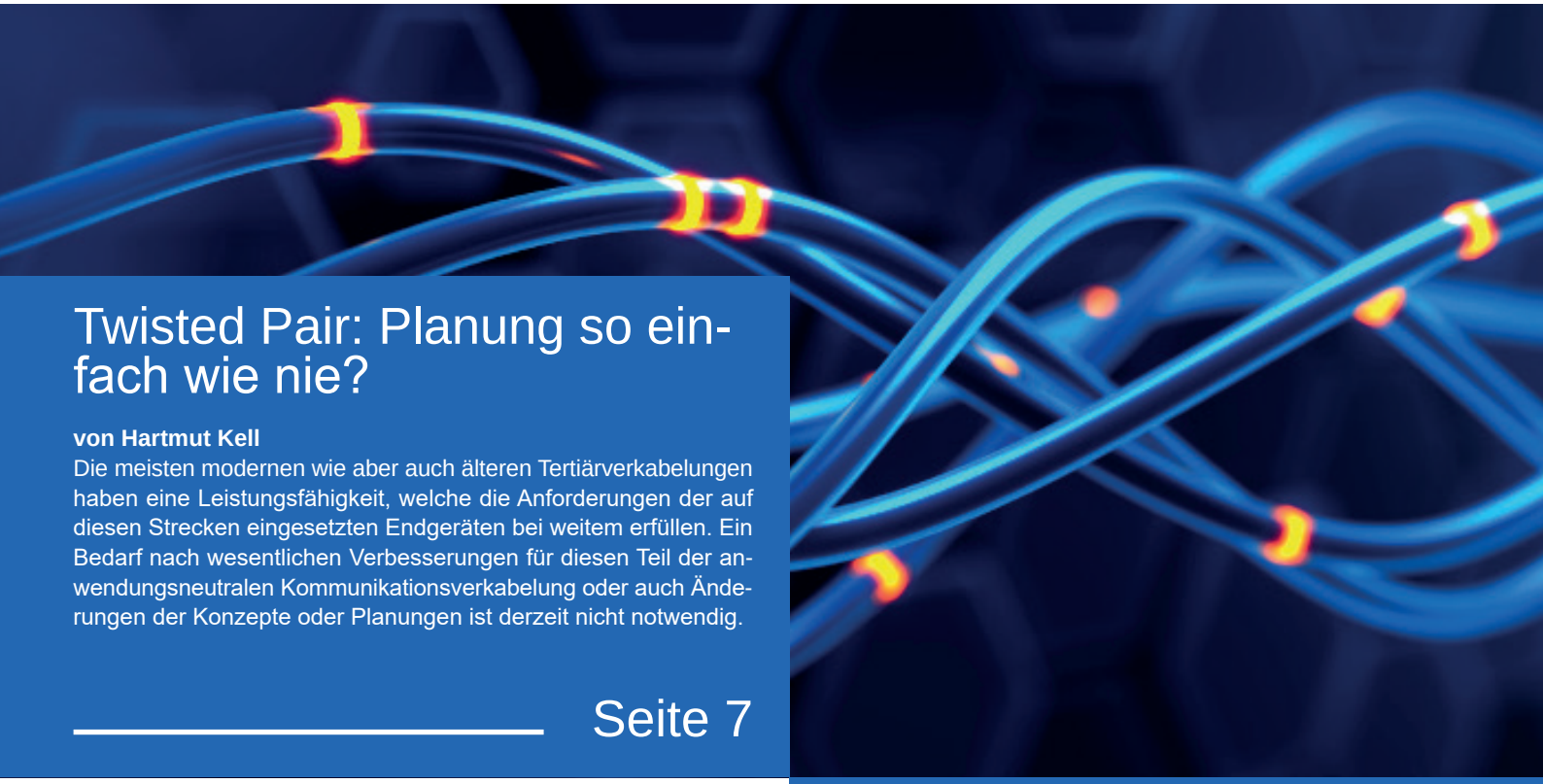
Mai 2024

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider



Twisted Pair: Planung so einfach wie nie?

