Frühjahr 2026

SECCOM

INSIDES

Perspektiven aus ITK, Gebäudesicherheit und Gesundheitswesen

Foto: istock, wiksarut sakorn

MobiCloud: Mehr Sicherheit für alle

Seite 8
Sensorik entlastet Personal
Kirsch Pflegeeinrichtungen

Seite 10
Contact-Center im Wandel
Servicechancen durch KI

Seite 12
Kommunikationssysteme
Schutzregeln beachten

Inhalt

Foto: phive2015 - istockphoto.com

Foto: DOM

04 **Titelthema**
Sicherheitsplus auch für kleine Anwender

06 **Healthcare**
Effizienz trifft Empathie

07 Energiekosten jetzt reduzieren

08 **Healthcare**
Anwenderbericht
Kirsch Pflegeeinrichtungen

10 **Kommunikationstechnik**
Künstliche Intelligenz verändert
Contact-Center

11 Voicebot für Routineanrufe

12 **Kommunikation und Sicherheit**
Systeme vor Sicherheitsrisiken schützen

14 **IT-Sicherheit**
Handlungsbedarf durch NIS-2-Regelung

15 Staatliche Förderprogramme

Impressum:

Herausgeber:

SEC-COM Sicherheits- und
Kommunikationstechnik GmbH
Bochumer Str. 6
45661 Recklinghausen
Tel.: 02361/9322-0
E-Mail: info@sec-com.de

Redaktion SEC-COM:
Folker Lück, tellyou redaktionsbüro

Layout & Umsetzung:
Tanja Otterbein, SEC-COM GmbH

Reproduktion & Vervielfältigung:
Nur nach ausdrücklicher
Genehmigung der SEC-COM GmbH

qualityaustria
SYSTEMZERTIFIZIERT
ISO 9001:2015 NR.21628/399

Willkommen im neuen SEC-COM **INSIDES**

Liebe Leserinnen und Leser,

Digitalisierung bedeutet längst nicht mehr nur, Prozesse effizienter zu gestalten, sondern sie schafft neue Verbindungen zwischen Welten, die früher getrennt waren. IT-Security, Kommunikationsinfrastruktur und Gebäudeschutz verschmelzen zunehmend zu einem gemeinsamen Ökosystem, in dem Daten, Geräte und natürlich wir Menschen nahtlos interagieren. Genau aus diesem Grund führen wir unsere beiden bisherigen Kundenpublikationen, das Sicherheitsmagazin SEC-COM Security und das Telekommunikationsmagazin SEC-COM Display, jetzt zu einem neuen, gemeinsamen Format zusammen: dem Magazin SEC-COM Insides.

Diese Entscheidung spiegelt eine Entwicklung wider, die wir täglich in Projekten und im Austausch mit unseren Kunden beobachten. Wenn heute eine Produktionshalle vernetzt wird, ist das keine Frage mehr einzelner Systeme, sondern eines ganzheitlichen Ansatzes. Eine moderne Kommunikationslösung sorgt nicht nur für reibungslose Zusammenarbeit, sie trägt aufgrund verschlüsselter Übertragung auch aktiv zur IT-Sicherheit bei. Ebenso sind Zutrittskontrollsysteme längst digital vernetzt und Teil der Unternehmens-IT – sie kommunizieren über IP. Moderne Cloud-Plattformen müssen denselben Sicherheitsstandards genügen wie sämtliche Infrastruktur, die vor Ort „on premise“ in Betrieb ist.

Kleine und mittelständische Unternehmen stehen heute an einem entscheidenden Punkt: Die Grenzen zwischen physischer und digitaler Sicherheit lösen sich auf, während die Anforderungen an Verfügbarkeit, Datenschutz und Skalierbarkeit massiv wachsen. Nicht zuletzt trägt die geopolitische Lage dazu bei, dass wir alle diese Themen heute außerordentlich ernst nehmen müssen. SEC-COM Insides begleitet Sie genau in diesem Spannungsfeld. Wir möchten nicht mehr getrennt über Sicherheits- oder Kommunikationslösungen berichten, sondern über das Zusammenspiel von beidem – praxisnah, verständlich und mit Blick auf die Chancen, die sich daraus ergeben.

Mit dieser ersten Ausgabe starten wir in eine neue Phase. Wir laden Sie ein, mit uns über das nachzudenken, was unsere vernetzte Welt wirklich besser und sicherer macht – intelligente, integrierte Systeme und Menschen, die das Potenzial dieser Verbindungen verstehen und gestalten.

Herzlichst, Ihr

Guido Otterbein
Geschäftsführer und Inhaber

Alarmserver-Lösung aus der Cloud gehosted von SEC-COM und NTB

Sicherheitsplus auch für kleinere Anwender

Foto: istock, alvarez

Foto: istock, V

Alarmserver kennt man aus Krankenhäusern oder aus der Industrie. Für kleinere Anwender wie Arztpraxen, Anwaltskanzleien oder den Bildungsbereich waren diese Lösungen bislang oft zu groß und damit auch zu kostspielig. Moderne Cloud-Technologie und die Kooperation zweier renommierter Systemhäuser sorgen jetzt dafür, dass die Technik auch für kleinere Anwender perfekt passt.

Alarmserver können per Tastendruck für Schutz und schnellste Hilfe sorgen. Beispielsweise dann, wenn Mitarbeitende (z.B. am Empfang) von Kunden bedroht werden. Ein Alarm kann aber auch dann ausgelöst werden, wenn etwa eine wichtige IT-Lösung versagt, oder sich ein Mitarbeiter bei Wartungsarbeiten plötzlich nicht mehr bewegt. Tritt unerwartet Gas, Wasser oder Rauch aus, kann ein Alarmserver ebenfalls für schnellste Sicherheitsmaßnahmen sorgen.

Wie Alarmserver funktionieren

Basis der Technologie ist eine zentrale Plattform, die Störungen oder Meldungen aus verschiedenen Systemen sammelt, auswertet und gezielt an zuständige, zuvor definierte Personen weiterleitet. Erhalt und Auslösung sind über unterschiedlichste Wege, beispielsweise per Telefon, SMS, E-Mail oder App möglich. Kritische Ereignisse werden somit nicht nur sofort erkannt, sondern auch zuverlässig bearbeitet.

Moderne Alarmserver lassen sich dabei nahtlos in vorhandene IT-, Telefonie- und Sicherheitsinfrastrukturen integrieren. Über standardisierte Schnittstellen können vorhandene Systeme meistens ganz einfach angebunden werden. Ein Zusammenspiel mit Zugangskontrollsysteme, Feueralarmen, Einbruchmeldeanlagen, Video- oder Umgebungsüberwachung ist möglich.

