Was schiefgehen kann, wird auch schiefgehen

Von Sascha Puppel und Sebastian Brose

Sascha Puppel

öffentlich bestellter und vereidigter Sachverständiger der Handwerkskammer Aachen für Sicherheitstechnik im Elektrotechniker-Handwerk inkl. Sicherheitskonzepte

sp@sicherheit-puppel.de

Die Erstveröffentlichung des Beitrags erfolgte in der Ausgabe 1/2023 der Zeitschrift s+s report.

www.vds.de/sus-report

Wir bedanken uns für die Abdruckgenehmigung.

Die Sicherungskette reicht technisch betrachtet vom einzelnen Bewegungsmelder oder Magnetkontakt über verschiedene Busmodule, Zentralen, Übertragungseinrichtungen, Alarmempfänger, Gefahrenmanagementsysteme, Leitstellen oder Interventionsstellen bis hin zur Interventionskraft. Der Weg ist lang und es gibt nicht nur viel Technik, sondern auch viele Verantwortlichkeiten in der Sicherungskette. Sowohl auf technischer als auch auf menschlicher/organisatorischer Ebene sind vielfältige Kettenglieder zu koordinieren und detaillierte Abstimmungen erforderlich. Das beginnt bei der Planung und endet bei der Intervention. Und wir alle wissen: Eine Kette ist nur so stark wie ihr schwächstes Glied.

Murphy's Law oder Kölsches Grundgesetz?

„Wenn es mehrere Möglichkeiten gibt, eine Aufgabe zu erledigen, und eine davon in einer Katastrophe endet oder sonst wie unerwünschte Konsequenzen nach sich zieht, dann wird es jemand genauso machen", formulierte einst Edward A. Murphy, Ingenieur bei der U.S. Air Force. In seiner verkürzten Form – „Alles, was schiefgehen kann, wird auch schiefgehen" – wurde die Aussage als „Murphy's Law" oder Murphys Gesetz weltberühmt. Dieses Gesetz bedeutet also, dass jedes unerwünschte, mit Schäden für Menschen und Sachen verbundene Ereignis, dessen Eintrittswahrscheinlichkeit auch noch so klein sein mag, irgendwann eintreten wird. Wir wissen nur nicht, wann. Und tatsächlich beweist sich die Wahrheit dieser Gesetzmäßigkeit im Alltag immer und immer wieder …

Im Rheinland kennt man dagegen landläufig eine andere Risikomanagementstrategie, den Artikel 3 des sogenannten „Kölschen Grundgesetzes": „Et hätt noch emmer joot jejange!" (Hochdeutsch: „Es ist noch immer gut gegangen!") Daraus wird in der Praxis nicht selten abgeleitet: „Was gestern gut gegangen ist, wird auch morgen noch funktionieren." Und leider neigt der Mensch dazu, aus den vielen Fällen, in denen sich ein Risiko nicht realisiert hat, den Trugschluss zu ziehen, das Risiko sei nicht (mehr) existent. Und bleiben wirklich einmal Restzweifel bzw. Restrisiken, werden diese mit dem „Prinzip Hoffnung" aufgewogen.

Oftmals bleibt uns auch nichts anderes übrig als zu hoffen, wenn die Kosten für die Sicherheit in einem ausgewogenen Verhältnis zum erwarteten Schadenausmaß stehen sollen. Oder, wie es die Versicherungslehre definiert: „Risiko ist die Möglichkeit des Schadeneintritts durch Verwirklichung einer versicherten Gefahr, also Risiko = Schadenhöhe x Eintrittswahrscheinlichkeit." Diese Berechnung birgt allerdings die Gefahr, dass wir davon ausgehen, dass das errechnete Risiko de facto zu vernachlässigen ist! Murphy lehrt uns jedoch, dass alles, was eine Eintrittswahrscheinlichkeit größer null hat, auch irgendwann eintreten wird. Wenn der hierbei zu erwartende Schaden erheblich bzw. nicht tolerierbar wäre, sind wir im Rahmen des Risikomanagements verpflichtet, uns damit zu beschäftigen.