von Hartmut Kell
Die meisten modernen wie aber auch älteren Tertiärverkabelungen haben eine Leistungsfähigkeit, welche die Anforderungen der auf diesen Strecken eingesetzten Endgeräten bei weitem erfüllen. Ein Bedarf nach wesentlichen Verbesserungen für diesen Teil der anwendungsneutralen Kommunikationsverkabelung oder auch Änderungen der Konzepte oder Planungen ist derzeit nicht notwendig.

Seite 7

VMware: Ende einer Ära?

von Dr. Behrooz Moayeri
In der Aprilausgabe des Netzwerk Insider habe ich darauf hingewiesen, dass Hersteller und ihre Kunden unterschiedliche Interessen haben. An keinem anderen Beispiel wird dies zurzeit so deutlich wie im Falle von VMware. Seit der Übernahme des führenden Herstellers von Virtualisierungslösungen durch Broadcom gibt es viel Unruhe unter den VMware-Kunden.

Seite 2

Videoüberwachung – Datenschutz & Datenintegrität

von Marcus Steinhorn
In Zeiten, in der technologische Fortschritte unaufhörlich unsere Gesellschaft prägen, steht auch die Videoüberwachung immer wieder im Zentrum komplexer Debatten um Privatsphäre, Sicherheit und Ethik. Während diese Technologien das Potenzial bieten, unsere öffentlichen und privaten Räume sicherer zu gestalten, werfen sie gleichzeitig bedeutende Fragen hinsichtlich des Datenschutzes und der Datenintegrität auf.

Seite 27

Webinar der Woche

Security-Zertifizierungen – Orientierung

Seite 26

Hintertür in „liblzma“: Ein Supply-Chain-Angriff über eine Open-Source-Bibliothek

von Dr. Markus Ermes
Pünktlich zum Osterwochenende wurde eine Sicherheitslücke in einer quelloffenen Kom-pressionsbibliothek entdeckt, die in vielen Projekten zum Einsatz kommt.

Seite 23

VMware: Ende einer Ära?

von Dr. Behrooz Moayeri

In der Aprilausgabe des Netzwerk Insider habe ich darauf hingewiesen, dass Hersteller und ihre Kunden unterschiedliche Interessen haben. An keinem anderen Beispiel wird dies zurzeit so deutlich wie im Falle von VMware. Seit der Übernahme des führenden Herstellers von Virtualisierungslösungen durch Broadcom gibt es viel Unruhe unter den VMware-Kunden. Mit der auf den Abschluss der Firmenübernahme folgenden Ankündigung der neuen Lizenzpolitik von VMware wissen die meisten VMware-Kunden, dass sie in Zukunft wesentlich mehr für VMware-Lizenzen bezahlen müssen als bisher. Dies ist vor allem auf das Modell des Software-Abonnements (Subscription) zurückzuführen.

Fast jede Organisation ist betroffen

Nach Microsoft ist VMware der einzige Hersteller, dessen Produkte in der IT-Umgebung fast jeder Organisation genutzt werden. Die Marke VMware steht seit über 20 Jahren für Virtualisierung. Wie Virtualisierung die IT verändert hat, muss hier nicht ausgeführt werden. Ohne Virtualisierung gäbe es kein Cloud Computing, was nicht heißt, dass große Cloud-Anbieter VMware-Lösungen für die Virtualisierung nutzen. VMware-Kunden sind vor allem Organisationen, die in eigenen Rechenzentren Server für eigene Zwecke betreiben. Lange bevor es die großen Clouds gab, hat VMware mit ESX und vSphere die Lösung für Server-Virtualisierung angeboten, die jeder Kunde kaufen und betreiben konnte. Kurz bevor VMware große Verbreitung fand, war der Aufbau eines eigenen Rechenzentrums eine große Materialschlacht. Mir ist das Beispiel einer Bank gut in Erinnerung geblieben, die um die Jahrtausendwende ca. 2.000 Mitarbeiter und fast genau so viele physische Server hatte.

