

kein Wasser eindringen kann. Damit man es nicht einfach herausziehen kann, muss die Kamera hoch genug hängen. Eine separate Stromversorgung ist bei den meisten Modellen nicht erforderlich, sie werden in der Regel über Power over Ethernet (PoE), direkt über das LAN-Kabel im Zusammenspiel mit einem zusätzlichen Injector mit Energie versorgt.

Aufstellung und Integration

Bei der Suche nach dem richtigen Aufstellort gilt es die Kamera so auszurichten, dass Sie keinen öffentlichen Raum filmen. Dazu gehören auch Straße oder Gehweg, der Nachbargarten ist natürlich ohnehin tabu.

Die meisten Kameras nehmen per Smartphone-App automatisch Verbindung zum WLAN-Router auf. Möchten Sie mehrere Kameras zur Überwachung nutzen, empfehlen sich professionelle Alarmsysteme. Diese haben meist ein zusätzliches Gateway, das in der Regel im Set enthalten ist. Smart-Home-Systeme wie SmartThings von Samsung oder Magenta SmartHome der Telekom erlauben das Einbinden von Kameras verschiedener Hersteller. Hier wird die Kamera als neues Gerät zusätzlich eingebunden und ins System integriert. Ob das von Ihnen bevorzugte Modell für Ihre bereits vorhandene Smart-Home-Zentrale geeignet ist, erfahren Sie beim Hersteller oder innerhalb der App.

App-Steuerung

Die Einrichtung und Verwaltung der Kameras gelingt einfach per App. In einem Nutzer-Account geben Sie Ihre E-Mail-Adresse ein und legen einen Benutzernamen und ein Passwort fest. Anschließend werden Sie über einen Einrichtungs-Assistenten in der App durch die Installation geführt. In den meisten Fällen müssen Sie für den Verbindungsaufbau einen QR-Code auf der Kamera mit dem Smartphone absキャン. Einige Hersteller bieten zusätzlich auch die Konfiguration über ein Webinterface an.

Viele IP-Kameras lassen sich mit den Sprachassistenten von Alexa, Google und Apple verknüpfen. Nutzen Sie einen smarten Lautsprecher inklusive Display wie den Amazon Echo Show, können Sie das aktuelle Livebild der Kamera dann sogar unabhängig vom Smartphone sehen.

Was die einzelnen Kameras im Detail leisten, hängt vom Modell ab. In der Regel können Sie über die App das aktuelle Kamerabild abrufen und verschiedene Einstellungen vornehmen. Ist die Kamera

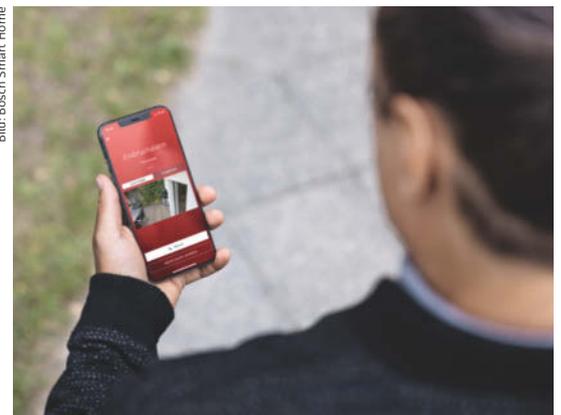
überwachung aktiviert, werden Sie bei unerwarteten Bewegungen per Pushnachricht informiert. Einzelne Hersteller erlauben die zusätzliche Benachrichtigung per E-Mail oder Telefonanruf. Anbieter wie Lupus und Verisure bieten optional einen kostenpflichtigen Notrufservice an, der bei Bedarf dann die Polizei oder Rettungskräfte informiert. Die heute gängigen Modelle bieten überwiegend eine HD, meist sogar Full-HD-Auflösung.

Damit die Überwachung auch im Dunklen zuverlässig funktioniert, sind IP-Kameras üblicherweise mit einem Nachtsichtsensor und Infrarotleuchten ausgestattet. Für eine direkte Kommunikation zwischen Smartphone und Kamera haben die meisten Modelle ein Mikrofon und einen Lautsprecher eingebaut. Höherpreisige Modelle von Ring und Netatmo sind sogar mit einem Fluchtlicht und einer Sirene ausgestattet.

