EURO SECURITY

Das Sicherheitsmagazin für Planer, Errichter und Anwender für die DACH-Region



IT-Sicherheit

G Data sieht Skepsis gegenüber KI im Unternehmen Datenschutz führt die Liste der Bedenken an

Kritische Infrastruktur

Intelion: KI-Lösung auf der GPEC 2025 mit neuesten Funktionen für KI-Analyse und polizeiliche Ermittlungen

Videotechnik

Marktbericht: Videobranche als Sensormarkt: Regierungsinitiativen für Wachstum verantwortlich

ISSN 09481249 • 12-2024 • ZKZ 16724 Postvertriebsstück bezahlt • 80383 BAY Germany ©SEC Global • euro-security.de

Inhalt



Impressum 3

Editorial 4
Deutsche Sicherheitsbranche im Wandel : Warum organisches Wachs- tum der Schlüssel zum Erfolg ist

COVERSTORY

Kentix 7
'Eine Lösung für Alles': Im Interview mit Geschäftsführer Thomas Fritz erfahren wir mehr über KentixOne, die innovative Lösung von Kentix, die physische Sicherheit und IT-Infrastrukturschutz in einer Plattform vereint.

GEBÄUDEMANAGEMENT

PCS Systemtechnik 22



Umfassende Gebäudesicherheit auf der Tagesordnung: Agenda setzt auf neues Sicherheitskonzept für das sanierte Firmen- gebäude

CES 37
Intelligentes Wohnraummanagement: Studierendenwerk Mannheim setzt



auf modernes Zutrittskontrollsystem AccessOne

IT-SECURITY

Fünf Tipps 40
E-Mail-Security NIS-2-compliant

Phishing-Angriffsmethoden im Jahr 2025 55
Die Threat-Analysten von Barracuda Networks haben dieses Jahr mehrere fortschrittliche Phishing-Methoden beobachtet und daraus acht Trends für das Jahr 2025 abgeleitet.

G Data 57
Skepsis gegenüber KI im Unternehmen Datenschutz führt die Liste der Bedenken an

Check Point Software Technologies 58
Zweiter Jahrestag von ChatGPT: Generationssprung der KI

TrendMicro 60
Deutschland und die NIS2-Richtlinie:Versäumte Chancen und dringende Notwendigkeiten

synaforce 61
Positive Bilanz und Prognose 2025

Nord VPN 64
Prognosen zu Cybersicherheitsbedrohungen 2025: Ein Blick ins Darknet

Armis Labs 66
KI-gestützte Cybersicherheit

Zehn Prognosen für das Jahr 2025

KRITISCHE INFRASTRUKTUREN

ISID 12
Intelion: KI-Lösungen für Ermittlungen: ISID wird auf der GPEC 2025 die neuesten Funktionen für KI-Analyse



und polizeiliche Ermittlungen präsentieren. Am 2. und 3. April 2025 wird ISID erneut als Aussteller an der General Police Equipment Exhibition & Conference (GPEC) in Leipzig teilnehmen.

Dallmeier electronics 17
Videosicherheit: Modular, zentral, cloudbasiert: Multifocal-Sensortechnik im Fernzugriff und modulare Management Software in der Azure-Cloud

Hamburg 34
Sicherheit im Hamburger Nahverkehr: Neue Informationsoffensive des hvv seit November 2024 - Waffenverbot - 80 neue Stellen im Sicherheitsbereich

KÜNSTLICHE INTELLIGENZ

KI-Bundesverbands 26
Cybersicherheit: Kritische Betrachtung des Impulspapiers des Verbands

Zweiter Jahrestag von ChatGPT 58
Generationssprung der KI



Künstliche Intelligenz in der Arbeitswelt 62
Chancen und Herausforderungen : Künstliche Intelligenz (KI) hat sich als treibende Kraft der digitalen Transformation etabliert und verändert die Arbeitswelt in einem rasanten Tempo.

PRODUKTE

Dallmeier electronic 44



Kompakt, intelligent und sicher: Neue Einstiegskamera „Picoline“

FTS Hennig 53
Mobilfunkversorgung als Basis für eine zukunftsfähige Ladeinfrastruktur

SICHERHEITSINDUSTRIE

Securitas 21
Transformative Trends im Sicherheitssektor: Einblick in den 2025 Global



Technology Outlook Report von Securitas Technology

Handwerkskammer Cottbus 39
Impulse für das Handwerk und die deutsche Wirtschaft für die Zukunft

Genetec 46



Bewährte Verfahren: Risikomanagement und Beschaffung im Bereich physische Sicherheit

SMARTE TECHNOLOGIEN

SATEL 30
BE WAVE: Kabelloses Smart-Home-System mit Sicherheitsfokus - SLIM



LINE: Bewegungsmelder in stilvollem Design - Smart Thermostat: Intelligente Heizungsautomatisierung

STANDARDS

Smart Payment Association 49
Digital Operational Resilience Act: Position zur Kartenpersonalisierung

NIS2 und DORA 51
Ein Vergleich der Regelwerke und häufige Missverständnisse

VERSICHERUNGEN

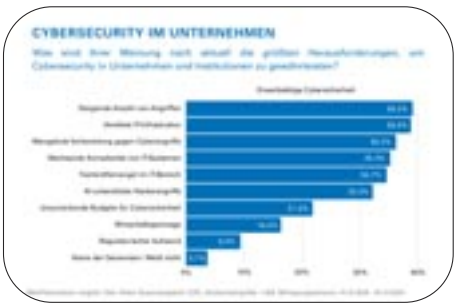
Allianz Commercial 28
Bericht „Directors and Officers (D&O) Insurance Insights 2025“

ZAHLEN & DATEN

marketsandmarkets 42
Videobranche als Sensormarkt: Regierungsinitiativen für Wachstum verantwortlich

Heise Online 45
Überwachungskameras für den Innenbereich: Heise Online hat zehn Indoor-Überwachungskameras getestet und wichtige Informationen für diese Produktart vorgestellt.

TÜV Rheinland 56



IT-Sicherheitslage in Deutschland verschärft sich weiter: Laut einer Civey-Umfrage im Auftrag von TÜV Rhein- land hat die Gefahr von Cyber-Angriffen weiter zugenommen.

Impressum

Euro Security Fachmedien (Verlagsvertretung); Grabenfeldstrasse 25, 83083 Riedering, Tel: +49 (0)8036 3035071; Email: redaktion@euro-security.de
Redaktion: ***Dr. Claudia Mrozek, Chefredak. (V.i.S.d.P., Herausgeber)***, *Caroline Best, Angela Kloose, Dirk Lehmanski, Maria Lehmen, Anne, Schneider, Heiko Scholz, Patricia Ovo, Cathy Thomens, Sophie Mrozek, Alexander Mrozek, Mariam Nassreddin; Marcus Smid, Angela Thorn*
Druckerei *D+L Print, Dorsten / Schmidl & Rotaplan Druck, Regensburg*
Aboverkauf *DCMN Marketing Agentur, Email: abo@sec-global.org*
Anzeigenverwaltung/-vertretung *DCMN Marketing Agentur Oberbayern, Bestellungen und Druckvorlagen: anzeigen@euro-security.de*
Copyright: *Der Markenverwerter SEC Global ist urheberrechtlich verantwortlich für Inhalt, Design und die Herstellung von Druckmaterialien/-erzeugnissen für die Fachzeitschriften Euro Security, Middle East Security und African Security. Ebenfalls betreffen allgemeine Copyrightrechte und -pflichten die Webseite „www.eurosecglobal.de“ und alle angeschlossenen Seiten, digitalen Services und Publikationen. Ohne Zustimmung des Verlags können weder ganze Artikel noch große Teile von Texten per E-Mail, über „Social Media“-Netzwerke oder auf andere Weise veröffentlicht werden. Eine wirtschaftliche Verwertung oder eine andere kommerzielle Benutzung ist nicht zulässig. In Verbindung mit der gedruckten Zeitschrift oder den veröffentlichten Texten auf der Website bzw. digitalen Anwendungen ist das Reproduzieren oder die Vervielfältigung von Marken/ Logos (wie “Euro Security” [ES] oder “Middle East Security” [MES] Name genauso wie andere verlagseigene Logos oder Handelsnamen nur mit schriftlicher Genehmigung der Verlagsleitung möglich. Das Kopieren oder die Verlinkung ganzer Textpassagen unter eigenem Namen sind ausschließlich für den persönlichen und nicht-kommerziellen Gebrauch zulässig. Der Ausdruck eines Artikels auf Papier ist zulässig, eine Vervielfältigung nicht. Genauso ist eine Speicherung für den privaten Gebrauch zulässig. Eine Verwendung, die über den nicht-kommerziellen Gebrauch hinausgeht, ist nicht erlaubt. Digitale Anwendungen sind pro Lizenz nur auf bis zu fünf getrennten Geräten zu verwenden. Auch aus diesen Quellen ist eine Reproduktion, Veränderung oder eine kommerzielle Verwendung nicht gestattet. Die Übertragung der Inhalte auf andere Webseiten, Newsgroups, Mailinglisten, elektronische Bulletins, Servern oder andere Medien, die mit einem Netzwerk verbunden sind oder regelmäßig oder systematisch Inhalte in elektronischer (einschließlich der im Rahmen jeder Bibliothek, Archiv oder ähnliche Dienstleistung) speichern, ist nicht gestattet. Jede Verwendung der im Druck oder Online publizierten Inhalte sind ausdrücklich untersagt. Anfragen auf Genehmigung bitte an eines unserer SEC Global unter copyright@sec-global.org senden. Eine Freigabe oder ein kostenpflichtiges Angebot wird Ihnen umgehend zugehen. © Sec Global*

EURO SECURITY Fachverlage und - medien ist förderndes Mitglied im BHE/Deutschland. BHE-Mitglieder erhalten im Rahmen ihrer Mitliedschaft regulär erscheinende Ausgaben der Euro Security DACH kostenlos.

Editorial

Deutsche Sicherheitsbranche im Wandel

Warum organisches Wachstum der Schlüssel zum Erfolg ist

In der deutschen Sicherheitsbranche ist ein Trend immer deutlicher zu erkennen: Die zunehmende Konzentration durch Fusionen und Übernahmen. Diese fusionsbasierten Wachstumsstrategien erscheinen zunächst als Lösung für Unternehmen, die im wettbewerbsintensiven Markt bestehen möchten. Doch dieser Trend hat seinen Preis: Der mittelständische Charakter, der lange Zeit das Rückgrat der Branche bildete, wird zunehmend durch große, fusionierte Konzerne ersetzt. Ihr Fokus liegt oft weniger auf nachhaltigem Wachstum und Innovation, sondern auf kurzfristigen Effizienzgewinnen. Der Verlust der traditionellen Struktur schwächt nicht nur die Innovationskraft der Branche, sondern hemmt auch die Dynamik, die für langfristigen Erfolg erforderlich ist.
Eine kürzlich veröffentlichte Studie der University of Michigan hinterfragt das traditionelle Narrativ von Fusionen und Übernahmen und zeigt, dass organisches Wachstum – also das Wachstum durch eigene Expansion und Innovation – langfristig stabiler und erfolgreicher ist.

Die Finanzkrise 2008 als Wendepunkt

Die Studie basiert auf Daten aus der Finanzkrise von 2008 und untersucht, wie die Krise das Wachstum und die Strategien von Unternehmen beeinflusste. Besonders auffällig war der Rückgang des organischen Wachstums, der hauptsächlich durch Entlassungen in bestehenden Unternehmen verursacht wurde. Unternehmen, die auf organisches Wachstum setzten, zeigten hingegen eine stabilere Entwicklung und mussten weniger Stellen abbauen. Diese Unternehmen entwickelten sich langfristig nachhaltiger und vermieden die typischen Probleme, die Fusionen und Übernahmen oft mit sich bringen.

Der Rückgang der Unternehmensgründungen

Ein weiteres zentrales Ergebnis der Studie ist der signifikante Rückgang der Unternehmensgründungen nach der Finanzkrise. Start-ups gelten als Treiber für Innovation und wirtschaftliches Wachstum. Doch in den Jahren nach der Krise stagnierte die Zahl der Neugründungen in der Sicherheitsbranche. Dies könnte auf die zunehmende Konzentration durch Fusionen und Übernahmen hinweisen, die den Wettbewerb verringerten und das Innovationspotenzial dämpften. Ohne den Wettbewerb und die Dynamik junger Unternehmen fehlt der Branche oft die Risikobereitschaft, die für neue Gründungen erforderlich ist.

Darüber hinaus zeigte die Studie, dass Fusionen und Übernahmen in Krisenzeiten nicht die erhofften Vorteile brachten. Der Markt für potenzielle Käufer und Investoren war drastisch geschrumpft, was die Chancen für erfolgreiche M&A-Transaktionen stark einschränkte. Unternehmen, die auf Fusionen setzten, anstatt auf organisches Wachstum, gerieten zunehmend in Schwierigkeiten.

Junge Unternehmen und das Dilemma der Wachstumsdynamik

Die Studie deckt auch auf, dass junge Unternehmen in den Jahren nach der Finanzkrise langsamer wuchsen als etablierte Firmen. Diese Erkenntnis widerspricht der weit verbreiteten Annahme, dass Start-ups automatisch schneller wachsen und innovativer sind. Der Grund dafür liegt in der begrenzten Management-Kompetenz und den fehlenden Ressourcen, die jungen Unternehmen oft zu schaffen machen. In wirtschaftlich schwierigen Zeiten sind es die etablierten Unternehmen, die mit ihren Erfahrungen und Ressourcen schneller auf Herausforderungen reagieren können.

In der Sicherheitsbranche, in der mittelständische Unternehmen traditionell eine Schlüsselrolle in der Innovationskraft und Flexibilität spielten, ist der Verlust dieser Struktur besonders spürbar. Viele dieser Unternehmen wurden durch Fusionen in größere, weniger agile Strukturen integriert, was sowohl ihre Flexibilität als auch ihre Innovationskraft geschwächt hat.



Fazit: Organisches Wachstum als langfristiger Erfolgsfaktor

Die Ergebnisse der Studie belegen eindeutig, dass organisches Wachstum eine stabilere und nachhaltigere Wachstumsstrategie darstellt. Unternehmen, die auf ihre eigene Entwicklung und Expansion setzen, investieren in ihre Zukunft und schaffen langfristig erfolgreiche Strukturen. In der deutschen Sicherheitsbranche, die zunehmend von Fusionen und Übernahmen dominiert wird, könnte eine Rückbesinnung auf organisches Wachstum der Schlüssel zu einer langfristigen Erholung und Stabilität sein.
Die Branche sollte ihre Wachstumsstrategien neu ausrichten und stärker auf die Förderung von Innovation sowie die Schaffung neuer Arbeitsplätze setzen. Organisches Wachstum, das auf einer soliden Basis von Fachwissen, Erfahrung und Innovationskraft beruht, ist der langfristige Erfolgsweg. Kurzfristige Lösungen wie Fusionen und Übernahmen mögen in Krisenzeiten verlockend erscheinen, doch für eine gesunde und zukunftsfähige Entwicklung ist es der Aufbau neuer Ideen und Strukturen, der das Fundament für eine stabile Wirtschaft bildet.
In einer Welt, die von Unsicherheit und sich schnell verändernden Märkten geprägt ist, müssen Unternehmen ihre langfristige Resilienz aufbauen, indem sie in organisches Wachstum und Innovation investieren. Der Weg der kontinuierlichen, nachhaltigen Entwicklung wird nicht nur einzelne Unternehmen stärken, sondern auch die gesamte Branche auf ein solides Fundament stellen, das den Herausforderungen der Zukunft gewachsen ist.

Dr. Claudia Mrozek

salto
INSPIRED ACCESS



Vielseitige Zutrittslösungen

> HOHE SICHERHEIT
Salto Lösungen basieren auf modernsten Zutritts- und Sicherheitstechnologien, binden sämtliche Zutrittspunkte ein und bieten ein umfassendes Zutrittsmanagement.

> OPTIMIERTE PROZESSE
Salto digitalisiert und automatisiert Abläufe durch die Integration mit Management- und IT-Systemen sowie die Einbindung in Workflows.

> EFFIZIENTER BETRIEB
Anwender profitieren von flexibler Raumnutzung, hoher Sicherheit, optimierten Prozessen und niedrigen Lebenszykluskosten.

saltosystems.de

Mehr zu den Vorteilen und zum Funktionsumfang unserer Systemplattformen.

SALTO WECOSYSTEM


KONTROLLE
ÜBERNEHMEN
My Data Center
KENTIX ONE

‘Eine Lösung für Alles’

Im Interview mit Geschäftsführer Thomas Fritz (Foto links) erfahren wir mehr über KentixOne, die innovative Lösung von Kentix, die physische Sicherheit und IT-Infrastrukturschutz in einer Plattform vereint. In einer Zeit, in der Unternehmen zunehmend auf integrierte Systeme setzen, um ihre Sicherheits- und Infrastrukturüberwachung zu optimieren, bietet KentixOne eine einzigartige Kombination aus IoT-basierter Sensortechnologie, Echtzeit-Datenüberwachung und flexibler Skalierbarkeit. Das System ermöglicht es Unternehmen, alle relevanten Sicherheitsparameter zentral zu überwachen, während es gleichzeitig auf die spezifischen Anforderungen von Rechenzentren und kritischen Infrastrukturen zugeschnitten ist. Im Gespräch erklärt Geschäftsführer Fritz, wie KentixOne nicht nur den Aufwand für IT- und Sicherheitsabteilungen reduziert, sondern auch die Sicherheits- und Datenschutzanforderungen der digitalen Zukunft adressiert.

? Wie gelingt es Kentix, sich im Markt für IT- und Sicherheitslösungen zu differenzieren, insbesondere im Vergleich zu Wettbewerbern im Bereich der physischen Sicherheitsüberwachung und IT-Infrastruktursicherung?

Fritz: Unsere klare Differenzierung liegt in unserer Plattformlösung KentixONE. Sie vereint acht integrierte Systeme in einer einzigen Lösung, die sowohl netzwerkfähige Hardware als auch Software umfasst. Damit ersetzen wir bis zu acht separate Sicherheitssysteme und bieten eine umfassende Überwachung für mehr als 40 verschiedene Bedrohungsszenarien. KentixONE ist im Grunde genommen ein „Walled Garden“ für physische Sicherheit – eine komplett geschlossene, sichere Lösung, die unseren Kunden die komplexe Systemintegration abnimmt. Gleichzeitig haben wir bewusst Integrationsmöglichkeiten geschaffen, die wir als „Türen im Gartenzaun“ bezeichnen. So können unsere Kunden über REST-APIs oder VDS-Protokolle nahtlos andere Systeme anbinden. Diese Kombination aus umfassender Funktionalität, einfacher Integration und unserer typisch deutschen Qualitätsarbeit macht uns einzigartig. Sie verschafft uns einen klaren Wettbewerbsvorteil gegenüber anderen Anbietern in der Branche.

? Welche Zielmärkte und Branchen betrachtet Kentix als strategische Wachstumsfelder, und wie richten Sie Ihren Vertrieb gezielt auf diese Bereiche aus?

Fritz: Unsere strategischen Wachstumsfelder liegen vor allem in drei zentralen Bereichen. Erstens richten wir uns auf mittelständische Industrieunternehmen mit einer Mitarbeiterzahl von 50 bis 5.000. Zweitens haben wir einen starken Fokus auf kritische Infrastrukturen, wie Telekommunikationsunternehmen, Stadtwerke, Carrier und Energieversorger. Drittens zählen Rechenzentren zu unseren Schlüsselbranchen, insbesondere Colo-Flächen und White-Space-Ausstattungen.

Unsere Lösungen sind speziell für verteilte Infrastrukturen konzipiert und bieten ein hervorragendes Kosten-Nutzen-Verhältnis. Wir liefern eine vollständige Komplettlösung für die physische Unternehmenssicherheit – unsere Kunden müssen sich nicht mit der Integration einzelner Komponenten auseinandersetzen. Alles lässt sich nahtlos in bestehende Netzwerkinfrastrukturen integrieren, was den Einsatz unserer Systeme besonders effizient macht.

? Kentix bietet eine integrierte Lösung zur Überwachung von IT-Infrastrukturen und physischer Sicherheit. Über welche Vertriebskanäle vermarkten Sie Ihre Komplettlösung an unterschiedliche Kundengruppen wie KMUs, große Unternehmen oder Rechenzentren?

Fritz: Unsere Vertriebskanäle sind fast ausschließlich im IT-Channel angesiedelt. Wir arbeiten eng mit Systemhäusern, Integratoren und teilweise auch Installateuren zusammen. Vor etwa zwei Jahren haben wir jedoch eine strategische Neuausrichtung vorgenommen und uns vollständig auf den Direktvertrieb konzentriert.

Diese Entscheidung hat es uns ermöglicht, einen deutlich besseren Service zu bieten und unser Versprechen – „Sicherheitstechnik wird einfach und digital“ – konsequent einzulösen. Gleichzeitig haben wir ein sehr leistungsfähiges Shopsystem für unsere Partner entwickelt. Es bietet zahlreiche Vorteile in der Partnerberatung und -betreuung, die herkömmliche Distributoren schlicht nicht leisten können. Mit dieser Kombination aus direktem Kontakt, hochwertigem Service und digitaler Unterstützung erreichen wir unsere verschiedenen Kundengruppen effizient und passgenau.

? Wie gestaltet Kentix seine langfristigen Partnerschaften und Allianzen, um die internationale Reichweite zu erhöhen, und wie strukturieren Sie den Vertrieb an internationalen Standorten?

Genial. 8-in-1. KentixONE.

Zutrittskontrolle
Einbruchalarmierung
Umgebungsmonitoring
Brandfrüherkennung
Videoüberwachung
Netzwerk Monitoring
Externe Störmeldungen
Power Monitoring



Unsere Software **KentixONE** integriert ach Sicherheitssysteme in einer einzigen **IoT-Plattform** und ist damit die moderne Alternative zu herkömmlicher Sicherheitstechnik.

Fritz: Wir stehen kurz vor dem nächsten großen Schritt: Im kommenden Jahr werden wir in den ersten internationalen Märkten in Europa starten. Dabei setzen wir auf eine direkte Vertriebsstruktur mit eigenen Beratern vor Ort, kombiniert mit unserer leistungsstarken E-Commerce-Plattform.
Schon heute nutzen viele unserer internationalen Kunden unsere Shop-Plattform, um direkt bei uns einzukaufen. Hier zeigt sich einer unserer großen Vorteile: die Einfachheit und Effizienz unseres kompakten Produktportfolios. Mit nur rund 30 Kernprodukten, die sich vollständig um unsere Plattformlösung KentixONE drehen, können wir komplexe Anforderungen mit minimalem Aufwand abdecken.Dieser Ansatz – eine Kombination aus direkter Vor-Ort-Präsenz und digitalem Vertrieb – bildet die Grundlage für den Ausbau unserer internationalen Reichweite und für starke, langfristige Partnerschaften.

? Wie begegnet Kentix der wachsenden Nachfrage nach Cloud-basierten Lösungen und SaaS-Angeboten, und welche Vertriebsmethoden setzen Sie ein, um diese Angebote in einem zunehmend digitalen und serviceorientierten Markt erfolgreich zu positionieren?

Fritz: Mit KentixONE haben wir bereits 2020 eine umfassende Lösung auf den Markt gebracht, die diesen Trend aufgreift. Die Plattform basiert auf einer modularen Softwarearchitektur und wurde von unserem agilen Softwareteam entwickelt, das aus über 15 erfahrenen Entwicklern besteht. Diese Architektur ermöglicht sowohl den Einsatz als Appliance-Lösung On-Premises als auch als virtualisierte Lösung – ein hybrider Ansatz, der uns maximale Flexibilität gibt.

Wir beobachten, dass die Nachfrage unserer Kunden, insbesondere in Deutschland, noch stark On-Premises-orientiert ist. Dennoch bewegt sich der Markt zunehmend in Richtung Managed Cloud und SaaS-Angebote. Der Bereich Physical Security öffnet sich zwar langsam für Cloud-basierte Lösungen, wird aber aufgrund regulatorischer Anforderungen nie vollständig darauf umstellen können. Deshalb bleibt On-Premises für viele unserer Kunden eine zentrale Komponente.

In spezifischen Anwendungsbereichen, wie beispielsweise der Zutrittskontrolle mit unserem Kentix SmartAccess, sehen wir jedoch eine deutlich höhere Nachfrage nach SaaS-Lösungen. Hier greifen wir gezielt mit digitalen Vertriebswegen und unserer starken E-Commerce-Plattform an, die eine einfache Bereitstellung und Verwaltung unserer Lösungen ermöglicht. Dieser hybride Ansatz – kombiniert mit unserer modularen Technologie – erlaubt es uns, flexibel auf die Anforderungen eines zunehmend digitalen Marktes zu reagieren und gleichzeitig den unterschiedlichen Bedürfnissen unserer Kunden gerecht zu werden.

Technologie im 8-in-1-Format

? Nach dem Überblick über die strategische Ausrichtung und die Marktposition von Kentix wollen wir uns nun intensiver mit den technischen Aspekten und den Services des Unternehmens beschäftigen. Dabei werfen wir einen genaueren Blick auf die Hauptkomponenten der Plattform KentixONE, die zugrundeliegenden Technologien und die umfassenden Sicherheitslösungen, die Kentix für IT-Infrastrukturen und physische Sicherheit bietet. Im Fokus stehen unter anderem die Integration in bestehende IT-Systeme, innovative Sensortechnologien, moderne Alarmierungsmechanismen, Sicherheitsmaßnahmen zur Datenübertragung sowie die Rolle von künstlicher Intelligenz bei der Analyse von Sicherheitsdaten. Wir starten mit einem Blick auf die Kernmodule von KentixONE und deren Verbindung zu bestehenden IT-Infrastrukturen. Welche Hauptkomponenten bietet KentixONE, und wie fügt sich die Plattform in bestehende IT-Infrastruktur-Management-Systeme ein?

Fritz: Das Herzstück von KentixONE ist unsere Software, die auf all unseren Hardwareprodukten läuft und gleichzeitig als zentrales Managementsystem dient. Diese „Eine-für-Alles"-Lösung sorgt für eine besonders einfache Bedienung und bietet

durch ihre dezentrale Struktur ein hohes Maß an Sicherheit.
Zu den wichtigsten Modulen gehören die Zutrittskontrolle, die Umgebungsüberwachung mit Einbruch- und Brandfrüherkennung sowie die Videoüberwachung. Ein interessanter Aspekt bei der Integration in bestehende Systeme ist, dass viele Kunden feststellen, dass sie ihre bisherigen Managementlösungen gar nicht mehr benötigen. KentixONE ersetzt diese oft vollständig, was erhebliche Einsparungen bei Investitions- und Betriebskosten ermöglicht. Für Kunden, die KentixONE in ihre bestehende Infrastruktur einbinden möchten, bieten wir eine bestens dokumentierte REST-API an. Die notwendigen Informationen sind ganz einfach auf docs.kentix.com abrufbar.

? KentixONE bietet eine Lösung zur Überwachung von IT-Infrastrukturen und physischen Sicherheitsaspekten. Welche Sensortechnologien werden verwendet, um kritische Umgebungsparameter wie Temperatur, Feuchtigkeit und Zugangskontrolle zu überwachen?

Fritz: Unsere Bestseller sind nach wie vor die MultiSensoren, mit denen Kentix bereits 2010 in den Markt eingetreten ist. Alle unsere Produkte basieren im Wesentlichen auf MultiSensor-Technologie und kombinieren eine Vielzahl von Einzelsensoren in einem Gerät. Ein hervorragendes Beispiel ist unser MultiSensor mit einer Wärmebildkamera, der sowohl für die Umgebungsüberwachung als auch für die Brandfrüherkennung eingesetzt wird.

Dieser Sensor integriert insgesamt neun verschiedene Messwerte – darunter Wärmebild, VOC (flüchtige organische Verbindungen), CO, Temperatur, Luftfeuchtigkeit, Bewegung, Beschleunigung und Druck. Diese Kombination ermöglicht es, Entstehungsbrände frühzeitig zu erkennen und so teure Ausfälle zu vermeiden.
Die sogenannte „Sensorfusion" – die Verschmelzung unterschiedlicher Sensoren – zieht sich durch all unsere Produkte und ist einer der Hauptgründe für die Einfachheit und reduzierte Produktvielfalt. Wir fassen viele Funktionen zusammen und machen diese über das Netzwerk verfügbar.

? Wie funktioniert die Alarm- und Benachrichtigungsfunktion in KentixONE? Welche Optionen zur Eskalation von Alarmen bietet das System?

Fritz: In KentixONE setzen wir auf mehrstufige und redundante Alarmierungsmechanismen. Die erste Stufe umfasst optische und akustische Alarmierungen vor Ort, die sofort auf das Problem aufmerksam machen. Darüber hinaus bieten wir verschiedene Fernbenachrichtigungen wie E-Mail, Push-Nachrichten und redundante SMS, die über ein integriertes 4G-Modem gesendet werden. Ein besonders interessantes Feature bei den Push-Nachrichten ist, dass wir diese auch im Silent-Modus des Smartphones ausliefern können, dabei jedoch eine akustische Meldung aktivieren, um die Alarmaufmerksamkeit zu erhöhen.
Zusätzlich bieten wir die VDS2465-Übertragung zu Leistellen als Standard, was eine weitere Eskalationsstufe ermöglicht. So stellen wir sicher, dass alle relevanten Stellen rechtzeitig informiert werden, um schnell reagieren zu können.

? KentixONE nutzt IoT-basierte Geräte zur Überwachung. Welche Sicherheitsmaßnahmen werden ergriffen, um die Datenübertragung zwischen den Geräten und dem zentralen Managementsystem zu schützen?

Fritz: Um die Datenübertragung zwischen unseren IoT-basierten Geräten und dem zentralen Managementsystem zu sichern, setzen wir auf mehrere Sicherheitsstufen. Zunächst verwenden wir zertifikatsbasierte Kommunikation über TLS, wodurch die Datenübertragung verschlüsselt wird. Zusätzlich schützen wir die Nutzdaten durch eine weitere Verschlüsselung. Ein weiterer wichtiger Sicherheitsmechanismus ist die IEEE 802.1X Portauthentifizierung an den physikalischen Netzwerkanschlüssen. Das bedeutet, dass keine speziellen IP-Ports für die Kommunikation geöffnet werden müssen. Unsere Lösung entspricht vollständig den gängigen IT-Sicherheitsstandards und lässt sich problemlos in bestehende Cyber-Security-Stra- tegien von Unternehmen integrieren.
Darüber hinaus verfolgen wir einen „Security by Design"-Ansatz. Das heißt, sicherheitsrelevante Konfigurationen, wie etwa die Passwortkomplexität oder die Multi-Faktor-Authentifizierung, müssen nach vorgegebenen Sicherheitsrichtlinien eingestellt werden. Auch die Gerätekommunikation erfolgt über eine sichere Schlüsselvergabe. Wir überwachen potenzielle Bedrohungen wie DDS- und Brute-Force-Angriffe und melden diese umgehend. Ein weiteres Sicherheitsfeature ist die Möglichkeit, die Kommunikation mit KentixONE und unseren Geräten in granulare Netzwerke oder VLANs zu integrieren. Dies nennt man Mikrosegmentierung und hilft, die Angriffsfläche zu minimieren und somit zusätzliche Sicherheit zu gewährleisten.

? Wie lässt sich KentixONE in eine bestehende IT-Infrastruktur integrieren, um Daten in Echtzeit zu überwachen und Berichte zu generieren? Welche Schnittstellen und APIs werden unterstützt?

