

SO SCHÜTZEN SIE SICH RICHTIG:

Verlässliche

IT-Sicherheit für

Kommunen



IT-Sicherheit - wer nicht investiert, verliert

Ist die IT Ihrer Kommune auf dem aktuellsten Stand?

Schadprogramme wie Viren, Phishing und Ransomware bedrohen die digitale Infrastruktur und somit die Arbeitsfähigkeit der Verwaltung. Cyber-Kriminelle verschaffen sich ganz einfach Zugriff auf relevante Daten und Systeme, verschlüsseln diese oder legen sie komplett lahm. Erst gegen Zahlung eines Lösegeldes ziehen sich die Kriminellen zurück und geben den Zugriff auf Programme und Daten wieder frei.

Doch wussten Sie, dass schon der Angriff über eine einzelne Komponente zum Ausfall der gesamten IT führen kann?

Der am schlechtesten gesicherte PC wird so zur verlockenden Einladung in die gesamte Verwaltungs-IT. Klassische präventive Maßnahmen wie der Virenschutz allein sind längst nicht mehr ausreichend. Deshalb ist es für Kommunen höchste Zeit, neue Wege zu gehen, um ihre Verwaltungen bestmöglich gegen Cyber-Attacken zu schützen. Ohne eine funktionierende IT-Infrastruktur und das erforderliche Know-how sind sie im Ernstfall nicht mehr arbeitsfähig.

Die fortschreitende Verwaltungsdigitalisierung und immer komplexer werdende Systeme erhöhen auch die Anforderungen an die IT- und Digital-Kompetenz von Kommunen. Zusätzlich wird der gravierende Fachkräftemangel zu einem echten Problem: Ein professionelles IT-Sicherheitsmanagement mit sehr gut ausgebildeten Spezialist*innen und marktüblichen IT-Gehältern ist jedoch mit den Tarifvertragskonstellationen in öffentlichen Verwaltungen nur schwer vereinbar.





Was bedeutet IT-Sicherheit heute?

- Lage: Die Komplexität der IT und deren potenzielle Bedrohungen nehmen ständig zu und erfordern entsprechende Infrastrukturen.
- Herausforderung: Der sichere und verfügbare Betrieb von IT ist für eine reibungslos funktionierende Verwaltung überlebenswichtig – alle erforderlichen Sicherheits-Features – Software, Virens Scanner, Firewalls uvm. – sind ständig und schnell zu aktualisieren.
- Lösung: Handeln Sie proaktiv und sorgen Sie vor – setzen Sie für den IT-Betrieb auf einen starken Partner mit jahrelanger Expertise in IT und Fachverfahren.

Vor welchen Aufgaben steht die Kommune von morgen?

- Immer mehr Verwaltungsdienstleistungen werden digital.
- Hinzu kommen neue Anforderungen durch mobiles Arbeiten, neue Arbeitsformen, Erreichbarkeiten und steigende Erwartungshaltungen von Bürger*innen an digitale Verwaltungsservices.
- Technologien entwickeln sich rasant und sind geprägt von neuen Möglichkeiten wie künstlicher Intelligenz und schnellen Innovationszyklen.

Wie sollten Sie dem Fachkräftemangel begegnen?

- Digitalisierung und Automatisierung sind nötig, um die Herausforderungen zukünftiger Verwaltungsaufgaben, steigender Cyber-Kriminalität und dem weiterhin zunehmenden Fachkräftemangel zu meistern.
- Vertrauen Sie auf professionelle Unterstützung und geben Sie Betriebsaufgaben an Profis ab, um zusätzliche Freiräume für Mitarbeitende zu schaffen, die sich wieder auf ihre Kernaufgaben konzentrieren können.
- Innovative Lösungen von IT-Expert*innen helfen nicht nur, kommunale IT-Systeme sicherer zu machen, sie kompensieren auch (etwas) den Mangel an eigenen IT-Fachkräften.

Ein Cyber-Angriff kann jederzeit kommen - er wartet nicht auf Stellenbesetzungen und beschränkt sich nicht auf die Arbeits- und Öffnungszeiten der Verwaltung.

