1. AUSGABE | 2025

NTA DISPLAY

DAS KOMPETENTE TK-/IT-MAGAZIN

Wie digitale Souveränität ihr Unternehmen stärkt

Bild: shutterstock.com/William Perugini

Neue Rufanlagen-Norm:
Änderungen betreffen alle Betreiber

EU-Richtlinie NIS-2:
Notfallplanung ist unverzichtbar

Widerstandsfähigkeit gegen Unwägbarkeiten stärken

In jedem Unternehmen müssen regelmäßig Anschaffungen getätigt werden, das gehört zum Geschäftsalltag. Der Zuschlag für neue technische Lösungen hat dabei meist eine beträchtliche Tragweite. Wer beispielsweise in ein Kommunikationssystem investiert, trifft eine Entscheidung, die sich über Jahre auswirkt und dem Unternehmen echte Vorteile verschafft. Das gelingt, wenn man sich auf Partner verlassen kann, die genau die Anforderungen des jeweiligen Unternehmens kennen, die über Expertise verfügen und nie aus dem Blick verlieren, in welche Richtung es weitergeht. Dazu gehört auch, dass der Kunde nicht langfristig in ungewollte Abhängigkeiten gerät.

Darum geht es im Titelthema dieser DISPLAY-Ausgabe: Digitale Souveränität! Gut beraten ist, wer für seine Organisation im Bereich der digitalen Infrastruktur und der eingesetzten Technologien immer einen »Plan B« hat. Jedes Unternehmen sollte danach streben, die eingesetzten Technologien nach den eigenen Bedürfnissen steuern, kontrollieren und beherrschen zu können. Wer die Kontrolle über die eigenen Daten, die Sicherheit der eigenen Netze und digitalen Ressourcen behält, ist widerstandsfähiger gegen Unwägbarkeiten. Das schafft Vertrauen bei Kunden und bringt Wettbewerbsvorteile. Wir empfehlen einen planvollen und schrittweisen Ausbau der digitalen Souveränität. Wer sich auf diesem Weg von einem kompetenten, neutralen Systemhaus partnerschaftlich und vorausschauend begleiten lässt, macht alles richtig!

Herzlichst

Torsten Marx
Geschäftsführer

Neufassung der Norm für Rufanlagen kommt

Die Änderungen betreffen alle Pflegeheime, Krankenhäuser und ähnlichen Einrichtungen

Am 21. März 2025 wurde der Entwurf DIN VDE 0834-1:2025-04 für die Neufassung der Norm veröffentlicht. Sie regelt die technischen und organisatorischen Anforderungen an die Sicherheit von Rufanlagen in Krankenhäusern, Pflegeheimen und ähnlichen Einrichtungen. Die Kommentierungsfrist endet am 21. Juli, und Experten rechnen mit dem Inkrafttreten der neu gefassten Norm im vierten Quartal 2025. Daraus ergeben sich auch für Betreiber neue Pflichten. So dient jede Rufanlage als technisches Hilfsmittel, mit dem sich etwa Patienten, Seniorenheimbewohner oder auch Inhaftierte in einer JVA jederzeit bemerkbar machen können. Die Pflicht für Betreiber besteht darin, durch die technischen und organisatorischen Maßnahmen den mit der aktuellen Norm konformen Betrieb der Rufanlage zu gewährleisten.

Bild: shutterstock.com/Bignai

Der Entwurf sieht eine Übergangsfrist von zwei Jahren für Anpassungen bei Bestandsanlagen vor, Inspektionen müssen ab Inkrafttreten Abweichungen dokumentieren. Neue Anlagen dürfen nur noch nach dem neuen Stand der Norm geplant, errichtet und betrieben werden. Der Entwurf beinhaltet auch organisatorische Neuerungen, wie die Einführung einer Protokollierungspflicht sowie dokumentierte Schulungen und Einweisungen für das Personal.

Ausblick: Betreiber von Rufanlagen sollten die Entwicklung genau im Blick behalten. Als Fachunternehmen mit zertifizierten Fachkräften sind wir ganz nah dran. Sobald dies verbindlich möglich ist, erhalten Sie bei uns alle benötigten Auskünfte.