Im Schadenfall und bei Gerichtsverfahren wird diesbezüglich gerne ein altes Gerichtsurteil des Oberverwaltungsgerichts Münster aus dem Jahr 1987 zitiert: „Es entspricht der Lebenserfahrung, dass mit der Entstehung eines Brandes praktisch jederzeit gerechnet werden muss. Der Umstand, dass in vielen Gebäuden jahrzehntelang kein Brand ausbricht, beweist nicht, dass keine Gefahr besteht, sondern stellt für die Betroffenen einen Glücksfall dar, mit dessen Ende jederzeit gerechnet werden muss." (AZ: 10 A363/86 vom 11. Dezember 1987)

Aus der Luftfahrt kennt man daher das Prinzip der Redundanz: Ein einzelner Fehler darf nicht zum Absturz führen. Deswegen sind viele Systeme zwei- oder sogar dreifach vorhanden und es gibt viele Rückfallebenen. Ebenso verhält es sich in der Sicherheitstechnik. Die Autoren von VdS-Richtlinien und Normen versuchen stets, eventuelle Ausfälle, Störungen oder Angriffe gedanklich zu antizipieren und einen „Plan B" in den Standards zu verankern. So gibt es Anforderungen an eine Notstromversorgung, zwei Übertra-

gungswege und einen Alarmplan für den Fall, dass trotzdem alles ausfällt. Und das nicht etwa, weil man den in der Praxis tätigen Planern und Errichtern Fehler unterstellt, sondern, da sich diese „Hosenträger zum Gürtel" meist aus sich fortwährend ändernden Tätervorgehensweisen ableiten. Das ist in der Sicherheitswelt nichts Neues und bereits seit Jahrhunderten bekannt, jedoch heute in einer ganz anderen Qualität und Quantität sowie zum Teil beeindruckend schneller Weiterentwicklung auf der Täterseite.

Die Praxis zeigt, dass es oft nicht der eine riesige Fehler ist, der zu einem großen Schaden führt, sondern eher die Mehrzahl kleinerer Fehler unterschiedlicher Personen, die sich „aufsummieren". Schnell spricht man von der „Verkettung ungünstiger Umstände". Objektiv und ehrlich betrachtet sind es aber nicht „ungünstige Umstände", sondern Kleinigkeiten, die nach dem oben zitierten „kölschen Grundsatz" eigentlich hätten gut gehen sollen. „Eigentlich"…

Man kann also – egal ob als Planer, Errichter, AES, Interventionsstelle oder Betreiber/Risikoträger – an vielen Stellen viel falsch machen. Aber kein Fehler ist so schlecht, dass man nicht noch etwas daraus lernen könnte. In dem Sinn soll dieser Beitrag praktische Erfahrungen widerspiegeln und Anregungen geben, wo sich ein genauerer Blick als lohnenswert erweisen könnte.

Planung und Errichtung

Bereits in s+s report 3/2019 (S. 34–37) wurde darauf hingewiesen, dass der Auswahl der Melder eine entscheidende Bedeutung zukommt. Auch die richtige Planung, Auswahl, Positionierung und Montage wurde bereits thematisiert (s+s report 2/2020, S. 42–45). Selbstverständlich müssen Melder passend zu den zu erwartenden Umgebungsbedingungen ausgewählt werden. Jedoch darf der Fokus nicht nur auf der Falschalarmsicherheit liegen, sondern auch die Detektionssicherheit als Kernaufgabe muss hinreichend durchdacht werden. Letzteres wird durch den Einsatz von Dualbewegungsmeldern, wenn es dafür keinen sachlichen Grund gibt, konterkariert.

Bei der Montage sollte die Installationsanleitung des Herstellers gewissenhaft gelesen und befolgt werden. Die dort gemachten Angaben sind ebenso Teil der VdS-Anerkennungsprüfungen wie das Produkt selbst. Oft enthalten die Anleitungen wertvolle Hinweise zu Optionen und Einstellmöglichkeiten, die – aus gutem Grund – in VdS- Anlagen erforderlich oder nur auf eine bestimmte Art und Weise zulässig sind. Jedoch sind die speziellen Anforderungen für VdS-Anlagen in Montageanleitungen auch für alle anderen – also nicht VdS-konformen – Anlagen sinnvoll.

Als Beispiel sei hier der Abhebekontakt genannt. Je nach Fabrikat muss dieser gesondert bestellt werden, ist nur bei der Nutzung bestimmter Befestigungspunkte aktiv oder es müssen bestimmte Empfindlichkeitseinstellungen vorgenommen werden. Werden diese Aspekte nicht beachtet, besteht ein Mangel an der VdS-Konformität der installierten Anlage mit u. U. weitreichenden Konsequenzen, wie Haftungsschäden, Mängelbeseitigung auf eigene Kosten etc.

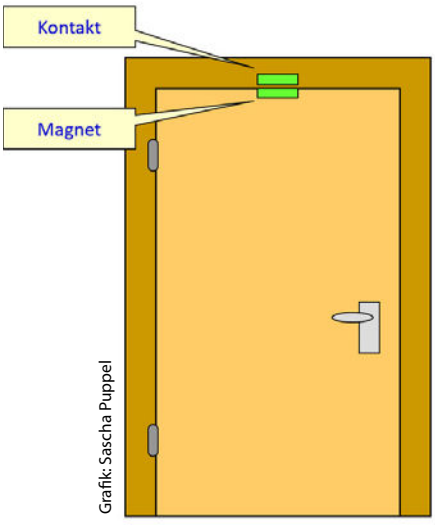
In den vergangenen Jahren ist im Rahmen von begutachteten Schäden deutlich geworden, dass Täter das Verdrehen von Bewegungsmeldern – also die Veränderung des Überwachungsbereiches – als zielführende Überwindungsmethode für sich erkannt haben (siehe auch s+s report 2/2021, S. 38–39).