Wofür Alarmserver eingesetzt werden

Zum Einsatz kommt ein Alarmserver überall dort, wo schnelle Reaktionszeiten entscheidend sind – entweder für die Betriebssicherheit oder sogar für Menschenleben. Weit verbreitet ist der Einsatz in Rechenzentren, in Krankenhäusern, in Leitstellen, bei Energieversorgern oder im Facility Management. Klar ist: Hier dürfen Alarme niemals übersehen werden. Notfallprozesse sind genau festgelegt, eingeübt und sie müssen reibungslos ablaufen.

Doch auch im kleineren Maßstab ist die Technologie wertvoll: In Anwaltskanzleien oder Arztpraxen kommt es leider immer häufiger vor, dass sich Patienten oder Klienten ungehalten bis aggressiv verhalten. Hier kann der Technologieeinsatz dafür sorgen, dass in solchen Extremfällen diskret, aber unverzüglich ein privater Sicherheitsdienst oder die Polizei alarmiert wird. Das gleiche gilt auch für Schulen oder andere Bildungseinrichtungen. Ambulante Pflegedienste oder therapeutische Praxis können die Technik nutzen, wenn es Patienten plötzlich schlecht geht oder wenn Mitarbeitende von Patienten bedroht oder belästigt werden.

Alarmserver leisten aber auch dann wertvolle Hilfe, wenn es nicht um potentielle Gewalttäter geht: Kommt beispielsweise eine normalerweise automatisch arbeitende Abfüllanlage außerplanmäßig zum Stehen, wird in einem Raum eine bedrohliche Gaskonzentration gemessen oder muss ein Gebäudeteil schnellstmöglich evakuiert werden, kann ein Alarmserver ebenfalls dafür sorgen, dass quasi in Echtzeit ein zuvor definierter Personenkreis informiert wird, der dann unverzüglich für Abhilfe oder weitere Maßnahmen sorgt.

Einsatzbereit ab 69 Euro Monatskosten

Bisher waren solche Lösungen gerade für Freiberufler, kleine Bildungseinrichtungen oder kleinere Produktionsbetriebe überdimensioniert und somit auch kaum erschwinglich. Ein Produkt des renommierten Anbieters NewVoice – gehostet von SEC-COM und NTB – ermöglicht jetzt aber einen Einstieg in die Technologie ab 69 Euro Monatskosten. Wir meinen: Damit gibt es keinen Grund mehr, auf dieses Plus an Sicherheit zu verzichten.

SEC-COM setzt hier auf modernste – aber erprobte - Technologie, aus der sich unter dem Strich ein Preisvorteil ergibt: Während Alarmserver früher stets stationär vor Ort („on premise“) integriert und betrieben werden mussten, stellt die MobiCloud eine zentrale Plattform dar, die komplett aus der Cloud heraus eingesetzt wird. Die Lösung ist sofort nutzbar und flexibel skalierbar. Die Technologie stammt von dem europäischen Spezialisten New Voice International AG. Das Unternehmen besteht seit 1991. Es fokussiert seit jeher das Alarm- und Notfallmanagement. Das Hosting der Cloud-Lösung erfolgt an zwei Standorten durch SEC-COM und durch das ostwestfälische Systemhaus NTB. Durch das Hosting von zwei New Voice-Partnerunternehmen an zwei Standorten bietet die MobiCloud eine besonders hohe Ausfallsicherheit.

Die Infrastruktur verteilt sich auf getrennte, georedundante Systeme, die unabhängig voneinander betrieben werden. So bleibt die Technologie selbst bei Wartungsarbeiten, Störungen oder Ausfällen an einem Standort jederzeit verfügbar. SEC-COM und NTB verfügen über eigenes, technisches Know-how, setzen gleichermaßen auf zertifizierte Rechenzentrumstandards und weitere Sicherheitsmechanismen. Die Anwender profitieren somit von einem mehrfach abgesicherten Cloud-Betrieb. Performance, Datenschutz und Betriebskontinuität erfolgen auf höchstem Niveau.

MobiCloud by NewVoice
hosted by SEC-COM & NTB

Wen adressiert die Alarmserver-Lösung ?
- ✓ Arztpraxen
- ✓ Anwaltskanzleien
- ✓ Ambulante Pflegedienste
- ✓ Kleine Dienstleistungsunternehmen
- ✓ Organisationen mit Alleinarbeit
- ✓ Einzelhandel (Einzelbesetzung)

Wofür eignet sich die Alarmserver-Lösung ?
- ✓ Übergriff / Bedrohung / Belästigung
- ✓ Medizinische Notfälle
- ✓ Sturz oder Unfall
- ✓ Technische Gefährdungen

Wie erfolgen Notrufe?
- ✓ Notruf über PC-Client und mobile App möglich
- ✓ Geeignet für stationäre und mobile Arbeitsplätze

Wirtschaftliche Vorteile?
- ✓ Schnelle Inbetriebnahme
- ✓ Keine komplexe Vor-Ort-Installation
- ✓ Keine lokale Serverinfrastruktur
- ✓ Planbare, laufende Kosten

Fazit:
Cloudbasierte Alarmserver ermöglichen ein professionelles Notrufmanagement ohne Hardware-Investition. Besonders für kleine Strukturen und Alleinarbeit bieten sie eine wirtschaftliche, skalierbare und sofort einsetzbare Sicherheitslösung.

Sie haben Fragen oder möchten mehr erfahren?
Dann rufen Sie uns einfach an unter der Telefonnummer +49 2361 9322 442
oder senden uns eine E-Mail an beratung@sec-com.de

Effizienz trifft Empathie

Die digitale Transformation der Pflege kann man als Rettungsanker betrachten, denn die Herausforderungen sind groß: Der demografische Wandel ist längst keine abstrakte statistische Größe mehr – und er wirkt sich immer deutlicher auf die Realität in deutschen Pflegeeinrichtungen aus. Moderne Technik, integriert von SEC-COM, kann für Entlastung sorgen.

Foto: SKW – stock.adobe.com

Unsere Lebenserwartung steigt dank medizinischen Fortschritts, doch parallel wächst der Druck auf ein System, das bereits heute an seinen Belastungsgrenzen operiert. Aktuelle Schätzungen gehen davon aus, dass die Zahl der pflegebedürftigen Menschen in Deutschland von derzeit etwa 4,2 Millionen bis Mitte der 2030er-Jahre auf über fünf Millionen ansteigen wird. In einem Bereich, die händeringend nach Fachkräften sucht, entsteht eine Versorgungslücke, die sich mit rein personellen Maßnahmen kaum noch schließen lässt. Technologie-Einsatz und Digitalisierung sind daher kein bloßes „Nice-to-have“, sondern zentrale Hebel, um das Gesundheitssystem weiter zukunftsfähig und bezahlbar zu halten.