Die Virtualisierung hat für die Betreiber von Rechenzentren den Aufbau von Serverfarmen wesentlich vereinfacht. Vor Jahrzehnten war es üblich, auf einem großen Server verschiedene Applikationen nebeneinander zu betreiben. Jede Applikation war somit von der einen Betriebssysteminstanz abhängig. Virtuelle Server schufen die Möglichkeit, eine Betriebssysteminstanz pro Applikation vorzusehen. Damit wurden die Abhängigkeiten zwischen Anwendungen minimiert und der Applikationsbetrieb wesentlich vereinfacht.

VMware war und ist nicht der einzige Lösungsanbieter für Virtualisierung, für die Betreiber privater Serverfarmen jedoch der größte. Viele Anbieter von Systemen und Applikationen haben auf die große Verbreitung von ESX und vSphere damit reagiert, dass sie ihre Lösungen auf Basis dieser VMware-Produkte angeboten haben.

VMware als führender Hersteller

Nicht nur hinsichtlich des Verbreitungsgrades blieben in den letzten zwei Jahrzehnten ESX und vSphere im Vergleich zu kommerziellen Alternativen wie Microsoft Hyper-V und offenen Lösungen wie KVM führend. Auch der Funktionsumfang der VMware-Virtualisierung war für viele RZ-Betreiber ein Grund, an VMware festzuhalten. Bei einer Reihe von wichtigen Funktionen im Zusammenhang mit der Server-Virtualisierung war VMware Vorreiter, so zum Beispiel bei Hochverfügbarkeit oder Verlagerung virtueller Maschinen, wofür der Name VMotion steht.

Der technologische Vorsprung von VMware beschränkte sich nicht nur auf Server-Virtualisierung. VMware ist sehr früh in den Markt für Netzvirtualisierung eingestiegen. Der Hype um Software Defined Networks (SDN) war noch recht neu, als in 2012 die Firma Nicira von VMware übernommen wurde. Aus dieser Akquisition erwuchs VMware NSX, bis heute die umfassendste Lösung für Network Function Virtualization (NFV), mit Funktionen wie Distributed Firewall bzw. Mikrosegmentierung, Routing, Lastverteilung etc.

Noch älter als das VMware-Engagement im Netzbereich ist die Client-Virtualisierung, die in der VMware-Geschichte sogar vor der Server-Virtualisierung kam. Aus der Client-Virtualisierung entwickelte sich die Virtual Desktop Infrastructure (VDI), d.h. Client-Virtualisierung auf Basis einer Serverfarm. VMware ist in diesem

Twisted Pair: Planung so einfach wie nie?

von Hartmut Kell

Die meisten modernen wie aber auch älteren Tertiärverkabelungen haben eine Leistungsfähigkeit, welche die Anforderungen der auf diesen Strecken eingesetzten Endgeräten bei weitem erfüllen. Ein Bedarf nach wesentlichen Verbesserungen für diesen Teil der anwendungsneutralen Kommunikationsverkabelung oder auch Änderungen der Konzepte oder Planungen ist derzeit nicht notwendig. Jede neue Gebäudeverkabelung, die eine Klasse-EA-Qualität sicherstellt, liefert am Arbeitsplatz „Rechenzentrumsqualität“ und sollte somit mehr als ausreichend sein. Insbesondere die in Deutschland meist vorzufindende Kombination von Kategorie-7/7A-Installationskabel und Kategorie-6A-Anschlusstechnik stellt eine Möglichkeit dar, ein einfaches „Upgrade“ der Verkabelung auf Klasse F/FA durchzuführen, ohne dass man von einer kompletten Neuverkabelung ausgehen muss. Jedem ist klar, dass heute dieses Upgrade nichts bringt, denn es gibt aktuell keine Anwendung oder kein Übertragungsverfahren, welches eine solche Verkabelungsqualität erforderlich machen würde.