Speicherung in der Cloud und auf SD-Karte

Ein besonders wichtiger Punkt bei der Auswahl einer Überwachungskamera ist die Speicherung von Aufnahmen. Hier setzen die meisten Hersteller auf Cloud-basierte Lösungen. Nach Anlegen eines Nutzerkontos können Sie die online gespeicherten Aufnahmen anschauen. Meist sind die Aufnahmen jedoch nur 24 Stunden kostenfrei verfügbar. Wer längere Aufzeichnungsintervalle oder erweiterte Funktionen haben möchte, muss hierfür zahlen. Arlo

Bild: Bosch Smart Home



Per App werden Sie auch unterwegs sofort informiert, wenn zu Hause ein Alarm ausgelöst wird.

Rechtliche Rahmenbedingungen für IP-Kameras und Videotürklingeln

Beim Einsatz einer Videoüberwachungsanlage bzw. IP-Kamera drängen sich Fragen des Datenschutzes auf. Das liegt zum einen daran, dass Videoaufnahmen einen Eingriff in das Recht auf informationelle Selbstbestimmung von Personen darstellen. Zum anderen ist es möglich, dass sensible personenbezogene Daten verarbeitet werden, welche durch die Datenschutz-Grundverordnung (DSGVO) besonders geschützt sind.

Das meiste, was für den Einsatz von Videoüberwachungsanlagen gilt, lässt sich dabei auf die hier ebenfalls besprochenen Videotürklingeln übertragen. Denn auch wenn die Videoübertragungen im Regelfall wesentlich kürzer sind, kann man manche Geräte individuell auf 24/7-Betrieb umstellen oder die Geräusch- und Bewegungserkennung aktivieren und sie auch zur Videobeobachtung verwenden.

Für alle IP-Kameras gilt: Auch beim Einsatz auf dem eigenen Grundstück kann die DSGVO Anwendung finden, da bei der Videoerfassung personenbezogene Daten erhoben und verarbeitet werden. Dabei macht es nach Ansicht der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) aus datenschutzrechtlicher Sicht keinen Unterschied, ob die Videogeräte aufzeichnen oder die Übertragung in Echtzeit ohne Zwischenspeicherung erfolgt.

Allerdings findet die DSGVO keine Anwendung bei Datenverarbeitungen, die ausschließlich zu persönlichen und familiären Zwecken erfolgen. Wann diese Ausnahme zur Anwendung kommt, sorgt regelmäßig für Diskussionsstoff unter Juristen. Nach der Rechtsprechung des EuGH (EuGH, Urteil vom 11.12.2014, Rechtssache C-212/13) ist für die Beurteilung der Frage, ob diese sogenannte „Haushaltsausnahme“ greift, ein wesentliches Kriterium, ob die Kameras auch den öffentlichen Bereich abdecken.

Wird beispielsweise die Straße vor dem eigenen Grundstück oder das Nachbargrundstück erfasst, kann man die Haushaltsausnahme nicht für sich in Anspruch nehmen. Die Konsequenz wäre, dass für den Privatanwender alle gesetzlichen Datenschutzvorgaben zu beachten wären und bei Verstößen die potenziell hohen Bußgelder der DSGVO oder Schadensersatzansprüche der betroffenen Personen in Betracht kämen.

Im Hinblick auf die Erfassung des öffentlichen Bereichs sind daher beispielsweise Videotürklingeln kritisch zu bewerten, die dauerhaft eingeschaltet sind und etwa in Mehrparteienhäusern den Eingangsbereich des Nachbarn erfassen.

Doch auch im Innenbereich ist Vorsicht geboten: So ist es zwar dem familiären Bereich zuzurechnen, wenn die Eltern das Kleinkind im Rahmen der eigenen Wohnung per Videokamera überwachen. Sollte allerdings Besuch von haushaltsfremden Personen anstehen, wären die Kameras auszustellen oder es müssten die Besucher vor Betreten der Räume gefragt werden, ob sie damit einverstanden sind, dass die Innenräume per IP-Kamera überwacht werden.

Ebenfalls nicht unter die Haushaltsausnahme fällt das Verfügbarmachen der Videoübertragung über das Internet für einen unbegrenzten Personenkreis. Sind die Aufnahmen dagegen mittels technischer und organisatorischer Maßnahmen ausreichend abgesichert und nur ein enger Familienkreis hat Zugriff auf diese, kommt wiederum die Haushaltsausnahme in Betracht.

