ADVERTORIAL

VITAKO AKTUELL

WIR MACHEN KOMMUNEN SICHER

4 **KOMM.ONE**
NOTFALLMANAGEMENT: RICHTIG REAGIEREN BEI CYBERATTACKEN

6 **ITEBO**
HANDLUNGSFÄHIG BLEIBEN IM KRISENFALL

8 **IT-VERBUND LANDSBERG**
CYBERSICHERHEIT NEU GEDACHT

9 **GOVERNIKUS**
DIGITALISIERUNGSPARTNER DER ÖFFENTLICHEN VERWALTUNG

9 **EGOMV**
ZUSAMMENHALT SCHAFFT SICHERHEIT

10 **OWL-IT**
DAS ISMS ALS GRUNDLAGE DER CYBERSICHERHEIT

11 **REGIO IT**
CYBER DEFENSE: IM SPIEL BLEIBEN

12 **PROSOZ**
AWARENESS ALS UNTERSCHÄTZTER ERFOLGSFAKTOR

14 **KDO**
IMPULSE FÜR DIE MODERNE VERWALTUNG

15 **GOVDIGITAL**
IT-NOTFALLÜBUNGEN FÜR MITGLIEDER UND TRÄGER

VITAKO MITGLIEDER: VORREITER BEI CYBERSICHERHEIT

Kommunen sind das Rückgrat der öffentlichen Daseinsvorsorge. Werden sie Ziel eines Cyberangriffs, fallen essenzielle Leistungen von heute auf morgen aus: Personalausweise können nicht ausgestellt, Wohn- und Kindergeldzahlungen nicht geleistet werden. Baugenehmigungen liegen monatelang brach. Die Folgen für Bürgerinnen und Bürger sind unmittelbar. Die gute Nachricht: VITAKO Mitglieder bieten den Kommunen umfassenden Schutz.

Ob Notfalltrainings, Warnsysteme oder KI-Anwendungen – mithilfe der innovativen Tools und Hilfestellungen sind Kommunen in der Lage, auf Angriffe schnell und wirksam zu reagieren. Zugleich unterstützen IT-Dienstleister die Kommunen dabei, neuen gesetzlichen Anforderungen wie NIS-2 gerecht zu werden. Eine Auswahl neuer Innovationen stellen wir in diesem Heft vor.

Notfallmanagement

RICHTIG REAGIEREN BEI CYBERATTACKEN

Am Tag X gilt es, besonnen, zügig und zielgenau zu handeln. Damit das klappt, muss bei Hackerangriffen das Notfallmanagement der Verwaltung greifen – gut geplant und eingeübt. Ebenso unerlässlich sind Incident Response Teams zur Gefahrenabwehr. Denn dank professioneller Unterstützung werden Kommunen rasch wieder handlungsfähig.

Ein Klick auf eine täuschend echt aussehende Phishing-Mail und schon ist es passiert. Was ist jetzt zu tun? Wer gut vorbereitet ist, kann rasch und richtig reagieren. An dieser Stelle setzt das Notfallmanagement einer Verwaltung ein. Vorab festgelegte Informationsketten werden aktiviert, Aktionen umgesetzt. Die Ziele sind klar definiert: Die Sicherheit der IT-Infrastruktur und die Handlungsfähigkeit der Kommune müssen wiederhergestellt werden. Ebenso soll ein Schaden verhindert oder, falls das nicht mehr gänzlich möglich ist, minimiert werden.

EIN STANDARD DER CYBERSICHERHEIT

Das kann jedoch nur ein leistungsstarkes Notfallmanagement erreichen. Ein Handbuch, das irgendwo im Regal steht und vielleicht erst noch gesucht werden muss, bringt nichts. Für die IT-Sicherheit öffentlicher Verwaltungen ist ein Notfallmanagement erforderlich, das von Minute eins an einsatzbereit ist. Es wäre gefährlich, zu denken, „uns passiert schon nichts“ und keinen Plan an der Hand zu haben. Der aktuelle Lagebericht zur IT-Sicherheit in Deutschland des Bundesamtes für Sicherheit in der Informationstechnik BSI spricht hier eine deutliche Sprache: Die Angriffe auf den Public Sector nehmen zu und sie werden zunehmend professioneller. Auch kleine Kommunen sind betroffen. Denn für Cyberkriminelle sind alle Behörden potenzielle Ziele. So kommt es beispielsweise bei Ransomware-Attacken per Mail, deren Ziel das Erpressen von Lösegeld ist, zu regelrechten Angriffswellen.

MIT KLAREN ROLLEN UND EINGESPIELTER ROUTINE

Was also braucht es, um ein funktionierendes Notfallmanagement aufzustellen? Im Ernstfall muss klar sein, wer was wann innerhalb der Verwaltung tun muss und mit welchen externen Stellen wie zusammengearbeitet wird. Das setzt eindeutige Rollendefinitionen und einen eingeübten Ablauf voraus. Nur so können Mitarbeiterinnen und Mitarbeiter ruhig und richtig handeln. Festgelegte Informationsketten geben Orientierung. Die Komm.ONE stellt ihren Kunden und Mitgliedern beispielsweise einen Notfall-Leitfaden für Sicherheitsvorfälle zur Verfügung, der den grundlegenden Ablauf aufzeigt.