Notfallpläne für die Kommunikation unverzichtbar

EU-Richtlinie NIS-2 mit hohen Anforderungen

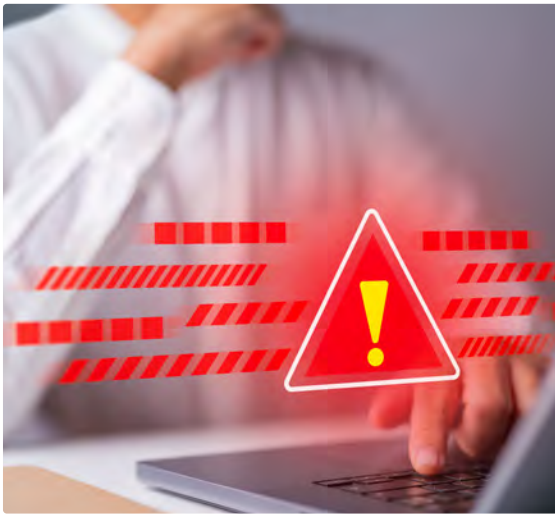


Bild: shutterstock.com/ RerF_Studio

Die NIS-2-Richtlinie betrifft allein in Deutschland über 30.000 Unternehmen. Die EU-Richtlinie zur Stärkung der Cybersicherheit sollte bis Oktober 2024 in deutsches Recht umgesetzt werden. Doch aufgrund der aktuellen politischen Ereignisse ist eine zeitnahe Umsetzung eher unwahrscheinlich. Das bringt betroffenen Unternehmen zwar einen Zeitgewinn, bedeutet jedoch nicht, dass Thema ad acta legen zu können. Neben den Einrichtungen der kritischen Infrastruktur (KRITIS) müssen noch Tausende Unternehmen teils strenge Sicherheitsmaßnahmen umsetzen.

Inhaltlich legt NIS-2 großen Wert auf Cybersicherheit. Gemeint ist hiermit die Umsetzung von grundlegenden Maßnahmen und Praktiken, die Unternehmen und Mitarbeitende im Betrieb ergreifen sollten, um den Schutz vor Cyberangriffen zu gewährleisten. Dazu gehören etwa das Einspielen von Patches und Updates, ein sicheres Passwortmanagement oder das kontinuierliche Erstellen von Backups.

Handlungsfähig bleiben

Auch im Bereich der Kommunikation stellt NIS-2 hohe Anforderungen. Die Unternehmen werden dazu verpflichtet, Notfallpläne aufzustellen und zu dokumentieren. Darin müssen Eskalationsverfahren (z. B. Alarmierungslösungen) und klare Kommunikationswege aufgeführt sein, nach denen eine Organisation im Ernstfall agieren kann. Unerlässlich ist, dass die erforderliche Technik hierfür vorhanden sein muss und jederzeit einsatzbereit ist. Für den Betrieb werden zudem Anforderungen an Kryptografie und die Verschlüsselung von Kommunikationsinhalten gestellt, um die hohen Schutzziele zu erreichen. Ebenfalls wichtig: Unternehmen müssen anhand verschiedener Kriterien selbst ermitteln, ob sie in den Geltungsbereich der NIS-2-Richtlinie fallen.

Studie deckt Brandschutzmängel auf

Sonderinspektion von Brandmeldeanlagen bei baulichen Veränderungen

Eine aktuelle Analyse im Bereich des technischen Brandschutzes belegt: Mehr als 70 Prozent aller sicherheitstechnischen Einrichtungen in Gebäuden weisen Mängel auf. Durch planungs- und baubegleitende Prüfungen sowie eine fachgerechte Wartung und Instandhaltung können solche Mängel aber wirksam reduziert werden.

Der Baurechtsreport des TÜV-Dachverbandes erfasst gesetzlich vorgeschriebene Prüfungen von sicherheitsrelevanten Anlagen in sogenannten Sonderbauten. Dazu gehören u. a. Schulen, Krankenhäuser, Pflegeeinrichtungen, Hotels und Hochhäuser. 27,1 Prozent der geprüften Brandschutzanlagen wiesen »wesentliche Mängel« und 43,9 Prozent »geringfügige Mängel« auf.