Fritz: Für uns bedeutet Echtzeitfähigkeit, dass Meldungen und Alarmdaten in weniger als einer Sekunde übermittelt werden. Um dies zu gewährleisten, setzt KentixONE eine spezielle State-Machine ein, die die eingehenden Daten priorisiert und entscheidet, welche Informationen die höchste Relevanz haben. So wird beispielsweise eine Brandmeldung vor einer Einbruchmeldung oder einer Temperaturwarnung verarbeitet.
Die Daten können dann über unsere gut dokumentierte REST-API oder über sogenannte Web-Hooks, also serverbasierte Events, in Echtzeit weitergegeben werden. Dabei können die Daten in verschiedenen Formaten wie JSON, TEXT oder XML strukturiert werden.
Für die Erstellung von Berichten bietet KentixONE ein eigenes Reporting-Modul,

das auf der gleichen REST-API basiert. Darüber hinaus unterstützen wir auch SNMP V2/3, einschließlich Traps, also Ereignismeldungen, die zur weiteren Verarbeitung genutzt werden können. Diese Flexibilität stellt sicher, dass KentixONE nahtlos in bestehende IT-Infrastrukturen integriert werden kann und eine umfassende Überwachung sowie detaillierte Berichterstattung ermöglicht.

? Was sind die Anforderungen an die Netzwerkarchitektur, um KentixONE effizient zu betreiben, insbesondere in großen oder verteilten Umgebungen?

Fritz: Im Grunde genommen kann KentixONE in jedem professionellen Netzwerk betrieben werden, unabhängig davon, ob es statisch oder dynamisch adressiert ist. Besonders vorteilhaft für größere oder verteilte Umgebungen sind jedoch segmentierte Netzwerke mit VLANs. Diese Struktur hilft, den Netzwerkverkehr effizient zu steuern und die Sicherheit zu erhöhen.
Wir haben zahlreiche Kunden aus den Bereichen Unternehmens- und Telekommunikationsumfeld, die KentixONE erfolgreich in weltweiten Netzwerken über mehrere Zeitzonen hinweg einsetzen. Die Flexibilität der Plattform ermöglicht es, auch in komplexen, global verteilten Infrastrukturen problemlos und zuverlässig zu arbeiten.

? Welche Funktionen bietet KentixONE zur Remote-Überwachung und -Steuerung, und wie kann es in eine zentrale Monitoring-Plattform integriert werden?

Fritz: KentixONE fungiert als zentrale Verwaltungsplattform für alle sicherheitsrelevanten Funktionen. Unser Ziel ist es, KentixONE als das zentrale System für das gesamte Sicherheitsmanagement zu etablieren. Die Plattform umfasst alle wichtigen Module, die für die Überwachung und Steuerung notwendig sind, darunter umfassende Logbücher, eine vollständige Visualisierung aller relevanten Daten und sogar Heatmaps zur Darstellung von Informationen. Zudem bietet KentixONE umfangreiche Reporting- und Alarmierungsfunktionen. Eine weitere wichtige Funktion ist die Möglichkeit zur Anbindung an LDAP- und AD-Dienste, was die Verwaltung von Tausenden von Benutzern vereinfacht. Zusätzlich können Nutzer über die Smart- phone-App auf dedizierte Funktionen zugreifen. So lässt sich KentixONE problemlos in eine bestehende Monitoring-Plattform integrieren und bietet eine umfassende Lösung zur Remote-Überwachung und -Steuerung.

? Wie wird die Skalierbarkeit von KentixONE sichergestellt, insbesondere bei der Überwachung von Standorten mit unterschiedlichen Sicherheitsanforderungen?

Fritz: Die Skalierbarkeit von KentixONE wird durch unsere moderne Softwarearchitektur und den dezentralen Ansatz gewährleistet. Das bedeutet, dass sich das System problemlos von kleinen Installationen mit wenigen Geräten bis hin zu großen Netzwerken mit Tausenden von Nutzern und Netzwerkknoten skalieren lässt. Dabei liegt der Fokus von Kentix jedoch nicht auf sehr großen zentralisierten Anwendungen wie in Städten oder bei Stadionüberwachungen. Vielmehr richten wir uns auf mittlere und verteilte Anwendungen, bei denen die Flexibilität und Anpassungsfähigkeit an unterschiedliche Sicherheitsanforderungen besonders wichtig sind.

? KentixONE bietet eine Software-as-a-Service-Lösung (SaaS). Welche Vorteile bietet diese Bereitstellungsform in Bezug auf Wartung, Updates und Skalierbarkeit?

Fritz: Der große Vorteil einer SaaS-Lösung wie KentixONE ist, dass sich unsere Kunden nicht um die technischen Details des Betriebs kümmern müssen. Die Software und alle Updates werden automatisch auf allen Hardwarekomponenten verteilt, was besonders bei sicherheitsrelevanten Updates sehr wichtig ist. Das komplette Deployment, wie etwa Sicherheitsupdates, erfolgt vollautomatisch. Ein weiterer Vorteil des SaaS-Modells ist die einfache Skalierbarkeit: Unsere Kunden können jederzeit neue Softwaremodule hinzubuchen, um KentixONE schnell an das Wachstum ihres Unternehmens oder Projekts anzupassen. Darüber hinaus bieten wir ein spezielles Modul, das unsere Kunden bei der Wartung und der Betriebsdokumentation unterstützt, sodass diese auch in diesem Bereich effizient arbeiten können.

? Welche Rolle spielt maschinelles Lernen oder künstliche Intelligenz bei der Analyse von Daten aus den KentixONE-Sensoren, insbesondere im Hinblick auf die Erkennung von Anomalien oder Sicherheits- vorfällen?

Fritz: Maschinelles Lernen und künstliche Intelligenz spielen eine zunehmend wichtige Rolle bei KentixONE, insbesondere wenn es darum geht, aus den gesammelten Sensordaten Anomalien zu erkennen oder Sicherheitsvorfälle frühzeitig zu identifizieren. Unsere Anwender profitieren bereits von einem KI-Assistenten, der die Nutzung der Dokumentation und Konfiguration erheblich vereinfacht.
Aktuell arbeiten wir an der Implementierung einer LLM (Large Language Model) Edge-Lösung, um die große Menge an Echtzeitdaten, die je nach Anwendung sehr umfangreich sein können, für den Nutzer besser aufzubereiten.
Das ist ein spannender Schritt, denn unsere moderne Softwarearchitektur ermöglicht es, diese Daten für KI-Systeme so zugänglich zu machen, dass sie kontinuierlich lernen und sich weiterentwickeln können. Das Besondere ist, dass wir mit dynamischen Echtzeitdaten arbeiten, was bedeutet, dass das KI-System ständig im Lernmodus ist und sich an neue Muster anpassen kann.
Außerdem freuen wir uns, auf unserem Partnertag am 15. Mai 2025 neue, interessante KI-Anwendungen vorzustellen, die unsere Lösung noch leistungsfähiger und effizienter machen werden.

[www.kentix.com] ml



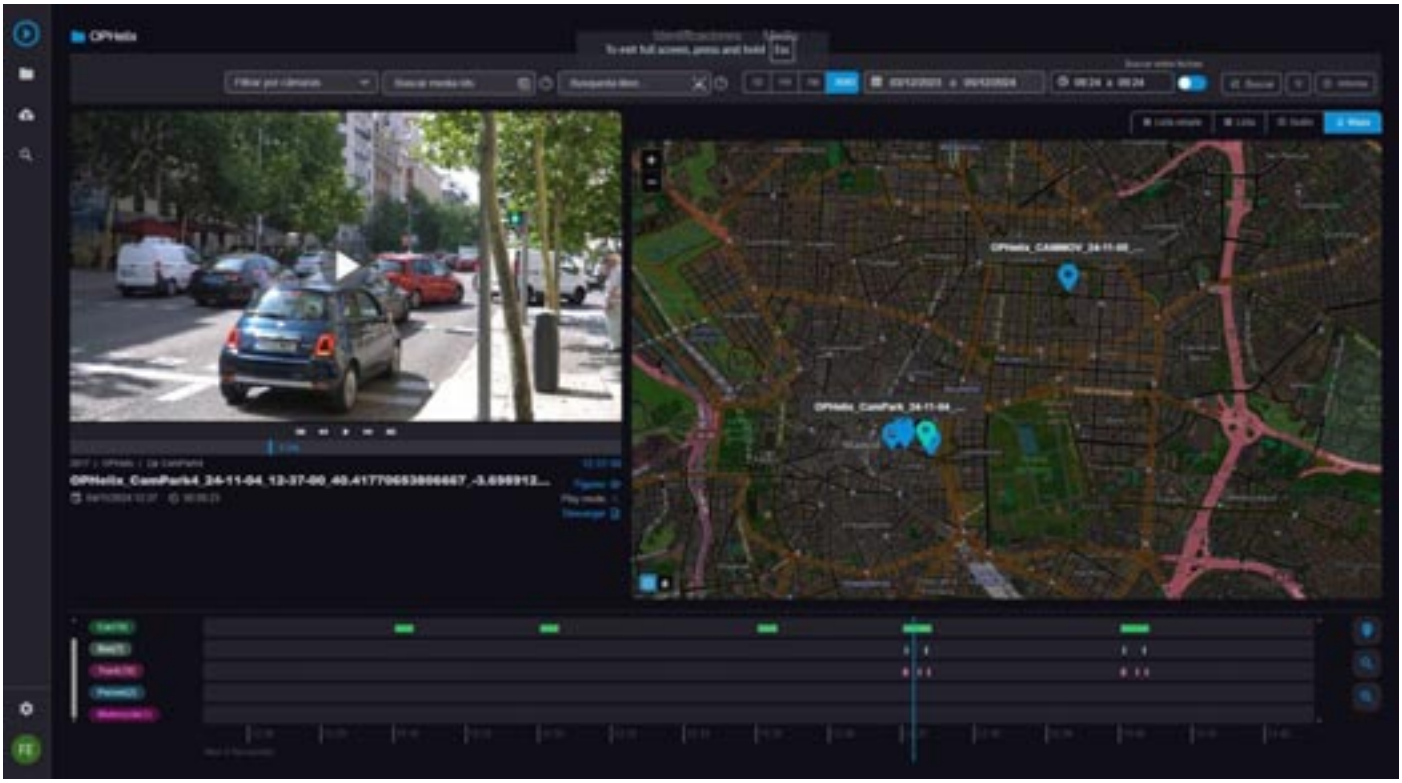
Schließanlage planen mit Blick auf Kosten & Sicherheit

ASSA ABLOY
Opening Solutions

Whitepaper Download: https://tinyurl.com/yc7nmars

Experience a safer and more open world

© ASSA ABLOY Sicherheitstechnik GmbH | WP1000_GB



Intelion: KI-Lösungen für Ermittlungen

ISID wird auf der GPEC 2025 die neuesten Funktionen für KI-Analyse und polizeiliche Ermittlungen präsentieren

Am 2. und 3. April 2025 wird ISID erneut als Aussteller an der General Police Equipment Exhibition & Conference (GPEC) in Leipzig teilnehmen. Die diesjährige GPEC Digital ist die Referenzveranstaltung für Strafverfolgungsbehörden zum Thema Digitalisierung und Elektronik für die öffentliche Sicherheit. Bei dieser Gelegenheit wird ISID die neueste Version seiner Intelion-Plattform für KI-Analyse und polizeiliche Ermittlungen präsentieren.

ISID, ein Technologieunternehmen mit Schwerpunkt auf KI-Lösungen und Plattformen für fortschrittliche Video- und Audiospeicherung und -analyse, wird erneut Aussteller auf der GPEC Digital 2025, sein, Europas führender geschlossener Fachmesse für Digitalisierung und Innovationen für die Polizei und alle Sicherheitsbehörden.

GPEC Digital 2025 in Leipzig

Die General Police Equipment Exhibition & Conference findet jedes Jahr im Congress Center in Leipzig statt. Die diesjährige Ausgabe ist die "GPEC Digital" und konzentriert sich mehr auf digitale Technologien und Software, die Strafverfolgungsbehörden und Geheimdiensten helfen sollen, ihre Arbeit effizienter, schneller und mit mehr Informatio zu erledigen, um bessere Entscheidungen treffen zu können. ISID stellt auf der GPEC aus, weil sich das Unternehmen hauptsächlich auf den öffentlichen und privaten Sicherheitsbereich sowie auf nationale Geheimdienste und Regierungsbehörden konzentriert.

Die ISID Lösungen sind darauf ausgelegt, die neuesten Technologien zu nutzen und Polizei- und Geheimdienstmitarbeiter bei ihrer Arbeit zu unterstützen, ihre Aufgaben zu vereinfachen und alle relevanten Informationen zu einem Fall bereitzustellen, die aus mehreren Quellen gesammelt und von KI analysiert und verarbeitet werden, um Ermittlungen zu verkürzen und zu beschleunigen und dabei zu helfen, mehr Fälle abzuschließen.

Die Intelion Plattform

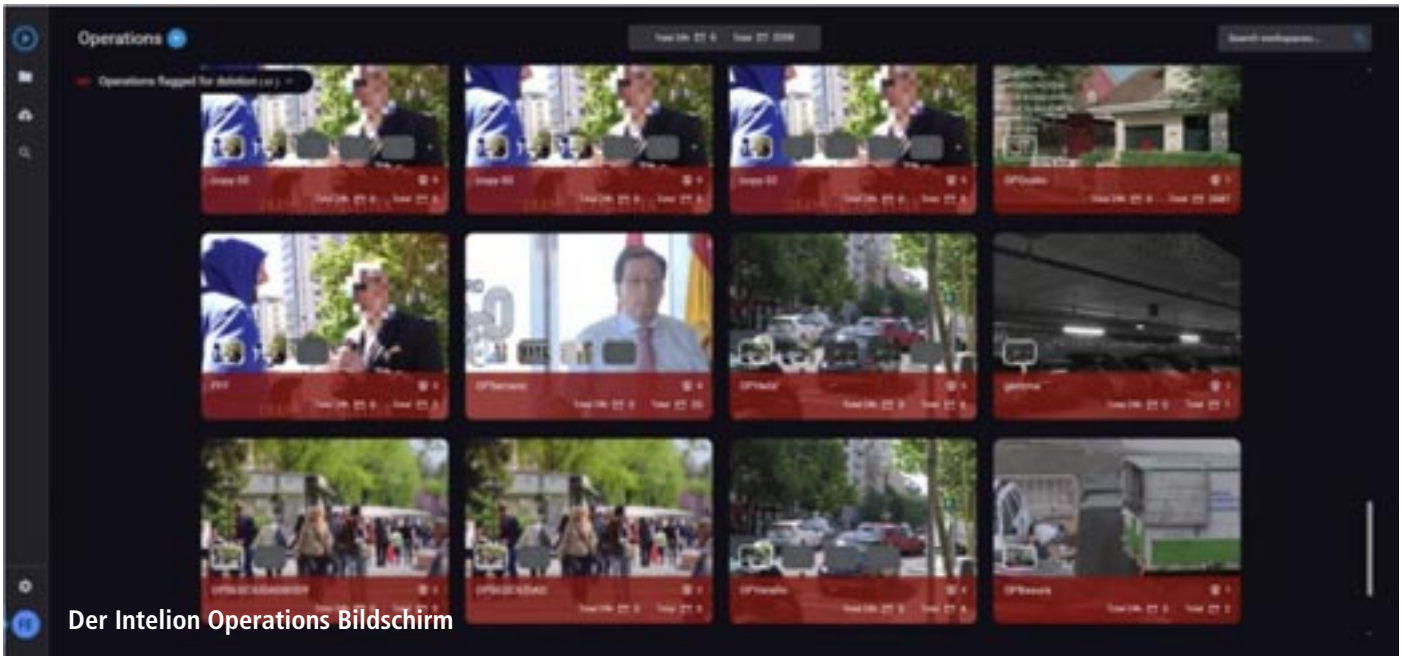
Unsere Intelion-Plattform für KI-Video- und Audioanalyse ist speziell auf den öffentlichen Sicherheitssektor zugeschnitten und bietet eine einzige Plattform, die alle Ermittlungsschritte und KI-Analysesysteme auf einem einzigen Bildschirm orchestriert. Die gleichzeitige Benutzung von anderen Systeme ist nicht erforderlich, da Intelion in vorhandene Geheimdienst- und Ermitt-

Verkada



Die führende Lösung für physische Sicherheit

Scannen Sie den QR-Code, um eine personalisierte Demo zu vereinbaren.



Der Intelion Operations Bildschirm

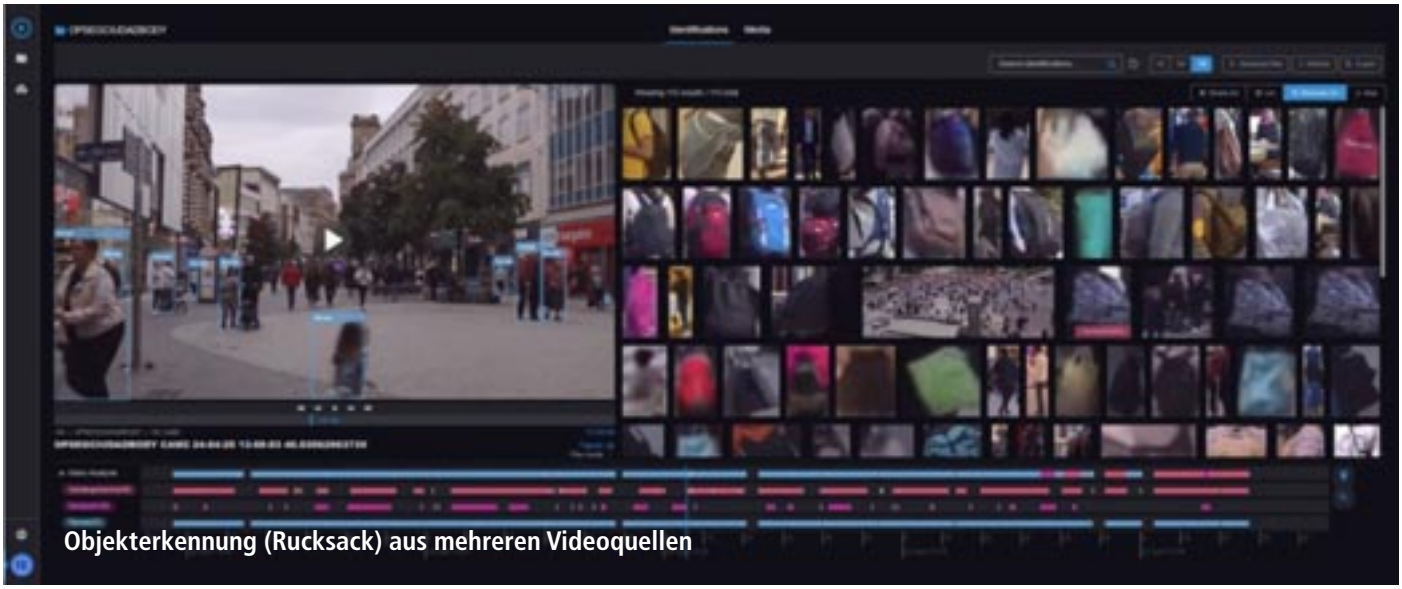
lungsplattformen integriert werden kann und dise informationen direkt anzeigen kann.

Der agnostische Intelion AI Bus ermöglicht die Verwendung beliebiger KI-Analysatoren von jedem Anbieter oder jeder Marke und integriert sie in den Ermittlungsablauf, um die Entscheidungsfindung, das Sammeln von Beweisen und die Verarbeitung von Hunderten von Kamera-Feeds, Video- oder Audiodateien zu erleichtern.
Das bedeutet, dass bereits vorhandene KI-Analysatoren beibehalten werden können, was die Gesamtbetriebskosten des Systems senkt, die Ersteinrichtung vereinfacht und die Lernkurve für alle Mitarbeiter verkürzt, die bereits mit ihren Analysatoren vertraut sind.

Analysefunktionen

Die Intelion-Plattform kann jeden Typ von KI-Analysator auf dem Markt integrieren, und die meistbenutzten sind bereits kompatibel und erfordern wenig bis gar keine Integrationsarbeit. Die Vielfalt der unterstützten Analysatoren reicht von Gesichtserkennung, Objekterkennung, Audio-Fingerabdruck, Sprache-zu-Text, Übersetzung, OCR und dergleichen bis hin zu spezifischeren Typen wie Drohnenmodellen für Lufterkennung oder geräuschresistente Transkription.

Jeder aktuelle oder zukünftige Analysator kann in die Plattform integriert und Teil des Workflows sein. Intelion unterstützt auch mehrere Analysatoren desselben Typs gleichzeitig (z. B. Sprache-zu-Text), um in


Objekterkennung (Rucksack) aus mehreren Videoquellen

jedem Fall die qualitativ hochwertigsten Daten zu erhalten, da die KI-Modelle, auf denen die Analysatoren basieren, unterschiedlich sind.

24/7-Überwachung mit Workflow-Automatisierung

Das Beobachten von Überwachungs- oder Verkehrskameras in einer Kommandozentrale ist mühsam und erfordert qualifiziertes Personal, das andernfalls interessantere und produktivere Aufgaben erledigen könnte. Deshalb kümmert sich Intelion um die gesamte Überwachung und erfordert nur dann Aufmerksamkeit, wenn etwas Bemerkenswertes passiert.

Intelion bietet eine einzige Schnittstelle mit allen verfügbaren Tools und arbeitet rund um die Uhr unbeaufsichtigt mit seiner benutzerprogrammierbaren Regel-Engine, die auf intelligente Weise Informationen von Überwachungskameras oder anderen A/V-Geräten sammelt und analysiert. Dieses anpassbare Modul zur Workflow-Automatisierung nimmt den Polizeibeamten den größten Teil der Analyselast ab und gibt ihnen so die Möglichkeit, wertvollere Aufgaben zu erledigen. Es ermöglicht die Festlegung von Prioritäten für die Bearbeitung wichtigerer Fälle und umfasst ein intelligentes Filtersystem, das die Belastung der Analyse-Engine um bis zu 70% senkt und nicht relevante Video- oder Audiosegmente (keine Bewegung, keine Personen, keine Autos usw.) ignoriert.

Systemsicherheit und Skalierbarkeit

Intelion ist aufgrund seiner Anwendung im Sicherheits- und Geheimdienstbereich als On-Premise-Lösung konzipiert, kann aber sicher mit externen Quellen verbunden werden, um Audio-/Videodateien oder Streams aufzunehmen. Die Plattform kann auch Dateien über das Internet in speziellen Ordnern empfangen, sodass die einkommenden Medien sofort analysiert werden können. An jede Videoquelle verbundene geografische Positionsdaten helfen bei der Ortung von Verdächtigen, wenn diese entweder anhand ihres Gesichts, ihrer Stimme oder eines Nummernschilds identifiziert werden, und lösen einen Alarm bei allen zuständigen Personen aus.

Das System selbst ist skalierbar und kann seine Leistung bei Bedarf und bei steigender Anzahl von Fällen mit digitaler Medienanalyse schrittweise anpassen. Durch einfaches Hinzufügen weiterer Hardware erhält die Plattform mehr Verarbeitungsleistung und erfordert fast keine Änderungen an ihrer Konfiguration oder in den meisten Fällen ist sogar das Anhalten der Plattform unnötig.

Intelion kann in bereits vorhandene VMS-Systeme integriert werden und bietet so dem VMS, das für die Verarbeitung der eingehenden Video-Feeds, Dateien und Streams zuständig ist, eine KI-Analyse-Intelligenzebene. Dadurch können die Analyseanforderungen von Intelion reduziert und gleichzeitig mehr Signale oder Dateien effizient verarbeitet werden.

Plattform-Anwendungsfälle

Intelion ist eine vielseitige Plattform und kann je nach Einsatz und spezifischen Anforderungen in verschiedenen Szenarien eingesetzt werden. Sie ist vollständig konfigurierbar und kann in den Bereichen





Das Intelion Leistungs-Dashboard

Strafverfolgung und Geheimdienst für verschiedene Zwecke eingesetzt werden. Zu den häufigsten zählen die folgenden:

- Media Investigation. Intelion Media Investigation wurde speziell zur Unterstützung polizeilicher und geheimdienstlicher Ermittlungen entwickelt und ist eine Lösung, die die Aufnahme großer Mengen von Multimediadateien oder Audio- und Videosignalen ermöglicht, die bei Überwachungsoperationen (z. B. von Kameras) generiert werden. Zudem automatisiert es die Analyse-, Dokumentations- und Überprüfungsaufgaben der Videos. Dadurch wird der Zeit- und Ressourcenaufwand für die Anzeige von Videoinhalten oder Kamera-Feeds reduziert und es werden automatische Analysen und Alarme bei Erkennungen bereitgestellt.

- Digital Evidence Management System. Moderne Beweise in Polizeifällen sind heutzutage größtenteils digital. Computer, Smartphones und das Internet liefern Videos, Fotos, Audioaufnahmen, Dokumente oder Social-Media-Inhalte, die zur Aufklärung eines Falles beitragen können. Die Datenmenge, die als digitale Beweise gesammelt werden kann, ist jedoch enorm und erfordert ein System, das in der Lage ist, alle Informationen zu verwalten, sie zu interpretieren, zu analysieren und aus den Daten Schlussfolgerungen zu ziehen. Intelion Digital Evidence Management bietet eine vollständige Umgebung zum Sammeln, Speichern, Analysieren und Teilen digitaler Beweise für Strafverfolgungsbehörden sowie zur Aufrechterhaltung der Beweiskette.

- Safe City. Die Intelion Safe City-Variante kann mit jedem VMS verbunden werden und die Sicherheitsinfrastruktur für eine Smart City- oder Safe City-Initiative verbessern. Intelion fügt dem VMS KI-Analyseebenen hinzu, sodass Hunderte oder Tausende von Kamera-Feeds überwacht und nach bestimmten Elementen wie Gesichtern, Nummernschildern, Objekten usw. durchsucht werden können. Intelion funktioniert sowohl in Echtzeit als auch auf ad hoc Basis.

Intelion Routen Analyse auf YouTube
youtube.com/watch?v=PUqS2mxlTws

ISID ist ein spanisches und globales Unternehmen, das Lösungen und Plattformen für die Verarbeitung, Analyse, Verwaltung und Speicherung von Audio und Video entwickelt. Unsere Lösungen integrieren fortschrittliche KI-Analysemodule (wie Biometrie, S2T, Übersetzung, Objekterkennung, Audio-Fingerabdruck und ID usw.) und werden in zahlreichen Sektoren eingesetzt, wie z. B. Sicherheit, Regierung und öffentliche Verwaltung, Strafverfolgung, Geheimdienst, Kommunikationsbehörden, Bildung, Gesundheitswesen und Recht. Sie sind KI-anbieterunabhängig und können in die Prozesse und Arbeitsabläufe der Kundenorganisation integriert werden.

[www.isid.com/sector/security]



Videosicherheit: Modular, zentral, cloudbasiert

Multifocal-Sensortechnik im Fernzugriff und modulare Management Software in der Azure-Cloud
Zentral verwaltete Videosicherheit auf fast 180 Bahnhöfen der dänischen Staatsbahnen

Die DSB betreiben den Personennahverkehr auf nahezu allen Eisenbahnstrecken in Dänemark. Auch die internationale Magistrale Schweden–Deutschland und das innerstädtische Schnellbahnnetz Kopenhagens fallen in ihren Verantwortungsbereich.
Bei der Sicherheit vertrauen die Dänischen Staatsbahnen (DSB) seit 20 Jahren auf die Videotechnik des deutschen Herstellers Dallmeier und bei der Betreuung und Vor-Ort-Installation auf das dänische Unternehmen SCANVIEW A/S.

Vor kurzem nahm die nächste Ausbaustufe ihren Betrieb auf:

laubt es beliebig vielen Operatoren von der DSB-Hauptzentrale in Kopenhagen aus individuell auf die Videobilder sämtlicher Standorte zuzugreifen.
Umfassende Darstellungs- und Vorfallsmanagement-Funktionen gewährleisten die effiziente Verfolgung, Intervention und Aufklärung eines Geschehnisses.

Dänische Staatsbahnen (DSB)
Die Danske Statsbaner (DSB) sind die dänischen Staatsbahnen, die den Personenverkehr auf den wichtigsten Eisenbahn- strecken in Dänemark und auf der internationalen Magistrale Schweden–Deutschland sowie den S-og von Kopen- hagen betreiben. Die DSB betreibt in der Umgebung der dänischen Hauptstadt Kopenhagen ein Nahverkehrssystem, die so genannte S-Bahn, die die verschiedenen Gebiete und Vororte des Großraums miteinander verbindet.

Anforderung: Kompatibel mit Microsoft Azure Cloud - Durchgängig gerichtsverwertbare Aufnahmen - Komplexes Nutzer- und Rechtemanagement - Flexibilität und Kompatibilität

„Durch die Kombination aus Dallmeier Kameratechnologie, Cloud-Deployment und der Management-Komponenten der Hemisphere® steht uns ein äußerst leistungsfähiges System zur Verfügung."
Søren H. Nielsen,
technischer Leiter Dänischen Staatsbahnen (DSB)

Mit den Dallmeier Hemisphere® Software-Komponenten in der Azure-Cloud und über 2.500 Kameras garantiert die DSB ihren Passagieren und Mitarbeitern ein Höchstmaß an Sicherheit.

Wo viele Menschen zusammentreffen, passieren auch unangenehme Dinge. Diebstähle und Handgreiflichkeiten, aber auch der Vandalismus an abgestellten Zügen oder Drogendelikte zählen zu den tagtäglichen Vorkommnissen an Bahnhöfen und Abstellgleisen. Um hier effizient und zeitnah intervenieren zu können, verlässt sich die Dänische Staatsbahn auf eine Videosicherheitslösung von Dallmeier. Diese er-

Flexibilität durch Cloud: Wesentliche Hemisphere® SeMSy® Komponenten laufen in Microsoft Azure

Von der Kopenhagener Hauptzentrale der Dänischen Staatsbahnen haben die zuständigen Sicherheitsverantwortlichen über die Hemisphere® SeMSy® Videomanagement-Lösung stets alle Geschehnisse an den Bahnhöfen im Blick. Dabei laufen die wesentlichen Software-Komponenten in der von der DSB als IT-Backbone betriebenen Microsoft Azure Cloud. So sind alle Prozesse wie das Management der Systeme, Rechte- und Userverwaltung aber auch die Zuwei-



sung von Rechenleistung zentral und flexibel möglich.

Aufgaben erfüllen ohne Ablenkung

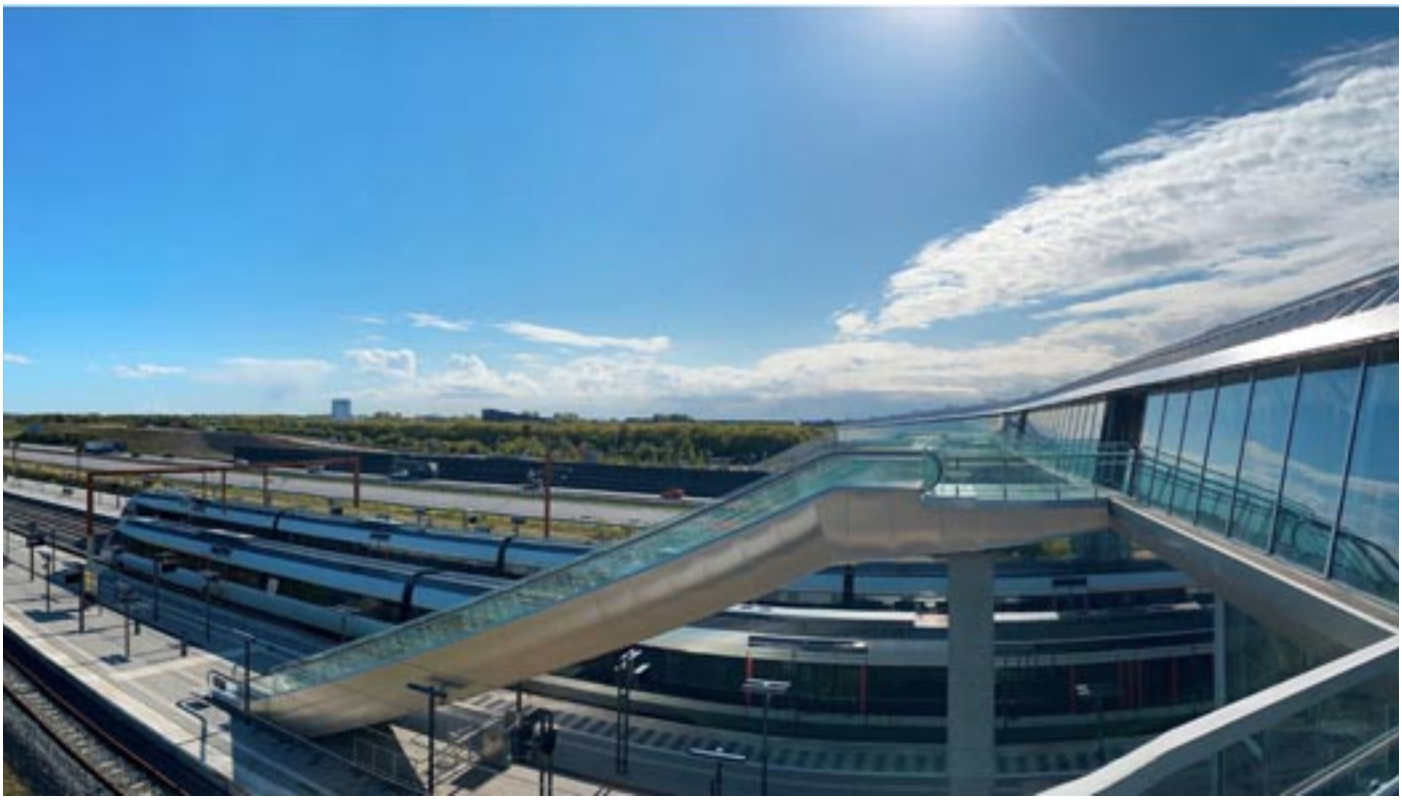
Durch die zentrale Bereitstellung der Komponenten können die Operatoren von dort schnell und mit optimaler Übersicht auf jede einzelne der 2.500 Single-Sensorkameras sowie auf alle Panomera® Multifocal-Sensorsysteme zugreifen. Eine individuelle Konfigurierbarkeit der einzelnen Arbeitsplätze und Ansichten der User stellt sicher, dass jeweils nur die für die spezifischen Tätigkeiten nötigen Widgets sichtbar sind. Somit können die Mitarbeiter ihre spezifischen Aufgaben ohne Ablenkung zielgerichtet erfüllen.