Dieser hat eine einfache Struktur. Zuerst müssen die IT-Verantwortlichen der Kommune schnellstmöglich benachrichtigt werden. Sie informieren dann sofort alle zuständigen Behörden, in Baden-Württemberg beispielsweise die Cybersicherheitsagentur BW und das Landeskriminalamt, sowie Partner und IT-Dienstleister. Hierbei müssen Meldepflichten für Sicherheitsvorfälle und Verdachtsfälle beachtet werden. Das sind zum Beispiel Fälle von Datenverschlüsselungen, Identitätsdiebstahl, Manipulation von Daten, Diebstahl oder Verlust von Endgeräten und erfolgreiche Phishing-Angriffe.

24/7 MOBIL UND FLEXIBEL IM EINSATZ

Externe Profis können dann von der ersten Stunde an unterstützen. Ideal ist ein Cyber Security Incident Response Team – kurz CSIRT – mit einer 24/7-Bereitschaft. Ein CSIRT nimmt in enger Zusammenarbeit mit den Behörden eine Einschätzung der Situation vor und ergreift erste Sofortmaßnahmen, wie beispielsweise die Abtrennung betroffener Computer von der IT-Infrastruktur. Es kann auch bei der Aufklärung, Rekonstruktion und Dokumentation, also der gesamten Forensik, mitwirken. Während das CSIRT vorwiegend im virtuellen Raum tätig ist, unterstützt das Mobile Incident Response Team, MIRT abgekürzt,

Gemeinsam stark für Cybersicherheit
Mehr zum Thema erfahren Sie beim Cybersecurity-Tag der Komm.ONE am 25.06.2026 in Nürtingen.

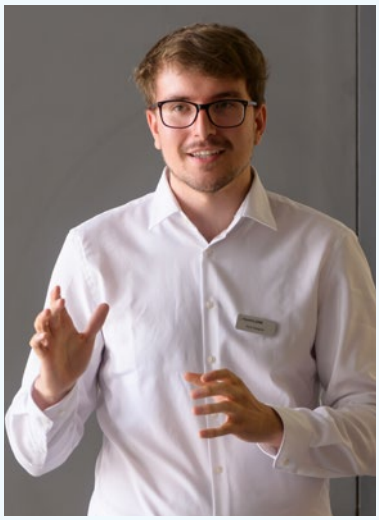
direkt vor Ort. Es baut eine neue rechtssichere, datenschutzkonforme IT-Umgebung auf und stellt Hardware, also beispielsweise Notfall-Laptops und Headsets sowie Software zur Verfügung. So bringt das MIRT die wichtigsten Fachverfahren und kommunalen Dienstleistungen erneut zum Laufen, die Kommune wird wieder handlungsfähig. Beide Incident Response Teams arbeiten eng zusammen.

PRIORITÄTEN IN DER PRAXIS

Vorrausetzung für eine effiziente Unterstützung durch externe Profis ist, dass in der Kommune eine Prioritätenliste vorliegt, die idealweise auch mit Fristen hinterlegt ist. Konkret geht es darum, dass im Vorfeld eine Rangliste erstellt wird, die festlegt, welche Dienste und Fachverfahren nach einem Sicherheitsvorfall am schnellsten wieder zur Verfügung stehen müssen. Das kann beispielsweise die Auszahlung von Sozialleistungen an Bürgerinnen und Bürger sein. Die Fristen geben an, wie lange die Dienstleistung ausgesetzt werden kann, ohne dass sich schwerwiegende Folgen ergeben. „Diese Planung und Priorisierung spart im Notfall viel wertvolle Zeit. Sie ist daher ein essenzieller Teil Ihrer Vorbereitung“, sagt Tom Kasper, Teamleiter Fachservice Informationssicherheit der Komm.ONE.

Ebenso gilt es, vorab den Bedarf an Hardware für den Notfall zu ermitteln. Der Wunsch nach einer optimalen Ausstattung sollte hier nicht den Blick auf das Mögliche verstellen. „Gehen Sie mit Pragmatismus an die Planung. Hundert oder mehr Laptops für Notfälle vorzuhalten, ist in der Regel nicht machbar. Das ist aber auch nicht erforderlich, denn Ihre Handlungsfähigkeit beginnt mit dem ersten Laptop, mit dem Sie in einer neuen sicheren Umgebung wieder Ihre wichtigsten Dienstleistungen anbieten können“, sagt Komm.ONE-Experte Tom Kasper.

Plan einmal erstellt und für immer auf der sicheren Seite – das trifft nicht auf das Notfallmanagement zu. Es muss fortlaufend geprüft werden. Drei Kriterien helfen bei der Qualitäts-Kontrolle. Zum einen sollte das Notfallmanagement auf die eigene Kommune abgestimmt sein. Ein guter Plan zeichnet sich dadurch aus, dass Rollen und deren Inhaber, Übergangspunkte und Informationsketten klar definiert und bekannt sind. Der zweite Aspekt ist die Awareness der Mitarbeiterinnen und Mitarbeiter. Je höher die Aufmerksamkeit, desto eher und schneller werden Angriffe entdeckt. Denn Cyberattacken beginnen häufig mit Phishing-Versuchen, deren Ziel es ist, an persönliche Zugangsdaten zu gelangen. Regelmäßige Sensibilisierungsmaßnahmen sind daher sinnvoll. Das dritte Qualitätsmerkmal schließlich ist das Training. „Üben, üben, üben“ lautet die Devise. Im Ernstfall muss jeder sofort wissen, was zu tun ist. Erfüllt das Notfallmanagement diese Kriterien, ist eine Kommune gut gewappnet. Check für die Cybersicherheit.