Status Quo der Vernetzung

Dass die Digitalisierung im deutschen Gesundheitswesen bereits Fahrt aufgenommen hat, zeigen die jüngsten Meilensteine der nationalen E-Health-Strategie. Statt analoger Insellösungen setzt sich zunehmend ein integriertes Ökosystem durch. Ein Beispiel ist das E-Rezept. Zuerst verspätet, dann kontrovers diskutiert, ist es inzwischen mit über einer Milliarde Einlösungen als Standard in der Arzneimittelversorgung etabliert. Auch die elektronische Patientenakte (ePA) gewinnt langsam an Relevanz: Ziel ist es, dass bis zum Jahr 2030 mehr als 20 Millionen Versicherte die ePA aktiv nutzen.
Parallel hat sich auch die Telemedizin weiterentwickelt. Sie bietet Potenziale insbesondere für den ländlichen Raum und stationäre Einrichtungen. Besonders für den Forschungsstandort Deutschland ist außerdem die Entwicklung des Forschungsdatenzentrums Gesundheit von Interesse, das seit Oktober 2025 als zentrale Anlaufstelle fungiert. Hier werden unter höchsten Datenschutzstandards Datensätze für Wissenschaftler und forschende Unternehmen verfügbar gemacht, die bis Ende 2026 in über 300 Forschungsvorhaben einfließen sollen.

Entlastung im operativen Alltag

Ein wesentlicher Schmerzpunkt in der Pflege ist der administrative Overhead. Dokumentationspflichten binden oftmals wertvolle Zeit, die am Bett des Bewohners fehlt. Intelligente Sprachverarbeitung und automatisierte Protokollierung sollen hier nach aktuellen Plänen des Bundesgesundheitsministeriums in den kommenden Jahren Entlastung bringen.

Sicherheit ohne Überwachung

Trotz aller technischer Euphorie stehen Entscheider oft vor ethischen und rechtlichen Hürden. Besonders in der Nachtwache oder bei geringer Personalbesetzung ist die Patientensicherheit ein kritisches Thema. Stürze, das unbemerkte Verlassen der Räumlichkeiten durch beeinträchtigte Patienten oder die Entwicklung eines Dekubitus bei Bettlägerigen sind Risiken, die zügiges Handeln erfordern. Klassische Überwachungssysteme wie Kameras stoßen hier schnell an ihre Grenzen, zwar nicht technisch, aber moralisch und rechtlich.

Genau an dieser Schnittstelle zwischen Schutzbedürfnis und Diskretion setzt moderne, vernetzte Sensorik an. Intelligente, kontaktlose Sensoren sind heute in der Lage, Vitalwerte, Bewegungen sowie Raumdaten präzise zu erfassen, ohne dabei die visuelle Privatsphäre zu verletzen. Es entstehen keine Videobilder, sondern Datenprofile, die Anomalien sofort identifizieren.

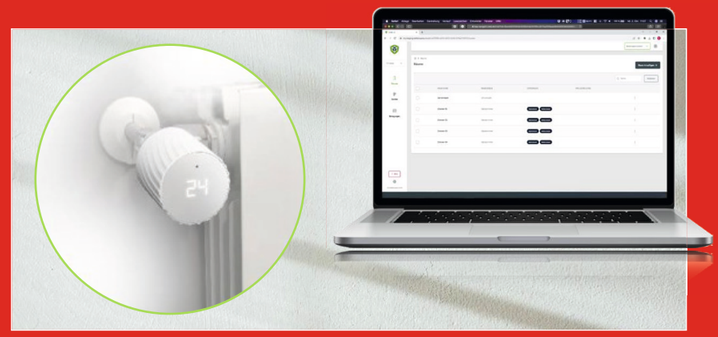
Als Systemhaus wissen wir bei SEC-COM, dass die beste Technologie wertlos ist, wenn sie die Komplexität für den Anwender erhöht. In der Vergangenheit scheiterten Digitalisierungsprojekte im Gesundheitsbereich oftmals an „App-Wildwuchs“ und unkoordinierten Informationen, die das Personal eher stressten als entlasteten. Unsere Antwort auf diese Herausforderung ist die Zusammenarbeit mit Carechamp, einem Unternehmen der österreichischen Schrack Seconet-Gruppe.

Der entscheidende Vorteil der Carechamp-Technologie liegt in der tiefen Integration. Anstatt eine weitere isolierte Softwarelösung zu implementieren, bündelt sie alle Informationen zentral und speist sie direkt in die bestehende Pflegesoftware, Alarmserver oder Rufanlagen ein. Für die Pflegekraft bedeutet das: Die Meldung erscheint genau dort, wo sie ohnehin kommuniziert und dokumentiert wird. Diese nahtlose Einbindung ermöglicht nicht nur einen flüssigen Workflow, sondern auch echte Prävention. Das Personal kann proaktiv reagieren, bevor ein gesundheitlicher Notfall eintritt. Das ist der Übergang von der reaktiven Gefahrenabwehr zum vorausschauenden Pflegemanagement.

Natürlich ist die Implementierung solcher Systeme auch eine Frage der Wirtschaftlichkeit. Steigende Gesundheitskosten erfordern mehr Effizienz. Durch Automatisierung und intelligente Sensorik werden Prozesse gestrafft. Doch der eigentliche Return on Invest liegt in der Zufriedenheit und Sicherheit der Menschen.

Die Digitalisierung in der Pflege ist kein Projekt, das irgendwann „abgeschlossen“ ist. Es ist eine fortlaufende Transformation. Mit den richtigen Partnern und einer klaren Strategie für Interoperabilität und Datenschutz können wir eine Pflegeumgebung schaffen, die den demografischen Herausforderungen gewachsen ist und die gleichzeitig die hohen ethischen Standards im deutschen Gesundheitswesen nicht aufgibt.

ENERGIEKOSTEN JETZT REDUZIEREN



Bei Bestandsimmobilien in der Pflege lassen sich häufig ohne große Bauarbeiten Energiekosten beträchtlich einsparen – und viele Betreiber übersehen diese Option. Gelingen kann dies mit einer zentralen Einzelraumsteuerung für Heizkörper.

In vielen Patientenzimmern stößt man immer wieder auf dasselbe Problem: Auch tagsüber im Bett liegende Personen mögen es „mollig warm“ und der Heizkörper steht auf höchster Stufe. Gleichzeitig will man „frische Luft“ haben, weshalb die Fenster gekippt sind. Das Resultat schmerzt: Die Heizkosten liegen bis zu 35 Prozent höher als es notwendig wäre. Eine nachgerüstete, zentrale Steuermöglichkeit für Heizkörper wäre zwar wertvoll, was im vorhandenen Bestand aber größere Umbauten erfordern würde und damit nicht wirtschaftlich realisierbar wäre.

Die smarte Alternative ist eine zentrale Einzelraumsteuerung der Heizkörper: Die individuelle Wohlfühltemperatur kann zimmerweise geregelt werden. Vermieden wird dennoch eine unnötige Beheizung von nicht genutzten Räumen, eine Beheizung bei geöffnetem Fenster und eine völlig unregulierte Beheizung durch Bewohner.

Aus dieser leicht integrierbaren Lösung ergibt sich ein Einsparpotential bis zu 35 Prozent! Die Technologie ermöglicht in den meisten Fällen einen Break-Even innerhalb der ersten 12 bis 36 Monate, wobei die Lebensdauer der Lösung zehn Jahre übersteigt.

