EHEALTHCOM
Magazin für Health-IT, vernetzte Medizintechnik und Telemedizin

Broadcast-Sturm in Med. IT-Netzwerken-Teil 1: Patientengefährdung

Expertenbeitrag von Armin Gärtner und Mahmoud El-Madani

Der vorliegende Beitrag zeigt anhand eines anonymisierten Vorkommnisses auf, welche Gefährdungen durch einen sogenannten Broadcaststurm in einem proprietären IT-Netzwerk einer Patientenüberwachungsanlage entstehen können. Der Broadcaststurm verhinderte nicht nur den Datentransfer zwischen den bettseitigen Überwachungsmonitoren und Zentrale sondern führte auch dazu, dass die angeschlossenen bettseitigen Überwachungsmonitore die elektronische Überwachung der Patienten einstellten.

Patientenüberwachung mit Netzwerken

Eine elektronische Patientenüberwachung erfolgt üblicherweise mit bettseitigen Überwachungsmonitoren (Monitore). Diese befinden sich in einem medizinischen IT-Netzwerk und sind mittels eines LAN-Switches (Netzwerk-Switch) mit einer Überwachungszentrale (Zentrale) am Pflegestützpunkt verbunden.

Ein solches medizinisches IT-Netzwerk arbeitet IP-basiert. Dieses bedeutet wiederum, dass sowohl den bettseitigen Überwachungsmonitoren als auch der Überwachungszentrale jeweils eine IP-Adresse (Netzwerkadresse auf OSI Schicht 3 / Layer 3) zugewiesen ist. Die fest zugewiesene IP-Adresse bildet die Basis für die Kommunikation der Geräte in diesem medizinischen IT-Netzwerk. Die Kommunikation zwischen den bettseitigen Monitoren und der Zentrale erfolgt über den LAN-Switch (Netzwerk-Switch).

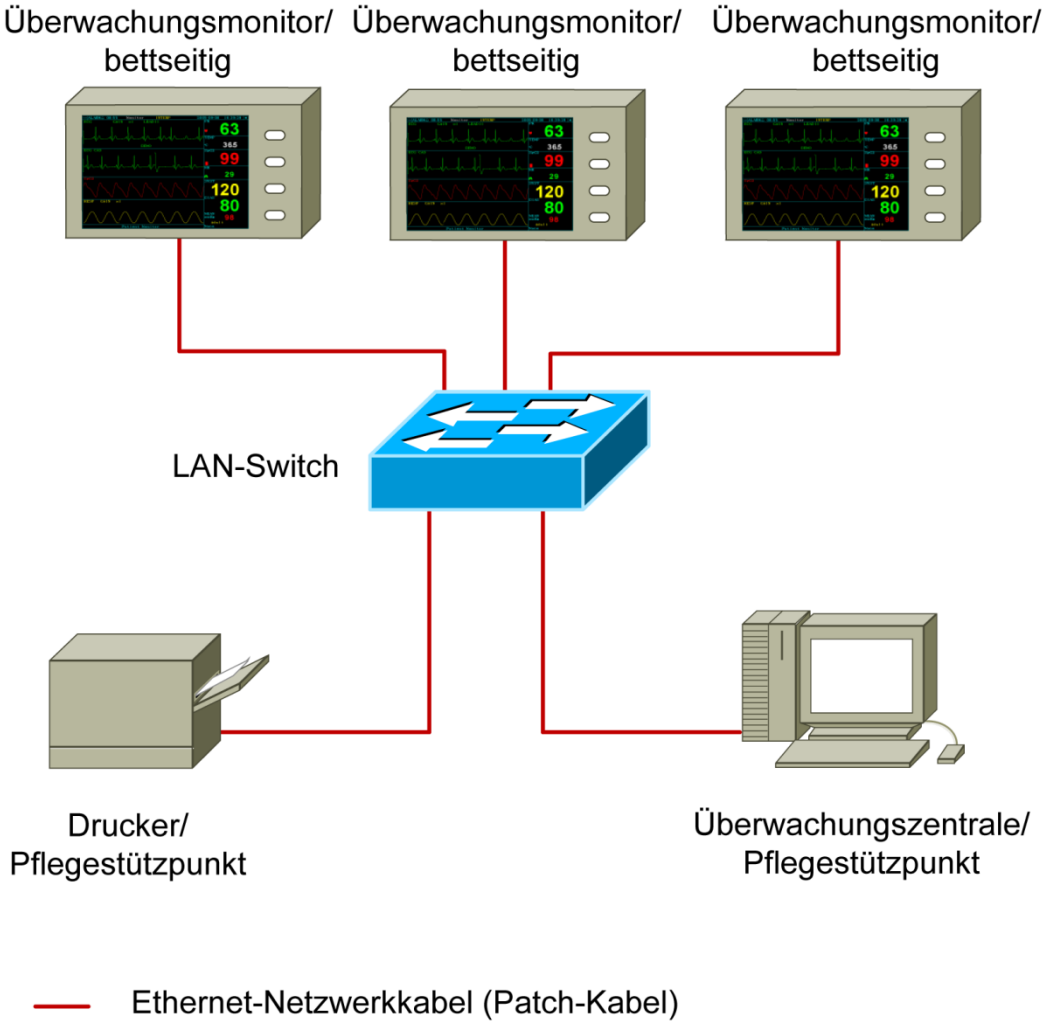

Abbildung 1: Medizinisches IT-Netzwerk für die Patientenüberwachung

Die Komponenten bestehen z. B. aus bettseitigen Monitoren, einer Zentrale und ggf. einem Drucker, zwischen denen eine permanente Kommunikation in Form des Austausches von Datenpaketen stattfindet. Die Kommunikation gliedert sich in drei Typen, die als Unicast, Multicast und Broadcast bezeichnet werden. Diese werden nachfolgend vorgestellt und ihre Funktion im Netzwerk einer Patientenüberwachungsanlage (als VLAN 100 bezeichnet) erläutert.