Die vorgenannte Rechtsprechung des EuGH stellt weiterhin klar, dass die Beurteilung, ob die Haushaltsausnahme greift, stets im Rahmen einer Einzelfallprüfung vorzunehmen ist. Auch bei hybrider Nutzung der Anlage nicht nur zu privaten, sondern auch zu geschäftlichen Zwecken, käme die Haushaltsausnahme nicht zur Anwendung. Private Videoanlagenbetreiber sollten also vorsichtig beim Einsatz sein und im Zweifel rechtliche Beratung in Anspruch nehmen.

Ein häufiger Irrtum: Auch wenn einige IP-Kameras Datenschutzaspekte berücksichtigen, sind reine Hersteller für sich genommen in der Regel keine datenschutzrechtlichen Verantwortlichen. Datenschutz muss also seitens des Herstellers nicht voreingebaut sein. Das bedeutet, dass die Person die IP-Kameras im Innen- oder Außeneinsatz einsetzt, stets selbst geltende Datenschutzvorgaben gewährleisten muss, – sofern die Haushaltsausnahme nicht greift. Hilfreich ist es dabei, sich schon vor dem Kauf über Einsatzzweck und Datenschutz-Features Gedanken zu machen.

In jedem Fall empfiehlt es sich bei IP-Kameras die von den Herstellern meist schon mitgelieferten Hinweisschilder gut sichtbar anzubringen. So können Besucher sofort erkennen, dass sie per Videokamera beobachtet werden.

Zudem sollten die Mikrofone grundsätzlich ausgestellt und lediglich für die Dauer des Gesprächs aktiv sein. Denn sollte der Betreiber beim Einsatz von IP-Kameras Audiosignale dauerhaft aufnehmen, kann er sich durch das unbefugte Aufnehmen des nicht öffentlich gesprochenen Wortes strafbar machen.

(Dr. Michael Koch, Jurist)

bietet innerhalb seines Cloud-Service beispielsweise eine Personenerkennung an. Ring verlangt je nach Abo-Modell zwischen 3 und 10 Euro im Monat beziehungsweise 30 und 100 Euro im Jahr.

Bei einigen Modellen werden die Daten direkt auf einem internen Speicher der zugehörigen Zentrale gespeichert. Damit sind die Daten jederzeit verfügbar und auch bei einem möglichen Ausfall des Cloudservers abrufbar. Viele Kameras haben zusätzlich einen SD-Kartenslot eingebaut, auf den Sie ebenfalls unabhängig einer Cloudanbindung direkt zugreifen können.

Gerade bei der Überwachung von größeren Innenräumen mit mehreren Kameras kommen Modelle mit externem Speicher oder Verknüpfung mit einem NAS-Laufwerk zum Einsatz. Sie setzen meist auf die Plattform ONVIF (Open Video Interface Forum) und werden mit einem zugehörigen Netzwerk-Video-Rekorder (NVR) ausgeliefert, der dauerhaft oder in Zeitintervallen aufzeichnet und es erlaubt, mehrere Kamerabilder gleichzeitig auf dem Rechner anzuschauen.

Hautier- und Personenerkennung

Wer ein großes Grundstück hat oder nur einen kleinen bestimmten Bereich überwachen möchte, sollte sich nach einer Kamera mit einstellbarem Sichtbereich umschauen. Hier können Sie innerhalb des Menüs einzelne Bereiche auswählen, die überwacht werden sollen, andere werden dann ausgeblendet. Kameras wie die Lupus LE 232 oder die Netatmo Presence haben eine Personenerkennung integriert. Der entsprechend von der Kamera erkannte Bereich muss hier eine bestimmte Größe haben, damit der Alarm auslöst. Im Garten herumlaufende Katzen oder Hunde werden aufgrund ihrer Größe also dann zum Beispiel nicht als Einbrecher identifiziert.

Welche Kameras gibt es?

Für den Einsatz im Außenbereich sind akkubetriebene Kameras besonders flexibel; sie sind nach IP-Zertifizierung ausreichend gegen Wasser und Staub geschützt. Eine permanente Stromversorgung per Kabel ist nicht nötig. Sie müssen den Akku jedoch zwischendurch aufladen. Wann dies nötig ist, hängt vom jeweiligen Modell und der Einsatzdauer ab. Einzelne Modelle wie die Spotlight Cam von Ring lassen sich mit einem Solarmodul betreiben und sind somit (fast) dauerhaft autark. Die



IP-Kameras mit Akkubetrieb und WLAN können Sie flexibel im Haus aufstellen.