Wir meinen: Gebäudesicherheit sollte stets ernst genommen werden, denn hier geht es im Ernstfall um die Rettung von Menschenleben. Setzen Sie hier auf die Zusammenarbeit mit Ihrem Systemhaus und schließen Sie einen Instandhaltungsvertrag ab. Wichtig zu wissen: Bei den in der TÜV-Untersuchung festgestellten Mängeln spielten technische Defekte nur eine untergeordnete Rolle. Häufig wurden hingegen bauliche Veränderungen vorgenommen, die aber im Brandmeldekonzept nicht berücksichtigt wurden. Deshalb ist es wichtig zu wissen: Nach jeder baulichen Veränderung besteht Handlungsbedarf. Es ist dann eine Sonderinspektion der Brandmeldeanlage notwendig. Ihr Systemhaus informiert Sie gerne!

Bild: shutterstock.com/ Kzenon

Wie digitale Souveränität Ihr Unternehmen stärkt

In einer zunehmend vernetzten Welt, in der digitale Technologien nahezu jeden Bereich unseres Lebens und Geschäfts beeinflussen, gewinnt der Begriff der »digitalen Souveränität« immer mehr an Bedeutung. Doch was genau steckt hinter diesem Konzept? Und warum sollten Unternehmer sich mit diesem Thema auseinandersetzen? In diesem Artikel erklären wir, was digitale Souveränität bedeutet, warum sie für Unternehmen relevant ist und mit welchen praktischen Maßnahmen sie gestärkt werden kann.

Was ist digitale Souveränität?

Digitale Souveränität beschreibt das Maß an Kontrolle, das Individuen, Unternehmen sowie öffentliche Einrichtungen und Staaten über ihre digitalen Ressourcen und Technologien haben. Sie bezieht sich auf die Fähigkeit, selbstbestimmt über den Umgang mit Daten, Technologien und digitalen Infrastrukturen zu entscheiden, ohne dabei in ungewollte oder risikobelastete Abhängigkeiten zu geraten.

Für Unternehmer bedeutet digitale Souveränität, dass sie nicht nur in der Lage sind, ihre Daten und ihre digitale Kommunikation zu schützen, sondern auch die digitale Infrastruktur und Technologien, die sie verwenden, nach eigenen Anforderungen zu steuern, zu kontrollieren und weiterzuentwickeln.

Bild: shutterstock.com/ William Perugini

Warum ist digitale Souveränität für Unternehmen wichtig?

In der heutigen Zeit sind digitale Technologien ein zentraler Bestandteil jedes Unternehmens. Vom Cloud-Computing über Kommunikationstools bis hin zu Software-as-a-Service-Angeboten – Unternehmen sind zunehmend auf externe Anbieter und digitale Technologien angewiesen. Die Gewährleistung des laufenden Geschäftsbetriebs, die Einhaltung rechtlicher Vorgaben (z. B. Datenschutz), die Wahrung vertraulicher Geschäftsinformationen und auch die Fähigkeit, neue Geschäftsmodelle zu entwickeln, sowie die Optimierung von Prozessen werden darum wesentlich von dem Grad der eigenen digitalen Souveränität mitbestimmt.