Unicast
In der Netzwerktechnik dient der Unicast für die Übertragung von Datenpaketen zwischen einem Absender und einem einzigen Empfänger. Die Unicast Kommunikation findet sich auf der OSI Schicht 2 (Layer 2) und OSI Schicht 3 (Layer 3) wieder.

Multicast
Der Multicast wird zur Übertragung von Datenpaketen von einem Absender an eine bestimmte Empfängergruppe wie die Überwachungsmonitore in der Abbildung 1

verwendet. Eine Multicast Kommunikation findet sowohl auf der OSI Schicht 2 (Layer 2) und OSI Schicht 3 (Layer 3) statt.

Broadcast

Der Broadcast kann in einem LAN bzw. VLAN unterschiedliche Funktionen abbilden. So dient er als „Rundruf “ oder „allgemeine Anfrage“, welche von einem Endgerät an alle anderen Endgeräten in einem LAN gesendet wird, um unbekannte IP Adressen eines anderen Endgeräts oder Netzwerkdienste in einem LAN zu finden. Ebenso kann der Broadcast zur Verteilung von Daten und Informationen, wie etwa der Uhrzeit, in einem LAN bzw. VLAN dienen. Eine Broadcast Kommunikation findet sowohl auf der OSI Schicht 2 (Layer 2) und OSI Schicht 3 (Layer 3) statt.

Was bedeutet nun ein sogenannter Broadcast-Sturm?

Ein sogenannter Broadcast-Sturm ist ein Netzwerkphänomen, das nur auf der OSI Schicht 2 (Layer 2) in Netzwerken entsteht, welche die Ethernet-Technologie als Grundlage für Kommunikation im Netzwerk verwenden.

Im nachfolgenden einfachen Beispiel (siehe Abbildung 2) soll erläutert, werden wie ein Broadcast-Sturm entsteht. Ausgangssituation ist ein sehr vereinfachter Aufbau einer Patientenüberwachungsanlage. Diese besteht aus einem bettseitigen Überwachungsmonitor (angeschlossen an Port 7 und der MAC-Adresse 22:22:22:22:22:22), einer Zentrale (angeschlossen an Port 6 und der MAC-Adresse 11:11:11:11:11:11) und einem LAN-Switch, welcher als Verbindungsknoten zwischen dem Überwachungsmonitor und der Zentrale fungiert.

Zur Veranschaulichung des Broadcast-Sturms wurde am LAN-Switch der Port 1 und der Port 3 direkt mit einem Netzwerkkabel (Patch-Kabel) verbunden und somit eine Netzwerkschleife (Loop) realisiert. Die Netzwerkschleife (Loop) bildet die Grundlage für einen Broadcast-Sturm.