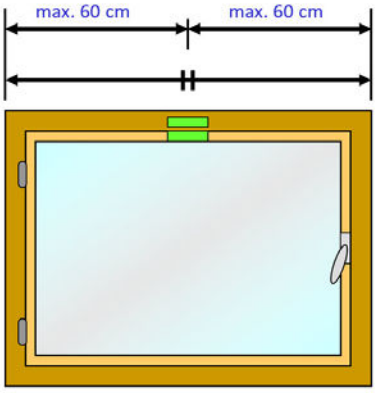
Das Beachten von Anleitungen ist nicht nur bei der physischen Installation von Bedeutung, sondern – in Zukunft wohl in zunehmendem Maße – auch für die softwareseitige Parametrierung. Als Beispiel sei genannt, dass bei manchen RFID-Lesern, die zur Scharf-/Unscharfschaltung eingesetzt werden, der für den VdS-konformen Betrieb vorgesehene Verschlüsselungsmodus bewusst aktiviert oder ausgewählt werden muss. Am Markt sind mittlerweile zahlreiche günstige Tools zum Auslesen und Kopieren von diversen RFID-Typen frei verfügbar. Auch die Sicherheitseinstellungen für Passwörter, Fernzugriff und evtl. Steuerfunktionen müssen kritisch geprüft werden. Salopp formuliert: Es reicht also nicht,

Sebastian Brose
Dipl.-Wirtschaftsjurist (FH)

ist stellv. Bereichsleiter und Abteilungsleiter Produktmanagement im Bereich Produkte und Unternehmen bei der VdS Schadenverhütung GmbH

sbrose@vds.de



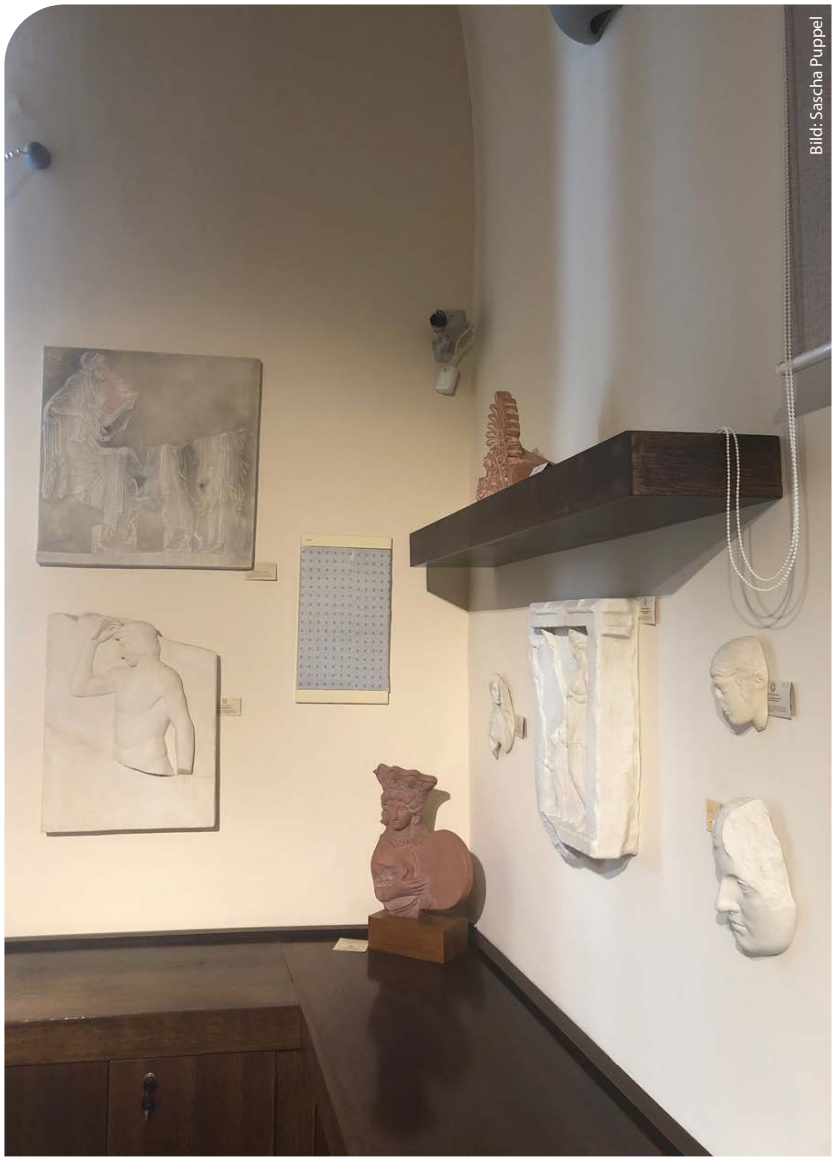


In den Richtlinien VdS 2311 werden wichtige Hinweise zur richtigen Platzierung von Magnetkontakten gegeben.

ein gutes Produkt richtig zu planen und an die Wand zu schrauben – man muss es auch richtig einstellen.

