Benutzer-zugängen, Sicherheitsvorkehrungen bis hin zu Handlungsanweisungen.

Netzwerkdokumentation ist also mehr als eine Inventarisierung und Visualisierung der vorhandenen Hard- und Software. Ihre Netzwerkdokumentation sollten Sie ständig aktuell halten, zum Beispiel, wenn Sie neue Geräte oder Programme anschaffen oder wenn Mitarbeiter Ihre Firma verlassen.



Behalten Sie stets den Überblick über all ihre Firmengeräte, -programme, -zugänge, etc.

1.1. Warum sollte Ihr Unternehmen keinesfalls darauf verzichten?

Weshalb Sie Zeit und Arbeitskraft investieren sollten, um eine grundlegende Dokumentation Ihres Netzwerks vorzunehmen und diese auch noch ständig aktualisieren sollten? Aus vier Gründen:

1	**Sie halten den künftigen Verwaltungsaufwand Ihres Netzwerks so gering wie möglich.**
2	**Sie können damit Kosten besser kalkulieren oder sogar senken.**
3	**Sie sorgen für den IT-Notfall vor, in dem schnell und richtig reagiert werden muss.**
4	**Sie steigern die Unabhängigkeit von Ihren IT-Administratoren.**

1.1.a) Verwaltungsaufwand minimieren

»Die Dokumentation jedes Netzwerks ist eine essentielle Hilfe: bei der Netzwerkadministration, -wartung und -pflege, bei allen Stör- und Notfällen sowie auch bei Neubeschaffungen«, weiß Anatol Badach, ehemaliger Professor im Fachbereich Angewandte Informatik der Hochschule Fulda. Der Autor des Buches Netzwerkprojekte. Planung, Realisierung, Dokumentation und Sicherheit von Netzwerken spricht damit vor allem IT-Administratoren an.

Vorteile einer IT-Dokumentation aus dieser technischen Sicht sind:

- ✔ **Schnelle Fehlersuche bei Störungen, um Ausfallzeiten zu minimieren**
- ✔ **Zügiger Neuaufbau von (Teil-) Systemen bei Upgrade oder Verlust**
- ✔ **Strukturiertes und effizientes Anlernen neuer Mitarbeiter**
- ✔ **Ganzheitliche Ermittlung möglicher Risiken bei geplanten Änderungen oder Erweiterungen der Netzwerkinfrastruktur**
- ✔ **Rechtzeitiges Erkennen von Schwachstellen und potenziellen Engpässen, um die Stabilität und Sicherheit des Firmennetzwerks zu erhöhen**

1.1.b) Kosten besser kalkulieren und sparen

Im laufenden Betrieb zielt der wirtschaftliche Wert und Nutzen einer Netzwerkdokumentation darauf ab, Kosten und Zeit zu sparen, und den Anforderungen des Gesetzgebers beziehungsweise Wirtschaftsprüfers gerecht zu werden.

Zudem hilft Ihnen eine IT-Dokumentation, den Überblick über Ihr Unternehmensnetzwerk zu behalten, damit sie eine effiziente und strategische Planung vornehmen können. Spätestens wenn Sie für Ihr Unternehmen eine ISO-Zertifizierung Ihrer IT anstreben, ist die vollständige Dokumentation Ihres Unternehmensnetzwerks sogar Pflicht.

1.1.c) Für den IT-Notfall vorsorgen

Bei einem Systemausfall, ganz gleich aus welchem Grund, verlieren Sie Geld. Hier kann die IT-Dokumentation der Rettungsring für Ihr Unternehmen sein: im besten Fall, um Ihr Netzwerk schnell und ohne großen betriebswirtschaftlichen Schaden wieder zum Laufen zu bringen. Im schlechtesten Fall, um die finanziellen Ausfälle, die durch den Ausfall Ihrer IT entstanden sind, durch eine Versicherung erstattet zu bekommen.

Im Schadensfall ist eine vollständige Netzwerkdokumentation oftmals die grundlegende Voraussetzung, damit die Versicherung überhaupt Bereitschaft zeigt, zu zahlen.