Tom Kasper,
Teamleiter Fachservice Informationssicherheit der Komm.ONE
tom.kasper@komm.one
ism-service@komm.one
www.komm.one

Komm.ONE

ITEBO

Notfallarbeitsplatz und Notfall-Kommunikationskoffer als Bausteine moderner kommunaler Resilienz

HANDLUNGSFÄHIG BLEIBEN IM KRISENFALL

Cyberangriffe auf Kommunen häufen sich. Gleichzeitig nehmen klassische Krisenszenarien wie Starkregen, Hochwasser, langanhaltende Stromausfälle oder Blitzeinschläge zu. Für Städte und Gemeinden bedeutet dies eine neue Realität: Verwaltungsarbeit, politische Entscheidungsfähigkeit und Bürgerkommunikation müssen auch dann gewährleistet bleiben, wenn zentrale IT-Systeme, Netze oder einzelne Gebäude nicht mehr verfügbar sind.

Ein IT-Ausfall ist dabei nicht nur ein organisatorisches Problem. Er kann schnell zu einem Sicherheits-, Reputations- und Vertrauensproblem werden. Die zentrale Frage lautet daher nicht mehr, ob eine Krise eintritt, sondern wie gut eine Kommune darauf vorbereitet ist.

KOMMUNIKATION ALS KRITISCHER ERFOLGSFAKTOR

In jeder Krisensituation ist funktionierende Kommunikation der Schlüssel zur Handlungsfähigkeit. Verwaltungsleitung, Krisenstäbe, Fachämter, externe Stellen und politische Gremien müssen Informationen austauschen, Entscheidungen abstimmen und Maßnahmen koordinieren können – unabhängig davon, ob die reguläre IT-Infrastruktur verfügbar ist.

DER NOTFALL-KOMMUNIKATIONS-KOFFER: SOFORT EINSATZBEREIT

Ein zentraler Baustein für die akute Krisenkommunikation ist der Notfall-Kommunikationskoffer. Diese mobile Lösung stellt sicher, dass Telefonie, Videokonferenzen und Chat-Funktionen auch dann zur Verfügung stehen, wenn die reguläre Kommunikationsinfrastruktur ausfällt.

Als IT-Service-Provider für den kommunalen Sektor setzt ITEBO auf den innovaphone Notfallkoffer. Dieser kann kurzfristig in Betrieb genommen werden und ermöglicht:

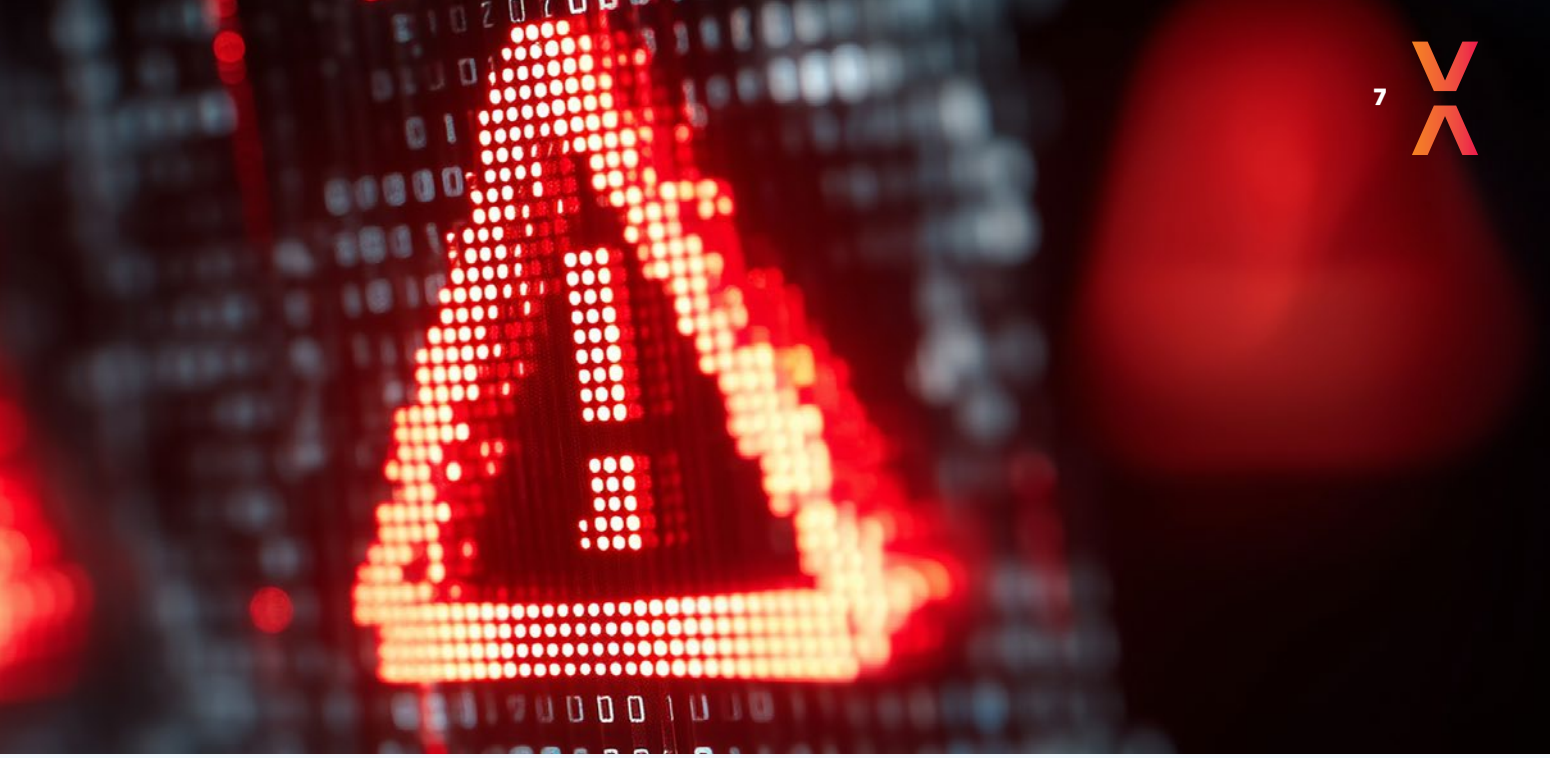
- Telefonische Erreichbarkeit für Krisenstäbe
- Videokonferenzen zur Lagebesprechung
- Sichere Chat-Kommunikation