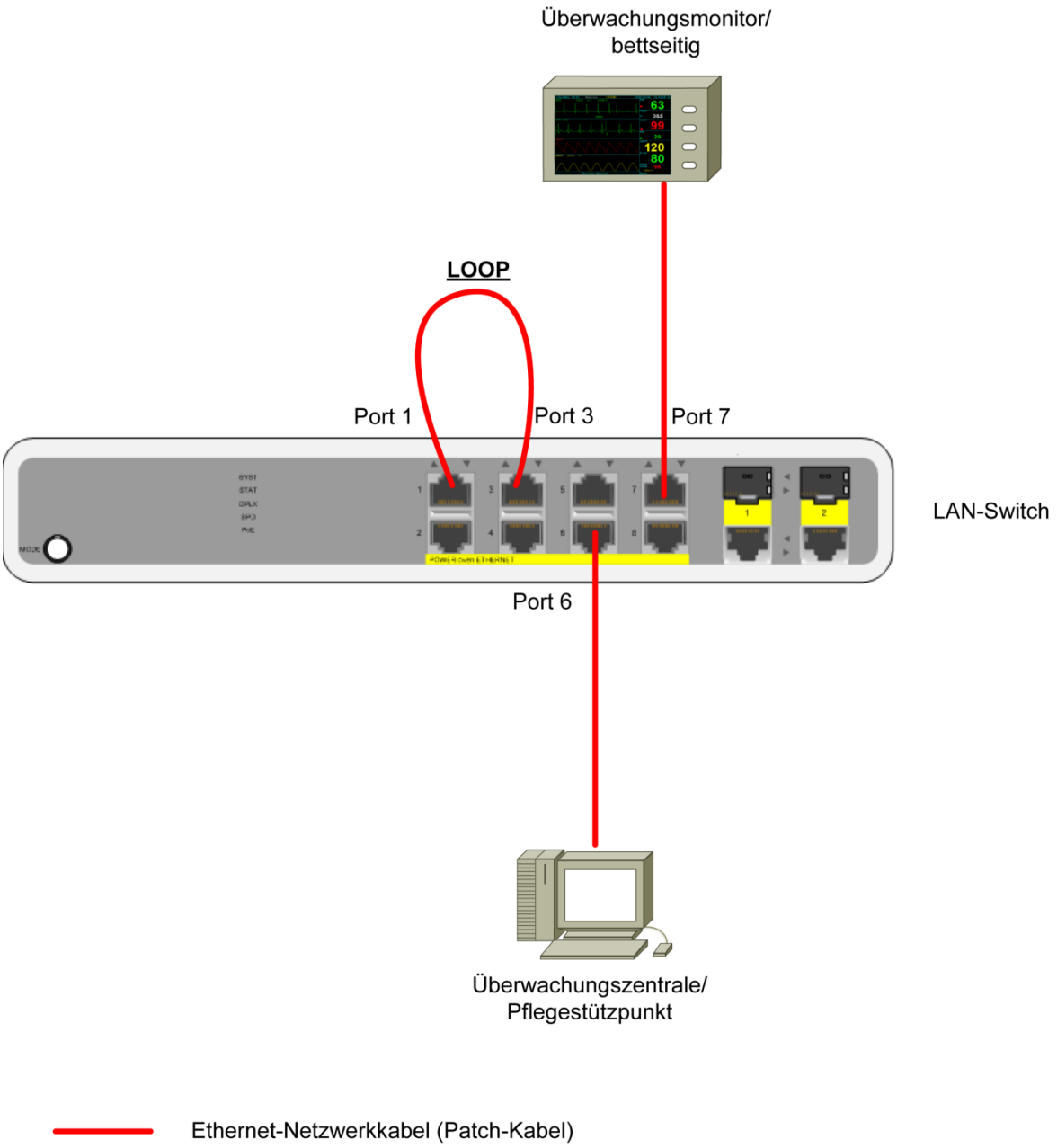

Abbildung 2: Aufbau einer Netzwerkschleife für einen Broadcast-Sturm

Grundsätzlich müssen alle Endgeräte, die sich in ein und demselben LAN-Segment befinden und kommunizieren möchten, Kenntnis über alle MAC-Adressen und IP-Adressen haben, welche sich in diesem LAN-Segment befinden. Damit sie diese Kenntnis erlangen, wird eine Adressabfrage mit dem Address Resolution Protocol (ARP – RFC 826) durchgeführt. Diese ARP-Abfrage wird mit einem Broadcast „Rundruf“ realisiert.

Im Beispiel sendet die Zentrale eine ARP-Abfrage, um die MAC- und IP-Adresse des Überwachungsmonitors zu erfragen (Abbildung 3). Da es sich bei dieser ARP-Abfrage um einen Broadcast handelt, wird als Empfänger-MAC-Adresse die

Broadcast-Adresse FF:FF:FF:FF:FF:FF und als Absender-MAC-Adresse die 11:11:11:11:11:11 verwendet.

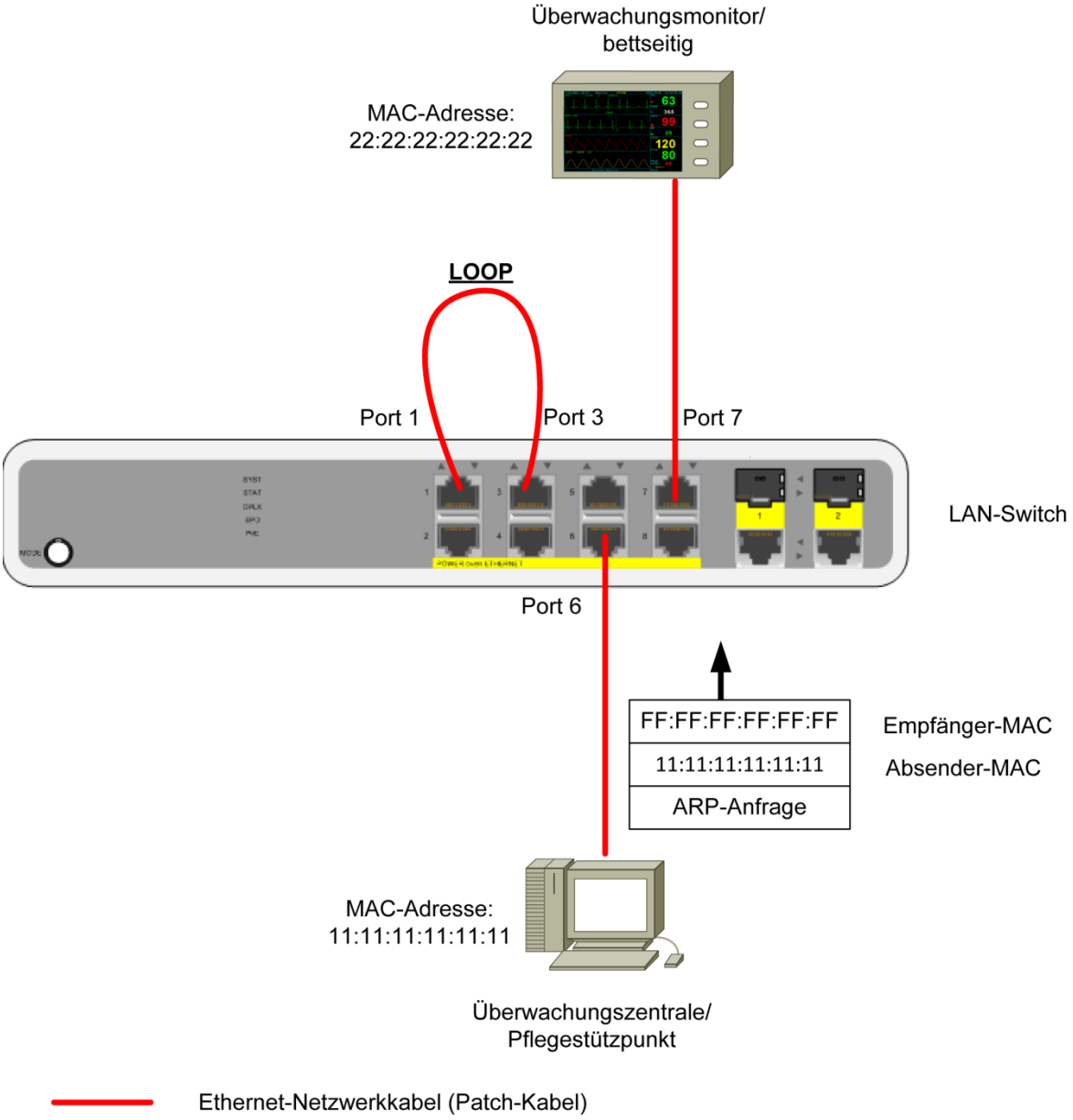

Abbildung 3: Versand der ARP-Anfrage mit Broadcast

Der Broadcast wird alle Ports (Port 1, 3, 7) des LAN-Switches gesendet und weitergeleitet (Abbildung 4).