202,7 Mrd. €

Schäden durch Cyberkriminalität 2022 in Deutschland

Quelle: Statista Research Department, Dezember 2022

136 %

mehr Cyber-Angriffe in den vergangenen Jahren

Quelle: BKA, Bundeslagebild Cybercrime 2021



IT-Standort Deutschland: So unsicher ist es bei uns



116,6

Mio. Schadprogramme mehr

Die Anzahl der Schadprogramme stieg 2022 gefährlich an.

Quelle: BSI, Bericht zur Lage der IT-Sicherheit in Deutschland 2022



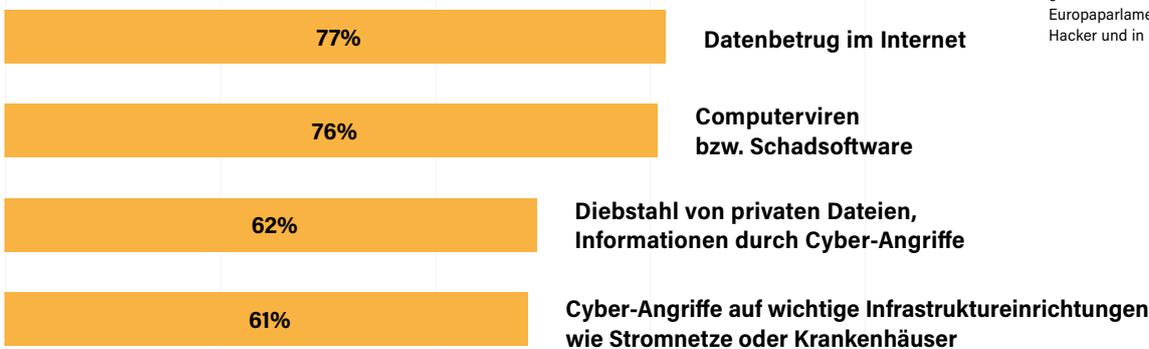
97%

der dt. Behörden erkennen die Gefahr

Die Kommunen sehen in der Abwehr von Cyber-Attacken und dem Schutz von Daten die Top-Herausforderungen der kommenden Jahre.

Quelle: Branchenkompass Public Sector 2022

Die größten Cyber-Risiken für die Menschen in Deutschland*



* Befragt wurden 404 Führungskräfte aus Unternehmen sowie 104 Abgeordnete aus Bund, Ländern und Europaparlament zu Risiken durch Hacker und in sozialen Medien.

Quelle: deloitte, Cyber Security Report 2021



207

Tage Katastrophenfall

Cyber-Attacke löst 1. digitalen Katastrophenfall in einer deutschen Kommune aus. Bürgernahe Dienstleistungen wie Elterngeld oder Kfz-Zulassungen konnten nicht erbracht werden.

Quelle: BSI, Bericht zur Lage der IT-Sicherheit in Deutschland 2022



100%

der Behörden wollen mehr Sicherheit

Die Kommunen halten eine stabile und flexible IT-Infrastruktur als entscheidend für eine hohe Resilienz.

Quelle: Branchenkompass Public Sector 2022



Wussten Sie eigentlich...?

Dataport.kommunal ist der kommunale Teil von Dataport und kann auf die Erfahrungen und Kompetenzen des IT-Dienstleisters zurückgreifen und so Mehrwert für Kommunen schaffen. Während Dataport länderübergreifend agiert, ist dataport.kommunal auf die Bedürfnisse von Kommunen spezialisiert. Kommunen in Schleswig-Holstein sind über den ITVSH außerdem Träger von Dataport – und so auch von dataport.kommunal. Sie verfügen damit über einen eigenen IT-Dienstleister und können dataport.kommunal vergabefrei beauftragen.