Kameras sind eher kompakt gehalten und lassen sich damit auch im Innenbereich gut in Ecken platzieren. Aber Vorsicht: Sie dürfen Personen nicht ohne ihr Wissen überwachen. Mehr dazu im Kasten auf Seite 16.

Für die Installation an der Decke zum Beispiel auf einer Terrasse sind Dome-Kameras gedacht. Mit ihrem 360-Grad-Rundumblick werden sie oft zur Überwachung von Hinterhöfen genutzt. Sie sitzen unter einer Glaskugel und sind somit gut gegen Witterungseinflüsse geschützt. Sie sind meist mit einer schwenkbaren Funktion ausgestattet. Per App können Sie dann den Sichtbereich individuell bestimmen. Auch Außenleuchten sind mit integrierter Kamera zu bekommen. Vor der Montage sollte man aber mit dem Vermieter klären, ob er mit einem Austausch einverstanden ist.

Last but not least, können Sie auch eine smarte Videotürklingel zur Überwachung nutzen. Viele Modelle erlauben das Aufrufen des aktuellen Livebildes und können auf Bewegungen reagieren, einzelne bieten zudem einen Radarsensor, um Bewegungen vor der Kamera in einem definierten Abstand zu erkennen. In unserer Rubrik „Schutz und Sicherheit dank Kameras“ ab Seite 78 haben wir IP-Kameras und Videotürklingeln von verschiedenen Herstellern getestet. (dwe)



Bild: Zinaida Sopina/shutterstock.com

Wann WLAN, wann Zigbee?

Vor der Anschaffung einer smarten Alarmanlage, einem smarten Türschloss oder einer IP-Kamera sollten Sie sich vorab auch über die jeweiligen Funkstandards informieren. Denn nicht jede Komponente arbeitet mit jeder Zentrale zusammen. Wir stellen die einzelnen Smart-Home-Funkprotokolle im Detail vor.

Von **Patrick Bellmer**

Der Verzicht auf Kabel erleichtert den Auf- und Ausbau vieler Smart-Home-Systeme. Statt Wände aufzustemmen, müssen Sie lediglich für einen ausreichenden Funkempfang sorgen. Doch damit alle Komponenten einer smarten Alarmanlage oder die smarte Lampe auch in der entlegensten Ecke des Hauses Kontakt mit der Zentrale oder einem anderen Befehlsgeber aufnehmen kann, gilt es die für Sie passende Funktechnik respektive das passende Funkprotokoll zu finden. Denn Bluetooth, DECT ULE, EnOcean, WLAN, Z-Wave und Zigbee weichen in wichtigen Punkten voneinander ab.

Deshalb sollten Sie vor dem Kauf nicht nur planen, welche Bereiche das Smart-Home-System künftig abdecken soll, sondern auch die dahinterstehende Infrastruktur berücksichtigen. Deshalb zeigen wir, welche Vor- und Nachteile die sechs weitverbreiteten Funktechniken bieten und inwiefern Sie löchrige Funknetze stopfen können.

Gute Funkverbindung wichtig

Eine Grundvoraussetzung für den reibungslosen Betrieb im Smart Home ist eine zuverlässige Kommu-

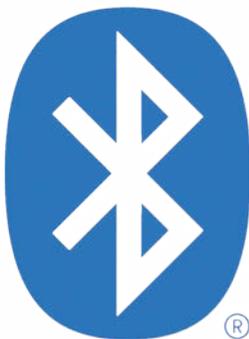
nikation zwischen Komponenten und Befehlsgeber. Soll auch der etwas weiter weg entfernte Bewegungsmelder mit den übrigen Komponenten kommunizieren, müssen die Informationen ihr Ziel problemlos erreichen. Ebenso sollte sichergestellt sein, dass auch wirklich alle eingebundenen Geräte in Bereitschaft gehen, wenn Sie den zentralen Ein-Ausschalter in der entsprechenden App unmittelbar vor dem Verlassen des Hauses betätigen.

Auf der anderen Seite muss das System auch mit der Außenwelt kommunizieren – sei es für die Abfrage bestimmter Daten aus dem Internet oder falls Sie die Alarmanlage oder Überwachungskamera von unterwegs per Fernzugriff bedienen möchten. In vielen Fällen bedeutet das: Zentrale und Router müssen miteinander kommunizieren können. Die meisten Smart-Home-Zentralen setzen dabei auf eine Verbindung per LAN-Kabel.