Schutz der Infrastruktur ist die Basis

Cyberangriffe auf die IT-Sicherheit von Unternehmen, Privatpersonen, aber auch auf Staaten befinden sich auf einem historischen Hoch und nehmen besorgniserregend zu. Für Unternehmen bildet die IT-Infrastruktur die Basis jedes Schutzkonzepts, mit dem sie die Hoheit über ihre Daten sichern und diese vor unberechtigtem Zugriff durch Hacker und Cyberkriminelle schützen. Der sogenannte Zero-Trust-Ansatz bildet dabei eine zunehmend verbreitete Grundlage eines modernen Sicherheitskonzeptes. Hierbei wird keinem Gerät, Nutzer oder Dienst standardmäßig vertraut – unabhängig davon, ob sie sich innerhalb oder außerhalb des Netzwerks befinden. Stattdessen erfolgen strenge Identitätsprüfungen und Zugriffsbeschränkungen. Unerlässlich sind Maßnahmen wie regelmäßige Sicherheitspatches und Updates sowie sichere Authentifizierungsverfahren. Zusätzlich helfen regelmäßige Sicherheitsaudits, Schwachstellen in der IT-Infrastruktur frühzeitig zu identifizieren und Sicherheitsmaßnahmen zu optimieren. Nicht vergessen werden darf dabei die physische Gebäudesicherheit (Zutrittskontrolle, Videoüberwachung usw.), mit der auch die Netze und Endgeräte vor unberechtigten Eingriffen geschützt werden.

Datenhoheit sichern

Bei der Nutzung von sogenannten Public-Cloud-Diensten oftmals globaler Anbieter kann sich die Frage stellen, wer genau Zugriff auf die Daten hat und inwieweit diese Daten rechtskonform verarbeitet werden. Durch mehr digitale Souveränität können Unternehmer besser gewährleisten, dass ihre Daten geschützt vor unberechtigtem Zugriff und Missbrauch verarbeitet werden. Optionen bieten hier Anbieter mit klaren Aussagen zur Datenverarbeitung, die Nutzung regionaler Rechenzentren oder der lokale Betrieb von unternehmenskritischen Anwendungen. Oftmals empfehlen sich auch hybride Modelle, in denen die verschiedenen Formen der Bereitstellung miteinander kombiniert werden. Darüber hinaus gewährleisten Unternehmen mit der Verwendung offener technischer Standards sowie der Nutzung üblicher Datenformate, dass sie im Bedarfsfall ihre Nutzerdaten von externen Betreibern der Datenverarbeitung einfach zurückerlangen können.

Mobilität managen

Das Arbeiten und die Zusammenarbeit mit Kollegen und Partnern finden spätestens seit der Pandemie nicht mehr alleinig oder vorrangig in den Betriebsräumen eines Unternehmens statt. Die Arbeitswelt ist mit Homeoffices und der Nutzung von mobilen Endgeräten von unterwegs wie Laptops, Tablets und Smartphones mobiler und flexibler geworden. Auf geschäftliche Anwendungen greifen Mitarbeiter über Weboberflächen zu, sei es von daheim über unterschiedliche private Netzanschlüsse, heimische Funknetze oder aus Hotels – letztlich von nahezu überall. Zu den entscheidenden Maßnahmen gehören hier die Absicherung privater Netzzugänge, Mehrfaktor-Authentifizierung sowie Verschlüsselung von Diensten. Ein konsequent umgesetztes Mobilitätskonzept stärkt die Robustheit des Unternehmens mit dezentraler Arbeit als Alternative zum Betriebsstandort.

In einer Welt, in der digitale Abhängigkeiten zunehmend das Geschäftsumfeld prägen, ist digitale Souveränität nicht nur eine Frage der Sicherheit, sondern auch eine strategische Sinnhaftigkeit für nachhaltigen Erfolg.

Mitarbeiterschulungen

Ein oft übersehener, aber sehr wichtiger Aspekt der digitalen Souveränität sind die Schulung und Sensibilisierung der Mitarbeiter. Die Kontrolle über Daten und Systeme ist nur so stark wie das Wissen der Mitarbeiter, diese korrekt zu nutzen und Gefahren zu erkennen. Regelmäßige Schulungen zu Themen wie Cybersicherheit, Datenschutz und sicherer Nutzung von digitalen Tools sind entscheidend, um die Risiken von Datenlecks und Sicherheitsvorfällen zu minimieren. Digitale Tools und zunehmend auch Anwendungen aus dem Bereich künstlicher Intelligenz sind zugleich wichtige Instrumente, um die Effizienz von betrieblichen Prozessen zu steigern und neue geschäftliche Anwendungen zu erkennen und einzuführen. Die Schulung von Mitarbeitern dient darum nicht nur dem Schutz, sie dient der digitalen Souveränität auch durch die Vermittlung von innovativen Anwenderkompetenzen.