Am Ende der Installation und vor ihrer Übergabe und Inbetriebnahme muss eine einhundertprozentige Überprüfung der Anlage stattfinden. In der Praxis ist es schon vorgekommen, dass man bei der Programmierung der Zentrale vergessen hat, z. B. einem Melder in Bus- oder Funktechnik eine Meldergruppe zuzuweisen. Prüft man den Melder nur per Gehtest-LED, fällt das nicht auf, da diese meist lokal angesteuert wird. Deswegen sollten die Prüfungen möglichst von Ende zu Ende durchgeführt werden, um die ganze Wirkungskette einzubeziehen. Dies gilt nicht nur für die Inbetriebnahmeprüfung, sondern auch für alle Inspektionen.

Zunehmend gewinnt die Cybersecurity der Anlagen und ihrer Konfigurationen an Bedeutung, vor allem durch neue Use-Cases und Geschäftsmodelle, die auf Remote-Services basieren. Die DIN EN 50710 und der VdS-Quick-Check für Errichter von Gefahrenmeldeanlagen (GMA) bieten gute Grundlagen, die Sicherheit auch dieser Aspekte im Blick zu halten und zu steuern.



Hier wurde ein Melder so verdreht, dass er in Richtung Decke zeigte und dadurch nutzlos wurde.

Alarmübertragung

Eine weitere Fehlerquelle ist die Alarmübertragung. Leider offenbart sich oftmals erst im Schadenfall, dass – entgegen der Vereinbarung und den Angaben im Attest bzw. in der Anlagenbeschreibung – keine „echte" DP4-Übertragung mit VdS-SecurIP parametriert oder gelebt wurde. DP4 bedeutet eben mehr als nur zwei Übertragungswege zur Leitstelle. Die zugrunde liegende Norm definiert eine Reihe von Leistungsmerkmalen und Funktionalitäten, die nur in ihrer Gesamtheit die erwartete Wirkung entfalten. Dazu gehört z. B., dass beim Ausfall des ersten Übertragungsweges die Überwachungszeit des zweiten Weges von fünf Stunden auf 90 Sekunden sinkt. Wird dieser Punkt nicht beachtet, dauert es bis zu fünf Stunden, bevor der Ausfall beider Übertragungswege erkannt wird! Zeit genug für einen Einbrecher.

In der Praxis werden teilweise veraltete Montage- bzw. Programmieranleitungen verwendet. Es sollten selbstverständlich stets aktuelle Dokumentationen und Anleitungen verwendet werden, die Änderungen an VdS-Richtlinien und Normen, aber auch Hard-/Softwareänderungen, Kompatibilitäten usw. berücksichtigen.

Ursachen für Fehler lauern auch bei einer unzureichenden Abstimmung mit der AES/NSL in Verbindung mit dem Betreiber der Anlage und der notwendigen Interventionsmaßnahmen. Um diese Information zu verbessern und zu standardisieren, steht neben dem Alarmdienst- und Interventionsattest auch der neue Anhang des EMA-Attests VdS 2170 zur Verfügung. Hiermit können die wichtigsten Informationen zur Anlage an die NSL dokumentiert übermittelt werden, was auch bei späteren haftungsrechtlichen Fragestellungen von erheblicher Bedeutung sein kann.

Alarmempfang/Alarmdienst

Zum Alarmdienst und der Aufgabe einer NSL gehört es zunächst, dass ein Kunde im Wege der Aufschaltung fachkundig beraten wird, und – ggf. in Absprache mit dem Errichter und Versicherer – risikogerechte Maßnahmen für den Fall von Alarmen und Störungen vereinbart werden. Leider sind Kunden, die eine mehrere Tausend

Euro teure Anlage haben installieren lassen, dann oft nicht bereit, die adäquate Sicherungsdienstleistung zu bezahlen. Sie scheuen etwaige Kosten für Falschalarmeinsätze und vereinbaren stattdessen: „Bei Einbruch oder Sabotage zunächst den Chef anrufen und auf weitere Anweisungen warten. Bei Sabotage oder Störungen nur Mo–Fr zwischen 8 und 18 Uhr anrufen." Derartig sinnfreie Interventionsmaßnahmen wurden in der Vergangenheit nicht selten auch bei Objekten mit hohem Sicherheitsbedürfnis umgesetzt, selbst bei Banken. Solche Maßnahmenpläne verdienen nicht nur den Namen nicht, sondern führen die ganze Investition in die Anlage ad absurdum. In aller Regel hat der Errichter einen richtig guten Job gemacht, jedoch war das schwächste Glied der Kette viel zu oft die Intervention bzw. die Interventionsmaßnahmen.