Der Notfallkoffer funktioniert unabhängig von bestehenden Systemen und kann als Service bezogen werden. Er eignet sich insbesondere für die erste Phase einer Krise, in der schnelle Abstimmung und klare Kommunikationswege entscheidend sind.

DER NOTFALLARBEITSPLATZ: VERWALTUNG BLEIBT ARBEITSFÄHIG

Über die reine Kommunikation hinaus stellt sich die entscheidende Frage, wie die Verwaltung inhaltlich weiterarbeiten kann. Hier setzt der Notfallarbeitsplatz an – eine Lösung, die Kommunen auch bei schwerwiegenden Cybervorfällen oder Systemausfällen handlungsfähig hält.

Der Notfallarbeitsplatz ist ein digital souveräner, unabhängiger Arbeitsplatz, der speziell für Krisensituationen konzipiert wurde.



DIGITALE SOUVERÄNITÄT ALS SICHERHEITSPRINZIP

Der Notfallarbeitsplatz der ITEBO basiert auf einer eigenen, in Deutschland betriebenen Infrastruktur in den Rechenzentren der ITEBO. Die Lösung ist:

- Microsoft-unabhängig
- Browserbasiert und endgeräteunabhängig
- Klar getrennt von der produktiven IT-Umgebung

So bleibt die Kommune selbst dann arbeitsfähig, wenn lokale Systeme kompromittiert oder isoliert wurden. Mitarbeitende können von nahezu jedem Endgerät aus arbeiten, ohne dass lokale Daten gespeichert werden.

FUNKTIONSUMFANG FÜR DEN ERNSTFALL

Ein moderner Notfallarbeitsplatz stellt alle wesentlichen Werkzeuge für den Verwaltungsbetrieb bereit:

- Textverarbeitung und Tabellenkalkulation
- Zentrale Fileablage mit Rollen- und Berechtigungskonzept
- E-Mail Funktionalität
- Videotelefonie und Zusammenarbeitstools
- Kanban-Boards zur Aufgabensteuerung

Darüber hinaus ist ein Zusammenspiel mit Unified-Communications-Systemen möglich. Auch eine Integration mit dem Notfall-Kommunikationskoffer kann vorgesehen werden, sodass Kommunikation und Arbeitsumgebung nahtlos ineinandergreifen.

Weitere Informationen unter
www.itebo.de//it-services/kommunikation-und-austausch/notfallarbeitsplatz

NOTFALLDOMAIN UND NACHHALTIGE SICHERHEIT

Ein häufig unterschätzter Aspekt von Cybervorfällen ist die Phase nach dem eigentlichen Angriff. Um erneute Risiken zu vermeiden, stellt ITEBO für den Notfallbetrieb eine separate Notfalldomain bereit. Diese trennt den Krisenbetrieb konsequent vom regulären Betrieb und ermöglicht technisch sichere Kommunikation.

TECHNIK ALLEIN REICHT NICHT: BCM IST PFLICHT

Technische Lösungen entfalten ihre Wirkung nur im Zusammenspiel mit einem funktionierenden Business-Continuity-Management (BCM). Jede Kommune sollte über ein eigenes, regelmäßig geprüftes Notfallkonzept verfügen. Dieses sollte unter anderem enthalten:

- Aktuelle Notfall- und Ansprechpartnerlisten
- Klar definierte Rollen und Zuständigkeiten
- Entscheidungs- und Eskalationswege
- Regelmäßige Tests und Übungen

FAZIT: VORSORGE IST FÜHRUNGSAUFGABE

Cybersicherheit und Krisenvorsorge sind heute Chefsache. Bürgermeisterinnen und Bürgermeister tragen die Verantwortung dafür, dass ihre Kommune auch in Ausnahmesituationen handlungsfähig bleibt. Der kombinierte Einsatz von Notfall-Kommunikationskoffer und Notfallarbeitsplatz bietet hierfür eine praxisnahe und kommunalspezifische Lösung.