Auch die nächste Generation der Klasse I und II, welche eine Datenrate von bis zu 40 Gbit/s sicherstellen soll, wird wohl kaum im Tertiärbereich sinnvoll Einzug halten, denn dazu sind die Kabellängen mit nicht einmal 30 m (nach Standard) wohl viel zu gering.

Der Zeitpunkt, wo funkbasierende Übertragungstechniken eine Tertiärverkabelung vollkommen ablösen werden, ist noch nicht erkennbar, deshalb werden auch weiterhin in neuen Bürogebäuden Planungen von Tertiärverkabelungen als Grundbestandteil einer IT-Infrastruktur notwendig sein.

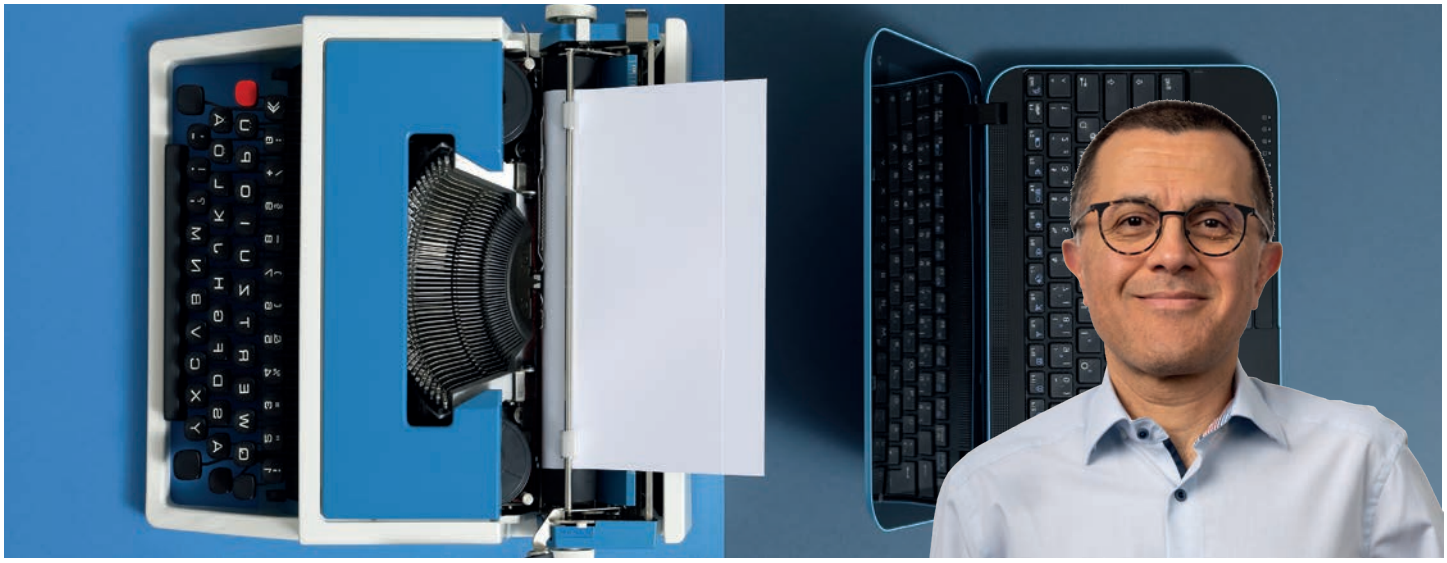
Ist das Thema „Tertiärverkabelung“ also so uninteressant, dass es sich nicht lohnt darüber zu schreiben? Mitnichten! Die Herausforderungen liegen in der Umsetzung der Konzepte. Diesen Punkten wird sich der nachfolgende Artikel widmen.