Und in der Praxis sind genau das die Punkte, wo Täter – mit Insiderwissen der Branche – ansetzen: Wenn nach einem Sabotageangriff eine gewisse Zeit lang nichts passiert, können sie in aller Ruhe zu Werke gehen und brauchen die Entdeckung nicht zu fürchten. Auch ist es keine Seltenheit, dass Täter bewusst mehrfach Alarme auslösen, die vermeintlich als Falschalarme interpretiert werden, um ein Abstumpfen oder Ausblocken/Abschaltung zu erreichen. Ein Sabotagealarm darf nicht einfach nur durch eine beliebige Person, z. B. der Interventionskraft, zurückgesetzt werden. Hier muss der Errichter (i. d. R. vor Ort) die Ursache ergründen, die betroffenen Geräte einer umfassenden Sicht- und Funktionsprüfung unterziehen sowie evtl. Sabotagehandlungen erforschen. Der Betreiber oder die Interventionskraft ist dazu nicht in der Lage.

Mittlerweile verfügen professionelle Täter nicht nur über umfassende Fachkenntnisse über die wesentlichen Komponenten der Sicherheitstechnik und insbesondere deren Überwindungsmöglichkeiten, sondern unsere Gegenspieler kennen oftmals auch detailliert die internen Abläufe bei Errichtern, Alarmempfangsstellen und Interventionsstellen. Dies gilt insbesondere für die Abläufe bei Errichtern hinsichtlich Instandsetzungen und speziell für den Umgang mit Sabotagealarmen und deren Löschung durch Servicetechniker und – leider viel zu oft – unzulässigerweise durch den Betreiber selbst. Nicht selten werden hier die Errichter bzw. deren Techniker durch Betreiber mit Verweis auf die angeblich so hohen Kosten dazu genötigt, auf einen – eigentlich dringend erforderlichen – Technikereinsatz vor Ort (ggf. in der Bereitschaft außerhalb der Geschäftszeiten) zu verzichten.

Oftmals werden auch Techniker bzw. Bereitschaftstechniker, wenn diese vor Ort tätig werden dürfen, durch den Betreiber unter Zeitdruck gesetzt. Somit können die Techniker ggf. nicht alle erforderlichen Sicht- und Funktionsprüfungen mit der notwendigen Sorgfalt durchführen. Gerne wird hier das Argument angeführt, dass der Mitarbeiter des Betreibers noch einen privaten Termin hat und eigentlich nur noch schnell die Anlage scharf schalten können möchte. Werden die eigentlich sofort erforderlichen Sicht- und Funktionsprüfungen auf einen Folgetermin in den nächsten Tagen während der Geschäftszeiten verschoben, kann dies zu spät sein, wenn der Täter in der darauffolgenden Nacht zuschlägt und die vorher vorgenommene Manipulation o. Ä. ausnutzt.