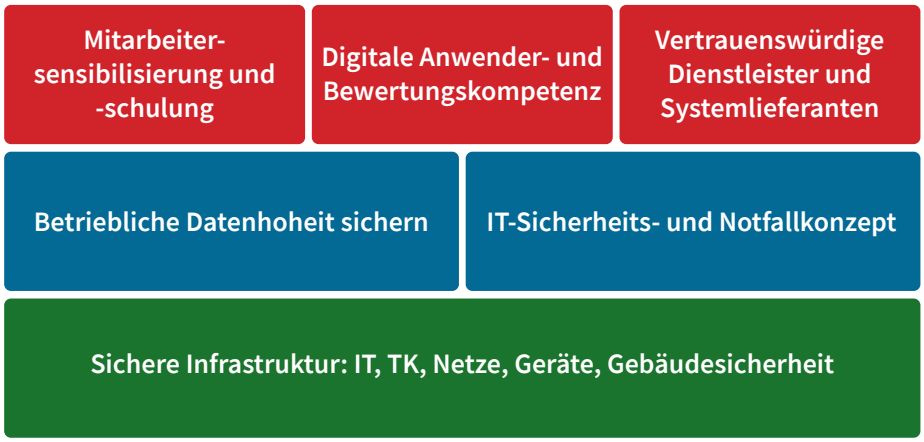
Konkrete Strategie

Digitale Souveränität ist kein abstraktes Konzept, sondern eine konkrete Strategie für Unternehmen, die sich in einer zunehmend digitalisierten Welt behaupten wollen. Sie bedeutet nicht nur, die Kontrolle über eigene Daten, die Sicherheit der eigenen Netze und digitalen Ressourcen zu behalten, sondern auch, selbstbestimmter und widerstandsfähiger gegenüber internationalen Unwägbarkeiten zu werden. Dies schafft Vertrauen bei Kunden und bringt neue Wettbewerbsvorteile. Die Bereitstellung sicherer und leistungsstarker Infrastrukturen ist die Voraussetzung für die Entwicklung und Nutzung innovativer Geschäftsmodelle.

Mit vertrauenswürdigen Partnern vorankommen

Wie soll ein solches Programm der zunehmenden digitalen Souveränität bewältigt werden? So lautet eine oft gestellte Frage. Fachkräftemangel und die hohen Anforderungen des Tagesgeschäfts scheinen hierfür die Handlungsspielräume allzu sehr zu beschneiden. Es geht jedoch nicht um ein Schwarz-Weiß-Denken oder nicht leistbare Kraftakte. Die gangbare Perspektive besteht in einem planvollen und schrittweisen Ausbau der digitalen Souveränität des Unternehmens. Dabei unterstützen wir Sie als kompetentes, neutrales Systemhaus partnerschaftlich und vorausschauend.

Dimensionen digitaler Souveränität



Buchtipp

Das neue Wirtschaftswunder

Der Mittelstand als Vorreiter der Digitalisierung

Bild: brand eins books

Das neue Wirtschaftswunder
Verlag brand eins books, Hamburg 2024
Gebunden, 128 Seiten
ISBN: 978-3-98928-020-5
Preis: 20,00 EUR

Der Mittelstand ist unbestritten die Stütze der deutschen Wirtschaft. Überwiegend aus kleinen und mittleren Unternehmen bestehend, macht er 99 Prozent aller Unternehmen in Deutschland aus. Doch die Mittelständler gelten gemeinhin als abwartend bei der Digitalisierung. Dass es auch anders geht, verdeutlicht Autor Philipp Garra. Er leitete bei einem großen Softwarekonzern zuletzt den Cloud-Vertrieb in Deutschland und kommt selbst aus einem Familienunternehmen.