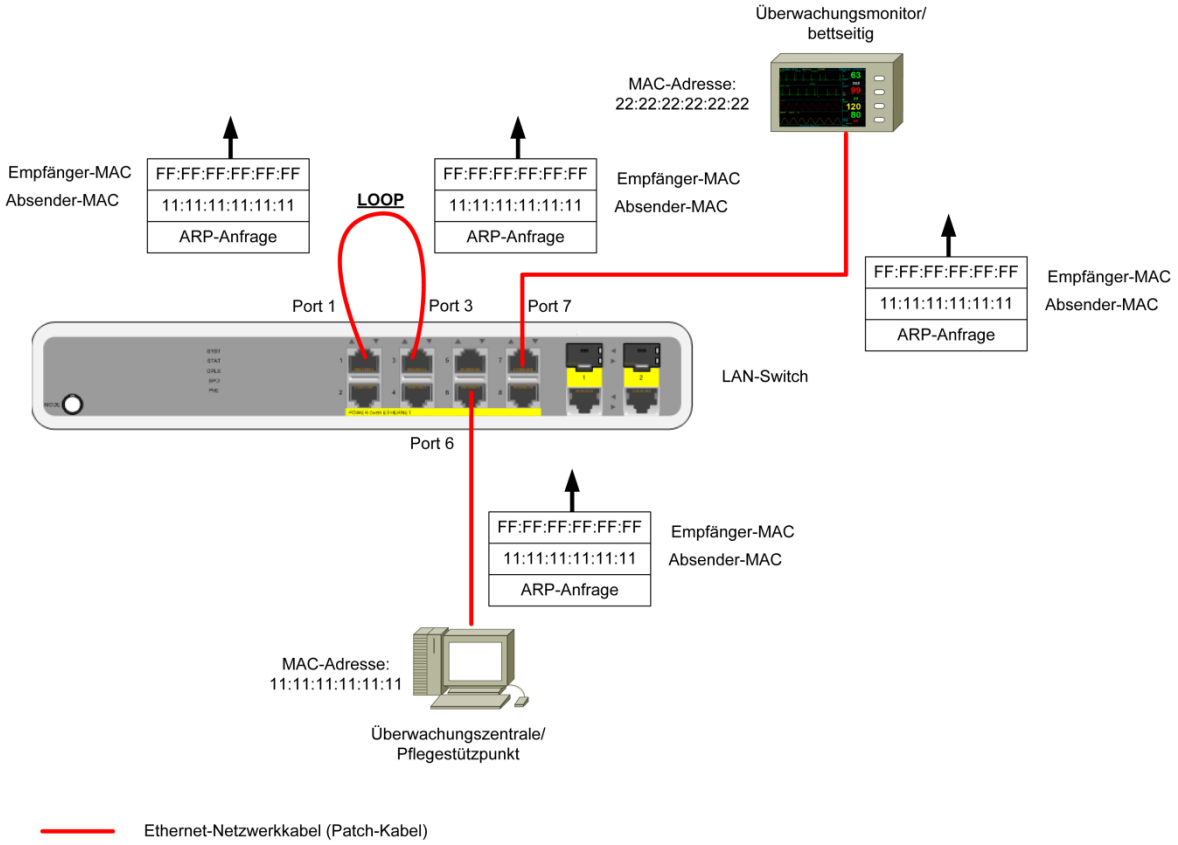

Abbildung 4: Verbreitung des Broadcast im Netzwerk

Da es in der Ethernet-Technik keine Erkennungsmöglichkeit für Netzwerkschleifen (Loops) gibt, wandert der Broadcast ungehindert über die verbundenen Ports 1 und Port 3 wieder zurück zum LAN-Switch. Der LAN-Switch erkennt den Broadcast und leitet diesen wieder an alle Ports weiter (Abbildung 5). Dieses permanente Weiterleiten von Broadcasts schaukelt sich innerhalb von wenigen Sekunden dermaßen auf, dass Unicast- bzw. Multicast-Datenverkehr zwischen dem Überwachungsmonitor und der Zentrale nicht mehr möglich wird.

Es kann auch nicht ausgeschlossen werden, dass der LAN-Switch aufgrund des Broadcast-Sturms Datenpakete verwirft.

Ein Broadcast-Sturm hat zur Auswirkung, dass kein normaler Datenaustausch mehr stattfindet, Alarme und Vitaldaten eines Patienten nicht an die Zentrale übertragen werden können und somit eine akute Gefährdungssituation für Patienten besteht.