Mehr erfahren

SEC-COM integriert Carechamp-Lösungen bei Kirsch Pflegeeinrichtungen

Patientensicherheit und Entlastung im Fokus

Ausgangslage: Hoher Zeitdruck bei vitalen Routineaufgaben.

Die stationäre Pflege ist von jeher durch einen Spagat zwischen menschlicher Zuwendung und dem hohen Zeitaufwand für wiederkehrende, aber lebenswichtige Routinetätigkeiten geprägt. Dies galt auch für die Pflegeeinrichtung „Am Backumer Tal“ der Kirsch Pflegeeinrichtungen in Herten, ein Haus mit 80 Betten. Das Personal auf den einzelnen Stationen ist täglich mit zeitintensiven Aufgaben wie der individuellen Körperpflege und Essensausgabe beschäftigt.

Zu den weiteren, täglichen Aufgaben zählt auch die Messung der Körpertemperatur der Bewohnerinnen und Bewohner. Diese Routine ist unverzichtbar, um beginnende Erkrankungen, insbesondere Infektionen, frühzeitig zu erkennen und entsprechend reagieren zu können.
Ebenso zeitkritisch und essenziell ist die Überwachung der Nachtruhe. Insbesondere muss hierbei festgestellt werden, ob die Bewohner in der Lage sind, sich selbstständig im Bett zu drehen. Ist diese Bewegungseinschränkung gegeben, erhöht sich die Gefahr eines Dekubitus (Druckgeschwür) drastisch. Das wiederum erhöht das Risiko schwerer, mitunter lebensbedrohlicher Infektionen. Um das zu verhindern, muss das Personal nachts mehrfach die Patientenzimmertüren öffnen und nach dem Rechten sehen. Neben vielen Laufwegen für Mitarbeitende bringt das mitunter auch eine mehrfach gestörte Nachtruhe für die Bewohner mit sich.
Ein weiteres allgegenwärtiges Risiko in der Altenpflege sind Stürze. Gerade betagte Menschen können sich hierbei schwer verletzen. Die resultierenden physischen Traumata und oft wochenlangen Krankenhausaufenthalte haben häufig tiefgreifende Auswirkungen auf die Psyche der Betroffenen: Sie werden ängstlicher, ziehen sich zurück, verlieren an Aktivität und können letztendlich schwerwiegend an Depressionen leiden.
Angesichts dieser Herausforderungen suchte die Einrichtung nach einer intelligenten technischen Lösung, um einerseits das Pflegepersonal nachhaltig zu entlasten und andererseits die Versorgungsqualität zu erhöhen und die Sicherheit der Bewohner zu verbessern.

Lösung: Sensorik für mehr Sicherheit und Effizienz

Fündig wurde die Kirsch Pflegeeinrichtung bei ihrem langjährigen Partner für Rufanlagen und Kommunikation: dem Systemhaus SEC-COM aus Recklinghausen. In einem informativen Beratungsgespräch wurden verschiedene Möglichkeiten zur digitalen Unterstützung erörtert. An diesem Gespräch nahmen seitens der Kirsch Pflegeeinrichtungen Geschäftsführer Magnus Kirsch und Einrichtungsleiter David Piatek teil. Das Systemhaus SEC-COM war durch Geschäftsführer Guido Otterbein vertreten. Ebenfalls anwesend war Carechamp-CTO Dr. Fabian Degenhart.

Das österreichische Unternehmen Carechamp hat sich auf Sensorik-Lösungen für die Pflege spezialisiert. Im Rahmen des Austauschs empfahl das Team von SEC-COM den Einsatz von drei spezifischen Carechamp-Lösungen:

MyFall by cogvis: Dies ist ein fortschrittliches System zur Sturzerkennung. Es nutzt künstliche Intelligenz und hochsensible Sensorik, um Stürze in Echtzeit zu erkennen und sofort das Pflegepersonal zu alarmieren. Der entscheidende Vorteil: Eine visuelle Überwachung findet nicht statt.

MyVital by Vitalerter: Dieses System dient zur kontaktlosen Vital- und Schlafüberwachung. Es wird unter der Matratze platziert und misst die Atemfrequenz, Herzfrequenz und Bewegungen der Bewohnerin oder des Bewohners im Schlaf.

Foto: Jo Gemke

Mehr Sicherheit im Schlaf: Der Bettsensor prüft regelmäßig die Atemfrequenz, Herzfrequenz und Bewegungen, ohne zu stören.

MyTemp: Hierbei handelt es sich um eine Lösung zur automatisierten, berührungslosen Messung der Körpertemperatur. Die Technik ermöglicht die kontinuierliche, aber diskrete Erfassung der Temperaturdaten, ohne dass das Personal dafür manuelle Messungen durchführen und die Bewohner entsprechend stören muss.

Foto: Jo Gemke

Keine Kamera, sondern künstliche Intelligenz und hochsensible Sensorik: MyFall by cogvis erkennt Stürze in Echtzeit und alarmiert dann sofort das Pflegepersonal.

Durch die Kombination dieser drei Sensorik-Systeme sieht die Einrichtungsleitung das Potenzial, Routineaufgaben zu automatisieren und das Sturzrisiko optimal zu adressieren. Sie entschließt sich für ein Pilotprojekt.

Schnelle Integration als Pilotprojekt

Die Implementierung der ausgewählten Carechamp-Technologie wurde durch das Systemhaus SEC-COM übernommen, welches die Kirsch-Unternehmensgruppe bereits seit rund zwei Jahrzehnten betreut. Als Pilotprojekt wurde die Lösung in 12 Zimmern einer Station des 80-Betten-Hauses aufgesetzt. Im Langzeittest sollten valide Erfahrungen vor einem umfassenderen Rollout gesammelt werden.
Vorab wurden alle Beteiligten – das Personal und die Bewohnerinnen und Bewohner – umfassend über das Vorhaben und die Funktionsweise der neuen Sensorik-Technologie informiert. Die Akzeptanz ist von Beginn an positiv - sowohl seitens der Bewohner, die ein Mehr an Sicherheit begrüßen, als auch seitens des Personals, das von Routineaufgaben entlastet wird.

Die Implementierung der Hard- und Software verlief störungsfrei, zeitlich pünktlich und zur vollsten Zufriedenheit der Kirsch Pflegeeinrichtungen. Ein wichtiger Faktor hierfür war das bereits auf der Station vorhandene, leistungsstarke WLAN, da die Carechamp-Technologie dessen Nutzung zwingend voraussetzt.
Nach der erfolgreichen Grundinstallation erfolgte die Feinjustierung. Dieser Schritt war notwendig, um beispielsweise anfangs aufgetretene, kleine Messfehler zu minimieren, wie David Piatek, der Einrichtungsleiter, berichtet: „Von ‚plug & play‘ kann man hier nicht sprechen, aber sobald uns Fehler aufgefallen sind, konnten diese innerhalb kürzester Zeit beseitigt werden. Nach etwa einem Monat war das Gesamtprojekt abgeschlossen, wobei die Technologie bereits während dieser Zeitspanne sukzessive in Betrieb genommen werden konnte. Da keine aufwändigen Bauarbeiten nötig waren, konnte der gesamte Pflegebetrieb wie gewohnt weiterlaufen und weder die Bewohnerinnen und Bewohner noch das Personal wurden gestört oder durch Lärm und Staub beeinträchtigt.