Weit mehr als Video: Maps und digitales Vorfallsmanagement

Die Module der Hemisphere®-Plattform erlauben neben dem klassischen Videomanagement ein benutzerfreundliches, schnelles Zusammenstellen und Erfassen aller relevanten Falldaten, wie Fotos, Videos oder Zeugenaussagen und das Weiterleiten derselben in einer digitalen Vorfallsakte.

Darüber hinaus integriert Hemisphere® einen genauen Lageplan der einzelnen Standorte. Mit Hilfe dieser Map-Funktion können Operatoren und Sicherheitsverantwortliche im Falle registrierter Vorfälle die





benötigte Kamera bequem anwählen. Die Bedienung der Systeme durch die Operatoren erfolgt über Dallmeier Workstations und eine Monitorwall bestehend aus 22 Hemisphere® SeMSy® Variodecodern.

Die einfache und verlustfreie Aufschaltung auf jeden einzelnen Bahnhof garantiert Dallmeier „PRemoteHD", ein durch Transcodierung bandbreiteschonendes Verfahren, das den Zugriff auf hochauflösendes Videomaterial selbst bei schwacher Internetanbindung ermöglicht.

„Hemisphere® SeMSy® ersetzt bzw. ergänzt viele der bisher durch die DSB verwendeten Systeme und verbessert so unseren Workflow in Effizienz und Qualität.

Durch die Kombination aus Dallmeier Kameratechnologie, Cloud-Deployment und der Management-Komponenten der Hemisphere® steht uns ein äußerst leistungsfähiges System zur Verfügung, das weit mehr bietet als klassisches Videomanagement, " erklärt Søren H. Nielsen, technischer Leiter DSB.

Die Modulare Dallmeier Hemisphere® Software-Plattform ermöglich neben einer Vielzahl von Management-Aufgaben z.B. auch das Erstellen und Weiterleiten einer digitalen Vorfallsakte bei entsprechenden Ereignissen.





Weite Strecken und große Flächen – kein Problem dank Panomera® Multifocal-Sensortechnologie

Die meisten Bahnhöfe in Dänemark sind weitläufig. Parkplätze, Shoppingmöglichkeiten und Warteplattformen sind alles Bereiche, die es zu überwachen gilt. Die Schwierigkeit lag darin, die hohe Mindestauflösungsqualität für eine Gerichtsverwertbarkeit der Aufnahmen (beschrieben in der DIN-Norm DIN EN 62676-4) auf der gesamten Fläche zu erfüllen. Bei der von der DSB eingesetzten, patentierten Panomera® Technologie sind bis zu acht Sensoren unterschiedlicher Brennweiten in einer optischen Einheit zusammengefasst. Das Ergebnis ist ein durchgängig hochauflösendes Gesamtbild, in das zudem live und in der Aufzeichnung beliebig viele Detail-Zooms erfolgen können. So erfasst Panomera® enorme Weiten und Flächen mit einem über den gesamten Objektraum gleichbleibenden Auflösungsraster in Echtzeit – und das mit sehr wenigen Kamerasystemen.
Das liefert nicht nur durchgängig gerichtsverwertbare Aufnahmen, sondern spart darüber hinaus einen Großteil der Infrastrukturkosten im Vergleich zu konventionellen Lösungen ein.
Der Bahnhof Køge Nord ist einer von 298 Bahnhöfen der Dänischen Staatsbahnen. Möglichst viel in einem Bild erfassen, und das in hoher Auflösung: Ein wesentlicher Aspekt für die Sicherheit bei großen Arealen.

Echte Enterprise-Fähigkeit für eine komplexe und dynamische Umgebung

Die Dänischen Staatsbahnen beschäftigen mehr als 7.000 Mitarbeiter. Davon finden sich über 1.000 Stellen in der Verwaltung. Derartige Größenordnungen bringen für die Videoüberwachung von derzeit 180 Bahnhöfen ein komplexes Nutzer- und Rechtemanagement mit sich.

Dazu kommt, dass nicht nur Mitarbeiter, sondern auch Behörden, wie die Polizei, auf das Videoinformationssystem zugreifen dürfen und auch müssen. Hier den Überblick über die Rechtevergabe zu behalten, ist aus Datenschutz- und Sicherheitsgründen von kritischer Bedeutung. Hemisphere® lässt sich deshalb nahtlos in die Active Directory Nutzerverwaltung der DSB integrieren.

Auch das stetige Aktualisieren der Anlagen birgt Herausforderungen. Bei komplexen Projekten, die über viele Jahre gehen, ist meist nur eine schrittweise Modernisierung umsetzbar. Im Zuge dessen spielt vor allem die Abwärtskompatibilität der neu implementierten Systeme eine ausschlaggebende Rolle. Hemisphere® bietet die Möglichkeit bereits bestehende Systeme, auch unabhängig vom ursprünglichen Anbieter, in eine neue Umgebung zu integrieren und ermöglicht den Kunden so, schrittweise zu migrieren. Umfassende Testphasen, wie der Dallmeier „Factory Acceptance Test" (FAT), runden diese Einbindung ab und gewährleisten sowohl umfassende Sicherheit als auch ein optimales Funktionieren der Anlage bei Inbetriebnahme.

„Bereits 2016 aktualisierten wir bei den Dänischen Staatsbahnen das Videomanagementsystem mit dem Dallmeier SeMSy III VMS-System. Mit der Migration zur Hemisphere® Plattform mit der neuen Generation des SeMSy VMS und weiteren Modulen im Jahr 2020 stand uns eine Art Baukastenprinzip aus Videomanagement, Datenmanagement und Frontend-Applikationen zur Verfügung. So konnten wir zusammen mit der DSB exakt die für die derzeitigen Anforderungen passende Gesamtlösung kostenoptimiert „zusammensetzen". Gleichzeitig sind wir durch die Vielzahl an weiteren Funktionen und Modulen für zukünftige Anforderungen bestens aufgestellt," so Torsten Ussing, MD SCANVIEW A/S.

Nicht nur die Produkte zählen

Seit den digitalen Wavelet-Rekordern der frühen 2000er Jahre verlassen sich die DSB auf Produkte des deutschen Herstellers Dallmeier und die operative und technische Betreuung durch seinen skandinavischen Exklusivpartner SCANVIEW. Um das Bestehen einer derart langen Zusammenarbeit aufrecht zu erhalten, bedarf es eines hohen Maßes an Flexibilität. Kurzfristiges Agieren, kundennahe Bevorratung von Ersatzteilen und kurze Lieferzeiten stellen dabei unumgängliche Prämissen dar.

Aber auch die Gewährleistung von Datenschutz und Cybersecurity sind notwendige Themen, gerade bei der Videobeobachtung im öffentlichen Raum und im Zeitalter der DSGVO. Die Entwicklung und Fertigung der Dallmeier-Produkte erfolgt zu 100 % in Deutschland und folgt den DSGVO-Richtlinien „Security by Design" und „Privacy by Design". Sowohl die Dänischen Staatsbahnen als auch ihre Passagiere profitieren so von höchsten Standards bei Datenschutz und Datensicherheit.

Transformative Trends im Sicherheitssektor

Einblick in den 2025 Global Technology Outlook Report von Securitas Technology

Im 2025 Global Technology Outlook Report präsentiert Securitas Technology eine umfassende Analyse der bedeutendsten technologischen Entwicklungen im Bereich elektronischer Sicherheitslösungen. Der Bericht beleuchtet, wie Unternehmen neue Technologien nutzen können, um Sicherheitsprogramme zu optimieren, operative Herausforderungen zu meistern und zukunftsweisende Strategien zu entwickeln. Im Fokus stehen die Bereiche Künstliche Intelligenz (KI), Cloud-Technologie, Cybersicherheit, Nachhaltigkeit sowie aufstrebende Technologien.

Kernpunkte und Erkenntnisse

Künstliche Intelligenz (KI) und Datenanalyse

KI und Datenanalyse setzen neue Maßstäbe in der Sicherheitsbranche. Durch KI-gestützte Videoanalysen und Anomalie- erkennung können Unternehmen Sicherheitsvorfälle proaktiv identifizieren und verhindern. Dies ermöglicht nicht nur eine zeitnahe Reaktion auf Bedrohungen, sondern entlastet auch Personal, indem repetitive Aufgaben automatisiert werden. Der Bericht betont jedoch die essenzielle Rolle des Menschen, insbesondere bei kritischen Entscheidungen. Diese symbiotische Beziehung zwischen technologischer Effizienz und menschlicher Urteilsfähigkeit ist entscheidend, um Sicherheitslösungen effektiv einzusetzen.

Cloud-Technologie

Die Migration zu cloudbasierten Sicherheitstechnologien erfährt eine zunehmende Akzeptanz. Cloud-Lösungen bieten eine Kombination aus Flexibilität, Kosteneffizienz und Skalierbarkeit. Zentralisierte Datenmanagementsysteme und fortschrittliche Analysefunktionen sind zentrale Vorteile, die die betriebliche Effizienz steigern. Dennoch bestehen Vorbehalte hinsichtlich der Cybersicherheit, insbesondere in Bezug auf Datenschutz und potenzielle Angriffe. Hybride Cloud-Modelle und kontinuierliche Schulungen werden als Lösungsansätze vorgestellt, um diese Bedenken zu adressieren.

Cybersicherheit und Datenschutz

Mit der zunehmenden Vernetzung von Sicherheitssystemen steigt das Risiko für Cyberangriffe. Der Bericht unterstreicht die Dringlichkeit eines „cyber-first"-Ansatzes, der Cybersicherheit in den Mittelpunkt strategischer Entscheidungen rückt. Best Practices, wie regelmäßige Software-Updates und Benutzerverwaltungsprotokolle, sind entscheidend, um Sicherheitslücken zu schließen. Internationale Regulierungen, etwa die NIS2-Richtlinie der EU, bieten Orientierungshilfen für Unternehmen, die eine robuste Cybersicherheitsstrategie implementieren wollen.

Nachhaltigkeit

Nachhaltigkeit hat sich zu einem zentralen Aspekt der Sicherheitsbranche entwickelt. Der Bericht zeigt auf, wie energieeffiziente Produkte und optimierte Gebäudenutzung mithilfe von Sicherheitsdaten zur Reduzierung des ökologischen Fußabdrucks beitragen können. Fernwartung und die Nutzung cloudbasierter Technologien reduzieren zusätzlich Emissionen. Unternehmen werden aufgefordert, mit Partnern zusammenzuarbeiten, die klare Nachhaltigkeitsziele verfol- gen und transparente Informationen über die Umweltver- träglichkeit ihrer Produkte bereitstellen.

Aufstrebende Technologien

Edge-Analytics, kontaktlose Biometrie und erweiterte Realität (AR/VR) gehören zu den innovativen Technologien, die Sicherheitslösungen revolutionieren. Edge-Kameras ermöglichen eine dezentrale Datenverarbeitung, wodurch die Abhängigkeit von zentralen Servern reduziert wird. AR-basierte Anwendungen verbessern die Effizienz von Wartungsarbeiten und senken Betriebskosten. Diese Technologien verheißen eine neue Ära der Sicherheitsverwaltung, die durch Effizienz und Innovation geprägt ist.

Empfehlungen für Unternehmen

- Strategische Investitionen: Unternehmen sollten in KI, Cloud-Technologien und fortschrittliche Analysewerkzeuge investieren, um Sicherheitsprogramme effektiver zu gestalten.
- Proaktive Cybersicherheitsstrategien: Die kontinuierliche Überwachung von Cybersicherheitsrisiken und regelmäßige Systemaktualisierungen sind unerlässlich, um Angriffe abzuwehren.
- Nachhaltigkeitsinitiativen: Sicherheitslösungen sollten darauf ausgerichtet sein, ökologische Ziele zu unterstützen, beispielsweise durch Energieeinsparungen und optimierte Betriebsabläufe.
- Schulung und Zusammenarbeit: Die Kombination von technologischen Innovationen und menschlicher Expertise ist entscheidend, um langfristige Erfolge zu erzielen.

Fazit

Der 2025 Global Technology Outlook Report skizziert eine klare Vision für die Zukunft der Sicherheitsbranche. Unternehmen stehen vor der Herausforderung, technologische Trends zu adaptieren und dabei Risiken zu minimieren. Gleichzeitig bietet sich die Chance, durch innovative Sicherheitslösungen Wettbewerbsvorteile zu sichern und nachhaltige Praktiken zu fördern. Die Sicherheitsindustrie befindet sich an einem Wendepunkt, an dem Fortschritt nicht nur durch Schutz, sondern auch durch betriebliche Effizienz und Umweltverantwortung definiert wird. Dieses Gleichgewicht zwischen Technologie und Verantwortung wird die Zukunft der Branche entscheidend prägen.Der Bericht Directors and Officers (D&O) Insurance Insights 2025 von Allianz Commercial beleuchtet die wichtigsten Risiken und Entwicklungen im Bereich der D&O-Versicherungen, die Unternehmen und Führungskräfte im Jahr 2025 betreffen.



Hier ist eine Zusammenfassung der zentralen Inhalte:Geopolitische und regulatorische Herausforderungen

- Globale Unsicherheiten: Der Krieg in der Ukraine, Spannungen zwischen den USA und China sowie andere Konflikte führen zu Risiken wie Lieferkettenstörungen, Geschäftsausfällen und regulatorischer Überprüfung.
- Regulatorischer Druck: Es gibt eine intensivere Überwachung der Einhaltung von ESG-Vorschriften (Umwelt, Soziales, Governance). Die Gefahr von Greenwashing-Klagen wächst, wie der Erfolg der australischen Regulierungsbehörde 2024 zeigt.
- Sanktionen: Nichteinhaltung internationaler Sanktionen kann zu rechtlichen und finanziellen Konsequenzen führen.

Technologische Risiken

- Künstliche Intelligenz (KI): Risiken wie "AI Washing" (übertriebene KI-Ansprüche), Datenschutzverletzungen, und KI-"Halluzinationen" (fehlerhafte Ergebnisse) stehen im Fokus. Die EU hat im August 2024 den weltweit ersten umfassenden AI-Gesetzesrahmen verabschiedet.
- Rechtsstreitigkeiten: In den USA stieg die Zahl der KI-bezogenen Sammelklagen. In einem Fall musste Meta eine Strafe von 1,4 Milliarden US-Dollar wegen Verstößen gegen Datenschutzgesetze zahlen.

Wirtschaftliche Unsicherheiten

- Insolvenzen: Steigende Insolvenzen (+11 % im Jahr 2024, +2 % erwartet für 2025) erhöhen die Haftungsrisiken für D&Os, da Aktionäre oder Gläubiger bei finanziellen Verlusten Klagen einreichen können.
- Branchenspezifische Herausforderungen: Bau, Einzelhandel und Dienstleistungen sind besonders betroffen, da sie unter erhöhten Kreditkosten und wirtschaftlichen Unsicherheiten leiden.

Entwicklungen im D&O-Versicherungsmarkt

- Preisrückgänge: Der Markt bleibt wettbewerbsintensiv, mit sinkenden Prämien und verbesserten Vertragsbedingungen.
- Regionale Unterschiede: In Asien und Europa sind die Prämienrückgänge ausgeprägter. In den USA stabilisieren sich die Raten, während die Schadenhäufigkeit steigt.
- Litigation Funding: Drittfinanzierung von Klagen führt zu mehr Klagen und höheren Streitwerten, was Versicherungen belastet.

Handlungsempfehlungen für Unternehmen und Führungskräfte

- Aktualisierung der Risikoüberwachung: Regelmäßige Updates zu geopolitischen und regulatorischen Änderungen sind unerlässlich.
- Sorgfältiger Umgang mit KI: Unternehmen sollten Richtlinien und Audits implementieren, um KI-Einsätze zu kontrollieren.
- Erweiterung von D&O-Deckungen: Vor allem mittelständische Unternehmen sollten D&O-Versicherungen in Erwägung ziehen, da steigende Klagekosten eine signifikante Bedrohung darstellen.

Der Bericht zeigt, dass Unternehmen in einem zunehmend komplexen Umfeld agieren, in dem D&O-Versicherungen eine zentrale Rolle im Risikomanagement spielen.



Abb.1: Das Rosenheimer Unternehmen Agenda ist ein führender Anbieter für betriebswirtschaftliche Software-Lösungen in Deutschland

Umfassende Gebäudesicherheit auf der Tagesordnung

Agenda setzt auf neues Sicherheitskonzept für das sanierte Firmengebäude

Das Rosenheimer Unternehmen Agenda ist einer der führenden Anbieter für betriebswirtschaftliche Software-Lösungen in Deutschland. Seit fast 40 Jahren bietet Agenda Steuerberatern, Buchhaltern sowie kleinen und mittleren Unternehmen ein Komplettsystem aus Software, IT-Lösungen, Service und Wissen. Mit ihrem breiten Angebot an betriebswirtschaftlichen (Cloud-)Lösungen wächst Agenda kontinuierlich. Arbeiteten vor 20 Jahren noch 48 Mitarbeitende bei Agenda, sind es inzwischen bereits rund 350.

Seit nunmehr sechs Jahren verfolgt das Unternehmen außerdem das Ziel, klimaneutral zu wirtschaften. Deswegen hat sich das Unternehmen eine „Green Agenda" auferlegt. Diese Neuausrichtung führte unter anderem dazu, dass Agenda eine teilweise Kern- und eine komplette energetische Sanierung des Firmengebäudes für eine nachhaltigere Arbeitsweise durch-



Abb. 2: Im Treppenhaus steuern Zutrittsleser die Türen zu den Arbeitsplätzen. Heute wechseln sich im Firmengebäude frei zugängliche Bereiche mit stark geschützten Zonen ab



Abb. 3: Der Mitarbeiterbereich wird durch eine Vereinzelungsanlage vom öffentlichen Bereich getrennt Alle Fotos ©PCS

führte. Die Agenda-Arbeitsplätze wurden mit viel Flexibilität, freier Arbeitsplatzwahl und abwechslungsreichen sozialen Inseln nach New-Work-Grundsätzen umgestaltet.

Mit der Modernisierung des Firmengebäudes setzt Agenda auf ein neues Sicherheitskonzept

Bereits in der Planungsphase für den großen Umbau des Firmengebäudes wandte sich Agenda an den Hersteller PCS Systemtechnik und ließ sich vom Expertenteam zum Thema Gebäudesicherheit beraten. Gemeinsam mit den Agenda-Projektverantwortlichen entwickelte und realisierte PCS ein umfassendes Sicherheitskonzept für alle Zonen auf dem Gelände. Da im großzügigen Erdgeschoss Kundenveranstaltungen oder Seminare stattfinden, ist diese Etage frei zugänglich. Andere Räume hingegen sind wiederrum mit batteriebetriebenen, mechatronischen Türterminals verschlossen.

Trennung von öffentlicheBereich vom Mitarbeiterbereich

Als betrieblicher Softwarehersteller arbeitet Agenda mit besonders sensiblen Kundendaten. Deswegen war es dem Rosenheimer Unternehmen besonders wichtig, den Zutritt zum internen Mitarbeiterbereich zu schützen. Der Zugang zu den Büros ist daher nur über eine moderne Vereinzelungsanlage möglich. Hier entschied sich Agenda für den Hersteller Wanzl. Die Anlage ist durch ihre interaktiven Leuchtelemente nicht zu übersehen und lotst berechtigte Personen selbsterklärend durch die Schleuse. Für Rollstuhlfahrer oder Lieferanten gibt es einen separaten Schwenkarm. Um den Besuchern einen reibungs- losen Zugang zum Unternehmen zu ermöglichen, installierte PCS für Agenda ein modernes Sicherheitssystem. Der Hintereingang ist nicht dauerhaft geöffnet. Jedoch können Besucher über eine hochwertige Behnke IP-Sprechstelle Zugang erhalten. Sobald Agenda die Sprechanlage betätigt, zeigt das System das Videobild des Besuchers automatisch auf dem Monitor an. Per OP-Telefonanlage kann das Empfangspersonal dann mit dem Besucher in Kontakt treten. Durch einen einfachen Mausklick gibt

Agenda dann den Zugang zur Tür frei.
Mitarbeiter bewegen sich innerhalb des Mitarbeiterbereichs frei – die meisten Büros und Besprechungsräume sind frei zugänglich. Agenda legt sehr viel Wert auf eine angenehme Arbeitsplatzkultur. Büros wechseln sich ab mit offenen Sozialzonen, wie Küchen oder Sitzgelegenheiten. Allen Mitarbeitenden stehen den ganzen Tag kostenlos Softdrinks, Kaffee und Obst zur Verfügung. Die Arbeitsplätze können teilweise vorab per PC oder Smartphone gebucht werden.

Neue Multifunktionskarten erleichtern den Arbeitsalltag

Mit dem Sicherheitskonzept entschied sich Agenda auch für eine zukunftsorientierte Einführung von Mitarbeiterausweise. Nach Beratung mit PCS erwarb Agenda aktuelle RFID-Karten mit verschlüsselter Technologie und Kapazität für verschiedenste Anwendungen der Büroorganisation. Die Mitarbeiter erhielten die neuen Ausweise im eleganten Agenda-CI – bedruckt mit dem persönlichen Foto. Die Ausweise sind vielseitig einsetzbar: Sie eignen sich für Zeiterfassung und Zutrittskontrolle, aber auch für die Buchung von Besprechungsräumen direkt an den digitalen Anzeigetafeln der Meetingräume.
Bei frei wählbaren Arbeitsplätzen befinden sich die persönlichen Arbeitsmaterialien wie Notebooks und Büroausstattung in Mitarbeiter-Spinden. Der persönliche Firmenausweis sperrt den Schrank auf. Außerdem lässt sich das Medium für die Offline-Zutrittskontrolle nutzen. Durch die erste Buchung an den vernetzten RFID-Zutrittslesern werden Zutrittsrechte für die mechatronischen Türsysteme auf die Karten geschrieben.
Die Zutrittsrechte sind immer nur für einen Tag gültig, so dass auch ein Verlust einer Mitarbeiterkarte kein Sicherheitsrisiko darstellt. Mit diesen Zutrittsrechten auf den Mitarbeiterkarten lassen sich Offline-Schließzylinder und Türbeschläge zum Beispiel an Sicherheitstüren bedienen. Projektleiter Lippert bringt es auf den Punkt: „Die neuen Karten haben die Organisation im ganzen Haus sehr vereinfacht, sie sind ein richtiger Gewinn."



Abb. 4: Am Haupteingang buchen Mitarbeiterende ihre Arbeitszeiten an den zwei INTUS 5600 Terminals.

Zufahrtskontrolle und Videomanagement mit Zutrittssoftware vernetzt

Auch die Zufahrt zur Tiefgarage ist in das Sicherheitssystem eingebunden. Das Tor wird über einen Weitbereichsleser geöffnet. Dafür erhalten alle Fahrzeuge mit Tiefgaragenberechtigung einen Wind Shield UHF-Tag-Aufkleber oder eine Wind Shield UHF-Karte. So lässt sich die Zufahrtskontrolle bequem aus dem Fahrzeug heraus bedienen. Radfahrende Mitarbeiter, die ihr Fahrrad sicher in der Tiefgarage parken wollen, können die zusätzlich verbauten RFID-Zutrittsleser mit ihren Mitarbeiterausweisen verwenden.

Zur Verwaltung der Zutrittskontrolle nutzt Agenda die Lösung DEXICON von PCS, die direkt an die ERP-Software von Agenda angebunden wurde. Zusätzlich wird das Zutrittskontrollsystem mit Videoüberwachung unterstützt. Die Videosoftware Qognify schaltet sich aktiv auf, sobald aus der Zutrittskontrolle ein Alarm gemeldet wird und speichert die Bilder zum entsprechenden Zutrittsereignis.

Zeiterfassungsterminals als optisches Highlight im Eingangsbereich

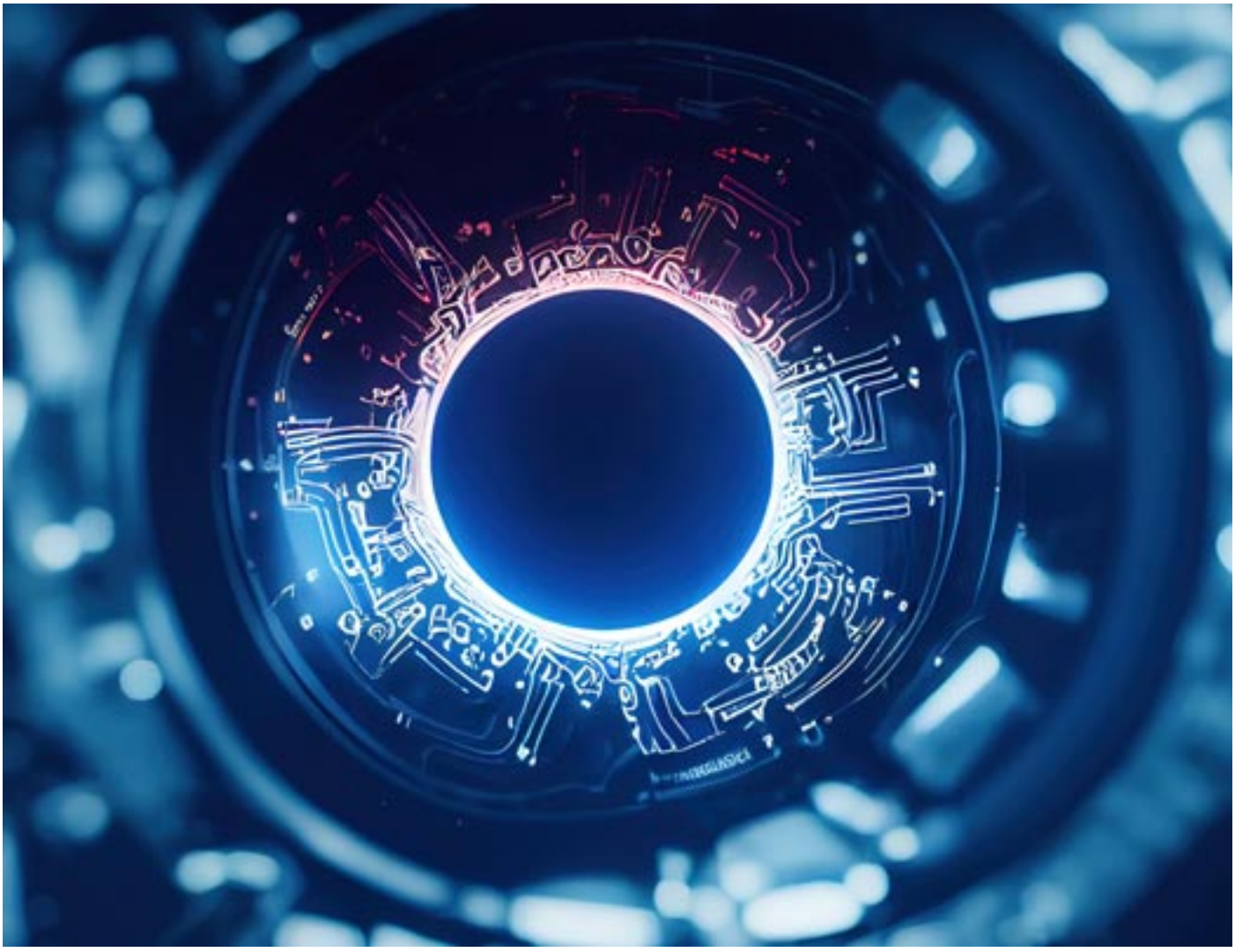
Zur Arbeitszeiterfassung nutzt Agenda die INTUS Zeiterfassungsterminals. Am Haupteingang sind die zwei INTUS 5600 Terminals auf Edelstahlsäulen ein Highlight. Sie passen perfekt zum architektonisch anspruchsvoll gestalteten Foyer mit hinterleuchteten Glaselementen und hochwertigem Fliesenboden. Weitere Zeiterfassungsterminals zur Buchung der Arbeitszeiten sind arbeitnehmerfreundlich direkt am Eingang aus der Tiefgarage oder in anderen Stockwerken montiert.

Projektleiter Lippert zieht ein rundum positives Resümee: „Es hat sich alles sehr vereinfacht mit PCS. Ich kann in der Software in einer Minute definieren, wer muss wo rein und hab auch in einer Minute das Profil wieder aufgeräumt. Ich bin alles in allem sehr zufrieden mit der PCS Lösung."

Cybersicherheit

Kritische Betrachtung des Impulspapiers des KI-Bundesverbands

Das Impulspapier des KI-Bundesverbands zur Bundestagswahl 2025 skizziert eine ambitionierte Vision für die Zukunft der Künstlichen Intelligenz (KI) in Deutschland. Der Fokus liegt auf der Notwendigkeit, technologische Souveränität zu erlangen, Innovationspotenziale zu erschließen und die Wettbewerbsfähigkeit der deutschen Wirtschaft zu stärken. Doch aus der Perspektive der Sicherheitsbranche und Cybersicherheit zeigt der vorgestellte Maßnahmenkatalog erhebliche Defizite, die eine kritische Betrachtung erfordern. Die fehlende Berücksichtigung von Cybersicherheitsaspekten könnte die vorgeschlagenen Initiativen untergraben und birgt Risiken für die Sicherheit von Daten, Infrastrukturen und Anwendungen.



Unzureichende Priorisierung von Sicherheitsaspekten

Der Maßnahmenkatalog des Impulspapiers hebt die Bedeutung von Investitionen in KI-Infrastruktur hervor, versäumt jedoch weitgehend, Sicherheitsaspekte als zentrale Anforderung zu definieren.

Besonders kritisch ist die vorgeschlagene Erleichterung des Zugangs zu öffentlich geförderten Rechenzentren. Ohne robuste Sicherheitsprotokolle könnte dies zu einer Exposition sensibler Daten aus Wirtschaft und Forschung führen. Es bedarf verbindlicher Sicherheitsrichtlinien, die sicherstellen, dass alle Investitionen und Infrastruk- turen dem Schutz vor Cyberangriffen und Datendiebstahl genügen.

Abhängigkeit von außereuropäischen Anbietern

Während das Impulspapier den Aufbau technologischer Souveränität propagiert, bleiben konkrete Maßnahmen zur Reduktion der bestehenden Abhängigkeit von außereuropäischen Anbietern vage.