Wer heute investiert, schützt nicht nur IT-Systeme, sondern sichert Vertrauen, Stabilität und die Funktionsfähigkeit der kommunalen Verwaltung – genau dann, wenn es am wichtigsten ist.

IT Verbund Landsberg

Wie die KI-Werkstatt des IT-Verbunds Mehrwert für Bürgerinnen und Bürger schafft

CYBERSICHERHEIT NEU GEDACHT

Die Digitalisierung der Verwaltung schreitet mit hoher Geschwindigkeit voran, ebenso wie die Bedrohungen im Cyberraum. Künstliche Intelligenz (KI) spielt dabei auf beiden Seiten eine zentrale Rolle: Sie beschleunigt Angriffe und erhöht das Risiko für eine Sicherheitslücke, eröffnet aber zugleich neue Chancen für sichere und bürgernahe Verwaltungsservices.

SICHERE DIGITALISIERUNG – SPÜRBARER NUTZEN FÜR DIE BEVÖLKERUNG

Mit der KI-Werkstatt verfolgt der IT-Verbund ein klares Ziel: Mehr Sicherheit, bessere Services und spürbare Entlastung für Bürgerinnen und Bürger in unserem Landkreis Landsberg am Lech. Praxisnahe Schulungen und Workshops richten sich insbesondere an Verwaltungsmitarbeitende, Bürgerinnen und Bürger profitieren davon unmittelbar:

- Schnellere Bearbeitungszeiten durch effizientere Prozesse
- Verlässliche und sichere digitale Angebote, die Datenschutz und Transparenz gewährleisten
- Bessere Erreichbarkeit der Verwaltung, unabhängig von Öffnungszeiten
- Weniger Fehlerquellen, weil Mitarbeitende Risiken frühzeitig erkennen und vermeiden

Weitere Informationen unter
www.itvll.de

DER MENSCH ALS SCHLÜSSEL FÜR VERTRAUEN UND SICHERHEIT

Dabei stärkt die KI-Werkstatt gezielt den Faktor Mensch. Denn: Gut geschulte Mitarbeitende erkennen Risiken, handeln souverän und sorgen dafür, dass digitale Verwaltungsangebote verlässlich funktionieren. So wird Cybersicherheit nicht zum Hindernis, sondern zur Voraussetzung für moderne, serviceorientierte Verwaltung.

Für die Bürgerinnen und Bürger in unserem Landkreis bedeutet das vor allem eines: mehr Vertrauen in digitale Services ihrer Kommunen – vom Online-Antrag bis zur digitalen Terminvergabe.

KI VERSTEHEN

Die KI-Werkstatt versteht sich als langfristiges Angebot für den gesamten Landkreis Landsberg am Lech. In enger Zusammenarbeit mit den Kommunen und externen Partnern wird erarbeitet,

- wo KI sinnvoll eingesetzt werden kann,
- welche rechtlichen und sicherheitsrelevanten Rahmenbedingungen gelten,
- und wie digitale Lösungen konkret den Alltag von Verwaltung und Bevölkerung verbessern.

Mit der KI-Werkstatt schafft der IT-Verbund Landsberg KU die Grundlage dafür, dass digitale Innovationen im Landkreis bürgernah, sicher und zukunftsorientiert umgesetzt werden – heute und in Zukunft.

„Die KI-Werkstatt ist ein Ort des Lernens und des Austauschs. Unser Anspruch ist es, KI so einzusetzen, dass Bürgerinnen und Bürger spürbar profitieren: durch sichere, verständliche und verlässliche digitale Verwaltungsangebote. Cybersicherheit, Kompetenzaufbau und Servicequalität gehören für uns untrennbar zusammen."

Hannah Rösch, Vorstandsreferentin des IT-Verbunds

Digitalisierungspartner der Öffentlichen Verwaltung

GOVERNIKUS

Ob elektronische Identitäten, rechtssichere Kommunikation oder vertrauenswürdige Daten Governikus entwickelt seit über 25 Jahren Lösungen, die im Alltag von Verwaltung, Justiz, Wirtschaft, der Gesundheitsbranche sowie Bürger:innen unverzichtbar geworden sind. Mit unseren Produkten und Projekten stehen wir als IT-Sicherheitsexperte für digitale Souveränität, höchste Sicherheitsstandards und praxisnahe Umsetzbarkeit.

Jetzt informieren!

20 eGo-MV Jahre

eGo-MV
ZWECKVERBAND ELEKTRONISCHE VERWALTUNG IN MECKLENBURG-VORPOMMERN

Zusammenhalt schafft Sicherheit

Der Zweckverband eGo-MV bündelt kommunale Kompetenzen für Informationssicherheit, Netzwerksicherheit und digitale Resilienz in Mecklenburg-Vorpommern.