> ***„Die gute Beratung vorab, die engagierte Betreuung während der Implementierungsphase und die schnelle Reaktion bei der Feinjustierung seitens SEC-COM und Carechamp haben wir als sehr positiv wahrgenommen.“***
>
> David Piatek, Einrichtungsleiter
> Pflegeeinrichtung Am Bakumer Tal, Kirsch Pflegeeinrichtungen

Mehr Patientensicherheit, Routineaufgaben reduziert

Der wichtigste Gewinn der durch SEC-COM integrierten Carechamp-Technologie ist die nachhaltige zeitliche und physische Entlastung des Pflegepersonals und die signifikant verbesserte Patientensicherheit. Ein zentraler Aspekt, der zur hohen Akzeptanz beiträgt, ist die Wahrung der Privatsphäre: Die Erfassung wichtiger Patientendaten erfolgt ausschließlich durch diskrete Sensorik. Das bewerten Bewohner und Angehörige durchweg positiv. In den kritischen Bereichen Sturzerkennung, Dekubitus-Prophylaxe und Nachtruhe, sowie bei der Früherkennung von Infektions-Erkrankungen ist eine positive Entwicklung klar erkennbar.

Sie haben Fragen oder möchten mehr erfahren?
Dann rufen Sie uns einfach an unter der Telefonnummer +49 2361 9322 442
oder senden uns eine E-Mail an beratung@sec-com.de

Wie Künstliche Intelligenz das Contact-Center verändert

Ohne Contact-Center-Agenten wäre die Kundenkommunikation vieler Unternehmen nicht denkbar – doch der Arbeitsalltag im Contact-Center verändert sich rasant. Mit dem Einzug Künstlicher Intelligenz (KI) verschiebt sich der Schwerpunkt vom reaktiven Support hin zu einer intelligent orchestrierten Serviceumgebung. Der Einsatz von KI macht Arbeitsabläufe effizienter, senkt Kosten und entlastet Mitarbeitende von Routinen. Unternehmen können dadurch neue Qualitätsmaßstäbe in der Kundeninteraktion setzen.

Die Agentin im Contact-Center erhält KI-Unterstützung, bleibt aber unverzichtbar

Foto: istock, skynesher

Laut dem Branchenverband CCV sind in Deutschland rund 560.000 Menschen in der Callcenter-Branche tätig – in unternehmenseigenen Centern ebenso wie bei Dienstleistern. Oftmals müssen Beschäftigte in Contact-Centern Routinetätigkeiten ausführen, also etwa dutzende Male pro Arbeitstag Kunden die Frage beantworten, wo sich gerade ihre Paketsendung befindet. Es gibt aber auch hochqualifizierte, umfangreich geschulte Contact-Center-Agents, die für Kunden sicherheitssensible Bank-Transaktionen ausführen oder Businesskunden bei komplexen IT-Problemen beraten. Diese Experten müssen oft mehrere IT-Systeme parallel bedienen. Sie können die Anliegen der anrufenden Kunden nicht mit Standardsätzen lösen, sondern müssen sich tief in einen Sachverhalt hineindenken, um „live“ eine Problemlösung zu erarbeiten.

Künstliche Intelligenz sorgt zunehmend für Veränderungen: AI-gesteuerte Routing-Systeme analysieren Sprache, Kundendaten und Anliegen in Echtzeit. Anrufe werden dadurch automatisch dem passenden Ansprechpartner zugewiesen, was Wartezeiten reduziert und Erstlösungsquoten verbessert. Auch KI-basierte Sprachassistenten sind im Einsatz, die via Datenbankzugriff häufig gestellte Fragen direkt beantworten – ohne menschliches Eingreifen. Das ist längst auch auf allen Kanälen möglich, sei es im Sprachdialog, mittels Chat oder beantworteter E-Mail. Damit sinkt die Belastung für Contact-Center-Teams, während der Durchsatz an Kundeninteraktionen steigt.

Kontextbezogene Informationen

Auch im zwischenmenschlichen Dialog kann KI wertvolle Unterstützung bieten: Systeme blenden während eines Gesprächs kontextbezogene Informationen ein – etwa Produktdetails oder Statusmeldungen zu laufenden Vorgängen. Wenn KI erkennt, dass ein Anrufer kein Muttersprachler ist, kann sie dem Agenten zudem in Echtzeit Rückmeldung geben, langsamer oder einfacher zu formulieren. Das Ergebnis ist eine merklich natürlichere Kommunikation mit höherer Verständlichkeit und Kundenzufriedenheit.

Emotionserkennung und Echtzeit-Übersetzung

Ein weiterer Effizienztreiber ist die emotionale Analyse. KI erkennt Stress, Frustration oder Aggression anhand von Stimmmerkmalen und kann Mitarbeitende warnen oder das Gespräch an deeskalationsgeschulte Experten weiterleiten. Parallel ermöglichen Echtzeit-Übersetzungen barrierefreie Kundendialoge über Sprachgrenzen hinweg – inklusive Live-Untertitelung für Agenten. So beschleunigen KI-Systeme auch internationale Kommunikationsprozesse erheblich.

Autonome KI-Agenten als nächste Stufe

Fortgeschrittene Systeme agieren längst nicht mehr nur assistierend, sondern als eigenständige Serviceeinheiten. Diese „virtuellen Agents“ verstehen Kundenanliegen, bewerten Kontexte und lösen Standardanfragen vollautomatisch. Das geht über Telefon, Chat oder Messaging-Plattformen hinweg. Mit Rund-um-die-Uhr-Verfügbarkeit steigern sie die Effizienz, verkürzen Reaktionszeiten und verbessern die Servicequalität messbar.

Erste KI-Agenten übernehmen zudem proaktiv Aufgaben: Sie versenden Formulare, greifen systemübergreifend auf Daten zu oder kontaktieren Kunden selbst, etwa zur Produktberatung oder Vertragsverlängerung. Besonders stark nachgefragt sind solche Lösungen derzeit in Finanzdienstleistungs-, Handels- und Energieunternehmen.

KI als Partner – nicht als Ersatz

Aktuelle KI-Modelle beherrschen mittlerweile über 100 Sprachen und agieren mit zunehmender emotionaler Feinfühligkeit. Statt bloß Antworten zu liefern, erkennen sie Gesprächsstimmungen, passen Wortwahl und Tonalität situativ an und können damit das Serviceerlebnis nachhaltig verbessern.