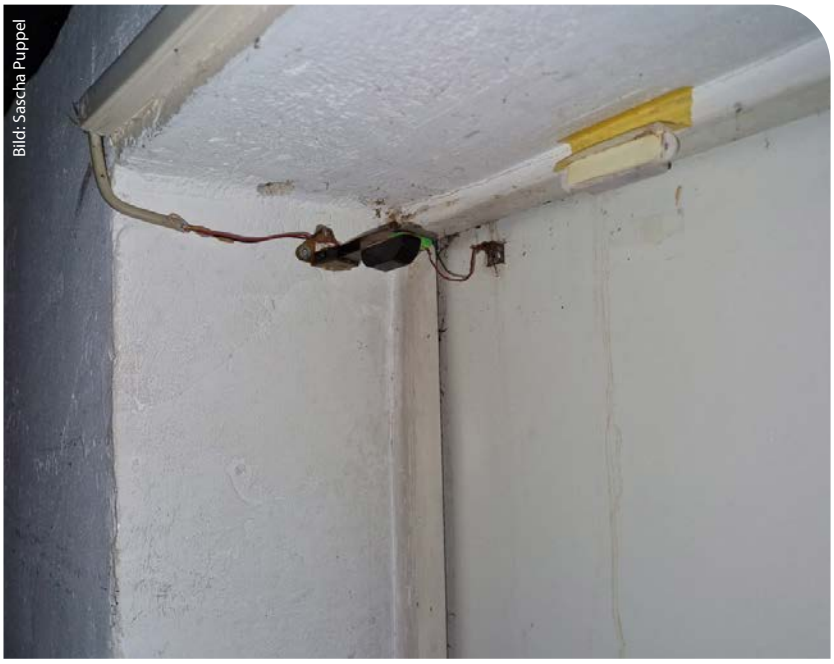


Bild: Sascha Puppel

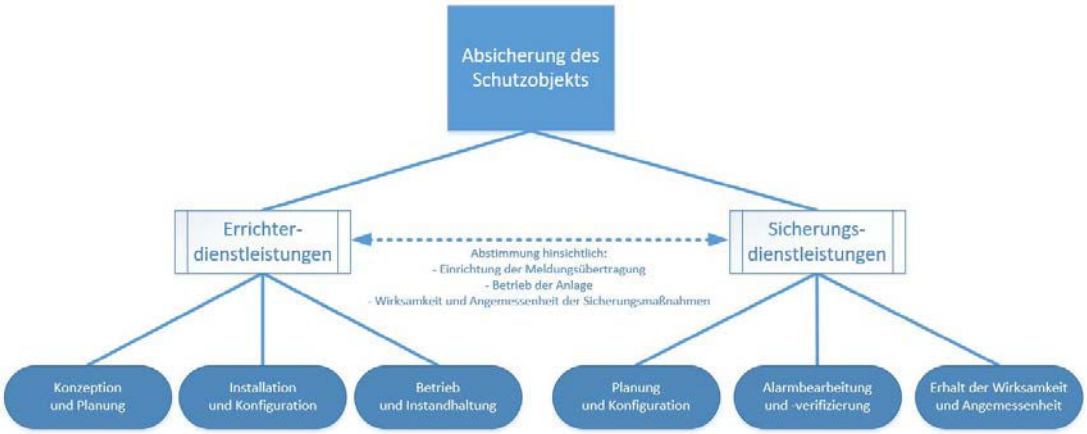
Hier addieren sich gleich mehrere Fehler auf, Einbrecher haben leichtes Spiel.

Die daraus resultierenden und nachfolgend beschriebenen Praktiken sind deshalb absolut gefährlich und begünstigen Schadenfälle und Haftungsansprüche der Beteiligten:

Errichter, insbesondere Bereitschaftstechniker, erklären telefonisch dem Betreiber, wie z. B. ein Sabotagealarm gelöscht werden kann (inkl. dem Öffnen der Einbruchmeldezentrale (EMZ) und dem Betätigen der Reset-Taste).

Der Errichter fährt vielleicht zum Objekt und setzt einen Sabotagealarm zurück, überprüft aber nicht, ob die betroffenen Geräte (z. B. Melder, Kontakte, Sensoren) noch voll funktionstüchtig sind und nicht manipuliert wurden (z. B. ob in dem Verteiler oder Busmodul die Alarmspinne noch angeschlossen ist oder ob der Bewegungsmelder noch die vollständige Reichweite bzw. den erforderlichen Überwachungsbereich hat).

Der Errichter blockt gestörte Melder per Fern-



Grafik: VdS

Bei der Absicherung eines Objekts greifen die unterschiedlichsten Dienstleistungen ineinander – und überall können Fehler gemacht werden.

zugriff aus, statt die Störung vor Ort zu ergründen. Täter kennen und nutzen dieses Verhalten und die Prioritäten von Betreibern und Errichtern aus (kurz vor Feierabend, kurz vor dem Wochenende, wo niemand noch auf einen Technikereinsatz warten möchte, oder z. B. im Einzelhandel gerne am Samstagsnachmittag):

Fallen bei einer DP4-Verbindung beide Übertragungswege aus, muss die Leitstelle so reagieren, als läge ein Einbruch- oder Überfallalarm vor. Das ist die „dritte Redundanz". Würde diese Anforderung der Richtlinien in der Praxis eingehalten, gäbe es weit weniger Schäden oder zumindest deutlich geringere Schadenausmaße. Täter wissen um diese Lücken. Sie kappen beide Übertragungswege und warten aus sicherer Distanz ab. Wenn nach einiger Zeit nichts passiert, haben sie „freie Bahn".

Intervention

Das letzte Glied in der Sicherungskette ist die Tätigkeit der Interventionskraft vor Ort. Bei einem Alarm ist es erforderlich, das Objekt gründlich abzusuchen, sowohl innen als auch außen. Clevere Täter verstecken sich z. B. in der Abhangdecke und haben ggf. von dort sogar einen Blick auf das Bedienteil der Einbruchmeldeanlage und können somit erkennen, ob die Anlage scharf geschaltet wurde. Keinesfalls darf voreilig von einem Falschalarm ausgegangen werden. Der ursprüngliche Sicherheitszustand muss wiederhergestellt werden. Betreiber, die aus Kostensparüberlegungen heraus bei einer Störung auf eine unmittelbare Instandsetzung oder kompensierende Bewachung verzichten, müssen von einem gewissenhaften Dienstleister auf das Risiko hingewiesen werden.