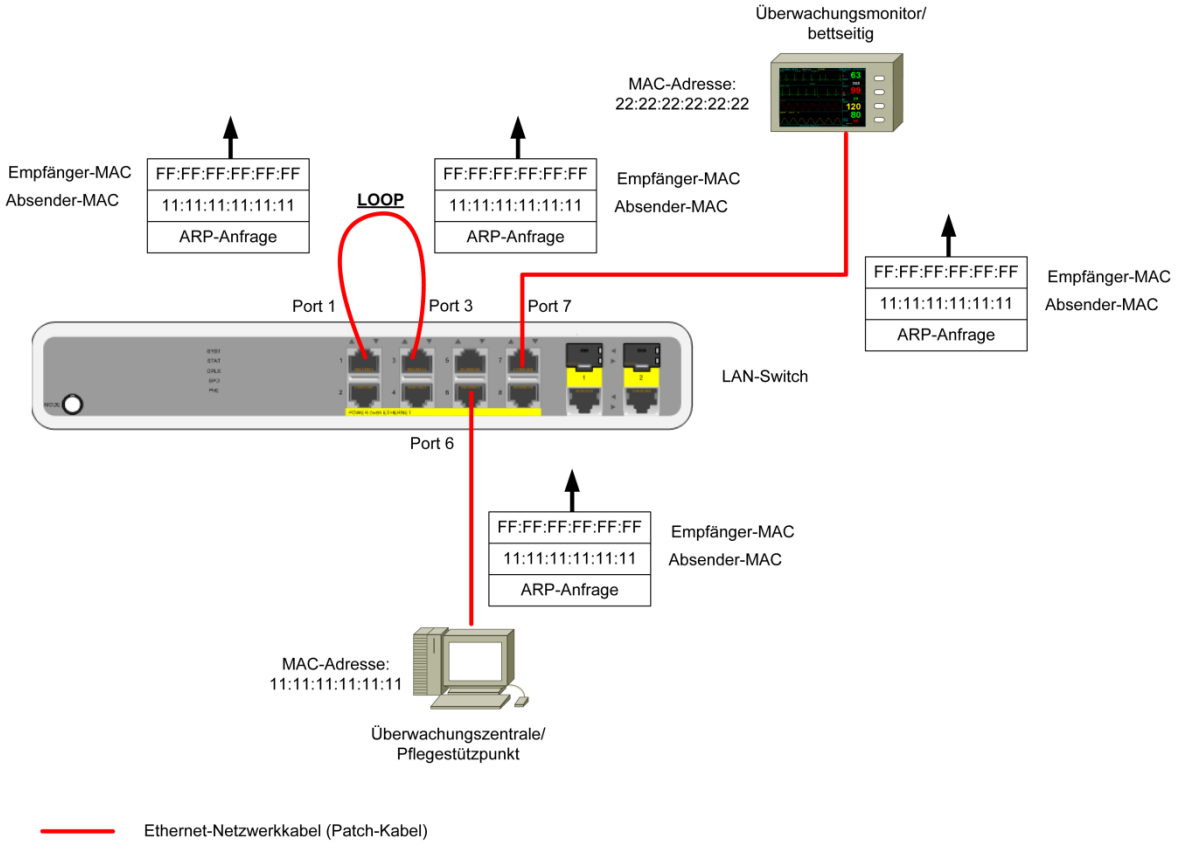

Abbildung 5: Entstehung des Broadcast-Sturms

Der Broadcast-Sturm kann nur durch die manuelle Entfernung der Netzwerkschleife (Loop) beendet werden, indem man das Netzwerkkabel absteckt oder indem man erweiterte Funktionen am LAN-Switch wie etwas Storm-Control einsetzt. (Abbildung 6)