Die algorithmischen Problemlöser werden dennoch nicht die Mitarbeitenden aus dem Contact-Center verdrängen. Die Zukunft des Contact Centers ist hybrid: Mensch und Maschine ergänzen sich. KI übernimmt repetitive Aufgaben, sammelt Daten, analysiert Emotionen und unterstützt in Echtzeit – während Mitarbeitende ihre Expertise dort einbringen, wo Empathie und Kontextverständnis entscheidend sind. Das Contact-Center der Zukunft wird also keineswegs menschenleer sein. Der Einsatz von KI wird die Kundeninteraktion aber effizienter machen. Für ein qualitativ hochwertiges Kundenerlebnis ist der Mensch aber unverzichtbar.

Einfacher Einstieg in die KI-Telefonie

VOICEBOT FÜR ROUTINEANRUFE

Nicht jedes Unternehmen benötigt die Unterstützung durch ein Contact-Center. Doch auch kleinere Teams oder Freiberufler kämpfen mitunter damit, dass immer wieder die gleichen Standardanfragen beantwortet werden müssen. Hier kann Künstliche Intelligenz in Form von Voicebots entlasten.

Sie kennen das: Viele geschäftliche Telefonate drehen sich um ein und dieselbe Frage. In der Autowerkstatt etwa, ob das Fahrzeug den TÜV bestanden hat und abgeholt werden kann. In der Arztpraxis geht es häufig um ein neues Rezept für ein regelmäßig benötigtes Medikament. Oder ein Kollege beim Kunden vor Ort benötigt kurzfristig technische Details zu einer Maschine. Solche Anfragen kehren immer wieder und binden Zeit.

Ein Voicebot erkennt über KI-basierte Spracherkennung die Worte des Anrufenden und beantwortet häufige Standardanfragen automatisch. Auch mehrere Anliegen in einem Gespräch lassen sich bearbeiten. Kommt der Bot einmal nicht weiter, wird der Anruf automatisch an die richtige Person oder Abteilung weitergeleitet.

SEC-COM unterstützt Unternehmen bei der Einführung solcher KI-Lösungen. Gemeinsam wird zunächst analysiert, welche wiederkehrenden Anfragen sich besonders gut automatisieren lassen. Darauf aufbauend wird der Voicebot so konfiguriert, dass er genau diese Aufgaben übernimmt und die Mitarbeitenden im Alltag spürbar entlastet.

Guido Otterbein kommentiert: „Unsere Kunden müssen für den Einsatz eines Voicebots keine komplett neue Kommunikationslösung aufbauen. Der Einstieg ist deutlich einfacher, als viele vermuten.“

Die KI-Telefonlösung bietet darüber hinaus volle DSGVO-Konformität.

Warum Ihre Telekommunikation ein Sicherheitsrisiko sein kann

Foto: istock, Andrey Zhuravlev

Kommunikationssysteme sind heute voll integrierte Bestandteile der IT-Infrastruktur. Sie verfügen über offene, standardkonforme Schnittstellen, die ein nahtloses Zusammenspiel mit Lösungen anderer Hersteller ermöglichen. Diese sinnvolle Offenheit kann allerdings auch ausgenutzt werden. Die Sicherheitsbehörde BSI hat deshalb klare Schutzregeln ausgearbeitet. SEC-COM Insides erläutert, was es damit auf sich hat.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die oberste, deutsche Behörde, wenn es um Cybersicherheit geht. In drei umfangreichen Ausarbeitungen (Kompendien) wird beschrieben, welche typischen Risiken in der modernen Telekommunikation existieren. Dazu gehören Abhören (Spionage), Betrug und Systemausfälle.
Um solche Bedrohungen so gering wie möglich zu halten, empfiehlt das BSI ein mehrschichtiges Schutzkonzept aus technischen, organisatorischen und personellen Maßnahmen. Kernbestandteile sind Netzwerksegmentierung, starke Authentisierung, Verschlüsselung, regelmäßige Updates und Schulung der Administratoren. Die gute Nachricht: Zu sämtlichen Anforderungen bietet Ihnen SEC-COM volle Unterstützung.

Die Kompendien verdeutlichen, wie TK-Systeme sicher aufgebaut, betrieben und gegen Angriffe geschützt werden. Es gilt, IT- und TK-Sicherheit eng zu verzahnen. Ziel: widerstandsfähige Kommunikationsinfrastrukturen. Ganz wichtig: Sicherheit kennt heutzutage keinen Stillstand mehr. Vielmehr handelt es sich um einen kontinuierlichen Prozess. Die Vorkehrungen sollte man regelmäßig prüfen und an neue Bedrohungen anpassen.

Typische Gefährdungen im Detail

Indem man Sicherheitsmaßnahmen gezielt umsetzt, machen Businessanwender ihre Kommunikationsinfrastruktur resilient gegen Cyberangriffe. Dennoch ist hundertprozentiger Schutz kaum zu erreichen, denn die Cyberkriminellen lassen sich immer wieder etwas Neues einfallen. Hilfreich ist es, wenn man weiß, was auf einen zukommen kann. Hierzu hat das BSI die gängigen Bedrohungen in drei Kategorien eingeteilt:

Technische Angriffe: Dazu gehören das Abhören von Gesprächen, das Ausspähen von Zugangsdaten, Spoofing (Verschleierung) von Rufnummern und Manipulation von Signalisierungsdaten. In IP-basierten Netzen können Angreifer Sprachpakete mitlesen oder gezielt Kommunikationsverbindungen stören.

Missbrauch und Betrug: Betrüger nutzen offene, schlecht gesicherte VoIP-Systeme, um kostenpflichtige Gespräche über fremde Anlagen zu führen. Solche „Toll Fraud“-Angriffe verursachen oft hohe finanzielle Schäden.

Verfügbarkeit und Ausfallrisiken: Auch Überlastungen durch DDoS-Attacken oder Fehlkonfigurationen können TK-Systeme lahmlegen. Wenn das ein ganzes Unternehmen betrifft, hat das unmittelbar geschäftskritische Auswirkungen.

Neben diesen technischen Aspekten sollte jeder Businessanwender auch organisatorische Schwächen bekämpfen. Hierzu zählen beispielsweise unklare Verantwortlichkeiten, fehlende oder oft verschobene Schulungen von internen Verantwortlichen oder auch die Vergabe von unsicheren Remote-Zugängen.

Zielsetzung der BSI-Empfehlungen

SEC-COM kennt die Behörden-Empfehlungen. Wichtig für Sie: Diese richten sich an IT- und TK-Verantwortliche. Ziel der Empfehlungen ist es, die Systeme über ihren gesamten Lebenszyklus hinweg abzusichern.

Das BSI hebt hervor, dass IT-Sicherheit und TK-Sicherheit heute untrennbar miteinander verbunden sind. Früher klar getrennte Welten – hier die Telefonanlage, dort der Computer - sind mit der Digitalisierung zusammengewachsen. Daher muss Sicherheit ganzheitlich betrachtet werden, einschließlich Netzsegmentierung, Zugangskontrolle, Verschlüsselung und Notfallvorsorge.