Haben Sie entsprechende LAN-Kabel und -Dosen nicht in mehreren Räumen in Ihrem Haus oder Ihrer Wohnung verlegt, wird die Zentrale meist in unmittelbarer Nähe zum Router ihren Platz finden. Je nachdem, welche konkrete Funktechnik die Smart-Home-Komponenten verwenden, kann dies zu Empfangsproblemen führen. Schließlich sind die Reichweiten stark unterschiedlich und neben der theoretischen Maximalreichweite spielen auch die Dämpfungseigenschaften verschiedener Materialien eine Rolle. Eine Betondecke kann auf Zigbee ganz anders wirken als auf ein 5-GHz-WLAN. Und nicht immer lassen sich Netze mit Repeatern erweitern.

Bluetooth: Smartphone statt Zentrale

Bluetooth spielt vor allem dann eine Rolle, wenn Sie Smartphones und Zubehör wie Fitnesstracker, Smartwatches oder Kopfhörer drahtlos miteinander verbinden wollen. Allerdings setzen auch einige Hersteller von smarten Türschlössern und anderen Komponenten fürs Smart Home auf diesen Funkstandard. Das hat vor allem einen Grund: Wie auch bei WLAN-Komponenten ist keine dedizierte Steuerzentrale nötig, stattdessen steuern Sie die Geräte über Bluetooth mit dem Smartphone oder Tablet. Steht fest, dass sich Ihr Smart Home auf ein einziges Türschloss beschränken wird, müssen Sie bei der Wahl von Bluetooth-Modellen keine Kosten für die Steuerzentrale und deren Betrieb berücksichtigen. Auf die Einrichtung anderer Komponenten



hat dieser Funkstandard keine Auswirkungen. Auch hier benötigen Sie die App des jeweiligen Herstellers, über die Sie die Geräte einmalig hinzufügen und anschließend konfigurieren.

Der größte Nachteil von Bluetooth ist die stark eingeschränkte Anzahl an Produkten, die Sie einbinden können. Ein anderes Manko betrifft den Mischbetrieb. Wollen Sie auf Bluetooth- und Produkte mit anderen Funktechniken eines Herstellers setzen, sind Sie oftmals auf mehrere Apps angewiesen.

Allerdings können Sie diesen Verlust an Komfort mit einer Universal-Steuerzentrale umgehen. Die unterscheidet intern zwar, auf der Bedienoberfläche ist dies in der Regel aber nicht erkennbar. Nutzen Sie einen smarten Lautsprecher respektive ein smartes Display von Amazon (Amazon Echo) oder Google (Nest) als Zentrale, ist auch die Einbindung in die jeweiligen Smart-Home-Plattformen (Amazon Alexa und Google Home) und die Bedienung per Sprache möglich. Ebenso können Sie auf diesem Wege im besten Fall verschiedene Komponenten unterschiedlicher Hersteller miteinander verknüpfen. Eine Möglichkeit, die viele nicht mit Bluetooth im Smart-Home-Umfeld in Verbindung bringen. Allerdings können Sie Firmware-Aktualisierungen in der Regel nur dann installieren, wenn die entsprechende Komponente mit dem Smartphone verbunden ist.

Mesh gibt es auch für Bluetooth

Ebenfalls weitestgehend unbekannt ist Bluetooth Mesh. Seit Bluetooth-Version 4 erlaubt der Standard vermaschte Bluetooth-Netze – zuvor waren lediglich direkte Punkt-zu-Punkt-Verbindungen möglich. Zwar erreicht Bluetooth im besten Fall Reichweiten von 200 m. In Innenräumen reicht es in der Praxis aber häufig nur für weniger als 20 m – je nach Beschaffenheit von Wänden und Decken mitunter nur für 10 m. Das bedeutet: Stehen Sie mit Ihrem Smartphone im Keller, können Sie das Türschloss im Obergeschoss mit hoher Wahrscheinlichkeit nicht steuern. Bluetooth Mesh knüpft hingegen ein Netz zwischen allen Bluetooth-Mesh-tauglichen Komponenten, darunter inzwischen auch smarte Nachrüstlösungen für Gasgrills. Ob die Komponenten dabei alle von einem Hersteller oder von mehreren stammen, spielt keine Rolle. Bluetooth Mesh ist als übergreifend arbeitendes System konzipiert, die Komponente von Hersteller A kann Daten an die von Hersteller B weiterleiten. Allerdings ist in vielen Fällen nicht ersichtlich, ob eine Komponente die Funktion überhaupt bietet. Ein guter Anhaltspunkt wäre ein Verweis auf die