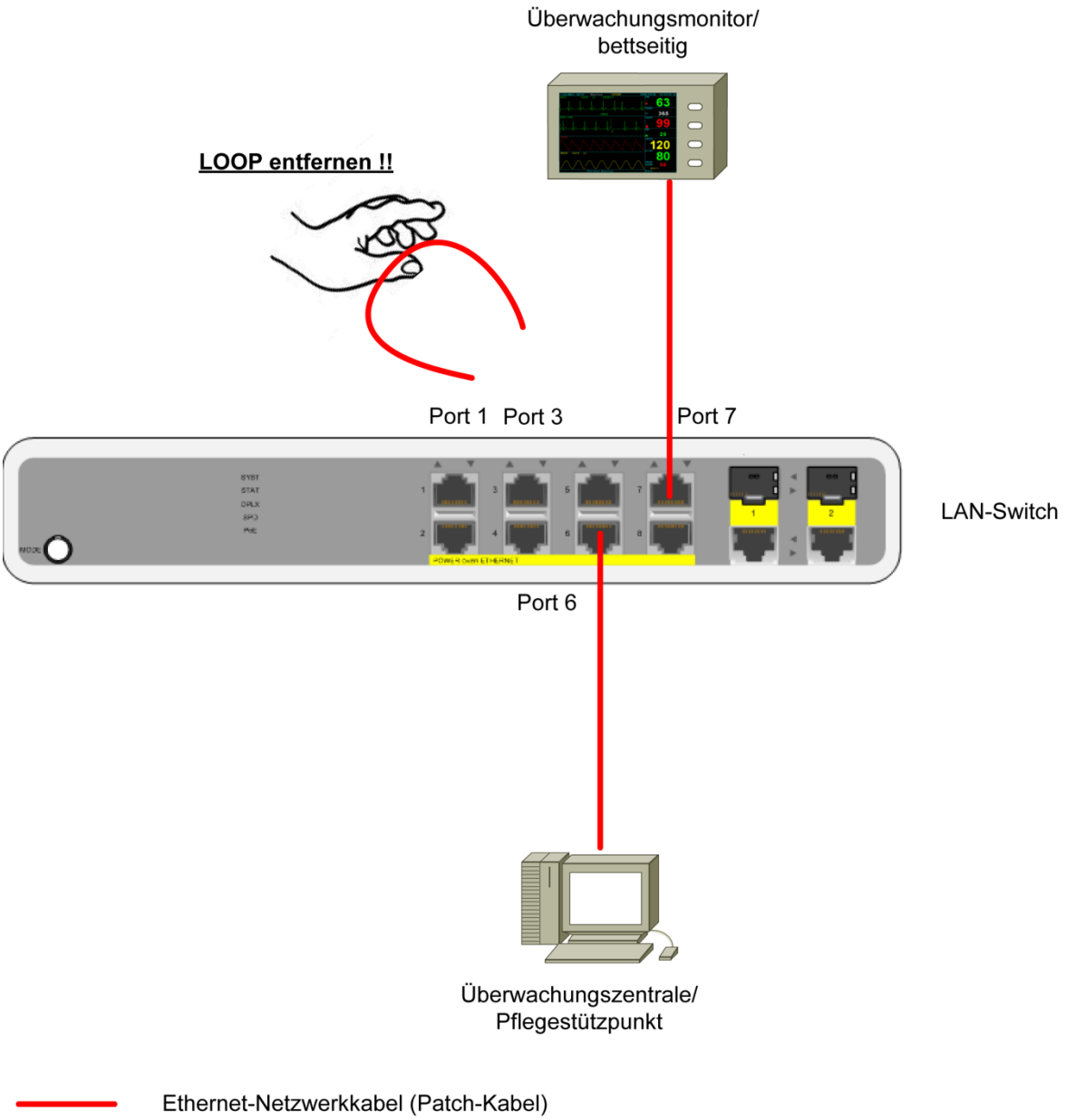

Abbildung 6: Manuelle Entfernung der Netzwerkschleife (Loop)

Mögliche Ursachen eines sogenannten Broadcast-Sturm

Ein sogenannter Broadcast-Sturm ist ein Netzwerkphänomen, das nur in der OSI Schicht 2 (Layer 2) in Netzwerken entsteht welche die Ethernet-Technologie als Grundlage für Kommunikation im Netzwerk verwendet. Durch diverse Fehlerquellen, welche im Folgenden ohne Vollzähligkeit beschrieben werden, kann es in einem Ethernet-basierenden Netzwerk zu einem Broadcast-Sturm kommen:

- Er entsteht durch eine schadhafte Netzwerkkarte eines Endgerätes oder LAN Switches.
- Fehlerhaftes Betriebssystem eines LAN Switches

- Unkenntnis über das Kommunikationsverhalten zwischen den Systemkomponenten. Hier muss eindeutig erkennbar sein, welche Art der Kommunikation (Unicast, Multicast, Broadcast) zwischen den System-komponenten verwendet wird.
- Deaktiviertes Spanning-Tree-Protokoll (STP IEEE 802.1w, IEEE 802.1s) im Netzwerk
- Einsatz von Netzwerk Hubs anstelle von LAN Switches.
- Versehentliches Stecken einer Schleife (Loop).

Diese Ursachen können zur Folge haben, dass LAN-Switche alle Ethernet-Rahmen über alle ihre physischen Ports an alle anderen LAN-Switches im Netzwerk weiterleiten. Der dadurch entstehende Dominoeffekt setzt sich solange fort, bis alle LAN-Switches ausschließlich mit dem Weiterleiten von Broadcast beschäftigt sind, wodurch es zu einer Blockade im Netzwerk kommt. Diese Blockade äußert sich in Form eines sogenannten Broadcast-Sturms, weil es zu einer Überflutung mit Datenpaketen kommt und ein zielgerichteter Datentransfer nicht mehr möglich ist.

Tritt so ein Broadcast-Sturm ein, führt dieser zur Überlastung des LAN-Switches und folglich zum totalen Stillstand aller Kommunikationsverbindungen. Alle bestehenden Kommunikationsverbindungen werden unterbrochen und neue können nicht aufgebaut werden.

Maßnahmen gegen einen Broadcast-Sturm

Ein Broadcaststurm in einem Med. IT-Netzwerk führt zu massiven Kommunikationsausfällen zwischen Medizinprodukten wie Patientenüberwachungsmonitoren. Es ist daher wichtig, nicht nur die möglichen Ursachen für einen Broadcast-Storm zu kennen sondern auch Präventionsmaßnahmen zu kennen und einzusetzen. Dabei kommen nachfolgende Maßnahmen bei der Planung von Patientenüberwachungsanlagen aber auch für bereits im Betrieb befindliche Anlagen in Frage:

- Segmentierung des LAN in VLANs (Virtual Local Area Network). Dadurch können die Broadcast-Domänen verkleinert werden.

- Das Spanning-Tree Protokoll (STP IEEE 802.1w, IEEE 802.1s) muss in einen LAN bzw. VLAN jedenfalls aktiviert sein. Unabhängig davon, ob nun eine redundante Netzwerkverbindung (Netzwerkverkabelung) besteht oder nicht.

  LAN-Switches, die kein Spanning-Tree Protokoll unterstützen, dürfen im Netzwerk nicht eingesetzt werden. Derartige LAN-Switches sind eigentlich Netzwerk-Hubs. Welche Funktionen und Protokolle wie z.B. Spanning-Tree

Protokoll ein LAN-Switch unterstützt, ist dem Datenblatt des LAN-Switches zu entnehmen.

- Vermeidung von Netzwerk-Hubs. Bei der Planung und Einrichtung von Medizinischen IT-Netzwerken muss darauf geachtet werden; dies gilt umso mehr, wenn für Medizinische IT-Netzwerke Netzwerkkomponenten eines Krankenhauses verwendet werden sollen. Netzwerk-Hubs dürfen auch nicht als Provisorium eingesetzt werden.

- Stichprobenartige Sichtüberprüfung der Netzwerkverkabelung bei Endnutzern, aber auch in Netzwerkverteilern und im Rechenzentrum. Zu achten ist z.B. auf:
  Wurde etwas verändert?
  Scheint ein Netzwerkkabel falsch angeschlossen zu sein?
  Wurde von Endnutzern oder einer externen Firma ein Netzwerk-Hub installiert?

- Kenntnisse über die im Netzwerk verwendeten Protokolle, ihre Funktionen und welche Kommunikationsart sie verwenden, d.h. werden Unicast, Multicast oder Broadcast verwendet.