Konzeptionelle Erneuerungen

Der Autor hat sich dem Thema „Arbeitsplatzverkabelung“ in einer ganzheitlichen Form zum letzten Mal vor 10 Jahren in einem entsprechenden Insider-Artikel gewidmet. Wie bereits gesagt, konzeptionell hat sich nicht viel geändert, aber es hat sich auch nicht „gar nichts“ verändert.

Lassen Sie uns kurz die Änderungen oder „Neuheiten“ der bereits auch schon in die Jahre gekommenen Verkabelungsnorm EN 50173-1 anschauen. Die letzte Aktualisierung dieser so wichtigen Norm war Ende 2018 (Version davor: 2011). Seitdem ist nichts mehr Neues passiert. Schließen wir die Nutzbarkeit der Kategorie 8-Komponenten und der Übertragungsklasse I/II im Tertiärbereich aus, gibt es eigentlich nichts, was die Norm von 2018 eingeführt hat und was sich wesentlich auf die Planungskonzepte auswirkt. Weiterhin wird

- eine eher konservative Längenplanung mit maximal 90 m vorgenommen,
- bei den meisten kein Bedarf nach Datenraten von mehr als 1 Gbit/s als notwendige Grundausstattung an jedem Arbeitsplatz gesehen, der Sammelpunkt eher selten eingesetzt (Tendenz jedoch zunehmend),
- die Kombination von Kabel der Kategorie 7/7A mit RJ45-Anschlusstechnik in Kategorie 6A bevorzugt, die klassische Handheld-Scanner-Messtechnik fast genauso wie vor 15 Jahren genutzt, bei den meisten Planungen wenigstens die Anzahl von 2 Kommunikationsanschlüssen pro Arbeitsplatz vorgesehen.



35 Jahre Informationstechnologie – ein Rückblick

Mit Dr. Behrooz Moayeri sprach Christiane Zweipfennig

Ein Leben ohne Internet, Handy oder Computer? Das ist für die meisten Menschen heute nicht mehr vorstellbar! Während in den 1980er Jahren viele Geräte aus "Zurück in die Zukunft" noch als utopische Visionen galten, sind sie heute längst real. Diese Entwicklung sagt alles über den unfassbaren technologischen Fortschritt der vergangenen vier Jahrzehnte aus.

Dr. Behrooz Moayeri gehört der Geschäftsleitung der ComConsult GmbH an und ist seit 1988 bei ComConsult beschäftigt. In über 35 Berufsjahren hat er hunderte Organisationen und deren IT kennengelernt. In diesem Interview erzählt er davon, welche historischen Meilensteine er in der Entwicklung der IT miterlebt hat.

Behrooz, deine Hausarbeiten in deiner Schulzeit bis Anfang der 1980er Jahre hast du noch handgeschrieben. Noch während deines Studiums in den 1980er Jahren wurde mit Büchern statt mit Suchmaschinen recherchiert. Wie hast du die Umstellung auf elektronische Datenverarbeitung damals erlebt?

Ich gehörte nicht zu den Pionieren unter den Jugendlichen, die bereits in den 70er Jahren mit den ersten Computern von Commodore & Co. experimentiert haben. Erst während des Studiums habe ich für die Studienarbeit, die Diplomarbeit und die Dissertation intensiv mit Computern gearbeitet, zunächst mit Unix-Rechnern, dann mit DOS und Windows. Heute fangen bereits kleine Kinder an, Computer der Kategorie Handy und Tablet zu nutzen, ohne wissen zu müssen, wie sie funktionieren. Bei mir war das anders: Ich habe zunächst viel Theoretisches über Computer gelernt, bevor ich mit ihnen gearbeitet habe. Ich habe sogar in einer Klausur Assembler-Code für IBM-Großrechner in Maschinensprache übersetzt, alles auf Papier. Bei der Studien-, Diplom- und Doktorarbeit habe ich zweierlei intensive Arbeit auf Computern durchgeführt: Programmieren und Textverarbeitung für die Ausarbeitung der Arbeiten. Das Programmieren endete bei mir mit der Hochschulzeit. Bei ComConsult sind dafür andere computergestützte Arbeiten dazugekommen. Ich fing bei ComConsult im Bereich Messen und Analyse an und habe in dem Zuge den Übergang von analogen zu digitalen Messgeräten und Analysatoren miterlebt. Gleichzeitig wurde die Nutzung von E-Mail, zunächst intern und dann extern, immer intensiver. Der nächste Schritt war die Nutzung des World Wide Web zur Informationsbeschaffung, gefolgt von Web-basierenden Suchmaschinen.