1.1.d) Unabhängigkeit steigern

Mit einer aktuellen Netzwerkdokumentation behalten Sie die Hoheit über Ihre Unternehmensdaten und schützen sich davor, erpressbar zu werden. Dabei geht es nicht darum, künstlich Dramatik zu erzeugen oder Panik zu verbreiten. Es geht vielmehr um ein Szenario, das bereits in Unternehmen vorgekommen ist und Ihnen die Wichtigkeit einer soliden Netzwerkdokumentation vor Augen führt.

Wenn Ihr IT-Administrator erkrankt, kündigt, in den Ruhestand geht oder plötzlich stirbt, dann geht sein Wissen mit ihm. Hinterlässt er keine vollständige, nachvollziehbare und aktuelle Netzwerkdokumentation, erhöht sich Ihr wirtschaftliches Risiko. Wenn Ihre Netzwerkinfrastruktur nicht funktionsfähig bleibt, ist der Geschäftserfolg je nach Digitalisierungsgrad Ihres Unternehmens gefährdet. Das Erstellen einer neuen IT-Dokumentation wird zur detektivischen Kleinarbeit – und frisst Zeit, Geld, Energie.

Machen Sie die Probe aufs Exempel

Simulieren Sie eine Netzwerkstörung oder einen Systemausfall und versuchen Sie dann, Ihr System wieder in Gang zu bekommen —
ohne Anruf bei Ihrem IT-Admin.

2. Selbsttest

	Wie gut haben Sie die Funktionsfähigkeit Ihrer Firmen-IT im Blick?	Ja	Nein	k. A.
1.	*Findet regelmäßig eine Inventur Ihrer Firmen-Hard- und Software statt?*			
2.	*Sind die Standorte jeder IT-Komponente in Ihrem Unternehmen in einem Lageplan eindeutig bestimmt?*			
3.	*Haben Sie einen Überblick über den Status Ihrer Software-Lizenzen?*			
4.	*Liegen schriftliche Handlungsanweisungen zu Standardprozeduren vor (Einrichtung eines neuen Arbeitsplatzes, Benutzers, Installation von Fremdsoftware)?*			
5.	*Verfügen Sie über eine zentral gesammelte Liste mit den Kontakten der wichtigsten Auftragnehmer und Lieferanten Ihres Firmennetzwerks?*			
6.	*Haben Sie die Konfigurationseinstellungen der einzelnen Netzwerk-komponenten in einem Datenblatt erfasst?*			
7.	*Ist die Rechtevergabe der Benutzer und Administratoren schriftlich festgehalten?*			
8.	*Sind die verwendeten Technologien, die Sie für Ihre Internetanbindung verwenden sowie deren Konfiguration und Installationsbeschreibung dokumentiert?*			
9.	*Haben Sie ein geregeltes Vorgehen im Falle von Sicherheits-verletzungen, z. B. durch Mitarbeiter, Angriffen aus dem Internet, Virenbefall, Datenverlust, Archivierung und Sicherung von Daten sowie zur Datenwiederherstellung, schriftlich fixiert?*			
10.	*Gibt es einen Konfigurations- und Wartungsplan für Geräte, die sicher-stellen, dass Ihre Firmen-IT über eine unterbrechungsfreie Strom-versorgung (USV) verfügt?*			

Sie können nicht jede Frage mit »Ja« beantworten? Dann ist ein Gespräch mit Ihrem IT-Team oder technischen Leiter sicherlich sinnvoll investierte Zeit, um die Stabilität und Funktionssicherheit Ihres Unternehmensnetzwerks grundlegend zu verbessern.

3. Netzwerksegmentierung als grundlegendes IT-Sicherheitskonzept

Ihre EDV-Systeme sind Dreh- und Angelpunkt für das IT-Sicherheitskonzept Ihres Unternehmens. Daher ist die Unterteilung Ihres Firmennetzes in voneinander abgetrennte Bereiche eine weitere, strategisch sinnvolle Maßnahme, um Ihr Unternehmen möglichst widerstandsfähig aufzustellen.

Das gilt im besonderen Maße für Unternehmen, die spezielle Branchenlösungen nutzen oder Produktionsmaschinen im Einsatz haben. Deren Funktionsfähigkeit ist häufig an ein EDV-System geknüpft, für das vom Hersteller eventuell kein Sicherheits-Support mehr erbracht wird.