- Kenntnisse über die Kommunikationsverbindungen im Normalbetrieb als auch im Fehlerfall, d.h. welche Komponenten kommunizieren untereinander? Welche Kommunikationsabhängigkeiten bestehen? Wie wird ein Fehlverhalten einer Komponente angezeigt? Wie leicht kann ein Fehler in der Kommunikationsverbindung erkannt und behoben werden?

- Nicht verwendete physische Ports deaktivieren. Alle Netzwerkanschlüsse und die damit verbundenen Netzwerkdosen, die nicht verwendet werden, müssen am LAN-Switch deaktiviert werden. Damit können ein versehentliches, falsches Anschließen von Netzwerkkabeln und daraus resultierende Netzwerkschleifen (Loop) leicht vermieden werden.

- Regelmäßige Netzwerk- und Datenverkehrsanalyse. Damit kann festgestellt werden, an welchem physischen Port eines LAN-Switches besonders viel

Broadcast Verkehrsaufkommen herrscht, bzw. woher ein Broadcast stammen könnte. Mit dieser Analyse können die „Top-Talker“ in einem Netzwerk festgestellt werden. Bei „Top-Talker“ handelt es sich um Endgeräte, z.B. die Zentrale einer Patientenüberwachungsanlage, die auffällig viel Datenverkehr versendet oder empfängt.

Unter Berücksichtigung der angeführten Maßnahmen kann im Rahmen der Planung für eine neue Patientenüberwachungsanlage bzw. bei einer bereits installierten Patientenüberwachungsanlage das Risikopotenzial eines Broadcast-Sturms und eines damit verbundenen Ausfalls bzw. einer Fehlfunktion vermieden werden.

Sachverhalt: Auftreten eines Broadcaststurms im proprietären Netzwerk einer Patientenüberwachungsanlage

Auf einer Überwachungsstation in einem Krankenhaus fielen unerwartet sämtliche bettseitigen, vernetzten Überwachungsmonitore inklusive der Überwachungszentrale aus. Dabei zeigten die Bildschirme der mobil als auch stationär einsetzbaren Überwachungsmonitore und der Überwachungszentrale nur noch ein schwarzes Bild an und stellten die Überwachung und Anzeige der Vitalparameter der angeschlossenen Patienten ein. Dadurch kam es über einige Stunden zu einer kritischen Situation für die zu überwachenden Patienten, weil eine elektronische Überwachung der Patienten auf Grund dieses Ausfalls nicht mehr möglich war und die Anzahl der Pflegekräfte für eine direkte personelle Überwachung zu gering war.

Erst die physikalische Trennung der einzelnen Überwachungsmonitore vom IT-Netzwerk führte dazu, dass die eingeschalteten Überwachungsmonitore automatisch neu starteten, im Stand-Alone Betrieb (ohne Netzwerkverbindung) wieder bestimmungsgemäß die angeschlossenen Patienten überwachten und somit ordnungsgemäß die entsprechenden Vitalparameterkurven und –zahlen anzeigten.

Der Versuch, die vorher vom Netzwerk getrennten Überwachungsmonitore wieder an das (weiterhin überlastete) IT-Netzwerk anzuschließen, führte dazu, dass nach Anschluss die Geräte wieder ihre Überwachung einstellten und erneut einen schwarzes Bild anzeigten.
Die Wiederherstellung der vollständigen Funktionalität des IT-Netzwerkes der Patientenüberwachungsanlage, d. h. die Überwachung der Vitalparameter der angeschlossenen Patienten und Darstellung auf der Überwachungszentrale, gelang den Mitarbeitern der Medizintechnik und der IT in Absprache mit dem Hersteller der Patientenüberwachungsanlage erst nach ca. drei Stunden. Dazu mussten alle bettseitigen Überwachungsmonitore, die Überwachungszentrale sowie der LAN-Switch nach Rücksprache mit dem Hersteller ausgeschaltet und neu gestartet werden.

Nachdem die Patientenüberwachung wieder hergestellt war und korrekt funktionierte, wurde der Hersteller der Patientenüberwachungsanlage beauftragt, die Anlage zu überprüfen. Bei dieser Überprüfung konnte das Ereignis reproduziert werden. Als Ursache des Ausfalls wurde zunächst ein Broadcaststurm im IT-Netzwerk der Patientenüberwachungsanlage diagnostiziert, durch den die bettseitigen Überwachungsmonitore und die Überwachungszentrale ihre Funktion vollständig einstellten. Durch die Reproduktion des Ereignisses wurde gezeigt, dass der Broadcaststurm an der Kommunikationsschnittstelle die Hauptfunktion der bettseitigen Überwachungsmonitore blockiert hatte.

Analyse der Ursachen, Schlussfolgerungen und Konsequenzen

Die bettseitigen Patientenmonitore der Überwachungsstation waren sowohl für den stationären als auch für den mobilen Betrieb vorgesehen. Dies bedeutet, dass die Geräte regelmäßig von einem Bettplatz genommen werden, um sie im Bedarfsfall an anderen Überwachungsplätzen anzuschließen oder sie als mobile Überwachungsgeräte für Patiententransporte einzusetzen.
Dieser Wechsel zwischen mobiler und stationärer Verwendung der Überwachungsmonitore stellte sich als primäre Ursache für den Broadcaststurm heraus, weil auf der betreffenden Überwachungsstation ein Anwender eine herunterhängendes Netzwerkkabel (LAN-Anschlusskabel / Patch-Kabel) eines Überwachungsmonitors an einem Überwachungsplatz versehentlich in eine freie Netzwerkdose steckte.

Dieser Fehlbedienung lag eine hohe Arbeitsbelastung bzw. eine niedrige Personalausstattung zugrunde. Aufgrund der Arbeitsbelastung wurde es ferner versäumt, zu prüfen, ob das Netzwerkkabel korrekt in die Netzwerkdose eingesteckt wurde. Der Anwender, der das Kabel in die falsche Dose gesteckt hatte, erkannte auf Grund des Arbeitsdrucks auch nicht, dass er auf diese Weise eine Netzwerkschleife (Loop) geschaltet hatte, durch die sich dann letzten Endes ein „Broadcaststurm“ entwickelte.