Diese Abhängigkeit stellt ein erhebliches Sicherheitsrisiko dar, insbesondere bei vertraulichen oder staatlich relevanten KI-Anwen- dungen. Cyberspionage und gezielte Angriffe auf diese Abhängigkeiten könnten die nationale Sicherheit gefährden und das Vertrauen in KI-Lösungen mindern.

Unterschätzung von Cyber-Bedrohungen
Mit der zunehmenden Verbreitung von KI in Wirtschaft und Verwaltung steigt auch die Angriffsfläche für Cyberkriminelle. Das Impulspapier stellt zwar die Innovations- und Wettbewerbsfähigkeit in den Vordergrund, bleibt jedoch die Antwort auf die Frage schuldig, wie die Sicherheit dieser Systeme gewährleistet werden soll. Ohne klare Leitlinien zur Absicherung von KI-Anwendungen drohen erhebliche Schwachstellen, die von Angreifern ausgenutzt werden könnten.

Fragmentierte Verantwortung und mangelnde Integration

Die vorgeschlagene zentrale Stabsstelle im Bundeskanzleramt als Übergangslösung für eine koordinierte KI- und Digitalpolitik ist ein pragmatischer Ansatz. Doch es fehlt ein ausdrückliches Mandat, Cybersicherheitsstrategien in diese Struktur zu integrieren. Ohne klare Zuständigkeiten für Sicherheitsthemen könnten diese in der Priorität nach hinten rücken, was fatale Folgen für die Resilienz der digitalen Infrastruktur hätte.

Fehlender Fokus auf Resilienz

Obwohl das Impulspapier Innovationen fördert, bleibt die Resilienz gegenüber gezielten Angriffen auf KI-Systeme unzureichend adressiert. Moderne KI-Modelle können durch Angriffe wie „adversarial attacks" manipuliert werden, was nicht nur die Funktionalität, sondern auch das Vertrauen in KI-Systeme massiv beeinträchtigen kann. Resilienz muss ein zentraler Bestandteil der KI-Strategie sein, um das Risiko solcher Angriffe zu minimieren.

Empfehlungen zur Stärkung der Cybersicherheit

Um die skizzierten Herausforderungen anzugehen, sollten folgende Maßnahmen in die KI-Strategie integriert werden:

1. Sicherheitsstandards als Pflicht: Jede Investition in KI-Infrastruktur sollte durch verbindliche Sicherheitsrichtlinien flankiert werden, um den Schutz sensibler Daten und Systeme sicherzustellen.

2. Integration von Cybersicherheitskompetenz: Cybersicherheitsexperten sollten Teil des vorgeschlagenen KI-Strategie-Boards sein, um Risiken frühzeitig zu identifizieren und Gegenmaßnahmen zu entwickeln.

3. Förderung sicherer KI-Entwicklung: Programme zur Förderung von KI sollten gezielt auf die Entwicklung sicherheitskritischer Anwendungen und die Abwehr von Manipulationsversuchen ausgerichtet sein.

4. Aufbau von Sicherheitskapazitäten: Parallel zur technologischen Entwicklung müssen nationale Kapazitäten zur Erkennung und Abwehr von KI-bezogenen Cyberangriffen gestärkt werden.

5. Reduktion von Abhängigkeiten: Durch gezielte Förderung europäischer Technologien und Anbieter können Abhängigkeiten von außereuropäischen Anbietern reduziert und technologische Souveränität erreicht werden.

6. Stärkere Einbindung der Sicherheitsverbände: Sicherheitsverbände sollten sich proaktiv in den Gestaltungsprozess der KI-Strategie einbringen. Ihre Expertise ist entscheidend, um praxisnahe Sicherheitskonzepte zu entwikkeln und umsetzbare Standards für den Schutz von KI-Systemen zu etablieren. Eine engere Zusammenarbeit zwischen der Sicherheitsbranche, der Politik und der Wirtschaft würde dazu beitragen, Sicherheitsrisiken frühzeitig zu erkennen und effektiv zu adressieren.

Fazit

Das Impulspapier des KI-Bundesverbands liefert eine wertvolle Grundlage für die Weiterentwicklung der KI-Strategie in Deutschland. Doch ohne die konsequente Integration von Cybersicher- heitsaspekten drohen die ambitionierten Ziele durch Sicherheitsrisiken untergraben zu werden. Eine nachhaltige und sichere Umsetzung der vorgeschlagenen Maßnahmen erfordert, dass Cybersicherheit als zentrale Dimension der KI-Strategie anerkannt und entsprechend priorisiert wird. Nur so kann Deutschland im internationalen Wettbewerb bestehen und eine vertrauenswürdige KI-Zukunft gestalten.

KI BUNDESVERBAND

D&O-Versicherungen 2025

Schutzschild in einer Welt voller Risiken und Chancen

Der Bericht „Directors and Officers (D&O) Insurance Insights 2025" von Allianz Commercial analysiert die zentralen Risiken und Entwicklungen, die Unternehmen und Führungskräfte im Jahr 2025 betreffen werden. Dabei beleuchtet er geopolitische, regulatorische und technologische Heraus- forde- rungen sowie wirtschaftliche Unsicherheiten, die die Bedeutung von D&O-Versicherungen als Instrument des Risikomanagements unterstreichen.

Geopolitische und regulatorische Herausforderungen

Globale Unsicherheiten, wie der Krieg in der Ukraine und Spannungen zwischen den USA und China, sorgen weiterhin für erhebliche Risiken. Dazu zählen Lieferkettenstörungen, Geschäftsausfälle und eine intensivere regulatorische Überprüfung. Besonders im Fokus steht die wachsende Bedeutung der Einhaltung von ESG-Vorschriften (Umwelt, Soziales, Governance). Der Erfolg der australischen Regulierungsbehörde im Jahr 2024 im Kampf gegen Greenwashing zeigt, dass die Gefahr von Klagen und Sanktionen in diesem Bereich steigt. Zusätzlich stellt die Nichteinhaltung internationaler Sanktionen ein wachsendes Risiko dar, das Unternehmen rechtliche und finanzielle Konsequenzen kosten kann.

Technologische Risiken

Auch technologische Entwicklungen bergen erhebliche Herausforderungen. Künstliche Intelligenz (KI) spielt hierbei eine Schlüsselrolle. Risiken wie „AI Washing" – die übertriebene Darstellung von KI-Fähigkeiten –, Datenschutzverletzungen und fehlerhafte Ergebnisse („KI-Halluzinationen") sind zentrale Themen.
Die EU hat im August 2024 den weltweit ersten umfassenden Gesetzesrahmen für KI verabschiedet, während in den USA die Zahl der KI-bezogenen Sammelklagen steigt. Ein prominenter Fall war die Verhängung einer Strafe von 1,4 Milliarden US-Dollar gegen Meta wegen Datenschutzverletzungen.

Wirtschaftliche Unsicherheiten

Die anhaltenden wirtschaftlichen Unsicherheiten führen zu steigenden Insolvenzen. Nach einem Anstieg von elf Prozent im Jahr 2024 wird für 2025 ein weiterer Zuwachs von zwei Prozent erwartet. Dies erhöht das Haftungsrisiko für Führungskräfte, da Aktionäre oder Gläubiger bei finanziellen Verlusten Klagen einreichen können. Besonders betroffen sind Branchen wie Bau, Einzelhandel und Dienstleistungen, die unter hohen Kreditkosten und wirtschaftlichen Unsicherheiten leiden.

Entwicklungen im D&O-Versicherungsmarkt

Der D&O-Versicherungsmarkt bleibt wettbewerbsintensiv. Die Prämien sinken weiterhin, während Vertragsbedingungen verbessert werden. In Europa und Asien sind die Preisrückgänge besonders ausgeprägt, während die Raten in den USA stabiler bleiben. Gleichzeitig steigt dort die Schadenhäufigkeit. Ein weiterer Trend ist das zunehmende Litigation Funding, also die Drittfinanzierung von Klagen. Dies führt zu einer höheren Klagefrequenz und steigenden Streitwerten, was die Versicherungswirtschaft vor Herausforderungen stellt.

Handlungsempfehlungen für Unternehmen und Führungskräfte

Unternehmen müssen ihre Risikoüberwachung anpassen und regelmäßig auf geopolitische und regulatorische Änderungen reagieren. Im Umgang mit KI sind Richtlinien und Audits unerlässlich, um den Einsatz von KI zu kontrollieren und Haftungsrisiken zu minimieren.

Zudem sollten insbesondere mittelständische Unternehmen über die Erweiterung ihrer D&O-Versicherungen nachdenken, da steigende Klagekosten eine existenzielle Bedrohung darstellen können.

Der Bericht zeigt, dass Unternehmen in einem zunehmend komplexen Umfeld agieren. Die aufgezeigten Maßnahmen und Trends bieten jedoch auch eine klare Orientierung, wie Unternehmen ihre Resilienz stärken können.

Die D&O-Versicherung bleibt dabei ein unverzichtbares Werkzeug, das nicht nur Risiken mindert, sondern auch das Vertrauen von Aktionären und Stakeholdern fördert. Der Ansatz der Allianz Commercial bietet zudem ein wertvolles Vorbild für andere Branchen und Unternehmen – insbesondere im Hinblick auf den Dialog mit Arbeitskräften und potenziellen Auszubildenden sowie die Stärkung des Risikomanagements in mittelständischen Betrieben.

Download der englischsprachigen Studie: https://tinyurl.com/88dnrbn7



Kommentar: Situation der Versicherung in Deutschland

Auf der Prämienseite hat sich die Situation entspannt und wir sehen einen größeren Prämiendruck in den überschüssigen Schichten. Im Primärsegment legen die Kunden weiterhin Wert auf Erfahrung, Zuverlässigkeit, Schadenexpertise, internationale Versicherungsprogramme und Service.
Viele Kunden und Versicherer schließen langfristige Verträge ab, um Planungssicherheit für beide Seiten zu haben. Wir sehen auch, dass Deckungserweiterungen wieder eingeführt werden, einschließlich längerer verlängerter Berichtszeiträume und Wiederinkraftsetzungen.
Der Markt verfügt wieder über ausreichende Kapazitäten und der Wettbewerb zwischen den Versicherungsgesellschaften hat leicht zugenommen. Auch der Wettbewerb zwischen großen Maklern hat zugenom- men.Die Ablehnung von Prämienerhöhungen und die Forderung nach Einsparungen sind das Ergebnis vieler Kostensenkungsprogramme von Kunden. Alternativ werden Prämieneinsparungen von Kunden oft in zusätzliche Überkapazitäten investiert.

Die Schadenfälle in Deutschland und der Schweiz sind hauptsächlich insolvenzbedingt. Dies kann auf Vorwürfe einer verzögerten Insolvenz oder auf Behauptungen zurückzuführen sein, dass das Management Zahlungen geleistet hat, obwohl das Unternehmen bereits insolvent war.
Letzteres ist für Manager weniger riskant, obwohl immense Summen rückwirkend geltend gemacht werden können. Es werden immer mehr D&O-Ansprüche nach einem Cyberangriff gemeldet, bei dem dem Management vorgeworfen wird, vor, während oder nach dem Vorfall nicht mit der erforderlichen Sorgfalt gehandelt zu haben.
Wir könnten diesen Trend auch bei der Einführung von KI beobachten. Wir haben auch mit vielen Fällen zu tun, die mit den USA zu tun haben. Wenn eine Sammelklage eingereicht wird, wird das Verfahren aufgrund der hohen Verteidigungskosten.
Die Preissteigerungen in Europa bedeuten, dass dies nicht mehr nur ein US-Problem ist. Wir gehen davon aus, dass der deutsche D&O-Markt 2025 in seiner Größe stabil bleiben wird.

Alfred Mora, Chief Underwriter Commercial Germany, Financial Lines, DE /CH Allianz Commercial



BE WAVE

Kabelloses Smart-Home-System mit Sicherheitsfokus

Die Anforderungen an moderne Smart-Home-Systeme sind in den letzten Jahren deutlich gestiegen. Nutzer erwarten nicht nur Komfort, sondern auch höchste Sicherheitsstandards. SATEL hat mit seinem neuen Produkt BE WAVE diese Erwartungen konsequent umgesetzt und bietet ein ALL-IN-ONE-System, das intelligente Haussteuerung mit umfassendem Schutz vereint.

Ein Herz aus moderner Technologie: Der BE WAVE HUB



Das BE WAVE System basiert auf dem leistungsstarken HUB, der als zentrale Steuereinheit fungiert. Dank der bewährten ABAX 2 Funktechnik, die weltweit von Fachleuten geschätzt wird, verbindet das System zuverlässige Kommunikation mit maximaler Flexibilität. Über die benutzerfreundliche mobile App können Nutzer das System einfach in Betrieb nehmen, konfigurieren und im Alltag bedienen. Funktionen wie Szenen, Routinen und Zeitpläne bieten umfassende Möglichkeiten zur Automatisierung des Zuhauses.



Vielseitige Produktfamilie für Sicherheit und Komfort

Das BE WAVE Sortiment deckt eine beeindruckende Bandbreite an Anwendungen ab. Zur Familie gehören:

- **Sicherheitslösungen:** Bewegungsmelder (innen/außen), Glasbruchmelder, Rauch- und Kohlenmonoxidmelder, Wassermelder, Signalgeber und Magnetkontakte.
- **Komfortelemente:** Intelligente Zwischenstecker, Heizkörperthermostate, Steuerungsmodule für Beleuchtung, Rollläden und Vorhänge.
- **Bedienmöglichkeiten:** Tastaturen, Handsender und intelligente Taster.

Durch diese Vielfalt ermöglicht BE WAVE eine vollständige Integration von Sicherheits- und Komfortlösungen in einem System.

Schnelle Installation und intuitive Bedienung

Eines der herausragenden Merkmale von BE WAVE ist die einfache Handhabung. Von der Installation bis zur täglichen Nutzung überzeugt das System mit seiner Benutzerfreundlichkeit. Die mobile App führt Errichter und Endnutzer durch alle Schritte der Konfiguration, sodass auch komplexe Szenarien mühelos umgesetzt werden können.

Fazit: BE WAVE als neuer Standard im Smart-Home-Bereich

Mit BE WAVE setzt SATEL neue Maßstäbe für kabellose Smart-Home-Systeme. Die Kombination aus benutzerfreundlicher Bedienung, umfangreichen Sicherheitslösungen und modernster Technologie macht das System zu einer idealen Wahl für Errichter, Distributoren und Endverbraucher gleichermaßen. Die nahtlose Integration von Komfort- und Schutzfunktionen gewährleistet ein sicheres und modernes Wohnerlebnis.

SLIM LINE

Bewegungsmelder in stilvollem Design mit modernster Technologie

In der heutigen Sicherheitsbranche müssen Geräte nicht nur funktional, sondern auch ästhetisch ansprechend sein. Mit der SLIM LINE Serie bietet SATEL eine perfekte Kombination aus modernem Design und leistungsstarker Bewegungserkennungstechnik. Diese Bewegungsmelder sind ideal für Anwendungen in Wohn- und Geschäftsräumen, die sowohl Sicherheit als auch Eleganz verlangen.



Design trifft auf Präzision

Die SLIM LINE Bewegungsmelder vereinen hochentwickelte Technologie mit einem eleganten Gehäuse aus hochwertigem Kunststoff.
In der Serie stehen 10 verschiedene Modelle zur Auswahl, sodass für jede Anforderung die passende Lösung gefunden werden kann.

Überragender Erfassungsbereich und Zuverlässigkeit

Mit einem beeindruckenden Erfassungsfeld von bis zu 20 m x 24 m und einem Öffnungswinkel von 90° sorgen die Melder für eine umfassende Überwachung. Die speziell in Japan entwickelten Linsen sowie ein intelligenter Algorithmus, der sich automatisch an Temperaturschwankungen anpasst, gewährleisten zuverlässige Ergebnisse auch unter wechselnden Umgebungsbedingungen.

Einfache Installation und flexible Anpassung

Die SLIM LINE Bewegungsmelder punkten nicht nur mit ihrer Funktionalität, sondern auch mit einer schnellen und unkomplizierten Installation:

- Flexible Anpassung: Dank austauschbarer Linsen können die Melder einfach an individuelle Raumgegeben- heiten oder die Wünsche des Kunden angepasst werden
- Wandmontage ohne Spezialwerkzeug: Die Geräte lassen sich bequem und sicher an der Wand befestigen. Für eine noch genauere Ausrichtung des Erfassungswinkels kann der BRACKET D verwendet werden.

Für anspruchsvolle Anwendungen in Wohn- und Geschäftsräumen

Ob für private Häuser oder moderne Büros – die SLIM LINE Bewegungsmelder bieten eine perfekte Mischung aus Stil und Leistung. Sie fügen sich nahtlos in jede Umgebung ein und gewährleisten gleichzeitig ein hohes Maß an Schutz und Komfort.

Fazit

Die SLIM LINE Serie von SATEL ist eine erstklassige Wahl für alle, die Sicherheitstechnik mit einem hohen ästhetischen Anspruch suchen. Mit einer breiten Palette von Modellen, innovativen technischen Features und einer einfachen Installation setzt diese Serie neue Standards in der Bewegungserkennung.



Smart Thermostat

Intelligente Heizungs-automatisierung



Die Digitalisierung hält Einzug in alle Lebensbereiche, und auch das Energiemanagement in Gebäuden bleibt davon nicht unberührt. Ein herausragendes Beispiel für moderne Heizungssteuerung ist der Smart Thermostat von BE WAVE. Dieses intelligente Gerät bietet eine einfache und effektive Lösung, um den Heizbetrieb von Heizkörpern sowohl in privaten Haushalten als auch in gewerblichen Gebäuden zu optimieren.

Perfekte Temperatur-kontrolle leicht gemacht

Der Smart Thermostat von BE WAVE übernimmt die Funktion eines persönlichen Heizungsspezialisten. Nutzer können über die intuitive BE WAVE App detaillierte Zeitpläne festlegen, um sicherzustellen, dass die Raumtemperatur stets optimal an die individuellen Bedürfnisse angepasst ist. Eine niedrigere Temperatur während der Nacht fördert nicht nur einen gesunden Schlaf, sondern hilft auch, Energiekosten zu senken. Zusätzlich bietet der ECO-Modus die Möglichkeit, unbewohnte Räume effizient zu beheizen, was den Energieverbrauch weiter reduziert. Die Kindersicherung „Child Lock" verhindert ungewollte Änderungen der Einstellungen, wodurch der Betrieb sicher und sorglos bleibt. Der Thermostat kann außerdem jederzeit manuell bedient werden, um eine maximale Flexibilität zu gewährleisten.

Effizienz und Komfort in einem

Besonders hervorzuheben ist die Möglichkeit, den Betrieb mehrerer Heizkörperzentral zu steuern. Mit nur einem Klick können Nutzer die Temperatur in einem gesamten Gebäude anpassen. Diese Funktion eignet sich nicht nur für private Häuser, sondern auch ideal für gewerbliche Objekte wie Büros, Werkstätten oder Hotels. Der Smart Thermostat erweist sich somit als äußerst vielseitig und kosteneffizient.

Smartphone-gesteuerte Heizungssteuerung

Die BE WAVE App bietet eine einfache Übersicht über die Temperatur in jedem Raum und ermöglicht Änderungen mit wenigen Klicks. Dies spart nicht nur Zeit, sondern macht die Bedienung auch von unterwegs aus möglich. Nutzer können bequem Modi und Zeitpläne anpassen, ohne direkt am Heizkörper agieren zu müssen. Ob im Urlaub, auf der Arbeit oder im Nachbarzimmer – die Heizungssteuerung bleibt immer in greifbarer Nähe.

Innovationen für Einsparungen

Der Smart Thermostat bietet eine Vielzahl an Funktionen, die Komfort und Energieeinsparung miteinander verbinden:
Boost-Funktion: Schnelles Aufheizen eines Raumes oder das Trocknen von Kleidung auf dem Heizkörper wird durch die vollständige Öffnung des Heizkörperventils möglich.
Fenster-Auf-Erkennung: Wird ein Fenster geöffnet, schließt der Thermostat automatisch das Heizkörperventil, um unnötige Wärmeverluste zu vermeiden. Nach dem Schließen des Fensters wird der Betrieb automatisch fortgesetzt.

Diese Funktionen tragen dazu bei, Energie effizient zu nutzen und den Komfort im Alltag erheblich zu steigern.

Das BE WAVE System – mehr als nur Heizungssteuerung

Der Smart Thermostat ist Teil eines umfassenden Systems. BE WAVE bietet zahlreiche weitere intelligente Geräte, darunter:

- Bewegungsmelder
- Intelligente Zwischenstecker
- Rauch- und Kohlenmonoxidmelder
- Steuerungsmodule für Beleuchtung, Rollläden und Vorhänge

Fazit

Mit dem Smart Thermostat von BE WAVE wird Heizungssteuerung nicht nur smarter, sondern auch effizienter. Egal, ob für Privathaushalte oder gewerbliche Gebäude – das Gerät bietet eine nahtlose Verbindung von Komfort, Einsparungen und moderner Technologie. Dank innovativer Funktionen und einer benutzerfreundlichen App setzen Nutzer auf eine Lösung, die den Alltag erleichtert und gleichzeitig nachhaltig ist. Ein Schritt in die Zukunft des intelligenten Energiemanagements!

Ressourcen für Errichter und Distributoren

Um Fachleute bei der Implementierung von BE WAVE zu unterstützen, stellt SATEL umfassende Marketingmaterialien bereit. Über das Support-Portal können Grafiken, Animationen und Fotos heruntergeladen werden. Zusätzliche Unterstützung bietet der SATEL SMART Vlog, in dem regelmäßig neue Anleitungen und Tipps zur Installation und Konfiguration des Systems veröffentlicht werden. **[www.satel.pl]**



Sicherheit im Hamburger Nahverkehr

Neue Informationsoffensive des hvv seit November 2024 - Waffenverbot - 80 neue Stellen im Sicherheitsbereich

Der Hamburger Verkehrsverbund (hvv) hat im November die Initiative „Sicher unterwegs im hvv" gestartet, um Fahrgästen umfassende Informationen zu den bestehenden Sicherheitsmaßnahmen im öffentlichen Nahverkehr bereitzustellen. Ziel ist es, Transparenz zu schaffen, die Nutzung der Sicherheitseinrichtungen zu fördern und hilfreiche Verhaltenshinweise für herausfordernde Situationen zu geben.
Im Zentrum der Initiative stehen die vielfältigen Sicherheitseinrichtungen im gesamten hvv-Netz: Notrufsäulen auf Bahnsteigen, Sprechstellen in den Bahnen sowie Überwachungskameras in Haltestellen und Fahrzeugen. Fahrgäste sollen ermutigt werden, diese Einrichtungen nicht nur in Notfällen zu nutzen, sondern auch, wenn sie sich unwohl fühlen, etwa beim Warten an einer Haltestelle.
Die Notrufsäulen bieten sowohl Notruf- als auch Informationsfunktionen. Gleichzeitig werden bei einer Meldung die nächstgelegenen Kameras zugeschaltet, um den Leitstellen eine bessere Einschätzung der Situation zu ermöglichen und schnelle Hilfe zu koordinieren. In den Zügen stehen Sprechstellen an den Türen zur Verfügung, über die Fahrgäste direkt mit dem Fahrpersonal kommunizieren können.

Sicherheit durch Kommunikation und Präsenz

Hamburgs Verkehrssenator Dr. Anjes Tjarks betont die Bedeutung der neuen Informationsoffensive: „Das Wissen über vorhandene Meldekanäle und Sicherheitseinrichtungen gibt Fahrgästen ein gesteigertes Sicherheitsgefühl. Bereits heute sorgen

mehr als 700 qualifizierte Sicherheitskräfte im hvv rund um die Uhr für Präsenz. Zudem ermöglicht der unkomplizierte Zugang zu Sicherheits- und Servicepersonal über Rufsäulen und Sprechstellen eine schnelle Hilfeleistung."

Auch Anna-Theresa Korbutt, Geschäftsführerin des hvv, hebt hervor, dass Sicherheit oberste Priorität hat: „Mit dieser Kampagne möchten wir nicht nur informieren, sondern unseren Fahrgästen helfen, ihre Reise sicher und mit einem gestärkten Sicherheitsgefühl zu erleben. Vielen ist nicht bewusst, wie einfach sie im Zweifelsfall Hilfe anfordern können."

Fahrgäste aktiv einbeziehen

Als Teil der Initiative wurde das Format „open hvv unterwegs" ins Leben gerufen. Dieses bietet Fahrgästen die Möglichkeit, bei Haltestellenbegehungen Sicherheitseinrichtungen selbst zu testen und Hemmschwellen abzubauen.
Dabei können sie ihre Ideen und Verbesserungsvorschläge direkt mit Verantwortlichen teilen. Die ersten Begehungen fanden bereits im November statt, ab Januar 2025 sind jährlich acht Termine geplant.

Verbesserte Haltestellenumfelder

Ein angenehmes Umfeld spielt ebenfalls eine wichtige Rolle für das Sicherheitsgefühl. Der hvv arbeitet mit Partnern wie der Stadtreinigung und den Bezirken zusammen, um Haltestellen und deren Zugänge besser zu beleuchten und regelmäßig zu reinigen.
Die Initiative wird an vielen Orten im hvv-Netz beworben, um Fahrgästen den Zugang zu Informationen und Sicherheitseinrichtungen noch leichter zu machen. Mit diesen Maßnahmen unterstreicht der hvv sein Engagement, den Nahverkehr in Hamburg sicher und attraktiv zu gestalten.
Hamburg verstärkt die Sicherheitsmaßnahmen im öffentlichen Nahverkehr:
Im kommenden Jahr soll das Personal bei Hochbahn und S-Bahn erheblich aufgestockt werden, ergänzt durch innovative Technik wie einen „stillen Alarm" für diskrete Hilfeleistungen.
Geplant ist, dass 80 neue Sicherheitskräfte eingestellt werden, wodurch die Gesamtzahl auf 750 steigen würde. Dieses zusätzliche Personal soll für eine stärkere Präsenz an verschiedenen Orten sorgen und schneller bei Vorfällen eingreifen können. Moderne Technologien sollen diese Bemühungen unterstützen.

Ein besonderes Highlight ist die Einführung eines stillen Alarms, der zunächst von der S-Bahn getestet wird. Fahrgäste können dabei per WhatsApp unangenehme oder bedrohliche Situationen melden, wie etwa pöbelnde oder alkoholisierte Personen.
Der Prozess ist so gestaltet, dass die Meldung unauffällig bleibt und die Aufmerksamkeit der betreffenden Personen nicht auf den Absender gelenkt wird. Ziel ist es, in solchen Fällen rasch Sicherheitspersonal vor Ort einzusetzen.
Auch der Einsatz von künstlicher Intelligenz soll zur Erhöhung der Sicherheit beitragen. Die Hochbahn plant, KI einzusetzen, um Überwachungskameras effektiver zu nutzen. Statt Bilder leerer Bahnsteige zu überwachen, sollen die Systeme potenziell gefährliche Situationen wie Auseinandersetzungen oder Personen im Gleis erkennen und priorisieren.
Zusätzlich wurde ein generelles Waffenverbot in allen Fahrzeugen und Stationen des Hamburger Verkehrsverbundes (HVV) eingeführt, um das Sicherheitsgefühl der Fahrgäste weiter zu verbessern. Dieses Maßnahmenpaket zeigt Hamburgs Engagement für mehr Sicherheit und könnte als Vorbild für andere Städte dienen.

Weitere Ausgestaltung im Dezember angekündigt

Innovative Ansätze für mehr Sicherheit im ÖPNV: KI, Messenger-Hilferuf und Personalaufstockung

Um das Sicherheitsgefühl der Fahrgäste im öffentlichen Nahverkehr nachhaltig zu stärken, setzen der Hamburger Verkehrsverbund (hvv), die Hamburger Hochbahn AG (HOCHBAHN) und die S-Bahn Hamburg auf eine Kombination aus moderner Technologie, digitaler Kommunikation und einer verstärkten Präsenz von Sicherheitskräften. Durch den Einsatz künstlicher Intelligenz (KI), den Ausbau digitaler Hilfsmöglichkeiten und die gezielte Erweiterung des Sicherheitsdienstes sollen die Fahrgäste den ÖPNV als noch sicherer wahrnehmen.

KI-gestützte Mustererkennung für schnelle Reaktion

Im Rahmen eines Pilotprojekts erprobt die HOCHBAHN den Einsatz von KI zur automatischen Analyse von Videobildern. Ziel ist es, sicherheitskritische Situationen, wie eine Person im Gleisbereich, tätliche Auseinandersetzungen oder Vandalismus, frühzeitig zu erkennen. Die KI analysiert bestehende Videodaten und liefert Hinweise an die Leitstelle, um eine schnellere Reaktion zu ermöglichen.

Das Projekt gliedert sich in zwei Phasen: Zunächst wird die bestehende Kameratechnologie mit KI kombiniert, um die Analyse von sicherheitsrelevanten Mustern zu testen. Anschließend erfolgt ein Vergleich mit neuen Kamerasystemen, um die Effektivität zu steigern. Dabei wird strenge DSGVO-Konformität sichergestellt, sodass Datenschutz und Datensicherheit gewahrt bleiben.

KI zur Steuerung von Sicherheitskräften bei der S-Bahn

Auch die S-Bahn Hamburg testet den Einsatz künstlicher Intelligenz, um die Verfügbarkeit und Präsenz von Sicherheitskräften zu optimieren. Mithilfe einer Software werden Einsatzorte basierend auf Faktoren wie Wetter, Zugauslastung oder betrieblichen Störungen vorgeschlagen. Diese datenbasierte Steuerung ermöglicht eine präzisere Planung und verstärkte Präsenz an besonders stark frequentierten oder sicherheitsrelevanten Orten.

Hilfe per WhatsApp: Digitaler Service für Fahrgäste

Im ersten Quartal 2025 startet die S-Bahn Hamburg ein innovatives Projekt, das Fahrgästen ermöglicht, über WhatsApp diskret und schnell Hilfe anzufordern.
Dieser digitale Service unterscheidet zwi-

Verkehrssenator Anjes Tjarks hebt die Bedeutung dieser Initiativen hervor: „Mit mehr Personal, innovativer Technologie und digitalen Lösungen wie dem Hilferuf via WhatsApp schaffen wir einen umfassenderen Schutz für die Fahrgäste. Alle Projekte werden datenschutzkonform umgesetzt und tragen dazu bei, das Sicherheitsempfinden weiter zu steigern."

schen Sicherheits- und Serviceanfragen, sodass drin- gende Fälle priorisiert werden können. Ohne Ortung des Absenders kann das Sicherheitspersonal anhand von Zeitstempel und Zugdaten die Situation nachvollziehen und gezielt eingreifen.

Verstärkung der Sicherheitskräfte

Um den gestiegenen Anforderungen und Fahrgastzahlen gerecht zu werden, erhöhen HOCHBAHN und S-Bahn ihre Sicherheits- und Prüfdienste um 80 zusätzliche Mitarbeitende, was die Gesamtzahl auf rund 750 erhöht. Seit 2020 wurde der Personalbestand bereits um 29 Prozent gesteigert, wodurch eine verstärkte Präsenz auf Bahnhöfen und in Zügen gewährleistet wird.

Ein sicherer ÖPNV als Gemeinschaftsprojekt

Die Maßnahmen ergänzen bereits bestehende Sicherheitseinrichtungen wie Videoüberwachung, Notrufsäulen und Sprechstellen in Bahnen.

Normen Wiegand, Geschäftsführer der HOCHBAHN-WACHE, betont die Kombination aus menschlicher Präsenz und technologischer Unterstützung: „Die Aufstockung des Personals und der Einsatz von KI zur Mustererkennung haben großes Potenzial, die Sicherheit im ÖPNV nachhaltig zu verbessern." "

Auch Jan Schröder, Vorsitzender der Geschäftsführung der S-Bahn Hamburg, begrüßt die Entwicklungen: „Durch den Ausbau der Sicherheitsmaßnahmen und digitale Hilfsmittel können wir künftig noch schneller und effektiver auf Sicherheitsfragen reagieren."