Leistungen für die kommunale Gemeinschaft

- Gemeinsame Informationssicherheitsbeauftragte
- Aufbau und Weiterentwicklung eines ISMS
- Richtlinien, Konzepte und Sensibilisierung
- Mitarbeiterschulungen
- Auditierungen zur Einhaltung der Anschlussbedingungen ans Landesdatennetz
- Penetrationstests und Schwachstellenanalysen

www.ego-mv.de

DAS ISMS ALS GRUNDLAGE DER CYBERSICHERHEIT

Täglich hören wir von Cyberangriffen – auf Firmen, öffentliche Institutionen und Kommunen. Die Forderungen nach besserem Schutz werden eindringlicher. Siehe die EU-Richtlinie Network and Information Security 2 (NIS-2), die einen wichtigen Schritt in Richtung verpflichtende Cybersicherheit für alle Institutionen darstellt. Ein gelebtes Informationssicherheitsmanagementsystem (ISMS) – zentrale Dienstleistung im Portfolio der OWL-IT – bildet eine optimale Grundlage, um deren Anforderungen gerecht zu werden und mehr Sicherheit zu verankern.

Ob und in welcher Form die Kommunalverwaltungen von NIS-2 betroffen sind, müssen nun die Bundesländer entscheiden. Fallen Behörden und Unternehmen darunter, müssen diverse Pflichten wie die Selbsteinordnung, Registrierung sowie Meldepflichten erfüllt sein. Außerdem müssen Anforderungen in den Bereichen Risikomanagement, Awareness, Schulungen, Verschlüsselung und Authentifizierung sowie Business-Continuity-Management und Krisenmanagement umgesetzt werden.

Viele dieser Aspekte sind bereits durch ein ISMS gewährleistet. Für Institutionen, die über ein etabliertes ISMS mit nachweislicher Umsetzung (Zertifizierung) verfügen, verringert sich der Aufwand bei der Durchführung der NIS-2-Anforderungen entscheidend.

OWL-IT FÜR STARKEN SCHUTZ

Die NIS-2 zeigt, wie wichtig es ist, einen funktionierenden Sicherheitsprozess zu haben. Seit ihrer Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz im Jahr 2007 als erster kommunaler IT-Dienstleister in Deutschland liegt ein zentraler Schwerpunkt der OWL-IT auf dem Schutz von Infrastruktur und Daten für ihre Verbandskommunen und dem eigenen Rechenzentrum.

Die Ostwestfalen-Lippe-IT (OWL-IT) bietet umfangreiche Lösungen im Bereich der Cybersicherheit an.
www.owl-it.de

Mit Fokus auf IT-Grundschutz erstreckt sich das Angebot von der Beratung über Schulungen bis zur Einführung und Weiterführung eines ISMS.

DIE VORTEILE EINES ISMS NACH IT-GRUNDSCHUTZ SIND INSBESONDERE

- interne Rechtssicherheit,
- Kontinuität der Arbeitsabläufe und
- definierte Eskalationswege.

Des weiteren macht die **lückenlose Dokumentation** eine schnelle Anpassung der Sicherheitsmaßnahmen bei Umstrukturierungen möglich. Außerdem sorgt sie für ein gesteigertes **internes Sicherheitsbewusstsein** der Beschäftigten und **schnellere Reaktionszeiten.**

Für die Einführung eines ISMS gibt es mehrere gangbare Wege, sei es auf Basis von WiBa (Weg in die Basisabsicherung), von IT-Grundschutz-Profilen oder von definierten Vorgehensweisen im BSI-Standard 200-2.

Die NIS-2 sollte als Chance gesehen werden, die eigene Institution zukunftssicher im Bereich der Cybersicherheit und Informationssicherheit aufzustellen, auch wenn der Geltungsbereich zunächst noch nicht festgelegt ist.

CYBER DEFENSE: IM SPIEL BLEIBEN

In einer komplexen, vulnerablen Welt gilt es, digitale Sicherheit als „unendliches Spiel“ zu begreifen und den Fokus auf Ausdauer statt auf Sieg zu legen. Ziel es muss sein, langfristige Sicherheit durch Anpassung, ständiges Lernen und Zusammenarbeit zu erreichen.

Denn Cyber Defense ist kein Wettkampf mit klaren Regeln. Sie ist ein fortlaufender Prozess, in dem sich Bedrohungen, Technologien und Angreifer ständig verändern. Künstliche Intelligenz spielt auf Angreifer-Seite eine immer größere Rolle.

Verteidiger sind daher gefordert, Organisationen so aufzustellen, dass sie dauerhaft widerstandsfähig bleiben, sich weiterentwickeln und im Spiel bleiben können.

BEDROHUNGSABWEHR RUND UM DIE UHR

Um Bedrohungen abzuwehren, arbeitet die regio iT mit dem Ansatz „Threat Intelligence“ – auf Deutsch etwa „Bedrohungsaufklärung“. Dabei geht es nicht nur um die Abwehr von akuten Cyber-Attacken, sondern vor allem um Prävention.

Das Computer Emergency Response Team „KomCERT“ kümmert sich rund um die Uhr um Cyber-Attacken, die Netze und Daten der regio iT sowie die ihrer Kunden bedrohen. Denn schließlich sind Angreifer oft in anderen Zeitzonen unterwegs.

Im Krisenfall geht es darum, schnellstmöglich und im Idealfall ohne Verluste wieder handlungsfähig zu werden. Sind Daten erst einmal verschlüsselt, ist die Wiederherstellung meist aufwändig. Dann sind Know-how, Technik und Ressourcen eine wertvolle Hilfe – auch dabei unterstützen die Experten der regio iT.