Verständlich und praxisnah erzählt er von Vorreitern der Digitalisierung im Mittelstand – beispielsweise vom Familienunternehmen Trumpf aus Tuttlingen bei Stuttgart, das künftig Quantencomputer entwickeln will. Das Buch will erreichen, dass man die Notwendigkeit der digitalen Transformation versteht. Dabei übersieht es nicht die Besonderheiten der mittelständischen deutschen Wirtschaft. Der Autor redet nichts schön, zeigt aber auf, dass der Mittelstand durchaus die Nase vorne haben kann. Dabei kommt das Sachbuch fast ganz ohne technischen Jargon aus, ist also gut lesbar. Mit einer Prise Humor ermutigt der Autor Verantwortliche im Geschäftsleben dazu, neue Wege zu finden und sich von alten Denkmustern zu befreien.

Zahl des Monats

20.000

Die ITK-Branche schafft neue Jobs

Die deutschen Unternehmen der IT- und Telekommunikationsbranche schaffen fortgesetzt neue Arbeitsplätze. So soll die Zahl der Beschäftigten in diesem Sektor laut Bitkom im Jahresverlauf 2025 um rund 20.000 auf bundesweit 1,371 Millionen anwachsen. Auch im zurückliegenden Jahr 2024 sind den Angaben zufolge 9.000 neue Arbeitsplätze entstanden. »Mittlerweile ist die ITK-Branche Deutschlands größter industrieller Arbeitgeber«, kommentierte Bitkom-Präsident Dr. Ralf Wintergerst die aktuellen Zahlen. Sie interessieren sich für eine Karriere in der IT- und Telekommunikationsbranche? Dann werfen Sie noch heute einen Blick auf die Website Ihres Systemhauses!

Bild: shutterstock.com/ Dragana Gordic

LEXIKON

Call Distribution mit KI

Künstliche Intelligenz unterstützt dabei, Kundenanrufe klug zu bearbeiten

Guter Kundenservice besteht aus mehr als freundlichen Worten und kurzfristiger Problemlösung. Im Idealfall führt er zu nachhaltig zufriedenen und treuen Kunden. Die Grundlage für guten, sprachbasierten Kundenservice ist seit vielen Jahren eine Automatic Call Distribution (engl. für automatische Anrufverteilung; auch ACD-System). Hierbei verteilt das Kommunikationssystem eingehende Kundenanrufe (»Inbound-Telefonie«) auf die einzelnen Servicemitarbeiter. Das erfolgte bisher meist nach vorher festgelegten, starren Regeln. Ein Beispiel: Der am längsten wartende Anrufer wird dem Mitarbeiter zugeteilt, dessen letztes Gespräch am längsten zurückliegt. Mithilfe künstlicher Intelligenz bestehen heute weitaus mehr Möglichkeiten. So kann eine intelligente Anrufweiterleitung mit KI-Unterstützung den Kunden an den Agenten weiterleiten, der bei dem Anliegen am besten weiterhelfen kann. KI-Tools können auch dafür genutzt werden, eine Verbindung mit demselben Agenten wiederherzustellen, der mit dem Kunden bereits gesprochen hat. KI hilft auch dabei, Kunden gezielt an lokale Callcenter in ihrer Nähe zu vermitteln. Der KI-Einsatz hört nicht auf, wenn der Kunde den Agenten erreicht hat: KI-Tools können ein Gespräch mitverfolgen und dem Agenten in Echtzeit Empfehlungen für die nächsten Schritte geben. Das kann z. B. die Hervorhebung von Ressourcen in der Wissensdatenbank sein oder eine Empfehlung von Upselling-Möglichkeiten.

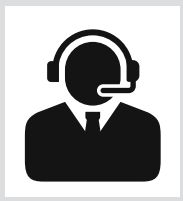


Bild: shutterstock.com/ Leonorea

Innovationen von damals

Dolmetschertelefon 1.0

Der Traum von »automatischer« Übersetzung begann vor 70 Jahren

Bild: »Der Aufstieg«

Moderne Kommunikationslösungen ermöglichen heute eine Echtzeit-Übersetzung bei Telefonaten via App. Was im Jahr 2025 problemlos möglich ist, beschäftigte die Menschen bereits vor rund 70 Jahren. Im Jahr 1958 veröffentlichte die damalige bundesdeutsche Monatszeitschrift »Der Aufstieg« eine Titelgeschichte mit der Ankündigung »Dolmetschertelefon in Sicht!«. Sie berichtete über den in Lüneburg lebenden Dolmetscher Fredo Nestler, der ein solches Dolmetschertelefon auf den Weg bringen wollte.