Sicherheit als oberste Priorität

Die neuen Projekte verdeutlichen das Engagement der Verkehrsunternehmen im hvv, die Sicherheit der Fahrgäste stetig zu verbessern. Durch eine Mischung aus traditioneller Überwachung, innovativer Technologie und direkter Kommunikation sollen Fahrgäste sich sicher und gut betreut fühlen – ein zentraler Baustein für einen attraktiven und vertrauenswürdigen öffentlichen Nahverkehr.

Kommentar

Sicherer ÖPNV in Hamburg: Innovativer Schritt in Richtung Zukunft

Die geplanten Maßnahmen der Hamburger Hochbahn und S-Bahn sind ein begrüßenswerter Schritt hin zu mehr Sicherheit im öffentlichen Nahverkehr. Die Aufstockung des Sicherheitspersonals um 80 Kräfte auf insgesamt 750 ist ein deutliches Signal, dass Sicherheit und Präsenz vor Ort ernst genommen werden. Gerade in einer Zeit, in der öffentliche Verkehrsmittel ein zentraler Bestandteil nachhaltiger Mobilität sind, ist es wichtig, das subjektive und objektive Sicherheitsgefühl der Fahrgäste zu stärken.

Besonders innovativ erscheint der stille Alarm per WhatsApp. Diese unauffällige Möglichkeit, Hilfe zu rufen, ist ein zeitgemäßes Angebot, das den Bedürfnissen der Fahrgäste in unangenehmen oder bedrohlichen Situationen gerecht wird. Es zeigt, dass die Verkehrsbetriebe nicht nur auf klassische Sicherheitskonzepte setzen, sondern auch moderne Kommunikationswege nutzen, um effizient und diskret zu reagieren.
Auch der Einsatz von künstlicher Intelligenz ist ein richtungsweisender Ansatz. Die Möglichkeit, gefährliche Situationen automatisch zu erkennen und gezielt zu reagieren, könnte die Effizienz und Präzision des Sicherheitspersonals erheblich verbessern. Dadurch wird nicht nur Zeit gespart, sondern auch die Wahrscheinlichkeit erhöht, kritische Vorfälle rechtzeitig zu entschärfen.

Abgerundet wird das Sicherheitskonzept durch das Waffenverbot im gesamten HVV-Gebiet, das eine klare Botschaft gegen Gewalt und Bedrohungen aussendet. Die Kombination aus zusätzlichem Personal, moderner Technologie und präventiven Maßnahmen ist ein ganzheitlicher Ansatz, der Modellcharakter für andere Städte und Regionen haben könnte.

Hamburg zeigt hiermit, wie öffentliche Verkehrsmittel nicht nur ökologisch, sondern auch sicherer gestaltet werden können. Ein Gewinn für alle Fahrgäste und ein wichtiger Schritt hin zu einer nachhaltigen und lebenswerten Stadt. (ml)



Intelligentes Wohnraummanagement

Studierendenwerk Mannheim setzt auf modernes Zutrittskontrollsystem AccessOne

Das Studierendenwerk Mannheim setzt auf das Zutrittskontrollsystem AccessOne von CES, um die Verwaltung der Wohnanlagen effizient und sicher zu gestalten. Mit über 200 elektronischen Beschlägen und mehr als 50 Zylindern im neuen Wohnhaus B6 ermöglicht das System den Studierenden, nur die von ihnen gemieteten Apartments oder Zimmer zu betreten. Dank der AccessOne-Software können Berechtigungsprofile flexibel erstellt und verwaltet werden, was den Aufwand bei Mieterwechseln oder für Handwerker und Reinigungspersonal minimiert. Zudem bietet die Software die Möglichkeit, die Parkbereichsverwaltung zu integrieren und Zeitmanagement für Facility- und Reinigungspersonal zu steuern. Ronald Ros vom Studierendenwerk Mannheim schätzt die Skalierbarkeit und die Schnittstellen zu weiteren Managementsystemen, wodurch AccessOne einen entscheidenden Mehrwert bietet.

Das Studierendenwerk in Mannheim ist für Studierende YOUR PARTNER ON CAMPUS, weil es bei den vielfältigen Themen zur sozialen Infrastruktur wie BAföG, Mensen, Kindertagesstätten für Kinder von Studierenden und sozial- und psychologischer Beratung die Studierenden unterstützt. Ein zentrales Angebot stellt dabei die Bereitstellung von bezahlbarem Wohnraum dar. Die Wohnhäuser des Studierendenwerkes bieten hochschulnahe und günstige Apartments oder WG-Zimmer: quer über die Stadt Mannheim verteilt, immer mit guter Anbindung zu den Studienorten und der Symbiose zum sorglosen Lernen und entspannten Leben.

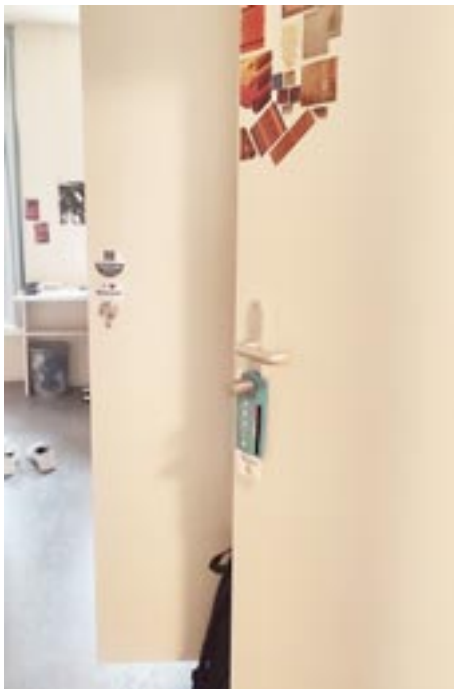
Das neue Studierendenwohnhaus B6 ist in hybrider Holzmodulbauweise als KfW-Energieeffizienzhaus nach dem Standard 40plus gebaut. Dadurch verbraucht es weniger Energie als über die hauseigene Photovoltaik-Anlage produziert wird. Es stehen 141 Einzel-Apartments, 48 Doubletten, drei Paarwohnungen, vier behindertengerechte und vier Eltern-Kind-Apartments zur Verfügung, alle voll möbliert. Auto und Fahrrad können bequem in der

Tiefgarage und im Fahrradkeller abgestellt werden. Die Wohnanlage befindet sich wie die neu errichteten Gebäude der Universität im B6-Areal und ermöglicht somit das Wohnen auf dem Campus.
Abteilungsleiter Ronald Ros vom Projekt- und Prozessmanagement des Studierendenwerkes Mannheim kennt die Herausforderungen, die bei der Organisation und Verwaltung verschiedener Gebäude und Wohnungen zu meistern sind. Daher schätzt er die Empfehlung von seinem Fachhändler Schlüssel Walter aus Mannheim auf das Zutrittskontrollsystem AccessOne von CES zu setzen.



„Die Projektplaner von CES waren sehr zuverlässig, das Berechtigungskonzept war gut geplant und das Arbeiten mit der Software war schnell selbstständig möglich, da auch die Bedienungsanleitung sehr gut hilft. Mit der partnerschaftlichen Umsetzung von CES und Schlüssel Walter bin ich überaus zufrieden. Es ist immer gut zu wissen, dass ein Ansprechpartner erreichbar und vor Ort ist."

Mit der AccessOne-Software verwaltet Ronald Ros in B6 die Berechtigungen von über 200 elektronischen Beschlägen und mehr als 50 Zylindern und organisiert dabei zuverlässig, dass die Studierenden jeweils nur das von ihnen angemietete Apartment oder Zimmer im Gebäude öffnen können und nicht die Wohnungen der Mitstudierenden.



An den Gebäudeeingängen lesen sich alle Zutrittsberechtigten mit ihrem Transponder an den Wandterminals ein und erhalten Zutritt zum Wohnhaus. In der Software werden je nach Bedarf Berechtigungsprofile definiert. Darin sind Schließgeräte in unterschiedlichen Nutzergruppen und Zeitmodellen zusammengefasst. Neue Studierende im Wohnhaus werden einfach dem entsprechenden Berechtigungsprofil zugeordnet. Das verringert den Aufwand und vereinfacht die Vergabe von Zutrittsberechtigungen, bei Mieterwechseln oder für Handwerker und Reinigungspersonal. Nur die Studierenden, die einen Parkplatz in der Tiefgarage gemietet haben, sind mit ihrem Identifikationsmedium in der Lage, auch das Einfahrtstor zur Tiefgarage zu öffnen. Die Option, die Parkbereichsverwaltung über die Zutrittskontrollsoftware zu managen und dass auch weitere Module wie das Zeitmanagement für Facility- und Reinigungspersonal integrierbar sind, überzeugen Ronald Ros. Für ihn ist klar, dass zukünftige Wohnanlagen mit der Mandantenfunktion bequem in AccessOne verwaltet werden.

„Entscheidend war für mich, dass das System skalierbar ist, um auf neue Anforderungen reagieren zu können. Das einfache Verwalten und Organisieren der vermieteten Wohnplätze sind eine Grundvoraussetzung. Die Funktionen, die andere organisatorische Prozesse unterstützen sowie die Schnittstellen zu weiteren Managementsystemen machen jedoch den entscheidenden Mehrwert von AccesOne für mich aus".













Handwerkskammer Cottbus

Impulse für das Handwerk und die deutsche Wirtschaft für die Zukunft

Die Handwerkskammer Cottbus setzt nicht nur Maßstäbe, sondern definiert das Handwerk mit ihrem vielseitigen Engagement ganz neu. Besonders hervorzuheben ist ihre unermüdliche Unter- stützung bei der Meisterprüfung, die den Grundstein für den Erfolg jedes Handwerkers legt und gleichzeitig zur Sicherstellung der hohen Qualitätsstandards im Handwerk beiträgt. Diese nachhaltige Förderung der fachlichen Exzellenz stärkt die gesamte Branche und sorgt dafür, dass die Wettbewerbsfähigkeit in einer immer komplexer werdenden Welt gewahrt bleibt.

Doch die Handwerkskammer Cottbus ist weit mehr als eine Institution der Fachqualifikation. Ihr politisches Engagement verdient ebenfalls größte Anerkennung. Mit einer klaren Haltung tritt sie für die Belange der Handwerksbetriebe ein, etwa bei der Unterstützung von Ausnahmeregelungen zu Einfahrtsverboten in Innenstädte. Hier zeigt die Kammer ihre Rolle als starke Interessenvertretung und sorgt für spürbare Erleichterung im betrieblichen Alltag. Ihre pragmatische Herangehensweise stellt sicher, dass die Bedürfnisse der Handwerker gehört und berücksichtigt werden.

Ein besonderes Highlight sind die Social-Media-Aktivitäten der Handwerkskammer Cottbus. Diese sind alles andere als gewöhnlich: Sie sind oft humorvoll, ironisch und manchmal auch politisch kritisch, was das Profil der Kammer klar schärft. Die Mischung aus Information und Unterhaltung spricht nicht nur die jüngeren Generationen an, sondern sorgt auch für einen lebendigen Austausch und regt zum Nachdenken an. Durch die Vorstellung von Berufsbildern und Ausbildungsmöglichkeiten wird jungen Menschen eine klare Perspektive geboten, während gleichzeitig die Leistungsträger des Handwerks und der regionalen Wirtschaft gewürdigt werden. Mit ihrem scharfsinnigen und teils provokanten Stil wird nicht nur Wissen vermittelt, sondern auch eine wertvolle Diskussion angestoßen.

Dieses beispielhafte Social-Media-Engagement hat weit über die Handwerkskammer Cottbus hinaus Wirkung. Es bietet nicht nur einen erfolgreichen Weg, den Dialog zu wichtigen Arbeitskräften und potenziellen Auszubildenden aufzubauen und auszubauen, sondern könnte auch als Vorbild für andere Kammern, Innungen und die Sicherheitsindustrie dienen.

Besonders im Hinblick auf die mittelständischen Unternehmen wird hier ein Weg aufgezeigt, wie eine praxisorientierte, offene Kommunikation und kritische Auseinandersetzung mit gesellschaftlichen Themen dazu beitragen können, das Handwerk und die gesamte Wirtschaft zukunftsfähig zu gestalten.

Diese ganzheitliche Herangehensweise macht die Handwerkskammer Cottbus zu einer unverzichtbaren Institution, die mit ihrer dynamischen Kommunikation und ihrem klaren Engagement sowohl die Gegenwart als auch die Zukunft des Handwerks und der deutschen Wirtschaft gestaltet.

5 Tipps

E-Mail-Security NIS-2-compliant

E-Mail ist der wichtigste Kommunikationskanal in Unternehmen und gleichzeitig der beliebteste Angriffsvektor für Cyberkriminelle. Daher spielt E-Mail-Security eine zentrale Rolle für die Cybersicherheit. Mit der neuen NIS-2-Richtlinie wachsen die Mindestanforderungen an Risikomanagement und Schutzmaßnahmen. Was müssen Unternehmen tun, um ihre E-Mail-Landschaft NIS-2-compliant zu machen?

Mit der NIS-2-Richtlinie will die EU die Cybersicherheit wichtiger und besonders wichtiger Einrichtungen stärken. Derzeit arbeiten die Mitgliedsstaaten daran, die Direktive in nationales Recht zu überführen. In Deutschland erfolgt das über das NIS-2-Umsetzungsgesetz, das im März 2025 in Kraft treten soll. Unternehmen wird dringend empfohlen, die Sicherheitsmaßnahmen für ihre E-Mail-Infrastruktur zu überprüfen, um die Compliance sicherzustellen.

Denn der Kommunikationskanal Nummer eins ist die häufigste Eintrittspforte für Cyberangriffe. Artikel 21 der Richtlinie fordert „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen, um Risiken für die Sicherheit der Netz- und Informationssysteme zu beherrschen und die Auswirkungen von Sicherheitsvorfällen zu verhindern oder möglichst gering zu halten."

Was das für die E-Mail-Umgebung bedeutet, zeigen die folgenden fünf Tipps von Romana Staringer, Senior Account Manager E-Mail Security bei Retarus.

1. Etablieren Sie erweiterten E-Mail-Schutz

Die meisten Unternehmen haben bereits einen Basisschutz für ihre E-Mail-Umgebung. Dazu zählen Virenscanner und Phishing-Filter, die gefährliche E-Mails herausfiltern, bevor sie zugestellt werden. Doch damit lässt sich nur ein Teil der Bedrohungen abfangen. Denn Cyberkriminelle entwickeln laufend neue Malware-Varianten, die von signaturbasierten Security-Systemen nicht erkannt werden, solange noch keine passenden Erkennungsmuster vorliegen. Außerdem sehen wir vermehrt Social Engineering-Attacken wie CEO-Fraud, die ihre Opfer austricksen und dazu bringen, hohe Geldsummen zu überweisen oder sensible Daten preiszugeben. Solche Betrugsmaschen arbeiten meist mit nahezu perfekt gefälschten E-Mails, die für herkömmliche Phising-Filter nur schwer von harmlosen Nachrichten zu unterscheiden sind. Um die Risiken für immer raffiniertere Cyberangriffe zu minimieren, brauchen Unternehmen erweiterten E-Mail-Schutz. Dazu zählen zum Beispiel KI-gestützte Analysen, die in der Lage sind, gefälschte Absender- und Domain-Adressen zu identifizieren. Wichtig ist zudem Time of Click Protection – eine Technologie, die alle in E-Mails enthaltenen Links überprüft und Aufrufe dahinter liegende Websites gegebenenfalls blockiert. Um neuartige Malware zu erkennen, sind darüber hinaus Sandbox-Analysen unverzichtbar, die E-Mails mit verdächtigen Anhängen auf bedrohliches Verhalten untersuchen.

2. Verschlüsseln Sie sensible E-Mails

Artikel 21, Absatz 2d der NIS-2-Direktive fordert Maßnahmen zur Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen. Auf E-Mail



übertragen bedeutet das: Sie sollten die Kommunikation mit Ihren Zulieferern und Partnern absichern. Dafür eignet sich Verschlüsselung. Absatz 2h NIS-2 schreibt explizit Konzepte und Verfahren für den Einsatz von Kryptographie vor. In der Praxis scheitert E-Mail-Verschlüsselung jedoch häufig an einer aufwendigen Administration der Schlüssel, an einer umständlichen Bedienung und daran, dass Kommunikationspartner keine Verschlüsselung nutzen und somit verschlüsselten E-Mails nicht lesen können. Gefragt ist daher eine Lösung, die ausgehende Mails mit nur einem Klick direkt im E-Mail-Client verschlüsselt, ohne dass sich der Absender mit technischen Details oder der Schlüsselverwaltung auskennen muss. Möglich wird das durch ein Secure E-Mail-Gateway, das alle gängigen kryptographischen Standards unterstützt. Empfänger ohne eigene Verschlüsselungslösung werden idealerweise über ein sicheres Webmail-Postfach eingebunden, über das sie die verschlüsselten Nachrichten lesen können.

3. Denken Sie an die Notfall-Kommunikation

Artikel 21, Absatz 2c der NIS-2-Richtlinie fordert Maßnahmen zur Aufrechterhaltung des Betriebs, Absatz 2j gesicherte Notfall-Kommunikationssysteme. Für den E-Mail-Bereich bedeutet das: Sie brauchen einen Plan B, falls Ihre E-Mail-Infrastruktur durch einen Cyberangriff außer Kraft gesetzt wird. Wie können Sie dafür sorgen, dass die Mitarbeitenden in so einem Fall weiterhin in der Lage sind, Nachrichten zu versenden und zu empfangen? In der Praxis haben sich Lösungen für E-Mail-Continuity bewährt, die im Hintergrund einen externen, unabhängigen und sicheren Webmail-Service bereithalten. Im Krisenfall können Sie sofort auf die Notfallinfrastruktur umschalten. Wichtig dabei ist, dass der Service vom Anbieter mit vorprovisionierten Postfächern zur Verfügung gestellt wird. Denn nur mit den E-Mails der vergangenen Wochen sowie den gespeicherten Kontaktdaten können Sie im Notfall wirklich nahtlos weiter kommunizieren.

4. Untersuchen Sie auch bereits zugestellte E-Mails

Artikel 21, Absatz 2b schreibt Maßnahmen zur Bewältigung von Sicherheitsvorfällen vor. Um solche Maßnahmen treffen zu können, müssen Sie in der Lage sein, Cyberangriffe schnell zu erkennen und zu untersuchen. Dafür ist es wichtig, die Eintrittspforte zu bestimmen und die Empfänger bereits zugestellter Schad-E-Mails schnell zu identifizieren. Möglich wird das über eine spezielle Patient-Zero-Detection-Technologie, die bereits beim E-Mail-Empfang einen digitalen Fingerabdruck aller Attachments erzeugt, in einer Datenbank speichert und dann kontinuierlich mit neuen Erkenntnissen aus der Malware-Forschung abgleicht. Sobald eine potenziell gefährliche Nachricht im Postfach eines Anwenders erkannt wird, kann diese – je nach Konfiguration – automatisch gelöscht oder in Quarantäne verschoben werden.

5. Verbessern Sie die Forensik

Artikel 23 der NIS-2-Richtlinie definiert strenge Meldepflichten. Betroffene Unternehmen müssen einen erheblichen Cybervorfall innerhalb von 24 Stunden bei der zuständigen Aufsichtsbehörde melden, nach 72 Stunden einen Folgebericht einreichen und nach einem Monat einen Abschlussbericht, der eine detaillierte Beschreibung enthält. Um diese Vorgaben zu erfüllen, brauchen Sie schnell Zugriff auf relevante Daten. Daher ist es wichtig, Security-Informationen aus der E-Mail-Umgebung in übergreifenden Sicherheitssys- temen wie einem SIEM (Security Information and Event Management) zu sammeln und auszuwerten. Eine entsprechende Lösung sollte die Daten in Form von Events in Echtzeit über eine geschützte Schnittstelle bereitstellen.

Fazit

NIS-2-konforme E-Mail-Sicherheit bedeutet mehr als ein- und ausgehende Nachrichten lediglich zu prüfen. Unternehmen müssen die gesamte E-Mail-Infrastruktur betrachten und Konzepte sowohl für die Prävention, die Bedrohungserkennung als auch die Bewältigung von Cyberangriffen entwickeln.

Darüber hinaus tragen Früherkennung und Schadensbegrenzung zu dem übergeordneten Ziel der Verbesserung der Cyber-Sicherheitslage in der EU bei. Daher empfiehlt es sich, eine integrierte Lösung zu wählen, die alle wichtigen E-Mail-Security-Funktionen unter einer Plattform vereint und modular bereitstellt. So können Unternehmen Management-Aufwand reduzieren und ihre bestehende Security-Infrastruktur ganz nach Bedarf ergänzen.



©boschsecurity.com/xc/en/news/product-news/3100i-fixed-cameras

Videobranche als Sensormarkt

Regierungsinitiativen für Wachstum verantwortlich

Rasche Fortschritte in Technologien wie maschinelles Lernen, Edge Computing und Kameratechnologien, positive Regierungsinitiativen und die Finanzierung von Videoüberwachung sowie die steigende Nachfrage nach Überwachung und Sicherheit sind einige der Haupttreiber für den Markt für Video als Sensor, so ein neuer Forschungsbericht. Der Bericht prognostiziert, dass dieser Sektor bis 2029 ein Volumen von rund 101,89 Milliarden US-Dollar erreichen wird, gegenüber 69,52 Milliarden US-Dollar im Jahr 2024, mit einer erwarteten jährlichen Wachstumsrate von 7,9 %.

Der Bericht von Marketsandmarkets weist auch darauf hin, dass die raschen Fortschritte bei AI und das Wachstum von Smart-City-Initiativen eine starke Chance für Video als Sensor bieten dürften. Darüber hinaus werden Datenschutz- und Sicherheitsbedenken sowie die Komplexität der Integration von Video als Sensorlösung voraussichtlich zu den hemmenden Faktoren für den Markt gehören. Herausforderungen im Bereich des Datenmanagements und der Datenspeicherung sowie einige Probleme im Zusammenhang mit der Anbieterbindung und der Interoperabilität werden den Markt für Video als Sensor voraussichtlich vor Herausforderungen stellen.

Software zur Verwaltung und Integration
Softwarelösungen für Video-as-a-Sensor werden im Prognosezeitraum voraussichtlich mit hohen jährlichen Wachstumsraten (CAGR) zunehmen, da sie eine wichtige Rolle bei der Verbesserung der Funktionalität und Effektivität von Videoüberwachungs- und Bildverarbeitungssyste-

men spielen. Dazu gehören Video-as-a-Sensor-Softwareanwendungen wie Video Management Software (VMS), intelligente Videoanalysesoftware, Algorithmen für maschinelles Lernen und maschinelle Lernverfahren sowie Integrationssoftware.

Es besteht ein Bedarf an Videoüberwachungsmanagement, -überwachung und -analyse, um das Wachstum von VMS voranzutreiben, während die Einführung von Echtzeit-Bedrohungserkennung durch künstliche Intelligenz und maschinelles Sehen die Entwicklung intelligenter Videoanalysesoftware vorantreiben dürfte, und die Einführung von Objekterkennungs- und prädiktiven Analysetechnologien das Wachstum von KI- und ML-Algorithmen fördern dürfte. Integrationssoftware nutzt in erster Linie die Interaktivität zwischen verschiedenen Hardwarekomponenten wie Kameras, Sensoren und anderen Softwaresystemen.

Hyperspektrale Bildverarbeitung für detaillierte Analysen

Hyperspektrale Bildgebung ist eine Bildgebungstechnologie, die Bilder in Hunderten verschiedener Wellenlängenbereiche des elektromagnetischen Spektrums erfasst und verarbeitet. Die meisten Kameras erfassen Bilder nur in drei Spektralbändern: Rot, Grün und Blau. Hyperspectral Imaging-Systeme erfassen Bilder über Hunderte oder manchmal Tausende von zusammenhängenden Spektralbändern, die detaillierte Spektralinformationen für jedes Pixel im Bild liefern. Anwendungsbereiche sind Umweltüberwachung, Landwirtschaft, Mineralogie, Fernerkundung, medizinische Bildgebung und Materialprüfung.

Sie liefern Spektren der abgebildeten Details und helfen bei der Durchführung anspruchsvoller Analysen und der Materialcharakterisierung, um wertvolle Informationen und wissenschaftliche Entdeckungen in Industrie und Forschung zu gewinnen. Zu den Unternehmen, die Lösungen für die hyperspektrale Bildgebung anbieten, gehören Specim and Spectral Imaging Ltd (Finnland) und Corning Incorporated (USA).

Staatliche Initiativen spielen eine Schlüsselrolle

Der Endanwendermarkt für Video als Sensor spielt eine Schlüsselrolle bei der Verbesserung der öffentlichen Sicherheit, der Steigerung der betrieblichen Effizienz und der Unterstützung verschiedener Verwaltungsfunktionen. Regierungen setzen Video als Sensortechnologie in vielen Bereichen ein, z. B. in der öffentlichen Überwachung, im Verkehrsmanagement und bei Notfalleinsätzen. Solche Systeme bieten die Vorteile der Echtzeitüberwachung und Datenerfassung.

Darüber hinaus können diese Informationen für die Entscheidungsfindung und die Formulierung von Richtlinien genutzt werden. Einer der wichtigsten Einsatzbereiche von Video als Sensortechnologie für Behörden ist die öffentliche Sicherheit. Regierungsbehörden installieren Videosensorlösungen in Städten, städtischen Parks und kritischen Infrastrukturbereichen, um Kriminalität zu überwachen und die Sicherheit zu erhöhen.

Städte wie London haben beispielsweise mehrere vernetzte Videoüberwachungssysteme installiert, die nicht nur bei der Prävention von Straftaten helfen, sondern auch die Polizei bei Ermittlungen durch forensische Beweise unterstützen.

Gefragte Technik für das Verkehrsmanagement

Die wichtigste Anwendung von Video als Sensortechnologie findet sich im Bereich des Verkehrsmanagements, wo es um die Optimierung von Verkehrssystemen und die Gewährleistung sicherer Straßenverkehrssysteme geht. Moderne Videoüberwachungs- und Analyselösungen sind wichtig für die Integration in effizientere Verkehrsüberwachungs-, -steuerungs- und -managementprozesse in städtischen Umgebungen mit wachsender Bevölkerung und erheblichen Stauproblemen.

Moderne Verkehrsmanagementsysteme sind mit Webschnittstellen oder mobilen Anwendungen für den Fernzugriff auf Videostreams und Analysen ausgestattet, so dass die Bediener die Verkehrssituation von überall aus steuern können. Unternehmen haben Videosysteme als Sensoren für das Verkehrsmanagement entwickelt. Teledyne Technologies Incorporated bietet beispielsweise fortschrittliche Softwarelösungen an, darunter eine hoch entwickelte Verkehrssoftware für ein effektives und effizientes Verkehrsmanagement und eine effiziente Verkehrssteuerung. Die Leitstellensoftware ist mit umfassenden Werkzeugen zur Überwachung und Verwaltung mehrerer Systeme und Prozesse ausgestattet.

Europa bietet große Wachstumschancen
Der Videoüberwachungsmarkt in Europa wächst aufgrund von Faktoren wie Veränderungen im Sicherheitssektor in der Region und technologischen Fortschritten schnell. Steigende Kriminalitätsraten und Terrorismus haben Regierungen und private Organisationen dazu veranlasst, in verbesserte Videoüberwachungssysteme zu investieren.

Diese Systeme schrecken vor kriminellen Handlungen ab, unterstützen die öffentliche Sicherheit und ermöglichen die Strafverfolgung. In Deutschland treibt der Schutz der Privatsphäre bei gleichzeitiger Verbesserung der Sicherheit den Markt an; Initiativen der britischen Regierung und private Partnerschaften unterstützen das Marktwachstum; und die Notwendigkeit, die öffentliche Sicherheit in Frankreich zu gewährleisten, fördert die Einführung von Video als Sensorlösung.

Befragte Unternehmen waren Honeywell, Motorola, Dahua, Bosch, Hikvision, AT&T, IBM, Cisco, Axis Communications, Johnson Controls, Sony, Sharp, Teledyne, Corning und Pixart Imaging sind einige der Hauptakteure auf diesem Markt, die in der Studie hervorgehoben werden.

[www.marketsandmarkets.com]



Kompakt, intelligent und sicher

Dallmeier electronic präsentiert neue Einstiegskamera „Picoline“

Dallmeier electronic erweitert sein Produktportfolio um die Einstiegskamera Picoline. Damit bietet Dallmeier eine kompakte und preiswerte Lösung für Anwendungen, die Aufnahmen mit höchster Auflösung bei Tag und Nacht (IR-Modus) erfordern. Ob für den Einsatz in einer Umgebung mit anspruchsvollen Lichtverhältnissen oder bei wenig Platz – die Picoline liefert hochwertige Ergebnisse.

Die Picoline vereint hohe Bildqualität mit bis zu fünf MP Auflösung, einer Vielzahl von Cybersecurity-Vorkehrungen und KI-Analysefunktionen in einem kompakten Aufputzgehäuse. Der kleine Formfaktor ermöglicht die Montage auf engstem Raum an Decken oder Wänden. Die Stromversorgung erfolgt über PoE. Als Allrounder ist die Einstiegskamera für zahlreiche Anwendungen konzipiert.

Domera OS – Cybersecurity „Made in Germany“

Sicherheit steht bei der Picoline-Serie an erster Stelle. Durch das abgeschottete Linux Betriebssystem Domera® OS profitieren Nutzer von umfangreichen Sicherheitsfunktionen. Regelmäßige externe Penetrationstests, Überwachung und Pflege gewährleisten darüber hinaus, dass die Software-Komponenten stets auf dem aktuellen Sicherheitsstandard sind.

Sicherheitsupdates über die gesamte Lebensdauer

„Made in Germany“ ist für die Kunden von Dallmeier gelebte Realität. Neben Funktionsupdates für mindestens fünf Jahre mit der Option zur Verlängerung stellt Dallmeier Sicherheits-Updates für bekannt gewordene relevante CVE-Sicherheitslücken (vorbehaltlich technischer Machbarkeit) für die gesamte Laufzeit der Software-Wartung zur Verfügung.

Effiziente Überwachung durch KI EdgeAnalytics

Mit der optionalen „Basic AI Objektklassifizierung“ kann die Picoline Objekte wie Personen oder Fahrzeuge erkennen und klassifizieren – unabhängig von Bewegungen im Hintergrund. Mit Hilfe der KI EdgeAnalytics Apps, wie „Loitering Detection“, „Intrusion Detection“ und „People Counting“, können Benutzer die für sie relevanten Ereignisse gezielt analysieren und auswerten.

Auswertung über jedes ONVIF-kompatible VMS und Steuerung von IoT-Devices

Die Kamera-Serie ist ONVIF-kompatibel, dadurch können Anwender sie problemlos in Dallmeier Client-Software sowie andere ONVIF-kompatible VMS-Systeme integrieren. Ereignismeldungen lassen sich per E-Mail versenden oder für die Steuerung von IoT-Geräten über MQTT und HTTPS verwenden.

Hohe Bildqualität auch bei anspruchsvollen Lichtverhältnissen

Für die optimale Aufnahme von kontrastreichen Szenen mit sehr hellen und dunklen Bereichen sind die Kameras mit einer WDR-Funktion (HDR) ausgestattet. Jedes Bild wird mit zwei speziellen Einstellungen erfasst, die in Echtzeit zu einem ausgewogenen Ergebnis kombiniert werden.

Der resultierende Video-Stream bietet wesentlich mehr Details sowohl in hellen als auch dunklen Bereichen und ist optisch sehr gut an die Wahrnehmung des menschlichen Auges angepasst.

Zusätzlich lokale Aufzeichnung „an der Edge“

Zwei Video-Streams mit unterschiedlichen Einstellungen gleichzeitig speichern? Das geht mit Hilfe von EdgeRecording auf einer integrierten SD-Karte mit bis zu 1TB. Die durch ein EdgeAnalytics-Ereignis ausgelöste Aufzeichnung ermöglicht es, kritische Momente mit einstellbarer Vor- und Nachlaufzeit festzuhalten. Zusätzlich kann der Video-Stream an ein Aufzeichnungssystem zur permanenten Sicherung übertragen werden.

