autolinguale it

Netzwerkaufnahme leicht gemacht

Wie eine Kommunikationsmatrix erstellt werden kann,
um ein Netzwerk neu zu gestalten und abzusichern.

Schritte

- Definition und Eingrenzung des aufzunehmenden Netzwerkbereichs
- IT und Automation ansprechen
- Dokumente und Schaubilder zum Stand des Netzwerks
- Messungen des Datenverkehrs
- Auswertung der Daten zur Absicherung des Netzwerks

HWI
wir integrieren IT

HWI hat es sich mit der autolingualen IT zur Aufgabe gemacht, Industrie-Netzwerke für die Produktion mit einem standardisierten Verfahren zu analysieren, auszumessen und eine Visualisierung der Kommunikationsbeziehungen zur Grundlage für ein Netzwerkdesign zu erstellen. Hier findet sich eine Übersicht, welche Vorgehensweisen möglich sind.

1 Organisation

Was soll aufgenommen werden?

Bei jeder Netzwerkaufnahme sollte man sich initial die Frage stellen, was denn eigentlich konkret aufgenommen werden soll. Hierbei geht es allerdings nicht nur um die Definition der aufzunehmenden Parameter (wie bspw. IP-Subnetze, VLAN-IDs, Switch-Hersteller, etc.), sondern vor allem auch um die Eingrenzung des Bereichs der aufgenommen werden soll. Um diese Eingrenzung vornehmen zu können, muss wiederum klar sein, wofür die Aufnahme erfolgen soll. Soll beispielsweise ein Netzwerk aufgenommen werden, um eine neue Anlage ans Netz zu bringen, interessieren Komponenten wie Datacenter-Switches kaum.
Die aktuelle Anbindung der Netzwerkinfrastruktur an die Firewall-Systeme wird hingegen besonders wichtig sein, da Anlagennetze so sicher wie möglich aufgebaut werden sollten. Bei der Anbindung von Serversystemen dürften jedoch die Switches im Access-Bereich eher uninteressant sein. Die Datacenter-Switches allerdings sind hierfür elementar.
Kurzum: Vor der Aufnahme sollten das Ziel und der daraus resultierende, aufzunehmende Bereich klar definiert sein.

Mit wem muss ich sprechen?

Um einen sauberen Informationsfluss, bzw. einen reibungslosen Ablauf bei der Aufnahme gewährleisten zu können, ist es wichtig zu wissen, wer für was zuständig ist. Besonders bei der Netzwerkaufnahme von Anlagen gibt es meist mindestens zwei Ansprechpartner – IT und Produktion.
Auch wenn durch die Aufnahme das Netzwerk nicht beeinflusst wird, sollten beide Parteien von Anfang an über die Vorgehensweise informiert werden. Dies schafft nicht nur „ein gutes Gefühl“, sondern bietet meist auch die Möglichkeit alle Beteiligten an einen Tisch zu bekommen.

Fazit

Aus diesen beiden Punkten resultieren im Bestfall bereits Dokumente wie Schaubilder zum aktuellen Stand des Netzwerks, Komponentenlisten, IP-Adress-Übersichten, etc.

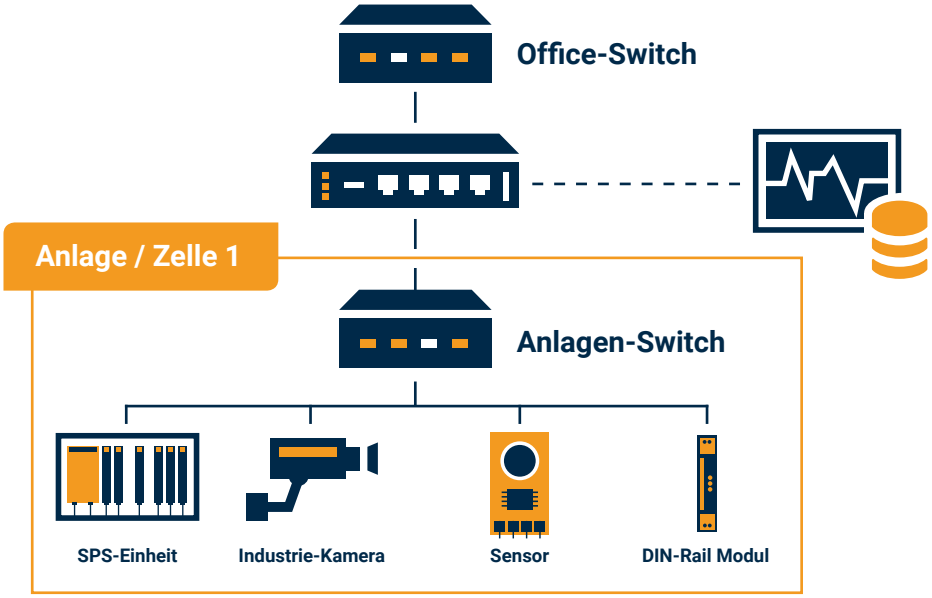
2 Technik

Organisation ist das halbe Leben – doch was nun?