Überspitzt formuliert: Mit gesundem Menschenverstand kommt keiner auf die Idee die Computer im OP-Saal mit dem Internet zu verbinden …

3.1. Netzwerksegmentierung – was ist das?

Netzwerksegmentierung beschreibt in der IT den Vorgang, das Unternehmensnetz in einzelne Bereiche zu unterteilen, die nicht oder nur noch bedingt miteinander vernetzt sind. Eine mögliche Unterteilung kann nach Abteilungen vorgenommen werden:

- Produktion
- Personalabteilung
- Buchhaltung
- …

Warum? Stellen Sie sich einfach folgende Frage:

Warum sollte der PC eines Buchhalters auf eine Produktionsanlage zugreifen können?

Wenn Sie keine Antwort darauf haben, sollten Sie die Segmentierung Ihres Netzwerks aktiv vorantreiben.

Praxis-Beispiel: Warum Segmentieren?

Produktionsanlagen werden meist auf lange Sicht angeschafft – für mindestens 10 bis 20 Jahre. Wenn die Betriebssoftware nach einigen Jahren keine Updates mehr erhält, die Maschine aber als solche noch voll funktionsfähig ist, muss sie nicht notwendigerweise ausgetauscht werden.

Eine Produktionsanlage, die beispielsweise nur mit einem alten Windows-XP-Rechner gesteuert werden kann, kann sicherheitstechnisch unproblematisch sein – solange der Rechner vom restlichen Netzwerk getrennt seine Arbeit verrichtet.

3.2. Warum brauchen Unternehmen Nachhilfe beim Netzwerkschutz?

Im Global Threat Intelligence Report 2015 untersuchte die NTT Group, ein weltweit agierender Provider von Telekommunikationsservices, Sicherheitsvorfälle und deren Ausgangslage. Heraus kam, dass viele der untersuchten Angriffe lediglich von einem Netzwerksegment ausgingen.

Von dort aus breitete sich der Angriff im gesamten internen Netzwerk aus. Daher sollte Netzwerksegmentierung »grundlegender Bestandteil der Netzwerk- und Sicherheits-infrastruktur von Unternehmen« sein.

Dafür sollten die unterschiedlichen Funktionsbereiche der Umgebung im Netzwerk ausreichend definiert sein, der Datenfluss überwacht und die Netzwerksegmente regelmäßig überprüft werden.

Merksatz: Je mehr ein Netzwerk segmentiert wird, umso sicherer wird es.

Durch eine schlüssige Netzwerksegmentierung können sich Unternehmen vier grundlegende Vorteile zunutze machen:

- ✔ **Erkennungs- und Abwehrmechanismen können verbessert werden**
- ✔ **Schadsoftware kann leichter identifiziert und in Schach gehalten werden**
- ✔ **Cyberangriffe können deutlich verlangsamt werden, weil sie schneller auffallen**
- ✔ **Gesetze und Richtlinien zum System- und Datenschutz können besser eingehalten werden**

3.3. Vier-Punkte-Plan

Allen Vorteilen zum Trotz: Eine Netzwerksegmentierung ist komplex und muss fachmännisch geplant und umgesetzt werden. Dennoch versuchen wir Ihnen hier einen groben Leitfaden an die Hand zu geben – quasi ein Vier-Punkte-Plan, worauf Sie bei der Unterteilung Ihrer IT-Infrastruktur besonders Acht geben sollten.

1	**Identifizieren Sie die Segmente in Ihrem Unternehmen, die kritische Daten, Prozesse und Systeme enthalten.**
2	**Definieren Sie Sicherheitszonen zur effektiven Segmentierung kritischer Bereiche auf Grundlage der Datensensibilität und Zugriffsanforderungen.**
3	**Legen Sie in Ihrem Firmennetzwerk Zonen fest, die der Zugriffskontrolle unterliegen und zu denen nur Personen mit IT-administrativen Funktionen Zugang haben.**
4	**Überprüfen Sie kontinuierlich die Trennung der Segmente, damit die Sicherheitskontrollen und die Funktionsfähigkeit Ihrer IT-Infrastruktur gegeben bleibt – selbst bei Erweiterungen oder Änderungen.**

Wichtiger Hinweis: Netzwerksegmentierung ist nur ein Teil eines ganzheitlichen IT-Sicherheitskonzepts – wenn auch ein wichtiger.

Umfassende IT-Sicherheit kann die Unterteilung des Netzwerks in einzelne Segmente allein nicht leisten. Das erreichen Sie vielmehr durch das Zusammenspiel vieler Schutzmaßnahmen wie beispielsweise Firewall-Management, Antivirus-Management und Patch-Management.