Die Picoline-Serie bietet Nutzern eine flexible, preiswerte und sichere Lösung für unterschiedlichste Überwachungsanforderungen. Wie alle Dallmeier Kameras liefert die Picoline Aufnahmen mit ausgezeichnetem Kontrast, brillanter Klarheit sowie höchste Detailauflösung und Farbtreue.

Überwachungskameras für den Innenbereich

Heise Online hat zehn Indoor-Überwachungskameras getestet und wichtige Informationen für diese Produktart vorgestellt. Weil zunehmend Sicherheit und Komfort in den eigenen vier Wänden immer wichtiger werden, stehen z.B. die Überwachung von Haustieren, die Sicherheit der Familie oder auch der Schutz des Eigentums für Menschen im Fokus. Durch künstliche Intelligenz (KI), HD-Videoqualität und viele Steuerungsoptionen werden auch im Consumerbereich die Lösungen immer komplexer.

Heise Online hebt in diesem Produktvergleich hervor, welche Überwachungskameras für den Innenbereich derzeit besonders überzeugen. Je nach individuellen Anforderungen bieten die Modelle High-End-Funktionen, ein gutes Preis-Leistungs-Verhältnis oder sind budgetfreundlich. Die Testreihe beleuchtet die wichtigsten Stärken und Schwächen von Produkten auf dem Markt.

Innovative Funktionen wie künstliche Intelligenz (KI), HD-Bildqualität und Bewegungsverfolgung ermöglichen vielseitige Einsatzmöglichkeiten und erhöhen die Sicherheit im Alltag. Die besten drei von zehn getesteten Modelle wurden mit besonderem Fokus auf Bildqualität, Ausstattung und Preis analysiert.

Der Testsieger

Die Eufy Indoor Cam S350 bietet mit ihrer einzigartigen Dual-Objektiv-Technologie eine beeindruckende Kombination aus Weitwinkel- und Teleaufnahmen. Dank einer 4K-Auflösung werden scharfe Bilder geliefert, die das gesamte Sichtfeld aber auch feinste Details wiedergeben. Eine automatische Bewegungsverfolgung sorgt dafür, dass die Kamera sich dynamisch an Bewegungen anpasst. Eine intuitive App, die Aktivitätszonen und Datenschutzeinstellungen erlaubt, macht die Kamera benutzerfreundlich.

Ein kleiner Nachteil ist, dass die Pan-Tilt-Zoom-Funktion eingeschränkt ist, wenn Datenschutzzonen aktiviert sind. Die Integration in Smart-Home- und NAS-Systeme enttäuscht. Der Preis ist für Nutzer attraktiv, gerade wegen der HD-Bilder, der KI-Funktionen sowie der Gesichtserkennung.

Der Preis-Leistungs-Sieger

Die TP-Link Tapo C225 bietet eine Bewegungs- und Geräuscherkennung. Auch eine QHD-Auflösung und eine zuverlässige Unterscheidung zwischen Menschen, Tieren und Fahrzeugen sind sinnvoll. Die Erkennung von Glasbruch oder das Überschreiten von virtuellen Linien sind ebenfalls implementiert.

Daten können lokal gespeichert werden. Interessant ist auch die Onvif-Konformität, gerade im Hinblick auf die Smart-Home-Integration. Nach Meinung der Heise-Experten ist ein kleiner Schwachpunkt die vergleichsweise leise Alarmfunktion, die in lauten Umgebungen auch überhört werden kann. Auch diese Kamera eignet sich sowohl als Babyphone als auch für die Überwachung von Haustieren.

Die Preisgünstige

Die Annke Crater 2 ist in der Anschaffung sehr günstig. Die Auflösung von drei Megapixeln und eine automatische Verfolgung von Bewegungen sind im Leistungsportfolio enthalten. Eine Zwei-Wege-Kommunikation ermöglicht es Nutzern, direkt über die Kamera zu sprechen. Die Android-App ist funktionsfähig.

In ein Smart-Home-System ist die Integration, auch wegen fehlender Onvif-Kompatibilität, schwierig. Einfache Überwachungsaufgaben sind aber kein Problem.

Fazit

Auch im niedrigen Preissegment ist eine Auswahl an Überwachungskameras für Privatanwender möglich, die auf hohe Bildqualität und innovative Funktionen wie KI-gestützte Gesichtserkennung setzen. Das Preis-Leistungs-Verhältnis und vielseitige Sicherheitsfunktionen sowie eine kostengünstige Überwachung sind möglich.

Professionelle Anbieter von Videosicherheitslösungen könnten jedoch Kritik an der langfristigen Zuverlässigkeit und der eingeschränkten Integration dieser Kameras in größere Überwachungssysteme üben. Häufig fehlen bei diesen Konsumentenmodellen fortgeschrittene Funktionen wie redundante Speicheroptionen, einheitliche Steuerungsplattformen oder die Möglichkeit, mehrere Kameras zentral zu verwalten.

Auch die Abhängigkeit von Cloud-Diensten und die damit verbundenen Datenschutzfragen sind Aspekte, die von Experten als potenzielle Schwachpunkte angesehen werden könnten. Für komplexere Sicherheitsanforderungen oder geschäftliche Anwendungen bleiben daher professionelle Systeme die bessere Wahl.

Der ganze Testbericht auf Heise Online: [https://tinyurl.com/3nc57n9d]

Bewährte Verfahren

Risikomanagement und Beschaffung im Bereich physische Sicherheit

Effektives Risikomanagement und eine durchdachte Beschaffungsstrategie sind essenziell, um Organisationen widerstandsfähig zu halten und partnerschaftlich erfolgreich zu agieren. Der Schutz physischer Sicherheitssysteme ist hierbei ein zentraler Bestandteil, der nicht nur den operativen Betrieb sichert, sondern auch den Ruf der Organisation schützt.



Risikomanagement im Fokus

Definition und Zielsetzung

Risikomanagement umfasst die Identifikation, Bewertung und Steuerung potenzieller Risiken, die Organisationen beeinträchtigen könnten. Im Bereich der physischen Sicherheit zielt es darauf ab, Bedrohungen wie Systemausfälle, nicht autorisierten Zugang oder Cyberangriffe zu antizipieren und entsprechende Gegenmaßnahmen zu ergreifen. Eine wirksame Strategie reduziert nicht nur die Wahrscheinlichkeit eines Vorfalls, sondern begrenzt auch den Schaden im Ernstfall.

Warum ist Risikomanagement notwendig?

Im Bereich der physischen Sicherheit gibt es eine Vielzahl von Risiken, die sowohl

durch interne Schwachstellen als auch durch externe Bedrohungen entstehen können. Beispiele hierfür sind unsichere Kameras oder IIoT-Geräte, die Cyberangriffe erleichtern.

Diese Schwachstellen könnten unbefugten Zugriff ermöglichen und sensible Daten gefährden. Ein strukturiertes Risikomanagement hilft, solche Gefahren frühzeitig zu erkennen und zu adressieren.

Vorteile eines systematischen Risikomanagements

1. Schutz von Ressourcen: Menschliche und materielle Vermögenswerte werden besser geschützt.
2. Reputationsschutz: Vorfälle, die das Vertrauen beeinträchtigen könnten, werden vermieden.
3. Geschäftskontinuität: Störungen werden minimiert, wodurch der Betrieb auch in Krisenzeiten aufrechterhalten werden kann.
4. Kosteneinsparungen: Frühzeitige Prävention vermeidet teure Schadensfälle und rechtliche Konsequenzen.

Die Rolle der Beschaffung im Risikomanagement

Beschaffung als Schlüsselkomponente

Die Beschaffung von Sicherheitslösungen und -diensten ist ein kontinuierlicher Prozess. Dabei geht es nicht nur um die Auswahl kosteneffizienter Produkte, sondern auch um die Bewertung der Vertrauenswürdigkeit von Lieferanten und deren Fähigkeit, langfristig mit der Organisation zu wachsen. Ein zentraler Aspekt ist die Integration von Cybersicherheitsstandards in den Beschaffungsprozess, um sicherzustellen, dass gekaufte Geräte den neuesten Sicherheits- anforderungen entsprechen. Dies ist besonders bei IIoT-Geräten von entscheidender Bedeutung, da diese oft Ziel von Angriffen sind.

Warum ein kontinuierlicher Prozess entscheidend ist

Einmalige Beschaffungen sind selten nachhaltig. Ein kontinuierlicher Prozess stellt sicher, dass:

- Organisationen Zugang zu den neuesten Technologien haben.
- Lieferanten regelmäßig überprüft werden, um ihre Leistung und Sicherheit zu gewährleisten.
- Anpassungen an sich verändernde Bedrohungslandschaften erfolgen.

Die Wahl der richtigen Partner

Langfristige Partnerschaften mit innovativen Anbietern tragen dazu bei, dass Organisationen flexibel und widerstandsfähig bleiben. Anbieter sollten nicht nur zuverlässige Produkte liefern, sondern auch in der Lage sein, diese kontinuierlich weiterzuentwickeln und neue Anforderungen zu erfüllen.

Eine umfassende Perspektive

Andrew Elvish, Vice President of Marketing bei Genetec, betont: „Es geht weniger um Technologie als vielmehr um die Kultur, die Menschen und die Prozesse, die im gesamten Unternehmen eingeführt werden. Für Beschaffungsexperten und die Personen am Vorstandstisch kommt es darauf an, die Risiken zu verstehen, Verantwortung zu übernehmen und die Entschlossenheit zu haben, entsprechend zu investieren."



Die Bedeutung einer Risikokultur

Förderung von Bewusstsein und Verantwortlichkeit

Eine Organisation kann noch so viele technische Lösungen implementieren – ohne eine Risikokultur bleiben Sicherheitsmaßnahmen ineffektiv. Diese Kultur umfasst:

- **Schulung:** Mitarbeitende auf allen Ebenen müssen die Bedeutung von Sicherheit verstehen und wissen, wie sie selbst Risiken minimieren können.
- **Verantwortlichkeit:** Klare Verantwortlichkeiten stärken die Eigenverantwortung und fördern die Bereitschaft, Sicherheitsmaßnahmen konsequent umzusetzen.
- **Kommunikation:** Regelmäßige Updates zu Sicherheitsrisiken und neuen Verfahren schaffen Transparenz und fördern die Akzeptanz.

Technologie als unterstützendes Element

Während eine Kultur des Risikobewusstseins entscheidend ist, spielen Technologien eine unterstützende Rolle. Sie helfen dabei, Risiken zu überwachen, Vorfälle zu erkennen und schnelle Reaktionen zu ermöglichen. Dabei sollten Systeme so gestaltet sein, dass sie menschliche Überwachung und Entscheidungen ergänzen, aber nicht ersetzen.

Sieben Schritte zu einer effektiven Risikomanagementstrategie

1. Lücken identifizieren und schließen: Analysen von Beinaheunfällen und Vorfällen ermöglichen es, Schwachstellen

zu erkennen und gezielte Maßnahmen zu ergreifen.

2. Mitarbeiter schulen: Mitarbeitende sollten nicht nur mit den Risiken, sondern auch mit den zugehörigen Präventions- und Reaktionsmaßnahmen vertraut sein.
3. Robuste Reaktionsprotokolle: Gut dokumentierte und getestete Protokolle gewährleisten, dass Organisationen auch in Krisensituationen handlungsfähig bleiben.
4. Cybersicherheit priorisieren: Mehrschichtige Sicherheitsansätze und die Einhaltung von Best Practices bei der Produktentwicklung sind essenziell.
5. Ressourcen bereitstellen: Zeit, Budget und Fachwissen sind nötig, um effektive Risikomanagementstrategien zu entwickeln und umzusetzen.
6. Verantwortlichkeit fördern: Teams und Einzelpersonen sollten klare Rollen im Risikomanagementprozess haben.
7. Regelmäßiges Testen: Übungen und Simulationen stellen sicher, dass Strategien in der Praxis funktionieren und kontinuierlich verbessert werden können.

Technologische Unterstützung und Systeme für Risikomanagement

Beispiel: Workflow-Automatisierung

Automatisierte Systeme reduzieren die Arbeitsbelastung von Mitarbeitenden und ermöglichen es, sich auf strategisch wichtigere Aufgaben zu konzentrieren. Diese Systeme können auf Basis vorab definierter Regeln Informationen analysieren und bei Abweichungen Warnungen ausgeben.

Skalierbare Systeme

Technologien, die sich an die Bedürfnisse einer Organisation anpassen lassen, sind langfristig effektiver. Skalierbarkeit gewährleistet, dass Systeme auch bei steigenden Anforderungen zuverlässig arbeiten.

Integration bestehender Systeme

Ein weiterer wichtiger Faktor ist die Fähigkeit, neue Technologien in bestehende Infrastrukturen zu integrieren. Dies minimiert Kosten und reduziert die Komplexität bei der Implementierung.

Zusammenfassung und Zukunftsaussichten

Ein effektives Risikomanagement in Verbindung mit einer durchdachten Beschaffungsstrategie ist unerlässlich, um Organisationen im Bereich der physischen Sicherheit widerstandsfähig zu machen. Es schützt nicht nur Ressourcen und Reputation, sondern stellt auch sicher, dass Organisationen flexibel und zukunftsfähig bleiben. Indem Technologien, Prozesse und Menschen harmonisch integriert werden, können Organisationen Bedrohungen proaktiv begegnen und eine Kultur der Sicherheit fördern, die langfristig Erfolg und Stabilität garantiert.

[www.genetec.com]



Digital Operational Resilience Act

Position der Smart Payment Association zur Kartenpersonalisierung

R&D - Normen / Standardisierung

Die Digital Operational Resilience Act (DORA) wurde am 14. Dezember 2022 verabschiedet und tritt am 17. Januar 2025 in Kraft. Ziel der Verordnung ist es, ein harmonisiertes hohes Maß an cyberoperativer Widerstandsfähigkeit innerhalb der Informations- und Kommunikationstechnologie (IKT) der europäischen Finanzindustrie sicherzustellen. Im Kern reguliert DORA die Beziehungen zwischen Finanzinstituten und externen IKT-Dienstleistern, insbesondere bei der Bewertung kritischer Abhängigkeiten und der Einhaltung spezifischer Resilienzstandards.



Die Smart Payment Association (SPA) argumentiert in ihrem Positionspapier, dass die physische Personalisierung von Zahlungskarten nicht in den Geltungsbereich von DORA gehört. Das Papier liefert eine detaillierte Begründung dieser Position.
Schlüsselargumente der SPA

1. Kartenpersonalisierung als industrieller Prozess

Nach Artikel 3(21) von DORA umfasst der Begriff „IKT-Dienstleistungen" digitale und datenbezogene Dienste, die über vernetzte Systeme bereitgestellt werden. Die Personalisierung von Zahlungskarten ist ein rein industrieller Prozess, bei dem Kartendaten offline in personalisierten Karten integriert werden. Dieser Vorgang findet in spezialisierten Produktionszentren statt und ist somit weder ein IKT-Dienst noch ein Teil der Bank- oder Zahlungssysteme.

2. Keine Integration in Zahlungsverkehrssysteme

Zahlungskartensysteme sind hochgradig vernetzte Infrastrukturen, deren Funktionsfähigkeit von Echtzeitkommunikation abhängt. Im Gegensatz dazu agieren Personalisierungszentren autonom und sind nicht mit diesen Systemen verbunden. Störungen im Personalisierungsprozess haben daher keinerlei Auswirkungen auf die Leistung oder Verfügbarkeit von Zahlungssystemen.

3. Offline und sicher isoliert

Die Personalisierung erfolgt offline und ist streng isoliert von den IKT-Systemen der Banken. Datenübertragungen zwischen Banken und Personalisierungszentren erfolgen über geschützte End-to-End-Verbindungen. Nach Abschluss der Personalisierung werden die Daten gelöscht, wodurch jegliche Rückwirkung auf die Bankensysteme ausgeschlossen wird. Dies minimiert potenzielle Risiken für die Bankensysteme erheblich.

4. DORA's Fokus auf Netzwerke und IKT-Systeme

DORA wurde entwickelt, um systemische Risiken durch die Interkonnektivität von IKT-Systemen in der Finanzindustrie zu adressieren. Da Personalisierungszentren keine vernetzten IKT-Systeme darstellen, können sie keine technischen oder systemischen Risiken erzeugen, wie sie von DORA reguliert werden sollen. Eine Verzögerung im Kartenversand ist ein logistisches Problem und nicht mit den cyberoperativen Risiken vergleichbar, die DORA adressiert.

Zusammenfassung und Schlussfolgerungen

Das zentrale Anliegen von DORA besteht darin, die Widerstandsfähigkeit von Finanzdienstleistungen gegenüber Cybervorfällen und systemischen Risiken zu stärken. Personalisierungszentren sind weder Netzwerkinfrastrukturen noch essentielle Komponenten von Zahlungssystemen und fallen daher außerhalb des Anwendungsbereichs der Verordnung. SPA fordert deshalb, die Kartenpersonalisierung explizit von den DORA-Vorgaben auszunehmen.
Mit dieser Position unterstreicht die SPA die Notwendigkeit, regulatorische Vorgaben zielgerichtet zu gestalten, um deren Effektivität und Anwendbarkeit zu maximieren, ohne industrielle Prozesse unnötig zu regulieren.

DORA-Verordnung

Stärkung der digitalen Resilienz im europäischen Finanzsektor

Die EU hat mit der DORA-Verordnung (Digital Operational Resilience Act) einen regulatorischen Rahmen geschaffen, der die digitale Widerstandsfähigkeit des Finanzsektors gegenüber Cyberangriffen, IT-Ausfällen und weiteren Risiken erheblich verbessern soll. Diese Verordnung, die am 17. Januar 2023 in Kraft trat und ab dem 17. Januar 2025 verbindlich wird, zielt darauf ab, einheitliche Standards für die IT-Sicherheit von Finanzinstituten und deren Dienstleistern in allen Mitgliedstaaten zu etablieren. Im Gegensatz zu einer Richtlinie erfordert DORA keine separate Umsetzung in nationales Recht, sondern gilt unmittelbar und harmonisiert die bestehenden Regelungen.

Stärkung der digitalen Resilienz im europäischen Finanzsektor

Die EU hat mit der DORA-Verordnung (Digital Operational Resilience Act) einen regulatorischen Rahmen geschaffen, der die digitale Widerstandsfähigkeit des Finanzsektors gegenüber Cyberangriffen, IT-Ausfällen und weiteren Risiken erheblich verbessern soll. Diese Verordnung, die am 17. Januar 2023 in Kraft trat und ab dem 17. Januar 2025 verbindlich wird, zielt darauf ab, einheitliche Standards für die IT-Sicherheit von Finanzinstituten und deren Dienstleistern in allen Mitgliedstaaten zu etablieren. Im Gegensatz zu einer Richtlinie erfordert DORA keine separate Umsetzung in nationales Recht, sondern gilt unmittelbar und harmonisiert die bestehenden Regelungen.

Breites Anwendungsspektrum der DORA-Verordnung

Die Verordnung richtet sich an eine Vielzahl von Akteuren im Finanzsektor, darunter Banken, Zahlungsdienstleister, Versicherungen und Entwickler von Finanzsoftware. Auch Drittanbieter, wie Cloud-Dienstleister und Rechenzentren, die wesentliche Services für diese Unternehmen erbringen, fallen unter die Regelung. Dies schließt alle Anbieter ein, deren Dienste eine zentrale Rolle für den reibungslosen Betrieb von Finanzdienstleistungen spielen. Verstöße gegen die Verordnung können mit empfindlichen Strafen geahndet werden, was Unternehmen dazu zwingt, die Anforderungen konsequent umzusetzen.

Die DORA-Verordnung deckt fünf zentrale Bereiche ab: das Management von IKT-Risiken, den Umgang mit Vorfällen, die regelmäßige Überprüfung der Resilienz, das Management von Risiken durch Drittanbieter sowie den Austausch sicherheitsrelevanter Informationen.

Kernanforderungen der DORA-Verordnung

1. IKT-Risikomanagement
Unternehmen müssen stabile IT-Systeme entwickeln, diese regelmäßig überprüfen und potenzielle Risiken systematisch bewerten. Dazu gehören präventive Maßnahmen zur Erkennung ungewöhnlicher Aktivitäten sowie die Implementierung von Notfallplänen, um den Betrieb auch bei Störungen aufrechtzuerhalten.

2. Umgang mit IT-Sicherheitsvorfällen
DORA verlangt die Einrichtung eines strukturierten Prozesses zur Bewältigung und Meldung von IT-Vorfällen. Innerhalb von 24 Stunden nach einem Vorfall ist eine erste Meldung bei der zuständigen Behörde erforderlich, gefolgt von detaillierten Berichten über Ursachen und Maßnahmen zur Schadensbegrenzung.

3. Regelmäßige Resilienztests
Die Verordnung schreibt vor, dass Unternehmen ihre IT-Infrastruktur regelmäßig auf Schwachstellen prüfen. Dazu zählen sowohl grundlegende Tests als auch realitätsnahe Penetrationstests, bei denen auch externe Dienstleister einbezogen werden müssen.

4. Kontrolle von Risiken durch Drittanbieter
Da viele Finanzinstitute auf externe Dienstleister angewiesen sind, müssen diese ebenfalls strenge Standards einhalten. Unternehmen sind verpflichtet, ihre Partner regelmäßig zu prüfen und sicherzustellen, dass diese den hohen Anforderungen der Verordnung entsprechen.

5. Förderung des Informationsaustauschs
Die Verordnung ermutigt Finanzinstitute, sicherheitsrelevante Informationen auszutauschen. Anonymisierte Daten und bewährte Praktiken sollen helfen, Bedrohungen besser einzuschätzen und effektive Gegenmaßnahmen zu entwickeln.

Technologische Maßnahmen zur Umsetzung von DORA

Eine erfolgreiche Umsetzung der DORA-Verordnung setzt den Einsatz moderner Technologien voraus, die die digitale Resilienz von Unternehmen stärken. Dazu gehören:

- Datenrichtlinien (Data Governance): Klare Prozesse für den sicheren Umgang mit Daten minimieren Risiken wie unbefugten Zugriff oder Datenverlust.
- Zugangskontrollen: Systeme wie Multi-Faktor-Authentifizierung und rollenbasierte Berechtigungen sorgen dafür, dass nur autorisierte Personen Zugriff auf sensible Informationen haben.
- Verschlüsselung: Durch den Einsatz starker Verschlüsselungstechnologien werden Daten sowohl im Ruhezustand als auch während der Übertragung geschützt.
- Penetrationstests: Diese simulieren reale Angriffsszenarien, um Schwachstellen in IT-Systemen zu identifizieren und zu beheben.
- Audit-Trails und Log-Management: Diese ermöglichen eine lückenlose Nachverfolgung sicherheitsrelevanter Aktivitäten und die frühzeitige Erkennung von Bedrohungen.
- Disaster Recovery: Strategien und Maßnahmen zur schnellen Wiederherstellung von IT-Systemen minimieren Ausfallzeiten und ihre Auswirkungen auf den Geschäftsbetrieb.

Zusätzlich bieten virtuelle Datenräume auf Basis sicherer Technologien wie Sealed-Clouds eine sichere Plattform für die Speicherung und den Austausch von Informationen.

DORA als Wegweiser für eine sichere digitale Zukunft

Die DORA-Verordnung setzt einen neuen Standard für Cybersicherheit und Resilienz im europäischen Finanzsektor. Sie fordert von Unternehmen, ihre internen Prozesse zu optimieren und sich gegen externe Risiken abzusichern. Dies stellt zwar eine Herausforderung dar, bietet jedoch gleichzeitig die Chance, langfristig wettbewerbsfähig zu bleiben und das Vertrauen der Kunden zu stärken. Unternehmen, die frühzeitig auf die Anforderungen reagieren, können nicht nur Strafen vermeiden, sondern auch ihre Position im Markt festigen. Die DORA-Verordnung ist damit ein entscheidender Schritt auf dem Weg zu einer sicheren digitalen Zukunft in Europa.



NIS2 und DORA

Ein Vergleich der Regelwerke und häufige Missverständnisse

Die Europäische Union hat mit der NIS2-Richtlinie und der DORA-(Digital Operational Resilience Act)-Verordnung zwei bedeutende Regelwerke geschaffen, um die digitale Resilienz und Cybersicherheit zu stärken. Obwohl beide Maßnahmen ähnliche Ziele verfolgen, unterscheiden sie sich in ihrer Anwendung und den adressierten Anforderungen. Unternehmen, die unter eines oder beide dieser Regelwerke fallen, sollten die Unterschiede und Überschneidungen genau kennen, um rechtliche Verpflichtungen einzuhalten und Cyberrisiken effektiv zu minimieren.

Wichtige Unterschiede zwischen NIS2 und DORA

Art der Rechtsvorschrift

Die NIS2-Richtlinie und die DORA-Verordnung unterscheiden sich grundlegend in ihrem rechtlichen Ansatz. NIS2 ist eine Richtlinie, die von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden muss. Sie legt allgemeine Ziele fest, während die Länder die Details individuell ausarbeiten können. In Deutschland wird dies beispielsweise durch das NIS2-Umsetzungsgesetz geregelt. Im Gegensatz dazu ist DORA eine Verordnung und somit unmittelbar in allen EU-Mitgliedstaaten geltendes Recht. Sie erfordert keine nationale Um-

NIS2 und DORA



setzung und hat Vorrang vor nationalen Vorschriften. Dieser Ansatz gewährleistet eine einheitliche Anwendung und Verbindlichkeit ab dem festgelegten Stichtag.

Umsetzungstermine
Die Umsetzungstermine verdeutlichen die praktischen Unterschiede: Während die NIS2-Richtlinie aufgrund nationaler Gesetzgebungsverfahren voraussichtlich erst im März 2025 in Deutschland greift, gilt DORA bereits ab dem 17. Januar 2025. Unternehmen, die unter DORA fallen, müssen daher ihre Maßnahmen bis zu diesem festen Datum umsetzen.

Anwendungsbereiche
Die NIS2-Richtlinie zielt auf eine Vielzahl kritischer Sektoren ab, darunter Energie, Gesundheitswesen, Transport und digitale Infrastrukturen. Sie umfasst Unternehmen und Organisationen, die für die Gesellschaft und Wirtschaft essenziell sind.
DORA hingegen ist spezifischer und fokussiert sich ausschließlich auf den Finanzsektor. Hierzu zählen unter anderem Banken, Versicherungen, Wertpapierfirmen, Zahlungsdienstleister sowie Anbieter von Krypto-Diensten und kritische Drittanbieter wie Cloud-Dienstleister.

Sanktionen bei Verstößen
Die Nichteinhaltung von NIS2 und DORA kann erhebliche Sanktionen nach sich ziehen, die sich jedoch in ihrer Ausgestaltung unterscheiden. NIS2 sieht Bußgelder von bis zu 10 Millionen Euro oder 2 % des Jahresumsatzes vor, abhängig von der Schwere des Verstoßes und der Art des betroffenen Unternehmens.
DORA legt keine festen Bußgeldbeträge fest, erlaubt jedoch Strafen von bis zu 1 % des durchschnittlichen weltweiten Tagesumsatzes eines kritischen IKT-Drittanbieters. Darüber hinaus können tägliche Strafen verhängt werden, bis die Einhaltung sichergestellt ist. Beide Regelwerke sehen die persönliche Haftung von Führungskräften bei grober Fahrlässigkeit oder vorsätzlichen Verstößen vor.

Häufige Missverständnisse über NIS2 und DORA

NIS2 betrifft nur den IT-Sektor
Ein verbreiteter Irrtum ist, dass NIS2 ausschließlich auf IT-Unternehmen abzielt. Tatsächlich deckt die Richtlinie zahlreiche kritische Sektoren ab, darunter Energie, Transport und Gesundheitswesen. Unternehmen aus diesen Bereichen müssen die umfassenden Sicherheitsanforderungen von NIS2 erfüllen, unabhängig von ihrer direkten Verbindung zur IT-Branche.

DORA ersetzt NIS2
Einige Unternehmen glauben, dass die Erfüllung der DORA-Vorgaben ausreicht, wenn sie unter beide Regelwerke fallen. Das ist jedoch nicht korrekt. Während DORA spezifische Anforderungen an den Finanzsektor stellt, deckt NIS2 allgemeine Sicherheitsstandards ab, die auch Finanzinstitute betreffen können. Bereiche wie die sektorübergreifende Zusammenarbeit und der Informationsaustausch, die von NIS2 gefordert werden, bleiben relevant.

Wenn man nur unter NIS2 fällt, ist DORA irrelevant
Auch wenn DORA speziell auf Finanzinstitute ausgerichtet ist, bietet sie wertvolle Orientierungshilfen für Unternehmen, die nur unter NIS2 fallen. DORAs präzise Vorgaben zu Sicherheits- und Resilienzmaßnahmen können als Best-Practice-Ansatz dienen, um bestehende Sicherheitsmaßnahmen zu stärken und mögliche Lücken zu schließen.

DORA und NIS2 sind unabhängig voneinander
Die beiden Regelwerke ergänzen sich in bestimmten Bereichen, insbesondere wenn Unternehmen sowohl im Finanzsektor tätig sind als auch kritische Infrastrukturen betreiben. Eine integrierte Compliance-Strategie ist daher unerlässlich, um beiden Regelungen gerecht zu werden.

Fazit

Die NIS2-Richtlinie und die DORA-Verordnung verfolgen das gemeinsame Ziel, die digitale Resilienz und Cybersicherheit in der EU zu verbessern. Während NIS2 einen breiten Sektoransatz verfolgt, legt DORA den Schwerpunkt auf den Finanzsektor und dessen kritische Drittanbieter. Unternehmen müssen sicherstellen, dass sie die spezifischen und allgemeinen Anforderungen beider Regelwerke einhalten.

Die Entwicklung einer umfassenden Compliance-Strategie, die technische, organisatorische und rechtliche Aspekte berücksichtigt, ist entscheidend. Nur so können Unternehmen sicherstellen, dass sie den neuen Anforderungen gerecht werden und gleichzeitig ihre digitale Resilienz stärken. Mit klaren Prozessen, modernen Technologien und einem tiefen Verständnis der Regelwerke können Unternehmen sowohl rechtliche Risiken minimieren als auch ihre Sicherheitsstandards auf ein neues Niveau heben.

FTS Hennig

Mobilfunkversorgung als Basis für eine zukunftsfähige Ladeinfrastruktur

Mit der zunehmenden Verbreitung von Elektrofahrzeugen wächst die Bedeutung einer leistungsfähigen Ladeinfrastruktur. Doch Tiefgaragen, ein entscheidender Ort für Ladestationen, stellen aufgrund ihrer baulichen Gegebenheiten eine besondere Herausforderung dar. Dicke Betonwände und Stahlträger schränken die Mobilfunkverbindung erheblich ein, wodurch die Kommunikation zwischen Ladestationen und Backend-Systemen häufig gestört wird. FTS Hennig bietet innovative Mobilfunklösungen, um dieses Problem zu lösen und eine zuverlässige Infrastruktur für die Elektromobilität der Zukunft zu schaffen.

Moderne Ladetechnologien erfordern eine kontinuierliche Verbindung zu Backend-Systemen, um Daten wie Ladezustand, Verfügbarkeiten und Abrechnungsinformationen in Echtzeit zu übermitteln. Fehlt diese Mobilfunkverbindung, können erhebliche Einschränkungen auftreten. Die Nutzung der Ladeinfrastruktur wird unzuverlässig, Abrechnungsfehler häufen sich, und Wartungsprozesse verzögern sich. Ohne eine stabile Netzabdeckung ist eine zukunftsfähige Ladeinfrastruktur in Tiefgaragen kaum realisierbar.

FTS Hennig bietet hierfür eine effiziente Lösung in Form leistungsstarker Repeateranlagen. Diese Systeme bestehen aus Außenantennen, die das Mobilfunksignal von außen empfangen, Repeatern, die dieses Signal verstärken, und Innenantennen, die das verstärkte Signal in der gesamten Tiefgarage verteilen. Solche Anlagen gewährleisten, dass Mobilfunksignale aller großen Netzbetreiber – Telekom, Vodafone und Telefónica – zuverlässig verfügbar sind.