> Assembler-Code für IBM-Großrechner in Maschinensprache übersetzen - auf Papier

Wie sah Ende der 1980er Jahre eine typische IT-Infrastruktur im Unternehmen aus?

Die meisten IT-Umgebungen waren Insel-Lösungen und nicht miteinander vernetzt. Einige Organisationen hatten Großrechner und

Hintertür in „liblzma“: Ein Supply-Chain-Angriff über eine Open-Source-Bibliothek

von Dr. Markus Ermes

Pünktlich zum Osterwochenende wurde eine Sicherheitslücke in einer quelloffenen Kompressionsbibliothek entdeckt, die in vielen Projekten zum Einsatz kommt. Dabei sind zwei Aspekte besonders interessant:

1. Diese Bibliothek wird über Umwege in einigen SSH-Servern bei verschiedenen Linux-Distributionen eingesetzt, und

2. diese Sicherheitslücke ist vorsätzlich eingebaut worden. Es handelt sich also eigentlich um eine Hintertür!

Verschiedene einschlägige Webseiten haben sich mit dem Thema beschäftigt und auch die betroffenen Distributionen benannt. Diese Punkte sollen hier nicht noch einmal im Detail erläutert werden. Es wird lediglich kurz darauf eingegangen, was die Bibliothek macht und wie die Hintertür in die Software gelangen konnte.

Außerdem werde ich auf die Folgen solcher Angriffe eingehen, die vermutlich nicht weniger werden.

Liblzma – eine Kompressionsbibliothek

Die Software, die von der oben genannten Hintertür betroffen war, mag auf den ersten Blick unscheinbar aussehen: Es handelt sich um eine Bibliothek, die sich mit Kompression und Dekompression von Daten im sogenannten „xz“-Format beschäftigt. Viele von uns werden mit diesem Format nicht allzu viel anfangen können. Ich zum Beispiel weiß, dass es dieses Format gibt, doch über die zugehörige Bibliothek habe ich mir vor dem 30. März noch nie Gedanken gemacht.

Allerdings, wie in der Einleitung bereits erwähnt, kommt diese Bibliothek zum Beispiel indirekt in SSH-Servern zum Einsatz. Und nicht nur dort: Liblzma ist Teil einer jeden Linux-Distribution, die auf SystemD basiert. Und das sind heutzutage die meisten, insbesondere die im Unternehmensumfeld verbreiteten Distributionen von Red Hat und Suse. Und über SystemD kann die Bibliothek auf Umwegen in den SSH-Server gelangen.

Wie kam die Hintertür in die Bibliothek?

An dieser Stelle wird es perfide: Das „Einpflanzen“ der Hintertür war ein langwieriger und gut organisierter Prozess. Der Angreifer, der ab 2021 auf Github aktiv war, unterstützte das liblzma-Projekt und schaffte es, dieses Projekt sogar zu übernehmen. Hierzu hatte er Komplizen, die die (ursprünglichen) liblzma-Entwickler unter Druck gesetzt haben. Einmal erfolgreich, erstellte der Angreifer fertige Pakete mit der Hintertür und versuchte, diese bei verschiedenen Distributionen aggressiv zu bewerben.