Grundprinzipien des Schutzes

Ganz in Einstimmung mit dem BSI empfehlen auch die erfahrenen Experten von SEC-COM ein mehrschichtiges Sicherheitskonzept, das technische, organisatorische und personelle Maßnahmen kombiniert. Zentrale Punkte sind:

Netzwerksegmentierung: TK- und IT-Systeme sollten klar getrennt, aber kontrolliert verbunden werden. So wird verhindert, dass ein Angriff auf ein Büro-PC-Netz direkten Zugang zur Telefonanlage ermöglicht.

Starke Authentisierung: Zugänge zu Administrationsoberflächen müssen über starke Passwörter oder Mehrfaktorauthentifizierung gesichert werden.

Verschlüsselung: Sprach- und Signalisierungsdaten sollten über sichere Protokolle wie TLS und SRTP übertragen werden.

Aktualität und Patchmanagement: Firmware-Updates und Sicherheits-Patches sind regelmäßig einzuspielen – ohne Ausnahme.

Monitoring und Protokollierung: Die Überwachung von Anomalien im Datenverkehr hilft, Angriffe frühzeitig zu erkennen.

Awareness und Schulung: Administratoren und Nutzer müssen für Risiken sensibilisiert werden – etwa durch regelmäßige Schulungen zur sicheren Nutzung von TK-Diensten.

Integration in den BSI-IT-Grundschutz

Die BSI-Materialien ergänzen die IT-Grundschutz-Methodik, die bereits für IT-Systeme etabliert ist. Durch eine Übertragung dieser Prinzipien auf TK-Systeme entsteht ein insgesamt konsistentes Sicherheitsniveau. Besonders wichtig ist die Verzahnung von Netzwerksicherheit, IT-Betrieb und physischem Schutz, da TK-Systeme häufig physisch exponiert sind (z. B. in öffentlich zugänglichen Räumen oder außerhalb gesicherter Rechenzentren).

Fazit: Sicherheit als Daueraufgabe

Kommunikationssysteme entwickeln sich technologisch rasant weiter. Dadurch ergeben sich neue Angriffsmöglichkeiten, aber auch bessere Schutzstandards. Betreiber sollten regelmäßig prüfen, ob ihre Systeme noch aktuelle Sicherheitsanforderungen erfüllen und eine Verantwortlichkeit für diesen Prozess festlegen.

BSI-Kompendien zur Sicherheit in der Kommunikationstechnik

1. Kompendium
„Grundschutz in TK-Systemen“

Dieses Dokument bietet eine Einführung in den Sicherheitsprozess für Telekommunikationsinfrastrukturen. Im Mittelpunkt stehen die Schritte Risikoanalyse, Maßnahmenpriorisierung und Umsetzung. Es beschreibt, wie bestehende IT-Grundschutz-Bausteine auf TK-Systeme übertragen werden können.

2. Kompendium
„Sicherer Betrieb von TK-Systemen“

Hier liegt der Fokus auf dem Alltagsbetrieb. Es wird erläutert, wie Betreiber ihren TK-Dienst sicher administrieren, wie Rollen und Zuständigkeiten verteilt werden und welche Abläufe sich bewährt haben. Hierzu zählen unter anderem eingerichtete Rollen- und Rechtekonzepte, regelmäßige Sicherheitsprüfungen und Penetrationstests, Schutz von Managementschnittstellen durch VPN und Firewalls.

3. Kompendium
„Abwehr typischer Angriffe auf TK-Systeme“

Dieses Kompendium bietet praxisnahe Szenarien und Gegenmaßnahmen. Es zeigt typische Angriffsarten – etwa SIP-Hijacking, Man-in-the-Middle-Angriffe oder Denial-of-Service – und erläutert jeweils geeignete Schutzmechanismen. Das Kompendium betont, dass Prävention meist günstiger und effektiver ist als nachträgliche Schadensbegrenzung.

Sie haben Fragen oder möchten mehr erfahren?
Dann rufen Sie uns einfach an unter der Telefonnummer +49 2361 9322 442
oder senden uns eine E-Mail an beratung@sec-com.de

NIS-2-Regelung in Deutschland in Kraft getreten

Was Unternehmen jetzt wissen und tun müssen

Nach einer längeren Verzögerung ist das NIS-2-Umsetzungsgesetz im Dezember 2025 in Kraft getreten. Damit gelten die Anforderungen der europäischen NIS-2-Richtlinie (Network and Information Security Directive 2) nun auch hierzulande verbindlich. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) betrifft dies mehr als 29.000 Unternehmen.

Mit dem neuen NIS-2-Umsetzungsgesetz zieht die EU die Schrauben bei der IT-Sicherheit deutlich an. Dabei unterscheidet das Gesetz zwischen „besonders wichtigen Einrichtungen“ und „wichtigen Einrichtungen“. Beide gelten als systemrelevant - sie sichern das tägliche Funktionieren von Wirtschaft und Gesellschaft hierzulande.

KRITIS im Fokus

Zu den besonders wichtigen Einrichtungen zählen vor allem Betreiber kritischer Infrastrukturen (KRITIS). Das sind Organisationen, die für das Gemeinwesen unverzichtbar sind. Fallen hier ITK-Systeme aus, kann das weitreichende Folgen haben: von Versorgungsengpässen bis hin zu massiven Störungen der öffentlichen Sicherheit. Ende September 2025 waren beim Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits 1.177 KRITIS-Betreiber registriert. Sie stammen aus den Bereichen Energie, IT und Telekommunikation, Transport, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Abfallentsorgung.
Mit NIS-2 kommen weitere Bereiche hinzu. Nun rücken auch Unternehmen aus dem verarbeitenden Gewerbe, der Forschung und der Digitalwirtschaft in den Geltungsbereich. Sie alle müssen sektorübergreifende IT-Sicherheitsanforderungen erfüllen.

Selbstverpflichtung

Unternehmen sind verpflichtet, selbst zu ermitteln, ob sie unter NIS-2 fallen und welcher Kategorie sie angehören. Maßgeblich sind dabei Schwellenwerte wie Mitarbeiterzahl und Umsatz. Für „wichtige Einrichtungen“ gelten als Richtwert: weniger als 50 Mitarbeitende oder ein Jahresumsatz beziehungsweise eine Bilanzsumme von maximal 10 Millionen Euro. Zur Orientierung stellt das BSI ein Online-Tool und einen Entscheidungsbaum bereit, mit denen Unternehmen ihre Einstufung überprüfen können.

Was Unternehmen jetzt tun müssen

Unabhängig von ihrer Kategorie gelten für alle Einrichtungen zentrale Pflichten.

Registrierung: Zunächst müssen sich Unternehmen über „Mein Unternehmenskonto“ (MUK) anmelden, anschließend über das BSI-Portal. Das BSI bietet dazu umfassende Hilfeseiten an („NIS-2-Betroffenheitsprüfung“).