Besonders wichtig sind sogenannte 5-Band-Repeater, die alle relevanten Frequenzbereiche von 2G bis 5G abdecken. Für kleinere Tiefgaragen bietet FTS Hennig kosteneffiziente Lösungen wie Huaptec-Repeater an, während für größere Anlagen und komplexere Anforderungen die digitalen Multiboost-Repeater eine präzise und wartungsfreundliche Option darstellen. Diese modernen Geräte passen sich automatisch an die jeweiligen Gegebenheiten an und ermöglichen eine Fernwartung, um Betriebsunterbrechungen zu minimieren.





Mit über 25 Jahren Erfahrung ist FTS Hennig ein verlässlicher Partner bei der Planung und Umsetzung von Mobilfunklösungen. Das Unternehmen unterstützt Kunden in jeder Projektphase, von der individuellen Planung über die Bereitstellung aller notwendigen Komponenten bis hin zur fachkundigen Montagebegleitung. Diese umfassende Betreuung garantiert, dass jede Lösung optimal auf die spezifischen Anforderungen zugeschnitten ist.

Ob kleine Tiefgarage oder großflächiger Parkkomplex, FTS Hennig liefert die passende Mobilfunkinfrastruktur, um die Elektromobilität voranzutreiben. Betreiber können sich auf eine stabile Verbindung und reibungslose Funktionalität verlassen – ein entscheidender Schritt, um eine zukunftssichere Ladeinfrastruktur zu gewährleisten.

Phishing-Angriffsmethoden im Jahr 2025

Die Threat-Analysten von Barracuda Networks haben dieses Jahr mehrere fortschrittliche Phishing-Methoden beobachtet und daraus acht Trends für das Jahr 2025 abgeleitet.



Die Threat-Analysten von Barracuda Networks Inc., Cybersicherheitsunternehmen für umfassenden Schutz vor komplexen Bedrohungen, haben mehrere fortschrittliche Phishing-Angriffsmethoden beobachtet, die zunehmend von Angreifern genutzt werden, um Sicherheitsmaßnahmen zu umgehen und schädliche E-Mails überzeugender, plausibler und personalisierter zu gestalten. Mit Blick auf das Jahr 2025 geht das Threat-Analysten-Team von Barracuda unter anderem von Folgendem aus:

- Phishing-as-a-Service-Kits (PhaaS) werden im kommenden Jahr die Hälfte aller Angriffe mit dem Ziel, Anmeldedaten zu stehlen, ausmachen – im Vergleich zu 30 Prozent heute. Sie werden sich außerdem dahingehend weiterentwickeln, auch Multifaktor-Authentifizierungsdaten (MFA) zu stehlen.
- Gezielte Angriffe werden zunehmend personalisierte, emotionale Call-to-Actions enthalten, die auf einer Analyse der Social-Media- und Kommunikationshistorie des potenziellen Opfers basieren. In diesem Zusammenhang wird auch die Zahl der Erpressungs- bzw. Sextortion-Angriffsversuche zunehmen.
- Angreifer werden zunehmend Techniken zur Vermeidung von Erkennung nutzen, darunter ASCII-basierte QR-Codes, Blob-URLs und die Verlagerung der Phishing-Inhalte vom Textkörper der E-Mail in den Anhang.
- Angreifer werden zunehmend Online-Plattformen zur Erstellung und Veröffentlichung von Content missbräuchlich nutzen.

Konkret sieht das Team von Barracuda für das Jahr 2025 folgende Trends hinsichtlich Phishing-Angriffsmethoden:

Phishing-as-a-Service (PhaaS) und Diebstahl von Zugangsdaten

Von Barracuda erhobene Daten zeigen, dass im Jahr 2024 mehr als 85 Prozent der Phishing-Angriffe auf Kunden darauf abzielten, Anmeldedaten zu stehlen. Barracuda geht davon aus, dass dieser Anteil im Laufe des kommenden Jahres auf 90 Prozent oder mehr ansteigen wird.PhaaS ist für diese Art von Angriff besonders relevant. In den kommenden zwölf Monaten werden neue, fortschrittliche PhaaS-Kits verfügbar werden, die in der Lage sein werden, auch Multifaktor-Authentifizierungsdaten für Phishing-Angriffe auf Anmeldedaten zu stehlen.

Barracuda geht davon aus, das PhaaS-basierte Phishing-Angriffe derzeit rund 30 Prozent der identifizierten Angriffe mit dem Ziel, Anmeldedaten zu stehlen, ausmachen. Die Threat-Analysten erwarten, dass dieser Anteil im kommenden Jahr auf mehr als die Hälfte ansteigen wird.

Missbrauch legitimer URL-Schutzdienste

Das Barracuda-Team konnte außerdem feststellen, dass im Jahr 2024 Angreifer im Rahmen von Phishing-Angriffen zunehmend legitime URL-Schutzdienste missbräuchlich nutzten, um Phishing-Links zu verbergen, darunter auch Dienste führender Sicherheitsanbieter. Diese Taktik konnte das Team von Barracuda bereits im Juli 2024 beobachten und sie kommt nach wie vor zum Einsatz.

QR-Code- und Voicemail-basiertes Phishing

QR-Code- und Voicemail-basiertes Phishing machen derzeit etwa 20 Prozent aller erkannten Phishing-Angriffe aus. Im Oktober 2024 konnte Barracuda bereits eine zunehmende Nutzung von QR-Codes identifizieren, die mit ASCII/Unicode-Textblöcken erstellt wurden.

ASCII-basierte QR-Codes und die Nutzung speziell gestalteter Blob-URL-Links durch Angreifer dienen dazu, die frühzeitige Erkennung von Angriffen zu vermeiden. Das Threat-Analysten-Team von Barracuda geht davon aus, dass sich diese Taktik und andere Ansätze zur Vermeidung von Erkennung im Jahr 2025 und darüber hinaus noch weiterentwickeln und zunehmend zum Einsatz kommen werden.

HR-Identitätsdiebstahl

Barracuda geht ebenfalls davon aus, dass Phishing-Angriffe, bei denen sich die Angreifer als Mitarbeiter der Personalabteilung eines Unternehmens ausgeben, zunehmen werden. Solche Angriffe machen aktuell rund 10 Prozent der erkannten Angriffe aus. Im kommenden Jahr wird das Volumen dieser Angriffe jedoch weiter zunehmen, insbesondere zu Zeiten, an denen wichtige Steuerfristen anfallen.

Missbräuchliche Nutzung von Online-Plattformen zur Erstellung und Veröffentlichung von Content

Rund 10 Prozent der im Jahr 2024 von Barracuda identifizierten Angriffe wurden auf CCP- (Content Creation Platform) oder DDP-Webseiten (Digital Document Publishing) gehostet. Barracuda konnte diese Taktik bereits im September 2024 beobachten. Die Analysten gehen davon aus, dass sich auch dieser Trend fortsetzen wird, da Angreifer auf eine immer größere Auswahl entsprechender Webseiten zugreifen können, um Phishing-Angriffe zu hosten.

Schädliche Anhänge

Die Nutzung schädlicher Anhänge wird ebenfalls weiter zunehmen. Das Threat-Analysten-Team von Barracuda konnte bereits zahlreiche Phishing-E-Mails identifizieren, bei denen die Phishing-Inhalte in einem HTML- oder PDF-Anhang zu finden waren, während der Textkörper der E-Mail leer war oder nur sehr wenig Text enthielt. Dieser Ansatz ist ein Versuch, Analysen des E-Mail-Textkörpers, die auf Machine Learning basieren, zu umgehen und es ist zu erwarten, dass sich dieser Trend auch im kommenden Jahr fortsetzen wird.

Personalisierte Erpressungsversuche

Im Jahr 2024 konnte Barracuda Millionen von Erpressungsversuchen bei Kunden beobachten, die sich im November 2024 dahingehend weiterentwickelt hatten, potenzielle Opfer mithilfe von Google Street View-Aufnahmen und Fotos ihres Hauses oder ihrer Straße einzuschüchtern. Diese Taktik wird auch im Jahr 2025 weiterhin zum Einsatz kommen. Das Team von Barracuda erwartet, dass die Erpressungsversuche sogar noch weiter personalisiert werden und höhere Erpressungsgelder verlangen werden.

KI überall

Angreifer nutzen zunehmend KI sowie legitime Webseiten und Weiterleitungen, um ihre Phishing-Angriffe so echt wie möglich aussehen zu lassen. Mithilfe von KI können Angreifer beispielsweise noch überzeugendere Phishing-E-Mails erstellen, die wie E-Mails legitimer Absender wirken, unter anderem aufgrund von personalisierten Inhalten, präziserer Grammatik und sogar menschenähnlichen, emotionalen Calls-to-Actions, die auf einer Analyse der Social-Media- und Kommunikationshistorie des Empfängers basieren.

Schutz vor fortschrittlichen Angriffsmethoden

Phishing ist nach wie vor eine signifikante Cyberbedrohung, da sich diese Angriffsmethode relativ kostengünstig und mit nur geringen Vorkenntnissen schnell und einfach umsetzen lässt und potenziell hohe Erfolgschancen bietet.
Phishing-Methoden haben sich im Jahr 2024 rasant weiterentwickelt und das Threat-Analysten-Team von Barracuda geht davon aus, dass Cyberangreifer ihre Methoden auch im Jahr 2025 weiter verfeinern werden, um traditionelle Sicherheitsmaßnahmen zu umgehen.

Wie die verschiedenen Beobachtungen von Barracuda aus dem Jahr 2024 zeigen, werden Phishing-Angriffe vielfältiger, opportunistischer und ausgefeilter. Um dieser sich kontinuierlich weiterentwickelnden Bedrohung stets einen Schritt voraus zu sein, empfehlen sich agile, innovative und mehrstufige Sicherheitsmaßnahmen und das Etablieren einer starken Sicherheitskultur im Unternehmen.

TÜV Rheinland

IT-Sicherheitslage in Deutschland verschärft sich weiter

Angespannte Bedrohungslage: Laut einer Civey-Umfrage unter Cybersecurity-Fachleuten im Auftrag von TÜV Rheinland hat die Gefahr von Cyber-Angriffen in den vergangenen zwölf Monaten weiter zugenommen.

Die IT-Sicherheitslage in Deutschland verschärft sich weiter. Das zeigt eine Umfrage unter Fachleuten für Cybersecurity, die TÜV Rheinland anlässlich des internationalen Tages für Computersicherheit am 30. November in Auftrag gegeben hat. In der von Civey im Oktober 2024 durchgeführten Online-Umfrage geben neun von zehn Befragten (90,2%) an, dass die Gefahr von Cyber-Angriffen für Unternehmen und Institutionen in Deutschland in den vergangenen zwölf Monaten zugenommen hat. Befragt wurden deutschlandweit rund 1.000 Personen, die im Bereich Cybersicherheit tätig sind. „Unsere Befragung zeigt: Unternehmen sind mehr denn je mit Cyberangriffen konfrontiert – und müssen entsprechend in ihre Cybersecurity investieren", sagt Daniel Hanke, Experte für Cybersecurity bei TÜV Rheinland.

Das bestätigt der Bericht zur Lage der IT-Sicherheit in Deutschland, den das Bundesamt für Sicherheit in der Information- stechnik (BSI) Mitte November veröffentlicht hat: Das BSI schätzt die Situation als „angespannt" ein, auch wenn es eine Verbesserung in der Resilienz gegenüber Cyberangriffen sieht. „Anders gesagt: Es stellt sich längst nicht mehr die Frage, ob ein Unternehmen Opfer eines Cyberangriffs wird, sondern wann und wie sich mögliche Schäden durch Cyberangriffe durch vorbeugende Maßnahmen verringern lassen", so Cybersecurity-Experte Hanke.

Veraltete Infrastruktur und mangelnde Vorbereitung als Herausforderungen

TÜV Rheinland ließ ebenfalls danach fragen, welches die größten Herausforderungen für die Gewährleistung von Cybersicherheit in Unternehmen und Institutionen sind. Dabei sticht ein Aspekt hervor: Die ausgemachten Herausforderungen lassen sich nicht auf wenige, einzelne reduzieren.



Die „Steigende Zahl von Angriffen" (39,2%), „Veraltete IT-Infrastruktur" (38,9%) und „Mangelnde Vorbereitung gegen Cyberangriffe" (36,3%) werden von den Befragten am häufigsten genannt. Ähnlich herausfordernd werden die „Wachsende Komplexität von IT-Systemen" (35,3%), der „Fachkräftemangel im IT-Bereich" (34,7%) und „KI-unterstützte Hakkerangriffe" (32,3%) wahrgenommen. Mangelnde Budgets sind hingegen nur für jeden Fünften (21,9%) eine Herausforderung.

„Einerseits haben die meisten Verantwortlichen offenbar erkannt, dass man an Cybersecurity nicht sparen sollte – andererseits ist es besorgniserregend, dass jeder Dritte die Unternehmen schlecht vorbereitet auf Cyberangriffe sieht", kommentiert TÜV Rheinland-Experte Daniel Hanke.

Handlungsdruck durch neue Regulierungen

Zur Bedrohungslage kommen Veränderungen auf Ebene der Reglierung hinzu. So führt die „Network and Information Security Directive 2" (NIS-2-Richtlinie) der Europäischen Union strengere Vorschriften zur Cybersicherheit für mehr Sektoren und Unternehmen ein. Ab März 2025 müssen damit Unternehmen ab 50 Mitarbeitenden und mit mehr als 10 Millionen Euro Umsatz in 18 Sektoren verstärkte Cybersecurity-Maßnahmen umsetzen.

Das Ziel: der Schutz von essentiellen, wichtigen Sektoren und (kritischen) Infrastrukturen sowie eine höhere Widerstandsfähigkeit gegenüber Cyberangriffen. Ebenfalls auf der Regulierungsebene setzt der Cyber Resilience Act an. Hiermit führt die Europäische Union verbindliche Cybersicherheitsanforderungen für „Produkte mit digitalen Elementen" ein. Das Ziel auch hier: die Widerstandsfähigkeit gegen Cyberangriffe zu erhöhen und verlässliche digitale Dienste zu gewährleisten.

„Insgesamt führen die steigenden Risiken durch Cyberangriffe verbunden mit den neuen regulatorischen Anforderungen dazu, dass der Handlungsdruck in den Unternehmen steigt", sagt Daniel Hanke. „Die weltweit mehr als 250 Cybersecurity-Fachleute von TÜV Rheinland unterstützen dabei umfassend sowohl mit klassischen Cybersecurity-Dienstleistungen wie dem Pentesting wie auch bei der regelkonformen Umsetzung der Regulierungen."

[www.tuv.com/cybersecurity]

Skepsis gegenüber KI im Unternehmen

Datenschutz führt die Liste der Bedenken an

IT-Verantwortliche, Hersteller und die Politik müssen beim Thema Künstliche Intelligenz viele Vorbehalte aus dem Weg räumen

Künstliche Intelligenz (KI) ist in Unternehmen immer mehr auf dem Vormarsch, aber die Angestellten haben Bedenken beim Einsatz. Das belegt die repräsentative Studie „Cybersicherheit in Zahlen" von der G DATA CyberDefense AG, Statista und brand eins. Die größten Bauchschmerzen bestehen beim Thema Datenschutz, aber auch die mögliche Manipulation und die mangelnde Kontrolle der KI-Systeme sorgen bei je einem Drittel der deutschen Arbeitnehmenden für Skepsis. Die Ergebnisse zeigen, dass mehr Regulierung, Kontrollen und Schulungen für Mitarbeitende nötig sind.



Der Einsatz von Künstlicher Intelligenz hat für Unternehmen viele Vorteile, zum Beispiel die Steigerung der Effizienz von Produktionsprozessen. Die Ergebnisse der Studie „Cybersicherheit in Zahlen" belegen, dass KI-Tools bei deutschen Arbeitnehmerinnen und Arbeitnehmern noch nicht richtig angekommen sind. Es fehlen das Verständnis und die Erfahrung im Umgang, aber auch ein Regelwerk für die Nutzung ist in Firmen oft nicht vorhanden. Der letzte Aspekt betrifft nicht nur viele Unternehmen, auch auf der Gesetzesebene ist bisher keine Regulatorik erfolgt. Dabei würde dies bei IT-Verantwortlichen und der Belegschaft gleichermaßen für mehr Sicherheit sorgen.

Mitarbeitende sehen die Nutzung von KI kritisch: Insbesondere die Themen Datenschutz (36,6 Prozent), Manipulation von KI-Systemen (35,8 Prozent), mangelnde Kontrolle der KI-Systeme (33,7 Prozent) und Haftungsfragen bei Schäden oder Fehlern (33 Prozent) wecken Bedenken hinsichtlich der Technologie.

„Das Potential von Künstlicher Intelligenz lässt sich in Unternehmen nur erfolgreich ausschöpfen, wenn die Tools auch von den Mitarbeitenden akzeptiert und Bedenken abgebaut werden. Nötig sind klare Richtlinien zur Nutzung und eine Kontrolle, um Missbrauch vorzubeugen. Entscheidend ist aber insbesondere, die Belegschaft bei der Einführung von KI mitzunehmen und umfassend zu schulen", erklärt Andreas Lüning, Mitgründer und Vorstand der G DATA CyberDefense AG.

Innovationen erfordern Akzeptanz

Deutlich werden auch kulturelle Hürden. So zählen Akzeptanzprobleme bei Mitarbeitenden (29 Prozent) und moralische Bedenken (24,5 Prozent) zu den kritischen Punkten. Gleichzeitig nehmen die Befragten die Abhängigkeit von externen Anbietern (26,2 Prozent) als Risiko wahr. Neben einer Regulierung auf der technischen und juristischen Ebene, sind umfassende Schulungsangebote ein Schlüssel für mehr Akzeptanz und Erfolg beim Einsatz von KI in Unternehmen.

Cybersicherheit in Zahlen zum Download

„Cybersicherheit in Zahlen" erschien bereits zum vierten Mal und zeichnet sich durch eine hohe Informationsdichte und besondere methodische Tiefe aus: Die Marktforscher von Statista haben Zahlen, Daten und Fakten aus mehr als 300 Statistiken zu einem einzigartigen Gesamtwerk zusammengeführt. Mehr als 5.000 Arbeitnehmerinnen und Arbeitnehmer in Deutschland wurden im Rahmen einer repräsentativen Online-Studie zur Cybersicherheit im beruflichen und privaten Kontext befragt. Die Fachleute von Statista haben die Befragung eng begleitet und können dank einer Stichprobengröße, die weit über dem branchenüblichen Standard liegt, belastbare und valide Marktforschungsergebnisse im Magazin „Cybersicherheit in Zahlen" präsentieren. [**www.tinyurl.com/3w3x3xth**]



Zweiter Jahrestag von ChatGPT: Generationssprung der KI

Von Marco Eggerling, Global CISO bei Check Point Software Technologies

Künstliche Intelligenz (KI) ist über Jahrzehnte ein integraler Teil der Welt geworden und hat Innovationen in allen Bereichen vorangetrieben, von der Robotik hin zur prädiktiven Analytik. Die Einführung der generativen KI (GenAI), angeführt von der Einführung von ChatGPT vor zwei Jahren, markierte dabei einen revolutionären Wendepunkt. ChatGPT ist in der Lage, auf einer Ebene zu kommunizieren, zu erstellen und zu verstehen, die fast menschlich wirkt. Diese transformative Fähigkeit brachte KI aus dem technischen Bereich in den Alltag und demokratisierte den Zugang zu fortschrittlicher Technologie in noch nie dagewesener Weise.

ChatGPT wurde Ende 2022 gestartet und erreichte innerhalb von nur fünf Tagen eine Million Nutzer. Im Jahr 2024 ist die aktive Nutzerbasis von ChatGPT auf beeindruckende 200 Millionen angestiegen und hat sich damit als eine der am schnellsten wachsenden Anwendungen in der Geschichte etabliert.

Mit seiner Fähigkeit, kohärente, kontextbezogene Antworten in Echtzeit zu generieren, hat ChatGPT die KI zu einem allgemein bekannten Begriff gemacht. ChatGPT und andere ähnliche Tools sind branchenübergreifend und unterstützen Fachleute und Einzelpersonen gleichermaßen im Berufs- und Privatleben; im Zuge ihrer Entwicklung warfen sie jedoch auch kritische Fragen zu ihrem zweischneidigen Potenzial auf.

Der Aufstieg von ChatGPT: Branchenübergreifende Innovation fördern

Von der Kundenbetreuung bis zur Erstellung von Inhalten ist ChatGPT schnell zu einem allgegenwärtigen Werkzeug von Einzelpersonen und Unternehmen gleichermaßen geworden. Obwohl große Sprachmodelle (Large Language Models, LLMs) noch lange nicht an die menschliche Genialität heranreichen, hat ihre Fähigkeit, auf Anfrage passable Lösungen zu liefern, Fachleuten ermöglicht, sich auf kreative, analytische und strategische Aufgaben zu konzentrieren. Die Unmittelbarkeit und der Umfang, den die generative KI bietet, haben einen Paradigmenwechsel aus-

gelöst, bei dem die KI nicht nur ein Trend, sondern eine grundlegende Realität ist.

GenAI-Tools haben auch branchenübergreifende Unterstützung durch schnelle Problemlösungen ermöglicht, indem sie technische Fragen beantworten und Projektzeitpläne beschleunigen und so wochenlange Aufgaben auf Stunden komprimieren.
Die Fähigkeiten von GenAI-Tools wie ChatGPT erstrecken sich auch auf das Reverse Engineering, indem sie auf innovative Weise Sprachmodelle anwenden, um Funktionen zu entschlüsseln und komplexen Code zu verstehen.

Positiv zu vermerken ist zudem, dass sich generative KI zu einem unverzichtbaren Instrument der Verbesserung von Sicherheitsmaßnahmen entwickelt hat:

1. Beschleunigung der Arbeitsabläufe: Cyber-Sicherheitsexperten verwenden GenAI-Tools wie ChatGPT, um Fehler zu beheben, komplexe Probleme zu entschlüsseln und riesige Datensätze in verwertbare Erkenntnisse zu verwandeln – Aufgaben, die früher Wochen oder Tage dauerten.
2. Erkennung von Bedrohungen: Die Fähigkeit von GenAI, riesige Datenmengen schnell und aufschlussreich zu analysieren, ermöglicht es Unternehmen, Bedrohungen zu erkennen, die andernfalls vielleicht unbemerkt geblieben wären.
3. Reaktion auf Vorfälle: Generative KI wird erforscht, um bei der Zusammenfassung von Angriffsmustern zu helfen, die Reaktionszeiten zu verkürzen und die Abwehr zu stärken.

Der Aufstieg der generativen KI hat jedoch auch erhebliche Risiken mit sich gebracht. Ohne angemessene Sicherheitsvorkehrungen könnten sensible Unternehmensdaten, die in Tools wie ChatGPT eingegeben werden, versehentlich nach außen dringen.
Ein einziger falscher Umgang mit Daten könnte den Weg für verheerende Folgen ebnen, wenn diese Daten bei einem zukünftigen Verstoß offengelegt werden.

In gewisser Weise hat diese transformative Technologie die Tür für einen alarmierenden Missbrauch durch Cyber-Kriminelle geöffnet:

- **Entwicklung von schädlichem Code:** ChatGPT und ähnliche Tools ermöglichen es selbst unerfahrenen Angreifern, Malware zu erstellen und zu debuggen, wodurch die Einstiegshürde für Cyber-Kriminalität deutlich gesenkt wird.
- **Ausgefeite Phishing-E-Mails:** Generative KI ermöglicht es Hackern, realistische, kontextuell überzeugende E-Mails zu verfassen, die den Empfänger mit weitaus größerer Wahrscheinlichkeit täuschen als herkömmliche Phishing-Versuche, die in der Vergangenheit aufgrund mangelnder Eloquenz, Sprach- und Situationskenntnis von erfahrenen Augen als Betrug erkannt werden konnten.
- **Fälschungen:** GenAI-erstellte Videos und Audioclips, die oft nicht von der Realität zu unterscheiden sind, werden für Betrug, Desinformation und Erpressung verwendet, wodurch die Social-Engineering-Bedrohung durch DeepFakes eskaliert.

Diese Missbrauchsfälle machen eine ernüchternde Tatsache deutlich: Generative KI kann nicht nur die Verteidiger stärken, sondern auch die Fähigkeiten der Hacker ausbauen.

Sicher bleiben in einer GenAI-gesteuerten Welt

Die schnelle Einführung von GenAI erfordert einen präventiven Ansatz zur Risikominderung. Empfehlenswert sind die folgenden Schritte:

1. Mitarbeiter schulen und ausbilden: Die Mitarbeiter mit Wissen über GenAI-spezifische Bedrohungen und Risiken, zum Beispiele über realistische Phishing-E-Mails, Deepfakes und Halluzinationen, ausstatten, damit sie potenzielle Angriffe erkennen und melden können.
2. Datensicherheitsmaßnahmen implementieren: Tools verwenden, die verhindern, dass sensible Daten versehentlich mit KI-Plattformen geteilt werden, um so das Risiko von Lecks oder Missbrauch zu verringern.
3. Überwachung und Regulierung der KI-Nutzung: Klare Richtlinien für die ethische und sichere Nutzung generativer KI im Unternehmen festlegen und die Verantwortlichkeit für Nutzer und Entwickler gewährleisten.
4. Automatisierte Datenkontrollen: Sensible Informationen schützen, indem automatisierte Lösungenimplementiert werden, die den Datenaustausch mit KI-Systemen von Drittanbietern überwachen und einschränken.
5. Einführung von KI-gestützten Verteidigungsmaßnahmen: KI-Tools nutzen, um Angreifern einen Schritt voraus zu sein, und die eigene Fähigkeit zu verbessern, Bedrohungen zu erkennen und darauf zu reagieren.

Eine Vision: Verantwortungsvolle KI in der Cyber-Sicherheit

Es besteht kein Zweifel daran, dass generative KI-Programme wie ChatGPT eine immer wichtigere Rolle bei der Gestaltung der Cyber-Sicherheitslandschaft spielen werden. Die Herausforderung besteht darin, ihr Potenzial zum Guten zu nutzen und gleichzeitig die Risiken des Missbrauchs zu minimieren.

Der Vorteil des Einsatzes von generativer KI liegt auf der Hand: Man kann einen Algorithmus riesige Datenmengen untersuchen lassen, die zuvor nur schwer sinnvoll zu verarbeiten gewesen wären. Dennoch ist GenAI kein automatischer Ersatz für einen Menschen oder einen hochmodernen Algorithmus.

Um sicherzustellen, dass generative KI einen positiven Beitrag zur Cyber-Sicherheit leistet, müssen Unternehmen die Verantwortung für ihre Nutzung übernehmen, ob durch die Regulierung sensibler Anwendungen, die Förderung einer Kultur der KI-Kompetenz oder den Einsatz fortschrittlicher Überwachungstools – jede Branche muss sich mit der Technologie entwickeln.

Da wir den zweiten Jahrestag von ChatGPT feiern, dient dieser Meilenstein sowohl als Erinnerung als auch als Aufruf zum Handeln.
Das Potential von GenAI ist immens, aber auch die Verantwortung, die damit einhergeht. Indem wir wachsam und vorausschauend bleiben, können wir sicherstellen, dass solche Tools weiterhin Innovationen vorantreiben und wir gleichzeitig vor ihrem Missbrauch geschützt werden.

Deutschland und die NIS2-Richtlinie

Versäumte Chancen und dringende Notwendigkeiten

Die Einleitung eines Vertragsverletzungsverfahrens durch die Europäische Union gegen Deutschland markiert einen entscheidenden Wendepunkt in der Debatte über Cybersicherheit und die Umsetzung der NIS2-Richtlinie. Dieses Verfahren, ausgelöst durch die Verzögerung bei der Umsetzung der Richtlinie über Netzwerk- und Informationssicherheit sowie der Vorschriften zur Resilienz kritischer Infrastrukturen, verdeutlicht die gravierenden Defizite im deutschen Gesetzgebungsprozess.

Ein vorhersehbares Dilemma

Wie Dirk Arendt, Director Government & Public Sector DACH bei Trend Micro, in seiner Stellungnahme betont, kommt dieses Verfahren nicht überraschend. Angesichts der politischen Blockaden der letzten Jahre wird eine Umsetzung der NIS2-Richtlinie erst frühestens im Herbst 2025 erwartet. Diese Verzögerung sendet jedoch verheerende Signale – sowohl nach innen als auch nach außen.

Die deutsche Wirtschaft, die sich aktuell in einer tiefen Krise befindet, steht vor der Aufgabe, ihre Widerstandsfähigkeit gegenüber zunehmenden Cyberbedrohungen zu stärken. Die Bedeutung dieser Bedrohungen wird durch die jüngsten Zahlen der Bitkom-Studie zum Wirtschaftsschutz untermauert: 2024 stieg die Anzahl digitaler Angriffe weiter an, wobei 74 % der Unternehmen von Datendiebstahl betroffen waren. Der Gesamtschaden durch Cyberkriminalität belief sich auf 178,6 Milliarden Euro. Diese Zahlen verdeutlichen, dass Cybersicherheit nicht nur eine technische Herausforderung, sondern eine wirtschaftliche und gesellschaftliche Notwendigkeit darstellt.

Die Rolle der NIS2-Richtlinie

Die NIS2-Richtlinie zielt darauf ab, das Niveau der Cybersicherheit in der gesamten EU zu harmonisieren und zu erhöhen. Mit ihrer geplanten Ausweitung auf rund 30.000 Unternehmen in Deutschland wird die Richtlinie umfassende Auswirkungen auf Wirtschaft und Gesellschaft haben. Sie stellt klare Anforderungen an die Cybersicherheitsstrategie und Resilienz von Unternehmen und öffentlichen Einrichtungen.

Ihre Bedeutung geht jedoch über wirtschaftliche Aspekte hinaus: Cyberangriffe auf kritische Infrastrukturen können massive Störungen verursachen und das Vertrauen in den Staat und seine Infrastruktur nachhaltig schädigen.

Hybride Bedrohungen und die Zeitenwende

Deutschland und Europa befinden sich zunehmend im Fokus hybrider Bedrohungen. Diese umfassen nicht nur Cyberangriffe, sondern auch Desinformationskampagnen und andere Instrumente, die auf die Destabilisierung staatlicher und wirtschaftlicher Systeme abzielen. Eine effektive Cybersicherheitsarchitektur ist daher nicht länger optional, sondern eine strategische Notwendigkeit.

Die EU hat diesen Handlungsbedarf erkannt und reguliert verstärkt, um das Schutzniveau innerhalb der Union zu harmonisieren. Diese Bemühungen sind zu begrüßen, insbesondere da sie ein engeres Zusammenstehen im Cyberraum erfordern – ein zentraler Baustein der Zeitenwende.

Ein Appell an die Politik

Arendt weist darauf hin, dass es vermutlich nicht möglich sein wird, die erforderlichen Gesetze in der laufenden Legislaturperiode zu verabschieden. Der Ball liegt somit bei der nächsten Bundesregierung. Diese muss Cybersicherheit endlich die Priorität einräumen, die sie verdient. Dies erfordert:

1. Ausreichende Ressourcen: Die Bereitstellung finanzieller und personeller Mittel zur Stärkung der Cybersicherheitsstrukturen.
2. Effiziente Sicherheitsarchitekturen: Eine klare Definition von Zuständigkeiten und eine bessere Koordination zwischen staatlichen Institutionen und der Wirtschaft.
3. Einbindung von Experten: Die Berücksichtigung von Vorschlägen und Einwänden aus Wirtschaft und Verbänden, um praxisnahe Lösungen zu entwickeln.

Der Weg zur „Cybernation" in Europa

Die Herausforderungen der digitalen Welt erfordern mutige und entschlossene Schritte. Deutschland hat die Chance, Vorreiter in der Cybersicherheit zu werden und damit nicht nur die eigene Wirtschaft zu schützen, sondern auch einen entscheidenden Beitrag zur Sicherheit der gesamten EU zu leisten.