Existieren keine Dokumente oder sollten tiefere Einblicke ins Netzwerk notwendig sein, können Messungen des Datenverkehrs Abhilfe schaffen.
Diese können auf verschiedene Arten durchgeführt werden. In jedem Fall wird jedoch eine Komponente benötigt, welche zum einen Datenverkehr mitschneiden und zum anderen den mitgeschnittenen Datenverkehr aufzeichnen kann. Das kann in Form von Hardware oder Software passieren. Welcher Weg hier gewählt wird, hängt sehr stark davon ab, ob die zu messende Infrastruktur kurzzeitig unterbrochen werden kann oder nicht, wie es bei den meisten Produktionsanlagen der Fall ist.

Messungen mit kurzzeitiger Unterbrechung des Datenverkehrs

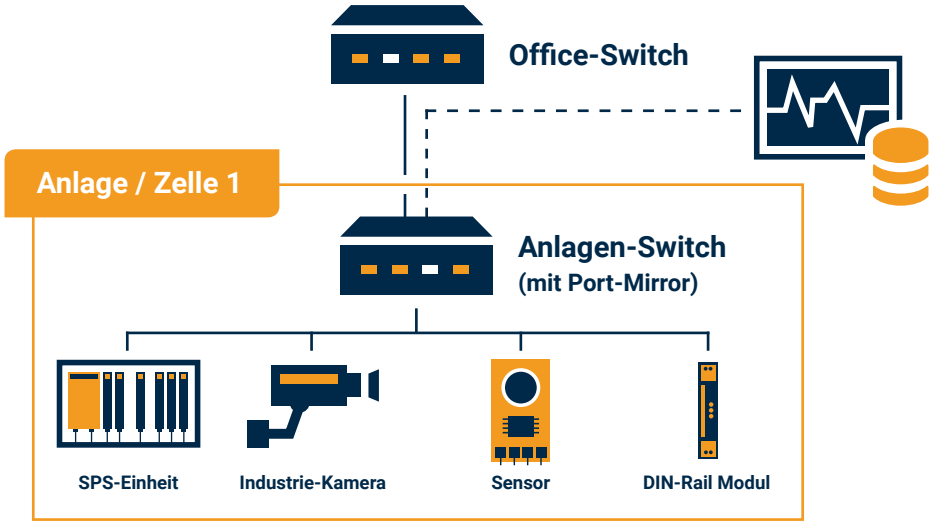
Besteht die Möglichkeit den Datenverkehr kurzzeitig auszusetzen, kann eine Messung mit Unterstützung von sogenannten Network TAPs erfolgen. Diese werden an einer passenden Stelle im Netzwerk, bspw. der Schnittstelle zwischen Anlagen-Switch und Office-Switch, eingebunden und spiegeln den gesamten Datenverkehr auf einen gesonderten Port, an welchem noch ein Datensammler (bspw. in Form eines Notebooks mit Wireshark oder Ähnlichem) angeschlossen ist.



Vorteil hierbei ist, dass die bestehenden Komponenten nicht beeinflusst werden und keine zusätzliche Last tragen müssen. Weiterhin werden auch fehlerhafte Pakete gespiegelt, wodurch der Datenverkehr bis ins kleinste Detail nachvollzogen werden kann

Messungen ohne Unterbrechung des Datenverkehrs

Soll eine Messung ohne Unterbrechung des Datenverkehrs durchgeführt werden, gibt es die Möglichkeit sogenannte „Mirror-Ports“ zu verwenden. Für die Verwendung von Mirror-Ports, wird lediglich ein Datensammler benötigt. Weiterhin muss einer der vorhandenen Switches über die Funktion „Port-Mirroring“ verfügen. Hierbei übernimmt der Switch die Funktion des Network TAPs und leitet alle Pakete über einen gesondert konfigurierten „Mirror-Port“ an den Datensammler.



Großer Vorteil hierbei ist die flexible und vor allem unterbrechungsfreie Anbindungsmöglichkeit. Da die meisten gängigen Switches die Funktion „Port-Mirroring“ auch unterstützen, ist diese Variante oftmals die präferierte.

Fazit

Egal, über welchen Weg die Daten gesammelt werden, im Nachgang gilt es, diese Daten auszuwerten. Hieraus resultiert dann eine Kommunikationsmatrix, welche aufzeigen soll, wer mit wem über welches Protokoll spricht.
Schlussendlich hat man auf diesem Wege alle benötigten Informationen gesammelt um ein klares Bild des Netzwerkes vor Augen zu haben. Dies ist die Grundlage für etwaige konzeptionelle Änderungen und die Absicherung von Netzwerken.