Nicht mit KI und Computer, sondern mittels bundesweit verfügbarer Dolmetscher wollte er einen europaweiten Dienst aufbauen. Um das Angebot zu nutzen, sollten die Anwender das Gespräch direkt bei der Firmenzentrale seines Unternehmens Tel-Interpret GmbH anmelden. Zudem benötigten sie den von ihm entwickelten und patentierten »Tel-Interpret«. Der Fernsprecher beherrschte das heute übliche Prinzip der Dreierkonferenz: Zwei Geschäftsleute (A und B) und ihr Dolmetscher (C) konnten auf einer Leitung sprechen, was eine direkte Übersetzung möglich gemacht hätte.

Jahrelang stritt sich der Tüftler mit der staatlichen Telefongesellschaft Deutsche Bundespost, bis er endlich eine Genehmigung zur Umsetzung seiner Vision erhielt. Selbst in China war man auf die Idee aufmerksam geworden und an der Lösung interessiert. Doch das »Dolmetschertelefon 1.0« ging nie in Betrieb. Nestlers »Tel-Interpret« fehlte es an Investoren. 15 Jahre später, im Jahr 1973, richtete die australische Einwanderungsbehörde einen ersten Dienst für »Telefondolmetschungen« ein. Vor allem im Gesundheitswesen und bei Gerichtsverfahren fand diese Kommunikationslösung weltweit Verbreitung.

Zu guter Letzt

Der teuerste Datenspeicher der Welt

Festplatten mit mehreren Terabyte Datenspeicher sind für unter 100 Euro erhältlich. Der Waliser James Howells besitzt jedoch eine 734 Millionen Euro teure Festplatte. Theoretisch zumindest.

Die Festplatte enthält nämlich die gespeicherten Bitcoin-Schlüssel für 8.000 Bitcoins. Ein solcher Schlüssel kostete im Jahr 2010 weniger als einen Euro. Doch der Kurs der Kryptowährung explodierte.

Im Sommer 2013 waren die auf seiner Festplatte gespeicherten Bitcoin-Schlüssel bereits das 230-Fache wert und heute entsprechen die 8.000 Bitcoin-Schlüssel einem Wert von rund 734 Millionen Euro! Dumm nur, dass die Festplatte im

Bild: shutterstock.com/BLKstudio

Rahmen einer Aufräumaktion versehentlich in der Mülltonne landete. Die Müllabfuhr beförderte den wertvollen Speicher ordnungsgemäß zur städtischen Deponie. Seither kämpft Howells darum, auf der Müllhalde der Stadt Cardiff nach seiner Festplatte suchen zu dürfen – bisher vergebens. Die Stadt hat umweltrechtliche Bedenken und weist darauf hin, dass alles, was einmal auf der Müllhalde landet, ohnehin zum Eigentum der Stadt wird.

Impressum

DISPLAY Ausgabe 1-2025

Produktion: VAF Bundesverband Telekommunikation e. V., Medienwerkstatt (www.vaf.de), Schulstraße 2, 40721 Hilden
Redaktion: Martin Bürstenbinder (V. i. S. d. P.), Folker Lück, Julia Noglik; Layout: Uwe Klenner; Lektorat: Christian Jerger;

KRITIS-Herausforderungen fest im Blick

Auf dem KRITIS-Tag am Hauptsitz in Mainz informierte NTA in Partnerschaft mit verschiedenen Herstellern über Anforderungen und Lösungsoptionen, für die Betreiber Kritischer Infrastrukturen. Zahlreiche Teilnehmer aus Behörden, Verkehr/Logistik, Bau-, Bildung, Gesundheit und Energie nutzten die Gelegenheit zur Information.