Sie möchten Ihre IT langfristig widerstandsfähiger machen? Sprechen Sie uns an.
Mehr Informationen zum KomCERT der regio iT:
www.regioit.de/unternehmen/komcert

MASSNAHMEN NACHHALTIGER CYBERSICHERHEIT:

- **„Just Cause“** – Ein übergeordnetes Ziel: Schutz von Daten, Vertrauen und digitaler Infrastruktur
- **Wachsamkeit statt Reaktion** – Proaktive Sicherheitskultur etablieren
- **Flexibilität statt Starrheit** – Systeme müssen sich an neue Bedrohungen anpassen können
- **Kooperation statt Konkurrenz** – Austausch zwischen Unternehmen, Behörden und Forschung
- **Lernen als Dauerzustand** – Schulungen, Simulationen, Lessons Learned

„Der wahre Wettbewerb besteht nicht gegen andere, sondern gegen die eigene Fähigkeit sich weiterzuentwickeln. Organisationen mit einer unendlichen Denkweise investieren in Anpassungsfähigkeit und langfristige Stabilität.“

Dr. Stefan Wolf,
Geschäftsführer
regio iT

Prosoz

Cybersicherheit in der kommunalen Verwaltung

AWARENESS ALS UNTER-SCHÄTZTER ERFOLGSFAKTOR

Cybersicherheit ist für Kommunen längst zu einem zentralen Handlungsfeld geworden. Mit der fortschreitenden Digitalisierung und der Verarbeitung sensibler Bürgerdaten steigen die Anforderungen an Schutz, Verfügbarkeit und Vertrauen in IT-Systeme stetig. Zugleich verschärfen Fachkräftemangel, Modernisierungsdruck sowie Cloud- und SaaS-Modelle die Bedingungen für den kommunalen IT-Betrieb. Digitalisierung ist dabei keine Option mehr, sondern eine notwendige Voraussetzung für eine leistungsfähige Verwaltung. Trotz aller technologischer Veränderungen bleibt der Mensch ein entscheidender Faktor für Sicherheit und Resilienz digitaler Verwaltungsstrukturen.

Awareness beschreibt das Bewusstsein und die Handlungssicherheit von Mitarbeitenden im Umgang mit IT-Systemen, Daten und potenziellen Bedrohungen. Auch modernste Cloud- und SaaS-Infrastruktur bieten keinen vollständigen Schutz, wenn Mitarbeitende nicht ausreichend für IT-Sicherheitsrisiken sensibilisiert sind. Gerade in Kommunen, in denen viele Beschäftigte täglich mit sensiblen Bürgerdaten arbeiten, spielt das Sicherheitsbewusstsein eine entscheidende Rolle für die Resilienz der gesamten IT-Infrastruktur. Bei Prosoz leben wir diesen Gedanken und involvieren die Mitarbeitenden durch verschiedene Maßnahmen, damit am Ende alle Daten geschützt bleiben.

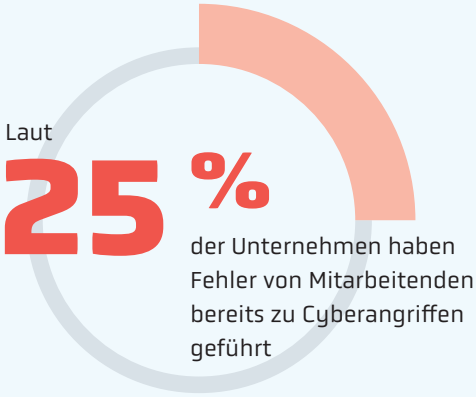
FAKTOR MENSCH ALS EINFALLSTOR

Bedrohungen wie Phishing, Social Engineering oder der unachtsame Umgang mit Zugangsdaten zielen typischerweise auf den „Faktor Mensch“ ab. Mehrere deutsche Studien und Umfragen belegen, dass der menschliche Faktor eine zentrale Rolle bei Cyberangriffen und IT-Sicherheitsvorfällen spielt. Trotz zunehmender technischer Schutzmaßnahmen bleiben mangelnde Sensibilisierung, fehlende Schulungen und Fehlverhalten von Mitarbeitenden eine der häufigsten Ursachen für Sicherheitsvorfälle.

Eine Studie von G DATA (2025) zeigt, dass über 60 Prozent der Beschäftigten in Deutschland keine regelmäßigen IT-Sicherheits- oder Awareness-Schulungen erhalten. Dies betrifft insbesondere Branchen mit hoher Datenverantwortung, darunter auch der öffentliche Sektor. Die Ergebnisse verdeutlichen, dass Security Awareness in vielen Organisationen nicht systematisch verankert ist, obwohl Mitarbeitende täglich mit sensiblen Informationen arbeiten.

Auch andere Untersuchungen bestätigen die Relevanz dieses Problems. Laut einer Trend-Micro-Studie berichten 25 Prozent der befragten deutschen Unternehmen, dass Fehler von Mitarbeitenden bereits zu erfolgreichen Cyberangriffen geführt haben. Phishing und Social Engineering zählen dabei zu den häufigsten Angriffsmethoden, da sie gezielt menschliche Schwächen ausnutzen.

Diese Befunde belegen, dass erfolgreiche Angriffe weniger auf reine technische Schwachstellen als vielmehr auf menschliche Verhaltensmuster zurückgehen und unterstreichen, dass Awareness kein einmaliges Schulungsthema, sondern ein fortlaufender Prozess sein muss.