3.4. Priorität versus Preis: Kosten kalkulieren

Netzwerksegmentierung hat sicherlich eine hohe Priorität, die jedoch auch Kosten verursacht. Schließlich geht es im weitesten Sinne um die Neugestaltung der gesamten Netzwerkarchitektur.

Das kann in der Phase der Umgestaltung die Funktionsfähigkeit der IT-Systeme zeitweise einschränken. Es besteht das Risiko finanzieller Ausfälle, da sich die Effizienz von Produktions- und Geschäftsabläufen zeitweise reduzieren kann. Daher sollten Sie nicht blind drauf los segmentieren: Stichwort »Über-Segmentierung«.

Kosten und Nutzen sind also abzuwägen. Es hilft, das gesamte Netzwerk so darzustellen, dass Daten und Geräte identifiziert werden, die eine unbedingte Segmentierung erfordern. Danach sollten Richtlinien als Grundlage für die weitere automatische Segmentierung von Geräten und Benutzern festgelegt werden. An dieser Stelle wären wir wieder bei der Netzwerkdokumentation, die diese Schritte erheblich vereinfacht und beschleunigt.

Kostenrisiko

Durch eine Netzwerksegmentierung nimmt meist auch die Menge des Datenverkehrs zu.

Diesen gilt es, auf Unregelmäßigkeiten zu prüfen. Das kann zusätzliche Investitionen in leistungsstärkere Systeme bedeuten.

4. Was Sie beachten sollten, bevor Sie einen Server kaufen

Server sind das Herzstück Ihrer IT-Infrastruktur. Sie liefern zuverlässig die notwendige Rechenleistung für Ihre Geschäfte und bündeln wichtige und sensible Daten. Kurz: Mit der Leistung eines Servers steht und fällt Ihr Geschäftserfolg. Die Anschaffung eines neuen Servers ist daher ein entscheidender, strategischer Faktor, um Ihre IT-Infrastruktur leistungsstark und widerstandsfähig aufzustellen.

Die 11 Fragen des folgenden Kriterienkatalogs können Sie bei der Server-Auswahl unterstützen. So behalten Sie den Durchblick beim tatsächlichen Server-Kauf und minimieren das Risiko von Fehlinvestitionen.

Server sind unersätzlich. Doch ob der Server nun in der eigenen Firma steht oder aber in der Cloud ist eine strategische Frage.

5. Mit 11 Kriterien zur zufriedenstellenden IT-Landschaft

1. Wofür wollen Sie den Server einsetzen? (Datensicherung, Webseitenperformance)
2. Gibt es »versteckte« Kosten für Wartung und Lizenzen?
3. Wie gestaltet sich das konkrete Preis-Leistungs-Verhältnis im Server-Vergleich?
4. In welchem Verhältnis stehen Anfangsinvestition und laufender Energieverbrauch?
5. Sind notwendige Betriebssysteme und Applikationen mit dem Server kompatibel?
6. Wer richtet den Server ein und betreut ihn künftig?
7. Wer kümmert sich um Sicherheit, Backup, Virenschutz und Zugriffskontrollen?
8. Ist der Server für den zeitgleichen Nutzerzugriff ausreichend dimensioniert?
9. Sind Speicherplatz und Geschwindigkeit aktuellen und künftigen Anforderungen gewachsen?
10. Ist der neue Server kompatibel und lässt er sich problemlos in Ihre vorhandene IT-Infrastruktur eingliedern?
11. Bieten sich Server-Miet-Modelle oder die Server-Migration in die Cloud als preiswertere, flexiblere und sinnvollere Alternativen zum Serverkauf an?

Wichtiger Hinweis: Dieser Kriterienkatalog ist keinesfalls ein vollständiger Ratgeber zur Auswahl der richtigen Server-Infrastruktur. Er bietet lediglich einige Anhaltspunkte. Insbesondere bei der Inbetriebnahme und Einrichtung sollte unbedingt IT-Fachwissen vorhanden sein.

neustifter.systems

Impressum

neustifter.systems
An der Reitbahn 12 | 93073 Neutraubling
Telefon: +49 9401 5395820
kontakt@neustifter.systems
https://neustifter.systems