Im Jahr 2024 waren laut BSI in Deutschland exakt 1.132 Betreiber mit 2.095 Anlagen registriert, die unter die KRITIS-Verordnung fallen. Sogar rund 30.000 Unternehmen in Deutschland – die ihre Zugehörigkeit zu den Bereichen »besonders wichtige« bzw. »wichtige« Einrichtungen eigenständig abklären müssen – sind von der NIS-2-Richtlinie betroffen. Eines der zentralen Kernziele beider Regelungen ist es, wichtige Infrastrukturen gegen IT-Störungen und Cyberangriffe besser zu schützen. Während die NIS-2-Richtlinie primär dazu beitragen soll, dass sich Unternehmen und Organisationen besser vor bestehenden Risiken absichern, geht es bei kritischen Infrastrukturen auch darum, dass diese von extrem wichtiger Bedeutung für das staatliche Gemeinwesen sind. Kommt es hier zu einem Ausfall oder einer Beeinträchtigung, kann dies zu gefährlichen Versorgungsengpässen, zu erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen.

Mit einer gut verständlichen Einleitung von NTA-Vertriebsleiter Sicherheitstechnik Kai Hardt startete der KRITIS-Tag. Im Fokus stand das neue KRITIS-Dachgesetz: Wer ist betroffen und welche

Bild: NTA

Rechte und Pflichten ergeben sich für Betreiber daraus? Nachfolgend beleuchteten Experten die Technik-Themen Zutrittskontrolle, Videoüberwachung, forensische Bildanalyse und Perimeterschutz sowie – nach einem Mittagsimbiss – Gefahrenmanagementsysteme im KRITIS-Umfeld. Die Referenten der Unternehmen Advancis, Axis, Honeywell, Milestone – und natürlich von NTA-Systemhaus – standen nachfolgend ausführlich Rede und Antwort.

»Viele Teilnehmende waren grundsätzlich über die Gesetzeslage gut informiert und nutzten den Tag, um sich zu technischen Fragen und Neuerungen ein noch genaueres Bild zu machen«, erläutert Kai Hardt. Ein wichtiges Anliegen seitens NTA war es zu verdeutlichen, dass das Systemhaus betroffenen Unternehmen und Organisationen ein Gesamtpaket zur Physischen Sicherheit anbieten kann. »Hierzu haben wir ein gutes Feedback erhalten«, ergänzt Hardt. Insgesamt wurde die Veranstaltung von den Teilnehmenden als »lehrreich« und »Informativ« bewertet. Grund genug für NTA, künftig weitere Veranstaltungen zu planen und anzubieten.

NTA-Standort Rhein Neckar

Zwei Technik-Experten feiern Firmenjubiläum


Bild: NTA

Marko Schock und Andreas Kuß gehören ab sofort zu den Urgesteinen der NTA Rhein Neckar GmbH – aber keinesfalls zum »alten Eisen«. Beide sind jetzt seit zehn Jahren für das Unternehmen tätig. Marko Schock ist Projekt-Teamleiter am Standort Mannheim und damit ein unverzichtbares Bindeglied zwischen dem Vertriebsteam und dem technischen Kundendienst. Andreas Kuß ist als Servicetechniker für moderne Unify-Kommunikationssysteme, Lichtrufsysteme und Lösungen von Schneider Intercom für Kunden in der gesamten Südpfalz unterwegs, um neue Technik zu montieren oder bestehende Installationen zu warten. Beide erhielten zu ihrem 10-jährigen Firmenjubiläum aus den Händen von Geschäftsführer Christoph Hafner eine Urkunde. Die Jubilare haben auch nach einem Jahrzehnt weiterhin ungetrübte Freude an ihrer interessanten Tätigkeit, am guten Betriebsklima und den flachen Hierarchien am NTA-Standort Rhein-Neckar. »Auf diese beiden Kollegen, ihr Engagement, ihre Leistungen und ihr Fachwissen können wir wirklich stolz sein«, freut sich Geschäftsführer Christoph Hafner.

NTA UNTERNEHMENSGRUPPE

NTA Systemhaus GmbH & Co. KG
Genfer Allee 2
55129 Mainz

Telefon: +49 (6131) 8845-0
E-Mail info@nta.de
Web www.nta.de