Ursachen

Abschließend wollen wir einen Blick auf die Ursachen der oben beschriebenen Fehler werfen.

Es gibt keinen eigenen Ausbildungsberuf für Sicherheitstechniker. Planer und Errichterunternehmen müssen selbst den Mitarbeitern alle notwendigen Kompetenzen vermitteln. Gleichzeitig erweckt die Technik immer mehr den Anschein von „Plug & Play", doch die Tücken stecken oft im Detail.

Technik und technische Möglichkeiten werden immer komplexer. Die Menschen, die als Planer, Techniker, Dienstleister, Entscheider, Versicherer usw. damit umgehen müssen, sind aber oft nicht (mehr) die „EMA- Spezialisten", sondern mehr und mehr „Generalisten", die sich zwangsläufig nicht so tief in die Materie einarbeiten können. Dies gilt insbesondere für Planungsbüros, die dem Irrglauben anhängen: „Wir können Elektroplanung, da machen wir so ein bisschen Sicherheitstechnik mal eben mit." Oftmals muss es dann der Errichter ausbaden oder er traut sich im schlimmsten Fall nicht, den Planer auf seine Fehler hinzuweisen. Er möchte ja noch weitere Aufträge von diesem Planer erhalten. Auch die Sachverständigen sind als Fehlerquelle nicht ausgeschlossen. Am Markt sind „Allround-Elektro-Sachverständige" tätig, die den Eindruck vermitteln, sich mit allen Bereichen der Elektrotechnik inklusive der gesamten Sicherheitstechnik auszukennen. Dies gilt insbesondere für eine Vielzahl von selbsternannten Sachverständigen, da die Bezeichnung „Sachverständiger" – bis auf den öffentlich bestellten und vereidigten Sachverständigen – gesetzlich nicht geschützt ist. Jedoch sind auch unter den öffentlich bestellten und vereidigten Sachverständigen solche selbsternannten Allrounder zu finden. Im Zweifelsfall muss der Sachverständige dann seinen, wie so oft in Gerichtsurteilen zitierten und erforderlichen, „deutlich überdurchschnittlichen Sachverstand" beweisen.

So bleibt vieles im Grauen und die Probleme treten oft erst im Schadenfall zutage. Hinzu kommt die deutlich gestiegene Frequenz, mit der Änderungen in der Produktwelt, aber auch

im Segment der Normen und Richtlinien in den Markt getragen werden.

Die Erfahrung aus anderen Bereichen zeigt auch: Gerade in der zunehmend softwaredominierten Welt ist eine gute Fehlerkultur unerlässlich. Ein Update ist kein Drama, sondern eine gern angenommene Verbesserung. Das Ausbleiben von Updates macht hingegen misstrauisch. Die in unserer Branche und insbesondere bei Herstellern noch nicht so stark ausgeprägte Fehlerkultur verhindert oft den offenen und transparenten Umgang mit Verbesserungen oder Bugfixes usw. Das betrifft sowohl die Firmware als auch die Parametrierung.

Manchmal hört man landläufig Aussagen wie: „Wenn die Einbruchmeldeanlage nicht gemäß VdS-Richtlinien 2311 attestiert werden muss, dann kann die Anlage gebaut werden, wie der Errichter es für sinnvoll erachtet." Daraus resultiert nicht immer, dass die Anlage gemäß DIN VDE 0833 Teil 1 und Teil 3 umgesetzt wird sowie ggf. vorhandene Abweichungen mit allen Beteiligten vereinbart und dokumentiert werden.

Auf solchen falschen Vorstellungen gründen einige der in diesem Artikel bzw. der anderen v. g. Beträge beschriebenen typischen Fehler, und gerne wird u. a. bei der falschen Wahl von Montageorten für Bewegungsmelder hierüber diskutiert.

Grundsätzlich gilt, dass auch bei nicht VdS-attestierten Einbruchmeldeanlagen die entsprechenden „Allgemein anerkannten Regeln der Technik" (z. B. DIN VDE, MLAR) sowie auch die Montageanleitungen der Gerätehersteller zu beachten sind.