Videoüberwachung – Datenschutz & Datenintegrität

von Marcus Steinhorn

In Zeiten, in der technologische Fortschritte unaufhörlich unsere Gesellschaft prägen, steht auch die Videoüberwachung immer wieder im Zentrum komplexer Debatten um Privatsphäre, Sicherheit und Ethik. Während diese Technologien das Potenzial bieten, unsere öffentlichen und privaten Räume sicherer zu gestalten, werfen sie gleichzeitig bedeutende Fragen hinsichtlich des Datenschutzes und der Datenintegrität auf. Diese Fragen gewinnen insbesondere vor dem Hintergrund der rasanten Entwicklung von Deep-Fake-Technologien an Brisanz. Deep Fakes, also durch Künstliche Intelligenz erzeugte manipulierte Videos, die kaum von der Realität zu unterscheiden sind, stellen eine völlig neue Herausforderung für die Authentizität und Verlässlichkeit von Videomaterial dar.

Für Fachleute, die sich an der Schnittstelle von Technologieentwicklung, rechtlichen Rahmenbedingungen und ethischen Überlegungen bewegen, birgt das Thema Videoüberwachung eine Vielzahl von Aspekten, die einer sorgfältigen Betrachtung bedürfen. Von den technischen Möglichkeiten und Grenzen der Videoüberwachungssysteme über die rechtlichen Vorschriften zum Schutz personenbezogener Daten bis hin zu den Implikationen für die persönliche Freiheit und die gesellschaftliche Ordnung – jede Facette verdient eine eingehende Analyse.

Videoüberwachung – Herausforderungen und Chancen

In der Praxis ist die Implementierung von Videoüberwachungssystemen weit mehr als nur die Installation von Kameras an neuralgischen Punkten. Es handelt sich um ein komplexes Zusammenspiel aus technischer Infrastruktur, Softwarelösungen und algorithmischer Verarbeitung, das darauf abzielt, ein Mehr an Sicherheit zu gewährleisten und gleichzeitig den rechtlichen Anforderungen und ethischen Standards gerecht zu werden.

Bei modernen Videoüberwachungssystemen haben IP-Kameras ihren analogen Counterpart in den letzten Jahren weitestgehend abgelöst, auch weil IP-Kameras nicht nur eine Betrachtung in Echtzeit ermöglichen, sondern auch fortgeschrittene Analysesoftware, die Gesichtserkennung, Bewegungserkennung und sogar Verhaltensanalysen durchführen kann. Diese Technologien werden durch künstliche Intelligenz und maschinelles Lernen verstärkt, wodurch die Effizienz der Überwachung erhöht und der Bedarf an menschlicher Bewertung der Szene reduziert wird.

Aber die hauptsächlichen Herausforderungen bei der Implementierung von Videoüberwachungssystemen liegen nicht nur in der zielgerichteten Umsetzung immer komplexer werdender Technologien. Auch Wahrung von Privatsphäre und Datenschutz, Sicherstellung der Datenintegrität und Vermeidung von Missbrauch sind in den vergangenen Jahren zunehmend in den Fokus gerückt. Denn dass diese Systeme, während sie das Potenzial bieten, die öffentliche Sicherheit zu verbessern, Kriminalität zu vermindern oder zumindest zu deren Aufklärung beizutragen, auch die Gefahr missbräuchlicher Kontrolle bergen, steht außer Frage. Durch die aus dieser Problematik hervorgegangenen Vorschriften und Regelwerke stellt die Speicherung und Verarbeitung von Videodaten, nicht erst seit Einführung der Datenschutz-Grundverordnung (DSGVO), eine signifikante rechtliche und planerische Herausforderung dar.

Die Einführung von Videoüberwachungstechnologien wirft auch ethische Fragen auf, insbesondere hinsichtlich der Balance zwischen Sicherheit und Privatsphäre. Die Entscheidung, wann und wo Kameras installiert werden, wie die gesammelten Daten verwendet werden, wer Zugang zu diesen Daten hat und wie lange