Vorfallsmanagement: Sicherheitsrelevante Zwischenfälle - etwa gravierende Betriebsstörungen - müssen dem BSI gemeldet werden. Dazu sind Prozesse nötig, die Vorfälle erkennen, bewerten, bearbeiten und nachverfolgen.

Risikomanagement: Ziel ist es, erhebliche Sicherheitsvorfälle von vornherein zu vermeiden. Dafür müssen technische und organisatorische Schutzmaßnahmen eingeführt und dokumentiert werden.

Das BSI nennt als Mindeststandard zehn zentrale Maßnahmen:
- ✔ Risikoanalyse und IT-Sicherheitskonzepte
- ✔ Incident Response und Notfallbewältigung
- ✔ Business Continuity Management inklusiv Backup und Krisenmanagement
- ✔ Sicherheit in der Lieferkette und bei Dienstleistern
- ✔ Sichere Entwicklung, Wartung und Beschaffung von IT-Systemen
- ✔ Wirksamkeitsprüfung der Sicherheitsmaßnahmen
- ✔ IT-Sicherheitsschulungen und Sensibilisierung
- ✔ Nutzung von Kryptografie-Konzepten
- ✔ Zugriffskontrolle, Personal- und Asset-Management
- ✔ Einsatz von Multi-Faktor-Authentifizierung und gesicherter Kommunikation

Die Verantwortung für die Umsetzung liegt bei der Unternehmensleitung - sie haftet persönlich und ist gesetzlich zu einer Schulung verpflichtet. Das BSI hat dafür eine eigene Handreichung mit Empfehlungen veröffentlicht.
Einrichtungen der Kategorie „besonders wichtig“ stehen zusätzlich unter Aufsicht des BSI. Gefordert sind regelmäßige Audits, engmaschige Prüfungen. Bei Verstößen drohen harte Sanktionen.

Fortschritte und Ausblick

Die Umsetzung der NIS-2-Anforderungen läuft in vielen Betrieben bereits auf Hochtouren. Allerdings ist einer aktuellen Umfrage von Statista im Auftrag des Sicherheitsanbieters G Data jedes vierte Unternehmen noch gar nicht aktiv geworden und damit in Verzug. Wichtig zu wissen: Das Gesetz gilt ohne Übergangsfrist – Verstöße können schon jetzt teuer werden.

NIS-2 in Zahlen

Von den rund 29.500 Unternehmen in Deutschland, die von der NIS-2-Richtlinie betroffen sind, haben sich nach Angaben des BSI bisher rund 11.500 Unternehmen über das BSI-Portal registriert, was verpflichtend vorgeschrieben ist. Allein in der letzten Woche vor Ablauf der Frist kamen mehr als 4.000 Registrierungen neu hinzu.

29.500
Unternehmen von NIS-2 betroffen

11.500
Unternehmen haben sich fristgerecht registriert

Weitere Informationen:
https://portal.bsi.bund.de

Allerdings verfolgt das BSI bisher einen eher beratenden Ansatz und unterstützt Unternehmen bei der Umsetzung, anstatt sofort zu sanktionieren.

Schutzschild

NIS-2 soll kein Bürokratiemonster sein, sondern ein Schutzschild gegen wachsende Cybergefahren. BSI-Präsidentin Claudia Plattner rechnet damit, dass die IT-Sicherheitslage in Deutschland durch die Umsetzung deutlich stabiler wird.

Die zeitnahe Umsetzung von NIS-2 bleibt insbesondere für kleinere Unternehmen mit begrenzten Ressourcen eine große Herausforderung.
Das Team von SEC-COM unterstützt ihr Unternehmen gerne bei allen Fragen und Anforderungen zu NIS-2. Am besten nehmen Sie noch heute Kontakt zu uns auf.

Jetzt Fördermittel für IT-Sicherheitsberatung erhalten

STAATLICHE FÖRDERPROGRAMME

Die Digitalisierung ist heute eine wesentliche Voraussetzung für nahezu alle Unternehmen, um wettbewerbsfähig zu bleiben und nachhaltig auf dem Markt zu agieren. Doch wie digitalisiert man so, dass man nicht Cyberkriminelle auf den Plan ruft? Niemand will schließlich zwei Schritte nach vorne und einen Schritt zurück gehen! Hier ist Beratung unverzichtbar!

IT-Sicherheit ist heute unverzichtbar für jedes Unternehmen, das mit digitalen Lösungen arbeitet – die weltweite Bedrohungslage lässt keinen anderen Schluss zu. Täglich hunderttausende Attacken durch Cyberkriminelle und Risiken durch potentielle Datenverletzungen sind Faktoren, die heute den Fortbestand selbst außerordentlich erfolgreicher Betriebe gefährden können. Doch wie verhindert man Datenlecks richtig? Wie schützt man sich wirkungsvoll vor Cyberangriffen, die sich massiv auf die Geschäftskontinuität auswirken können? Wer hier auf eine falsche Strategie setzt, „verbrennt“ Geld und ist am Ende doch nicht vernünftig abgesichert. Eine auf Ihre Anforderungen zugeschnittene IT-Sicherheitsberatung mit genauer Ist-Analyse und genauer Roadmap für die weiteren Maßnahmen ist deshalb unverzichtbar!

Um hier zeitnah vorwärtszukommen, benötigen Sie Beratungsleistung von ausgebildeten Experten. Diese Beratung ist individuell und kostet Geld, doch der Staat unterstützt Unternehmen mittels einer finanziellen Förderung dabei, sich in wichtigen Themengebieten kompetent beraten zu lassen. Beim unvermeidlichen „Papierkrieg“ unterstützen wir Sie: Als BAFA-gelistetes Beratungsunternehmen begleiten wir Sie durch den gesamten Prozess der Fördermittelbeantragung. Wir prüfen für Sie, ob Sie Fördermittel erhalten können und begleiten Sie durch den gesamten Antragsprozess.

Kontaktieren Sie uns noch heute für ein unverbindliches Gespräch hierzu!
Telefon: 0 23 61 93 22 442
E-Mail: beratung@sec-com.de

Mehr erfahren

Unternehmensgruppe SEC COM

Ihr **Systemhaus** für Kommunikation, Sicherheit und IT

„Es ist nicht die stärkste Spezies, die überlebt, auch nicht die intelligenteste. Es ist diejenige, die sich am ehesten dem Wandel anpassen kann.“

Charles Darwin, britischer Evolutionsforscher

2 x in NRW

SEC-COM Sicherheits- und Kommunikationstechnik GmbH

Bochumer Str. 6
45661 Recklinghausen
Fon: 0 23 61 / 93 22-0

SEC-COM Sicherheits- und Kommunikationstechnik Ostwestfalen GmbH
Karl-Schurz-Straße 32
33100 Paderborn
Fon: 0 52 51 / 8 74 98-0

www.sec-com.de