Ein weiteres Ergebnis der Ursachenanalyse ergab, dass keine zusammenfassende Dokumentation der Beschaffung, Installation, Einrichtung und Abnahme der Patientenmonitoranlage in Form einer Technischen Dokumentation vorlag. Auch war kein Risikomanagement durchgeführt worden.

Ergebnisse und Schlussfolgerungen

Die Analyse des Zwischenfalls kommt zu folgenden Ergebnissen und läßt nachfolgende Schlussfolgerungen zu, warum es zu dem geschilderten Broadcaststurm mit Patientengefährdung gekommen war.

- Der Broadcaststurm hat über die Kommunikationsschnittstelle die Hauptfunktion der bettseitigen Überwachungsmonitore blockiert.

- Im IT-Netzwerk der Patientenüberwachungsanlage wurde auf Betreiben der Krankenhaus IT-Abteilung ein LAN-Switch beschafft und verwendet. Die Anforderungen des Herstellers der Patientenüberwachungsanlage an einen LAN-Switch und seine dafür erforderlichen netzwerktechnischen Funktionen wurden nicht validiert, sodass Protokolle und Überwachungsfunktionen, die einen Broadcaststurm verhindern können, nicht aktiviert waren.
- Es fehlte ein Projektmanagement und eine Technische Dokumentation über die Konzeption, Beschaffung und Installation sowie Abnahme der Patientenüberwachungsanlage.
- Eine Zusammenarbeit zwischen der Medizintechnik und IT-Abteilung für eine schnelle Behebung derartiger Ausfälle war nicht gegeben. Durch die fehlende Zusammenarbeit kam es zu einer zusätzlichen, erheblich verzögerten Bearbeitung des Ausfalls der Patientenüberwachungsanlage, die bei einer engen Zusammenarbeit nicht entstanden wäre.
- Die Medizintechniker des Krankenhauses verfügten über keine IT-Kenntnisse und konnten somit die Situation erst mit erheblicher Verzögerung durch einen Service-Mitarbeiter des Herstellers der Patientenüberwachungsanlage beenden. (Kenntnisse der Netzwerktechnik und des Datenaustausches über ein IT-Netzwerk sind insbesondere für die Medizintechnik-Abteilungen der Krankenhäuser immer wichtiger, um zu verstehen, welche IT-bedingten Gefährdungen auftreten können und wie man daraus resultierende Risiken möglichst vermeiden kann)
- Die Sorge der krankenhauseigenen IT-Abteilung vor „Haftungsproblemen“ beim Umgang mit Medizinprodukten führte dazu, dass es zu einer weiteren Verzögerung bei der Ursachenanalyse und der Behebung des Ausfalls der Überwachungsanlage kam.
- Es lag keine Risikomanagementakte in Form einer Dokumentation vor, die z. B. die erforderliche Personalausstattung der Station und erforderlicher Maßnahmen bei einem längerfristigen Ausfall der Patientenüberwachungsanlage betrachtete.
- Es gab auch keine Definition von Eskalationsprozessen für den Fall der längerfristigen Störung bzw. des Ausfalls der Überwachungsanlage über einen Zeitraum von mehr als nur Minuten.

Empfehlungen

Das vorstehend geschilderte, anonymisierte Beispiel ist kein Einzelfall, sondern bereits mehrfach in Krankenhäusern vorgekommen. Dieses Beispiel steht daher exemplarisch für IT-bedingte Gefährdungen, die ein systematisches Risikomanagement [1] soweit wie möglich verhindert soll.
Für ein solches Risikomanagement können die Normen DIN EN 80001-1, die Technical Reports der Reihe IEC /TR 80001-2-X [3] sowie die Norm DIN EN ISO 14971 [4] verwendet werden.

Literatur und Quellenangaben

1. Gärtner, A.; Verteilte Alarmsysteme, TÜV Media GmbH Köln, 2016, ISBN 978-3-8249-1990-1
2. DIN EN 80001-1:2011-11; VDE 0756-1:2011-11 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten
3. IEC TR 80001-2-5:2016 Anwendung des Risikomanagements für IT Netzwerke, die Medizinprodukte beinhalten - Teil 2-5: Anleitung für verteilte Alarmsystems
4. DIN EN ISO 14971:2013-04 Medizinprodukte - Anwendung des Risikomanagements auf Medizinprodukte

Diese Publikation ist ein Auszug aus dem gleichnamigen Beitrag des Fortsetzungswerkes Medizintechnik und Informationstechnologie digital -
MIT - Konzepte, Technologien, Anforderungen - TÜV Media GmbH, Köln
Die vollständige Fassung erscheint in der 22 Ergänzungslieferung des Fortsetzungswerkes im Dezember 2016.

Autoren

Armin Gärtner
Ingenieurbüro für Medizintechnik
Ö. b. u. v. Sachverständiger für Medizintechnik
Edith-Stein-Weg 8
40699 Erkrath
Tel.: 49 (0) 2104-8333706
E-Mail: armin.gaertner@t-online.de

Mahmoud El-Madani
Vertex Activity e.U.
Allgemein beeidigter u. gerichtlich zertifizierter Sachverständiger
+43 680 315 73 23
TÜV Zertifizierter Risikomanager f. medizinische IT-Netzwerke
maelmadani@vertex-activity.com
TÜV Zertifizierter ISMS ISO 27001 Auditor
https://www.vertex-activity.com
A-1150 Wien Henriettenplatz 3/1/16

Stand 08.11.2016