Am Beispiel eines falsch positionierten Bewegungsmelders lässt sich das konkretisieren: Nicht nur die VdS-Richtlinien und Normen, sog. „allgemein anerkannte Regeln der Technik" (a. a. R. d. T., siehe Kasten), sondern fast immer auch die Montage- und Installationsanleitungen zu den Bewegungsmeldern beschreiben genau, wie diese Melder zu installieren sind. Vor optischen oder praktischen Erwägungen wie etwa unsichtbarer Leitungsverlegung treten diese Regeln in den Hintergrund. Die Folge: Nicht selten reagieren diese Melder dann bei einem Einbruch zu spät oder überhaupt nicht.

Haftungsrechtlich ist es aus diesem Grund immens wichtig, dass der Errichter, wenn der Kunde eine Abweichung von den allgemein anerkannten Regeln der Technik fordert, diese auch nicht nur schriftlich – mit Bestätigung des Kunden – dokumentiert, sondern dass er besonders auch auf die Risiken und Gefahren hinweist, die sich durch die Abweichung ergeben.

Fazit

Es ist und bleibt spannend, getreu dem Kölschen Grundgesetz, Artikel 5: „Et bliev nix wie et wor" (Es bleibt nichts wie es war). Also sind wir offen für Neuerungen. Dies gilt insbesondere für die wesentlichen Regelwerke in unserer Sicherheitstechnikwelt, wie DIN VDE 0833 und VdS-Richtlinien.

VdS-Richtlinien erfüllen immer auch einschlägige Normen und geben auch dann wertvolle Orientierung, wenn keine VdS-Anlage gefordert ist. Wer die VdS-Richtlinien einhält, stellt damit immer auch sehr weitgehend sicher, dass er die allgemein anerkannten Regeln der Technik einhält. Als Leitfaden, Planungs- bzw. Montagehilfe und als Ratgeber sind daher – auch bei nicht VdS-attestierten Einbruchmeldeanlagen – die Richtlinien VdS 2311 und VdS 3134 dringend zu empfehlen. Sie geben auch wertvolle Hinweise für die Praxis (z. B. für die Montage/Anordnung von Magnetkontakten).

Auch wenn die VdS-Richtlinien aus Köln stammen, sollte hier jedoch nicht der Artikel 9 des Kölschen Grundgesetzes („Wat soll dä Kwatsch?" – „Was soll das sinnlose Gerede?") angewandt werden! Einen informativen und gebündelten Überblick für die wesentlichen Gewerke der Sicherheitstechnik sowie deren Anforderungen verschaffen auch die Praxisratgeber des BHE.

Allgemein anerkannte Regeln der Technik (a. a. R. d. T.)

Normen wie etwa die DIN VDE 0833-1/-3 haben nicht grundsätzlich einen Gesetzescharakter und ihre Anwendung ist so gesehen freiwillig. Weite Teile der Definitionen in diesen Normen stellen jedoch regelmäßig „allgemein anerkannte Regeln der Technik" (a. a. R. d. T.) dar.

Wurde im Rahmen der vertraglichen Vereinbarung zur Errichtung einer Einbruchmeldeanlage nicht die Beachtung der für das Projekt und Objekt entsprechenden Normen vertraglich vereinbart, so wird gerne – spätestens im Schadenfall – ausgiebig diskutiert, nicht selten langwierig und mit völlig ungewissem Ergebnis vor Gericht.

Ganz besondere juristische Bedeutung wird den allgemein anerkannten Regeln der Technik zuteil, weil bei Nichtbeachtung der entsprechenden Sicherheitsmaßnahmen zum Schutz von Leib, Leben und Sachwerten sehr schnell die Frage verhandelt wird, ob fahrlässiges Verhalten vorliegt.

Durch die gesetzlichen Regelungen, z. B. in den Landesbauordnungen (LBO), dass die allgemein anerkannten Regeln der Technik zu beachten sind, wird eine weitere rechtliche Grundlage für die strafrechtliche Verfolgung bei Zuwiderhandlung durch den Gesetzgeber geschaffen. In besonderen Ausnahmefällen – wie bei einzelnen Abweichungen – ist dieser Umstand dringend vor der Realisierung zu prüfen.

Zusammengefasst besteht also insbesondere in allen sicherheitsrelevanten Bereichen der Elektrotechnik eine „Quasi-Anwendungspflicht" von VDE-Bestimmungen und Normen. Jedoch können nicht nur Festlegungen in Normen die allgemein anerkannten Regeln der Technik widerspiegeln, sondern auch – insbesondere im Bereich der Einbruchmeldetechnik – einzelne Inhalte aus VdS-Publikationen wie den Richtlinien VdS 2311 und VdS 3134.

Im Rahmen der a. a. R. d. T. sind auch alternative – zu den in den Normen beschriebenen – Maßnahmen zulässig, die gleichwertige Ergebnisse erzielen. Jedoch ist der Nachweis der gleichwertigen Sicherheit der Alternativmaßnahmen für den Errichter oft schwer zu erbringen, wohingegen bei Einhaltung der Normen keine Fragen entstehen.