AWARENESS IN BEZUG AUF CLOUD- UND SAAS-MODELLE BEDEUTET KONKRET:

- Verständnis für neue Verantwortlichkeiten: Auch wenn Betrieb, Wartung und Teile der IT-Sicherheit beim SaaS-Anbieter liegen, bleiben Kommunen verantwortlich für den sicheren Umgang mit Daten, Rollen- und Berechtigungen sowie organisatorische Maßnahmen.
- Regelmäßige Schulungen und Sensibilisierung: Mitarbeitende müssen fortlaufend über Bedrohungen, sichere Arbeitsweisen und Meldewege informiert werden.
- Klare Prozesse und Sicherheitskultur: Awareness wirkt nur, wenn Sicherheitsregeln verständlich, praxistauglich und im Arbeitsalltag verankert sind. Eine offene Fehlerkultur hilft, Vorfälle frühzeitig zu erkennen.
- Unterstützung durch zentrale Strukturen: Einheitliche Standards und Leitlinien auf Bundesebene fördern einheitliche Sicherheitsniveaus und entlasten Kommunen.

FAZIT ZUR AWARENESS

Die Transformation der kommunalen IT hin zu Cloud- und SaaS-Modellen reduziert technische Risiken erheblich, ersetzt jedoch nicht die Notwendigkeit einer starken Sicherheitskultur. Awareness ergänzt technische Schutzmaßnahmen und organisatorische Vorgaben und bildet die dritte, oft unterschätzte Säule der IT-Sicherheit. Nur wenn Technik, Prozesse und Menschen gleichermaßen berücksichtigt werden, kann die digitale Verwaltung langfristig sicher, vertrauenswürdig und resilient gestaltet werden.

Tobias Kippert,
Informationssicherheitsbeauftragter
bei der PROSOZ Herten GmbH

KDO
Kommunal. Digital.

KDO | KOMPAKT

IMPULSE FÜR DIE MODERNE VERWALTUNG

Die KDO-Akademie erweitert ihr Portfolio und bietet nun ein vielfältiges Angebot an praxisnahen Veranstaltungsformaten für Mitarbeitende in Kommunen. Themen wie Digitalisierung, Cybersecurity, New Work und Microsoft Office ergänzen fachverfahrensbezogene Angebote und liefern konkrete Impulse für den Arbeitsalltag.

Besuchen Sie uns auf:

Jetzt den QR-Code scannen und alle KDO-Kompakt Impulsvorträge entdecken:

Cyberservices der govdigital

IT-NOTFALLÜBUNGEN FÜR MITGLIEDER UND TRÄGER

Die govdigital stellt ihren Mitgliedern sowie deren Trägern den Service „IT-Notfallübungen“ zur Verfügung. Ziel ist, die Handlungsfähigkeit bei Cyberangriffen, Systemausfällen oder Fehlkonfigurationen zu stärken. Denn im Ernstfall entscheidet nicht nur Technik, sondern ob Rollen, Entscheidungswege und Kommunikation funktionieren.

Der Service wird in Form eines Rahmenvertrages von der Firma Deloitte erbracht und unterstützt den gesamten Übungszyklus: Auswahl geeigneter Szenarien, Vorbereitung, moderierte Durchführung und strukturierte Nachbereitung. Inhalte orientieren sich an typischen Lagen wie Ransomware, Ausfall zentraler Infrastruktur- oder Cloud-Services, Störungen von Fachverfahren, Netzwerk-/Identitätsproblemen oder Ausfällen bei Dienstleistern. Je nach Reifegrad sind Tabletop-Übungen, Planspiele oder erweiterte Formate möglich.

Wesentlich ist der Nutzen aus der Übung: Erkenntnisse werden transparent dokumentiert, Lessons Learned abgeleitet und in einen priorisierten Maßnahmenplan überführt, mit konkreten Verbesserungen für Organisation, Technik, Dokumentation und Kommunikation.

Uwe Schwarz
CISO/Leiter Cybersicherheit
govdigital eG
cybersicherheit@govdigital.de

Weitere Cyberservices der govdigital

MALWARE INFORMATION SERVICE (MISP): BEDROHUNGSINFORMATION OPERATIONALISIEREN

- Abwehrmaßnahmen übergreifend ermitteln und teilen
- Angriffserkennung und Angriffsvermeidung
- Effizienzsteigerung durch geteilte Ressourcen
- Hohe Datenqualität und hohe Relevanz

BUSINESS CONTINUITY MANAGEMENT (BCM): VORBEREITUNG AUF DEN NOTFALL

- 3-tägiges Seminar
- Anwendung des BSI-Standards 200-4 auf kommunale Bedarfe
- Trainiert die verlässliche Absicherung des Verwaltungsbetriebs
- Aufbau eines Business Continuity Management Systems – BCMS für die kommunale Verwaltung

Weitere Informationen unter
govdigital.de/themen-leistungen/cybersicherheit

VITAKO-MITGLIEDER BIETEN SCHUTZ FÜR DIE KOMMUNEN – QUER DURCH DEUTSCHLAND

IMPRESSUM

Herausgeber:
Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e. V.
Charlottenstr. 65
10117 Berlin
Tel. 030/20 63 15 60
E-Mail: aktuell@vitako.de
www.vitako.de

V. i. S. d. P.: Lars Hoppmann, geschäftsführender Vorstand von VITAKO

Redaktion, Gestaltung:
Köster Kommunikation