Die Transformation zu einer „Cybernation" in einem starken Europa ist keine Option, sondern eine Notwendigkeit. Es liegt an der Politik, diese Vision konsequent zu verfolgen und den rechtlichen Rahmen für eine sichere digitale Zukunft zu schaffen.

[ML]

Positive Bilanz und Prognose 2025

Der IT-Dienstleister und Anbieter von High-End Data Center Solutions, synaforce, blickt auf ein herausforderndes Jahr 2024 zurück, in dem die Cybersicherheitslandschaft von tiefgreifenden Entwicklungen geprägt war. Steigende Professionalisierung der Cyberkriminalität, neue regulatorische Anforderungen wie die NIS2-Richt- linie sowie technologische Fortschritte im Bereich Künstliche Intelligenz stellten Unternehmen und Organisationen vor immense Herausforderungen. synaforce hat sich in diesem dynamischen Umfeld als verlässlicher Partner positioniert und Unternehmen unterstützt, ihre IT-Sicherheit zu stärken und sich auf kommende Gefahren vorzubereiten

Herausforderungen im Jahr 2024

Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erreichte die Zahl neuer Schadprogrammvarianten im Jahr 2024 mit täglich etwa 309.000 einen neuen Höchststand, was einem Anstieg von 26 % gegenüber dem Vorjahr entspricht. Cyberkriminelle nutzten verstärkt Zero-Day-Schwachstellen und boten modularisierte Angriffswerkzeuge wie Malware-as-a-Service an. Besonders im Fokus standen Angriffe auf Cloud-Systeme, kritische Infrastrukturen (KRITIS) und mobile Endgeräte. Parallel dazu haben Fortschritte im Bereich generativer KI die Bedrohungslage verschärft. Angreifer nutzten KI, um täuschend echte Phishing-Nachrichten zu erstellen, Schadprogramme zu programmieren oder Passwörter zu knacken. Dies erfordert von Unternehmen eine kontinuierliche Anpassung ihrer Sicherheitsstrategien. Auch regulatorisch gab es bedeu- tende Entwicklungen: Die NIS2-Richtlinie, die höhere Cybersicherheitsstandards in kritischen Sektoren vorsieht, sollte bis Oktober 2024 in deutsches Recht umgesetzt werden. Doch Verzögerungen im Gesetzgebungsprozess haben zu Unsicherheiten geführt, die Unternehmen vor zusätzliche Herausforderungen stellen.

synaforce: Strategische Maßnahmen

Trotz dieser komplexen Ausgangslage konnte synaforce seine Position als führender Anbieter moderner Cybersicherheitslösungen weiter festigen. Ein bedeutender Meilenstein war die erfolgreiche C5-Zertifizierung durch das BSI im März 2024. Diese bestätigt, dass die Cloud-Dienste des Unternehmens höchsten Sicherheitsstandards entsprechen, insbesondere für KRITIS-Kunden. Darüber hinaus bereitete sich synaforce proaktiv auf die NIS2-Richtlinie vor. Die bestehenden Zertifizierungen, darunter ISO/IEC 27001 und EN 50600, wurden durch die C5-Zertifizierung ergänzt. So bietet das Unternehmen seinen Kunden eine solide Basis, um die verschärften EU-weiten Standards zu erfüllen. Ein weiterer Höhepunkt des Jahres war die Partnerschaft mit TEHTRIS, die zur Einführung der TEHTRIS XDR AI PLATFORM führte. Diese KI-gestützte Sicherheitslösung überwacht Endpunkte, Netzwerke und Cloud-Dienste in Echtzeit und bietet Unternehmen eine zentrale Steuerung über ein intuitives Dashboard. Die Plattform ermöglicht es Managed Service Providern, proaktive Maßnahmen wie Managed Detection and Response (MDR) anzubieten, ohne selbst in teure Infrastrukturen investieren zu müssen.

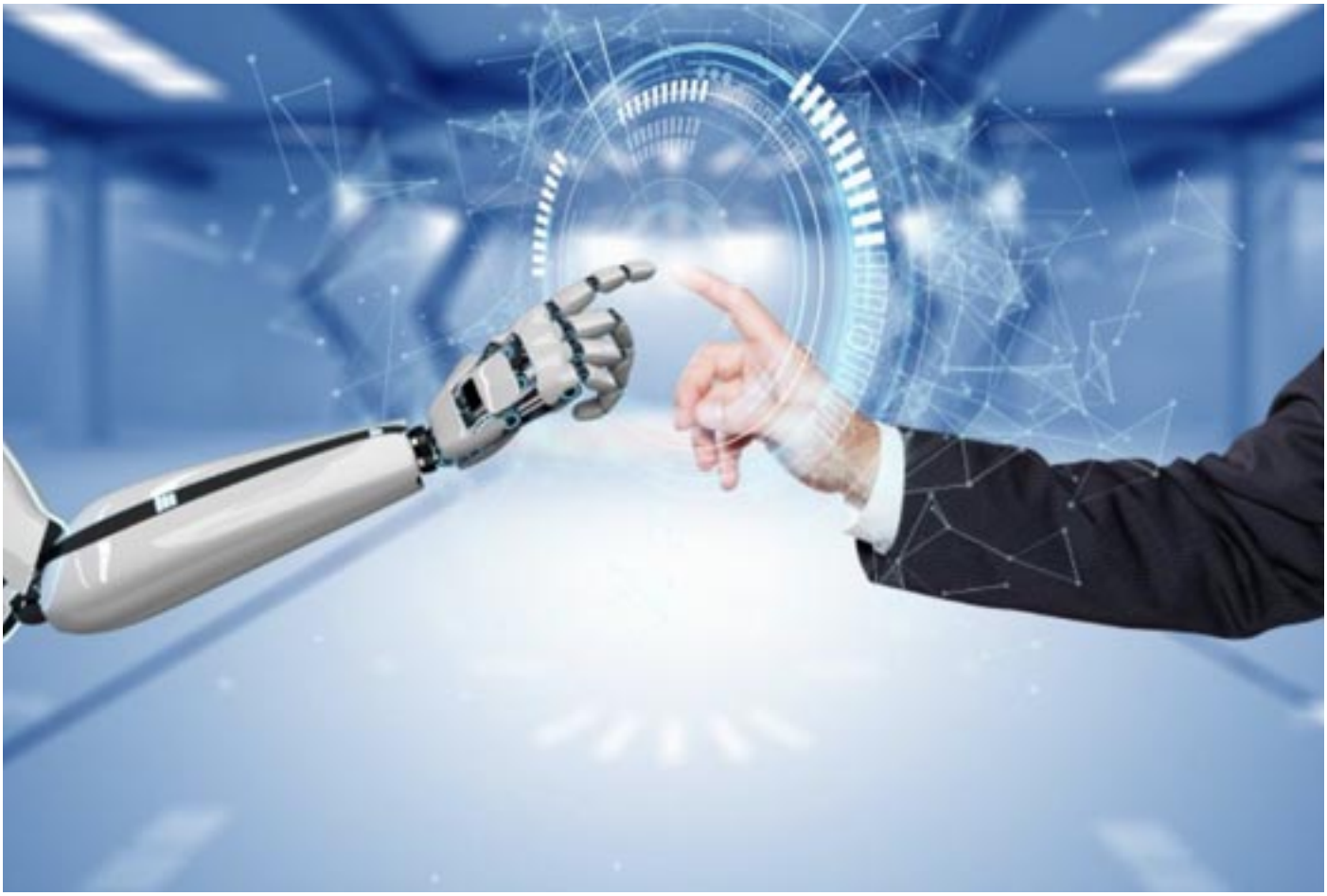
Ausblick auf 2025

Das kommende Jahr wird die Cybersicherheitslandschaft weiter prägen. Cyberkriminelle werden voraussichtlich zunehmend auf Deepfake-Technologien setzen, um Verifizierungsmechanismen wie Stimmerkennungssysteme zu umgehen. Besonders der Finanzsektor wird neue Abwehrstrategien entwickeln müssen, um diesen fortschrittlichen Täuschungsmethoden entgegenzuwirken. Zusätzlich gewinnen Advanced Persistent Threats (APTs) wieder an Bedeutung. Diese langfristigen, gezielten Angriffe ermöglichen es Cyberkriminellen, über längere Zeiträume auf sensible Daten zuzugreifen. KRITIS-Unternehmen bleiben dabei ein bevorzugtes Ziel, da ihre Systeme für die Gesellschaft essenziell sind. Zu den technologischen Risiken gesellt sich die anhaltende Unsicherheit über die Umsetzung der NIS2-Richtlinie in Deutschland. Obwohl die Frist zur Überführung der Richtlinie in nationales Recht bereits verstrichen ist, bleibt die endgültige Gesetzeslage unklar. Unternehmen sollten jedoch nicht auf klare Regelungen warten, sondern proaktiv Maßnahmen ergreifen, um ihre Systeme sicher zu halten.

„Die Bedrohungslage war 2024 bereits erheblich, und wir erwarten, dass sie sich 2025 weiter zuspitzt. Unsere kollektive Resilienz wird entscheidend sein, um die immer komplexeren Gefahren zu bewältigen", erklärt Andreas Braidt, CEO von synaforce. Er betont, dass die Umsetzung der NIS2-Richtlinie eine Schlüsselrolle spielt und synaforce Unternehmen mit Beratung, Planung und Implementierung gezielter Maßnahmen unterstützt, um Cyberrisiken effektiv zu minimieren.

Fazit

Mit einem Jahr voller Herausforderungen und Errungenschaften im Rücken geht synaforce gestärkt in das Jahr 2025. Durch innovative Partnerschaften, erstklassige Zertifizierungen und die Bereitstellung fortschrittlicher Technologien hat das Unternehmen bewiesen, dass es den steigenden Anforderungen der Cybersicherheitslandschaft gewachsen ist. Die kontinuierliche Weiterentwicklung bleibt jedoch essenziell, um Unternehmen und Organisationen auch in Zukunft die besten Lösungen gegen die wachsenden Bedrohungen der digitalen Welt zu bieten.



Künstliche Intelligenz in der Arbeitswelt

Chancen und Herausforderungen

Künstliche Intelligenz (KI) hat sich als treibende Kraft der digitalen Transformation etabliert und verändert die Arbeitswelt in einem rasanten Tempo. Laut dem Statistischen Bundesamt setzen derzeit lediglich rund 12 Prozent der Unternehmen in Deutschland KI-Technologien ein. In Österreich zeigt eine Umfrage von Statista, dass im Bereich der Informations- und Kommunikationstechnologie bereits 37% der Unternehmen KI verwenden, während es im Dienstleistungssektor nur 11,8% sind.

Dieser Trend verdeutlicht: KI wird zunehmend unverzichtbar. Unternehmen müssen sich dieser Entwicklung stellen, die Chancen nutzen und gleichzeitig die damit verbundenen Herausforderungen aktiv angehen.

Welche Chancen bietet die Nutzung von KI?

Die Integration von Künstlicher Intelligenz in den Arbeitsalltag bietet eine Vielzahl von Vorteilen, die die Effizienz und Innovationskraft von Unternehmen erheblich steigern können.

Effizienzsteigerung und Automatisierung



KI hat das Potenzial, Standardaufgaben zu automatisieren und so Arbeitsabläufe zu beschleunigen. Durch den Einsatz automatisierter Systeme können Unternehmen nicht nur die Effizienz steigern, sondern auch menschliche Fehler minimieren.

Neue Arbeitsfelder und Innovationen:

Die Einführung von KI schafft neue Möglichkeiten für Geschäftsmodelle und Berufsbilder. KI-gestützte Technologien ermöglichen tiefgehende Datenanalysen und die Entwicklung innovativer Lösungen, die neue Märkte eröffnen können. Diese Innovationen fördern nicht nur die Wettbewerbsfähigkeit, sondern tragen auch zur Schaffung neuer Arbeitsplätze bei.

Verbesserung der Arbeitsbedingungen

KI kann dazu beitragen, Arbeitsbedingungen zu verbessern. So reduzieren kognitive Assistenzsysteme und intelligente Schutzkleidung die physischen und psychischen Belastungen für Mitarbeitende.
Zudem unterstützen barrierefreie Technologien die Gestaltung inklusiver Arbeitsplätze, die den Bedürfnissen aller Mitarbeitenden gerecht werden.

Herausforderungen bei der Einführung von KI

Trotz der vielen Vorteile gibt es auch signifikante Herausforderungen, die Unternehmen bewältigen müssen, um das volle Potenzial von KI auszuschöpfen.

Veränderungen der Arbeitswelt und Unsicherheit

Der verstärkte Einsatz von KI kann bestehende Berufsbilder und Arbeitsplätze verändern. Während einige Tätigkeiten durch Automatisierung obsolet werden, entstehen gleichzeitig neue Berufsfelder. Dies erfordert eine kontinuierliche Anpassung der Qualifikationen der Mitarbeitenden und kann Unsicherheiten in Bezug auf die berufliche Zukunft hervorrufen.

Technologische und ethische Fragestellungen

Mit der Einführung von KI gehen technische Herausforderungen einher, etwa die nahtlose Integration in bestehende Systeme und die Sicherstellung der Datenqualität.
Auch ethische Fragen, wie der Umgang mit Datenschutz und die Notwendigkeit von Transparenz, müssen geklärt werden, um das Vertrauen in KI-Technologien zu sichern.

Regulierung und Sicherheit

Um das volle Potenzial von KI auszuschöpfen und gleichzeitig Risiken zu minimieren, ist eine klare und faire Regulierung notwendig.
Regierungen und internationale Gremien arbeiten an rechtlichen Rahmenbedingungen, die den verantwortungsvollen Umgang mit KI fördern und Innovationen nicht behindern.

Fazit: KI als Schlüssel zur Zukunft der Arbeit

Künstliche Intelligenz hat das Potenzial, die Arbeitswelt nachhaltig zu transformieren. Unternehmen müssen jedoch proaktiv handeln, um die Chancen der KI zu nutzen und gleichzeitig die damit verbundenen Risiken zu minimieren. Durch Weiterbildung, Anpassung der Arbeitsprozesse und den verantwortungsvollen Einsatz von KI können Unternehmen die Vorteile der Technologie optimal ausschöpfen.

Bei Trenkwalder setzen wir auf zukunftsorientierte Lösungen und gestalten den digitalen Wandel aktiv mit. Mit Expertise in den Bereichen KI, Automatisierung und Smart Data finden wir maßgeschneiderte digitale Lösungen für Ihre Bedürfnisse – sowohl im Frontend als auch im Backend. Unsere Innovationskraft und technische Kompetenz machen uns zu einem verlässlichen Partner für die Herausforderungen der modernen Arbeitswelt.

Prognosen zu Cybersicherheitsbedrohungen 2025

Ein Blick ins Darknet

Die Bedrohungslandschaft im Bereich Cybersicherheit verändert sich kontinuierlich, und die Experten von NordVPN, in Zusammenarbeit mit NordStellar Analytics, haben sich im Rahmen einer eingehenden Analyse der größten Dark-Web-Foren auf die am häufigsten diskutierten Bedrohungen des kommenden Jahres konzentriert. Von KI-gesteuertem Social Engineering über Desinformationskampagnen bis hin zu Schwachstellen im Smarthome-Sektor – die Bedrohungen, die im Darknet thematisiert werden, geben einen beunruhigenden Ausblick auf die Herausforderungen, die 2025 bevorstehen könnten.



„Die Vorhersagen des letzten Jahres sind nach wie vor von Bedeutung, doch ein besorgniserregender Trend zeigt sich: Die Nachfrage nach Hacking-Kursen und DIY-Cybercrime-Kits wächst", erklärt Adrianus Warmenhoven, Cybersicherheitsexperte bei NordVPN.

„Darüber hinaus sind weiterhin große Mengen an geleakten Kundendaten und persönlichen Medien im Umlauf, was die Gefahr von Missbrauch und Identitätsdiebstahl verstärkt." In diesem Jahr haben die Forscher noch weiter ausgeholt und fünf neue Bedrohungen identifiziert, die 2025 eine noch größere Rolle spielen dürften.

1. Das Kapern von Konten bleibt eine anhaltende Bedrohung

Ein besonders häufig diskutiertes Thema im Darknet sind sogenannte „Combo Lists", also Datenbanken mit Kombinationen aus Benutzernamen, Passwörtern und weiteren persönlichen Daten, die durch Sicherheitsverletzungen erlangt wurden. Diese Listen sind für Cyberkriminelle von enormem Wert, da sie eine einfache Möglichkeit bieten, Konten zu übernehmen (Account Takeover).

Über 26.000 Kommentare belegen die anhaltende Popularität dieser Bedrohung. Da viele Nutzer ihre Passwörter mehrfach verwenden, können Hacker die Daten zu betrügerischen Zwecken nutzen, sei es für Finanzbetrug oder Identitätsdiebstahl. Warmenhoven warnt, dass sich diese Art von Angriffen 2025 weiter ausbreiten wird, da die Angreifer durch neue Datenschutzverletzungen immer wieder an frische Anmeldedaten kommen.

2. Smarthome-Geräte: Ein neuer Fokus für Cyberangriffe

Das Darknet ist auch ein Schauplatz für Diskussionen über Sicherheitslücken in Smarthome-Systemen.
Fast 21.000 Kommentare thematisieren die Exploits, die Hacker nutzen können, um in Haushaltsgeräte wie intelligente Kühlschränke oder Videoüberwachungssysteme einzudringen. Laut dem Bericht zur IoT-Sicherheitslandschaft 2024 wurden weltweit über 9,1 Milliarden sicherheitsrelevante Ereignisse in Zusammenhang mit vernetzten Geräten registriert.

„Smarthome-Geräte bieten potenziellen Angreifern nicht nur einen Zugang zu persönlichen Daten, sondern auch eine Möglichkeit, die Privatsphäre von Nutzern zu gefährden", warnt Warmenhoven.

3. Identitätsdiebstahl: Eine nach wie vor hochprofitables Geschäft

Identitätsdiebstahl bleibt eine der lukrativsten Taktiken für Hacker. Im Darknet wird regelmäßig über neue Strategien und Tools diskutiert, die es ermöglichen, personenbezogene Daten zu stehlen und für betrügerische Zwecke zu nutzen.

Besonders besorgniserregend ist die Zunahme von „synthetischen Identitäten", bei denen echte und gefälschte Daten kombiniert werden, um die Authentizität zu erhöhen. Auch die Nutzung von Deepfake-Technologien nimmt zu, um den Betrug noch glaubwürdiger zu machen. Warmenhoven betont, dass sich diese Form des Diebstahls ständig weiterentwickelt und im kommenden Jahr wahrscheinlich noch raffiniertere Methoden auf den Markt kommen werden.

4. Desinformation als Dienstleistung – Ein neuer Trend im Darknet

Ein beispielloser Trend zeichnet sich ab: Die Verbreitung von Desinformation wird zunehmend kommerzialisiert.
Laut dem Global Risks Report 2024 des Weltwirtschaftsforums wird die Bedrohung durch KI-generierte Falschinformationen als eines der größten globalen Risiken betrachtet. Foren im Dark Web bieten mittlerweile Desinformations-Dienste an, bei denen gefälschte Social-Media-Profile und Spam-E-Mails genutzt werden, um gezielt falsche Informationen zu verbreiten und politische oder soziale Narrative zu beeinflussen.

„Cyberkriminelle bieten maßgeschneiderte Desinformationsdienste an, die es ermöglichen, präzise demografische Zielgruppen anzusprechen und die Wirkung von Fake News zu maximieren", erklärt Warmenhoven.

5. KI-gesteuertes Social Engineering: Manipulation auf einem neuen Level

Die Nutzung von Künstlicher Intelligenz zur Manipulation von Personen und Unternehmen nimmt immer raffiniertere Formen an. Foren im Darknet enthalten zunehmend detaillierte Anleitungen, wie KI eingesetzt werden kann, um menschliche Schwächen zu erkennen und Social Engineering-Angriffe effektiver zu gestalten.

Besonders im Unternehmensumfeld werden KI-basierte Techniken genutzt, um Mitarbeiter zu manipulieren und Zugang zu vertraulichen Informationen zu erhalten.

Warmenhoven verweist auf einen weiteren beunruhigenden Trend: Die „Manipulation und Ausbeutung von Unternehmen", bei der Kriminelle Unternehmensvertreter durch geschickt inszenierte Angriffe zu unrechtmäßigen Handlungen wie Rückerstattungen oder Ersatzforderungen verleiten.

Fazit: Ein beunruhigender Ausblick auf 2025

Die Sicherheitsbedrohungen, die in Dark-Web-Foren diskutiert werden, zeichnen ein düsteres Bild für die Cybersicherheit im kommenden Jahr. Von identitätsgestohlenen Daten über Smarthome-Angriffe bis hin zu KI-gesteuerten Manipulationen – Cyberkriminalität wird immer komplexer und gefährlicher.

Die zunehmende Kommerzialisierung von Desinformation und die raffinierte Nutzung von KI zur Täuschung von Menschen und Systemen machen deutlich, dass Unternehmen und Einzelpersonen 2025 mit einer Vielzahl neuer und ausgeklügelter Bedrohungen rechnen müssen. Es wird entscheidend sein, auf diese Entwicklungen frühzeitig zu reagieren und präventive Sicherheitsmaßnahmen zu ergreifen, um den Angriffen im digitalen Raum standzuhalten.

KI-gestützte Cybersicherheit

Zehn Prognosen für das Jahr 2025*



Andrew Grealy, Leiter Armis Labs

Schon seit vielen Jahren warnen Cybersicherheitsexperten auf der ganzen Welt vor den Gefahren KI-gestützter Cyberangriffe. Langsam werden diese Warnungen nun Realität. In diesem Jahr kam KI noch vor allem in Deepfake-, Phishing- und Spear Phishing-Kampagnen zum Einsatz. Für die kommenden Jahre ist aber mit einem deutlichen Anstieg der Anwendungsfälle zu rechnen. KI-gestützte Cyberangriffe werden mehr und mehr zu einem Alltagsphänomen werden.

Um hier effektiv gegenzusteuern, Risiken zu minimieren, Angriffe rechtzeitig zu erkennen und erfolgreich abzuwehren, wird es zunehmend erforderlich sein, als Verteidiger ebenfalls auf KI zu setzen – zur Unterstützung bei der Aufspürung, Analyse und Auswertung sowie der Beseitigung von Cyberbedrohungen.

Folgende Punkte zur KI-gestützten Cybersicherheit sollten Cyber- sicherheitsverantwortliche bei ihren Planungen und Überlegungen für das Jahr 2025 berücksichtigen:

1 Die derzeitigen geopolitischen Spannungen werden weiter schwelen. Von einer Zunahme staatlicher und halbstaatlicher Cyberangriffe auf kritische Unternehmensdaten und kritische Infrastrukturen ist auszugehen.

2 Dort, wie auch bei den Cyberangriffen regulärer Krimineller, wird der Einsatz von KI zunehmen und die Effektivität und Effizienz der Angriffe steigen.

3 Ein Hauptziel der Bedrohungsakteure werden dabei, nicht zuletzt, da sie ein wesentlicher Bestandteil vieler Anwendungen sind, Open Source-Softwarebibliotheken sein.

4 Die Verteidiger werden entsprechend reagieren und den Einsatz von KI-gestützten Cybersicherheitslösungen weiter ausbauen müssen – um ihrerseits Effektivität und Effizienz der Abwehr anzuheben.

5 Generative KI-Modelle werden dabei zunehmend an Bedeutung gewinnen. Sie werden den Verteidigern helfen, fortschrittliche Playbooks zu erstellen, Sicherheitsrichtlinien zu formulieren, Testfälle für Sicherheitslösungen zu generieren und für die Cybersicherheit relevante Prozesse, wie zum Beispiel die Patch-Verwaltung, zu optimieren.

6 Large Language Models (LLMs) werden dabei, aufgrund ihrer weit verbreiteten Anwendung und der ständigen Verbesserung ihrer Fähigkeiten, ihre Vorrangstellung behalten – zumindest kurz- und mittelfristig. Dass die Entwicklung alternativer KI-Technologien, von State-Space-Modellen (SSM) über neuronale Netze (Liquid Neural Networks) bis hin zur allgemeinen künstlichen Intelligenz (AGI), LLMs 2025 die Führung streitig machen wird, ist eher unwahrscheinlich.

7 Das Training der zum Einsatz gebrachten KI-Modelle wird dabei zunehmend über synthetisch generierte Daten erfolgen – um den nationalen und internationalen Vorgaben und Richtlinien bei Datenschutz und Datensicherheit zu entsprechen.

8 Der verstärkte Einsatz von KI wird den Sicherheitsteams dabei helfen, alle Arten von Cybersicherheitstools und -plattformen zu optimieren. Die Behebung von Schwachstellen kann zunehmend proaktiv erfolgen – durch eine strategische Vorfallspräven-tion und eine vorausschauende Reaktionsplanung mit Frühwarnsystemen.

9 Der Einsatz von Detection-as-Code (DaC) wird durch KI wesentlich erleichtert und optimiert werden, wodurch sich die eigene SOC-Leistungsfähigkeit spürbar anheben lassen wird.

10 Und schließlich wird KI auch die Arbeit mit SOAR-Plattformen verbessern. Die effektive Automatisierung komplexer Prozesse zur Erkennung, Analyse und Reaktion auf Bedrohungen wird unter Zuhilfenahme einer KI wesentlich unkomplizierter abgewickelt werden können.

Weltweit werden Cybersicherheitsverantwortliche im Jahr 2025 verstärkt auf den Einsatz von KI setzen müssen, um ihre Abwehrstrategien zu optimieren. Wer die hier vorgestellten Eckpunkte in seine Planung einbezieht, schafft eine solide Grundlage, um die KI-gestützte Cybersicherheit nicht nur für 2025, sondern auch für die folgenden Jahre zukunftssicher zu gestalten.

Kritische Betrachtung des Kommentars durch unserer Redaktion

Der Artikel „KI-gestützte Cybersicherheit – 10 Prognosen für das Jahr 2025" von Andrew Grealy und Michael Freeman beleuchtet die zunehmende Bedeutung von Künstlicher Intelligenz (KI) sowohl als Bedrohung als auch als Verteidigungsinstrument im Bereich der Cybersicherheit. Die Prognosen spiegeln die Dynamik wider, mit der sich die Cyberbedrohungslandschaft entwickelt, und betonen, dass Cybersicherheitsverantwortliche
2025 verstärkt auf KI-basierte Lösungen angewiesen sein werden, um sowohl Angriffe abzuwehren als auch ihre Abwehrstrategien zu optimieren. Der Artikel bringt einige wichtige und durchaus besorgniserregende Erkenntnisse, aber auch vielversprechende Ansätze für den Einsatz von KI zur Stärkung der Cybersicherheit.

KI-gestützten Angriffe steigen

Eine zentrale Erkenntnis des Artikels ist, dass KI-gestützte Cyberangriffe 2025 weiter zunehmen werden. Schon jetzt werden KI und maschinelles Lernen in Phishing-Kampagnen und Deepfakes eingesetzt, aber diese Technologien werden zunehmend auch in anderen Bereichen wie der Angriffsplanung, Automatisierung von Schwachstellenanalysen und Angriffsvektoren zum Einsatz kommen.

Die Autoren gehen davon aus, dass die Effektivität und Effizienz von Angriffen durch den Einsatz von KI erheblich gesteigert werden. Dieser Trend ist nicht nur beunruhigend, sondern auch realistisch, da die Technologie immer zugänglicher wird und Cyberkriminelle zunehmend in der Lage sind, KI für ihre eigenen Zwecke zu missbrauchen. Besonders der Fokus auf Open-Source-Softwarebibliotheken als potenzielles Ziel von Angriffen ist ein wichtiger Aspekt, da viele Unternehmen und Entwickler auf diese Ressourcen angewiesen sind.

KI als Abwehrmaßnahme

Der Artikel stellt jedoch auch klar, dass KI nicht nur als Bedrohung, sondern auch als Lösung dienen wird. Da Angreifer immer raffinierter werden, müssen auch die Verteidiger auf ähnliche Technologien zurückgreifen, um ihre Abwehrstrategien zu verbessern. Besonders hervorzuheben ist die Rolle von generativen KI-Modellen, die zunehmend dazu verwendet werden, Playbooks zu erstellen, Sicherheitsrichtlinien zu formulieren und Prozesse wie die Patch-Verwaltung zu optimieren. Dies zeigt, wie wichtig es ist, dass Unternehmen die Technologie nicht nur als Bedrohung, sondern auch als wertvolles Werkzeug in der Cybersicherheit betrachten. Die Autoren betonen die Notwendigkeit, dass Sicherheitsteams ihre Tools und Plattformen mit KI optimieren, um proaktive Schwachstellenbehebungen und eine vorausschauende Reaktionsplanung zu ermöglichen. Dies könnte helfen, die zunehmende Flut von Bedrohungen und die Komplexität moderner Angriffe zu bewältigen.

Die Rolle von Large Language Models (LLMs)

Eine interessante Prognose betrifft die anhaltende Dominanz von Large Language Models (LLMs) im Bereich der Cybersicherheit. Trotz der rasanten Entwicklung alternativer KI-Technologien wie neuronaler Netze und State-Space-Modellen sehen die Autoren LLMs auch 2025 noch an der Spitze. Diese Technologien, die auf riesigen Textkorpora trainiert werden, sind besonders gut geeignet, Muster in Angriffstechniken zu erkennen und die Erstellung von Phishing-Nachrichten oder schädlichen Skripten zu automatisieren. Auch wenn LLMs in ihrer Funktion als Bedrohungsanalyse-Tool noch nicht perfekt sind, so bieten sie doch eine wertvolle Grundlage, um fortschrittliche Sicherheitslösungen zu entwickeln.

Das Aufkommen von Detection-as-Code und SOAR-Plattformen

Ein weiteres zukunftsweisendes Konzept, das im Artikel zur Sprache kommt, ist „Detection-as-Code" (DaC). Diese Technologie könnte die Art und Weise, wie Sicherheitsereignisse erkannt und bearbeitet werden, revolutionieren, indem sie eine noch stärkere Automatisierung und Integration in DevOps-Umgebungen ermöglicht. KI-basierte Plattformen könnten Sicherheitsereignisse schneller identifizieren und analysieren, was eine schnellere und effizientere Reaktion auf Bedrohungen ermöglichen würde. Auch SOAR-Plattformen (Security Orchestration, Automation, and Response) werden durch den verstärkten Einsatz von KI erheblich profitieren. Diese Plattformen werden durch die Automatisierung komplexer Sicherheitsprozesse die Effizienz und Geschwindigkeit der Reaktion auf Angriffe deutlich verbessern.

Fazit: KI als Schlüsselkomponente der Cybersicherheit 2025

Die Prognosen für 2025 machen deutlich, dass Cybersicherheitsverantwortliche die Rolle von KI nicht nur als Bedrohung, sondern auch als unverzichtbares Verteidigungsinstrument erkennen müssen. Es wird erwartet, dass KI-basierte Angriffe immer ausgeklügelter werden, weshalb Unternehmen und Sicherheitsorganisationen ihre eigenen Abwehrmechanismen ebenfalls mit KI optimieren müssen.

Die Implementierung von KI-gestützten Lösungen für die Bedrohungserkennung, Schwachstellenma- nagement und automatisierte Reaktionsstrategien wird entscheidend sein, um in der sich rasant entwickelnden Bedrohungslandschaft Schritt zu halten. Die Prognosen bieten eine interessante und realistische Perspektive auf die Cybersicherheit im Jahr 2025 und verdeutlichen die Notwendigkeit, mit der Technologie Schritt zu halten und sie nicht nur als Reaktion auf Bedrohungen zu verstehen, sondern als aktives Mittel zur Vorbeugung und Abwehr. Wer diese Entwicklungen in seine langfristige Cybersicherheitsstrategie integriert, wird besser auf die Herausforderungen der Zukunft vorbereitet sein.

Autoren des ersten Teil des Artikels: Andrew Grealy, Leiter Armis Labs & Michael Freeman, Leiter Threat Intel- ligence bei Armis. Zweiter Teil SECG ML

TELENOT
Technik für Sicherheit

Kritische Infrastruktur physisch zuverlässig schützen

KRITIS-DachG: Fakten, Technik, Lösungen