Kund*innen stehen für uns im Mittelpunkt. Bei Fragen oder Problemen erreichen Sie uns schnell und unkompliziert – wir helfen Ihnen prompt. Unsere Preise, Leistungen und Servicelevel vereinbaren wir verlässlich und maßgeschneidert in Verträgen mit Ihnen. Über eine halbjährliche Kundenversammlung stehen wir mit Ihnen im stetigen partnerschaftlichen Austausch zu Produkten, Entwicklungen und Ihren Anforderungen.

Interview

„Cyber-Angriffe sind eine permanente Herausforderung.“



Uwe Störmer ist Abteilungsleiter im Bereich Kommunale Infrastrukturen beim IT-Dienstleister [dataport.kommunal](https://www.dataport-kommunal.de). Das Unternehmen begleitet im Norden Regionen und Kommunen bei der Digitalisierung. Er kennt sich also nicht nur aus mit Cyber-Angriffen und Datendiebstahl, sondern weiß auch, was man dagegen tun kann.

Was ist aus Ihrer Sicht der wichtigste Faktor, um sich erfolgreich gegen digitale Angriffe zu wehren?

Um aktuellen Cyber-Bedrohungen erfolgreich zu begegnen, ist der entscheidende Faktor ganz klar Schnelligkeit: Ob es um die Beseitigung von Sicherheitslücken und dem Schutz vor bekannten Schadrissen geht oder um die Behebung und Eingrenzung im Schadensfall, die dann ebenfalls nicht nur schnell, sondern auch wirksam erfolgen müssen. Dazu gehört, sich mit den Bedrohungsarten auszukennen und entsprechende Vorkehrungen zu treffen. Um potenzielle Angriffe erfolgreich abzuwehren, müssen sich Kommunen für den Wettlauf mit stetig wechselnden Bedrohungen rüsten.

Viele Anliegen, wie etwa Zahlungen von Wohngeld oder die Anmeldung eines Autos, stehen online für die Bürger*innen bereit. Es werden stetig mehr. Wie können solche wichtigen Funktionen vor gezielten Angriffen geschützt werden?

Die beste Entscheidung ist die Nutzung gemeinsamer Online-Infrastrukturen aller Kommunen und des Landes sowie das Outsourcing des IT-Betriebs an Expert*innen, die einen hohen Sicherheitsstandard gewährleisten können. Dienstleister wie Dataport kennen sich mit professionellem Betrieb und einem effizienten Sicherheitsmanagement aus und schützen jede Verwaltung.

Ist damit zu rechnen, dass die Cyber-Kriminalität auch wieder zurückgehen wird?

Leider nicht. Die Welt wird immer digitaler. Und obwohl uns die Technologie Fortschritt bringt, birgt sie auch neue Risiken. Cyber-

Angriffe sind, das muss uns klar sein, in Zukunft eine permanente Herausforderung. Als spezialisierter IT-Dienstleister prüfen wir deshalb regelmäßig unser Sicherheitsniveau, etwa mit Hilfe von simulierten Cyber-Angriffen. So ermitteln wir Schwachstellen und können gezielt darauf reagieren. Hinzu kommt, dass wir im regelmäßigen Austausch mit Branchenvertreter*innen und Verbänden stehen. So bleiben wir auf dem aktuellsten Stand und können unseren Kund*innen die Sicherheit bieten, die wir ihnen versprechen.

Sie möchten mehr erfahren oder haben Fragen? Ich helfe Ihnen gern weiter.

Telefon:
0431 3295-6768

E-Mail:
uwe.stoermer@dataport-kommunal.de

Die richtige Checkliste für jedes IT-Problem

Was macht eine IT-Infrastruktur nicht nur sicher, sondern auch effizient? Und wie können Sie dafür sorgen, dass die von Ihnen in Auftrag gegebenen Maßnahmen auch zukünftige Cyber-Attacken abwehren? Diesen Fragen gehen wir nachfolgend auf den Grund und erklären Ihnen Stück für Stück, worauf es wirklich ankommt.

Wie Sie Ihre IT-Systeme für die Zukunft wappnen:

- Ausfallsicherheit:** Achten Sie auf ein System, für das Ausfallsicherheit an erster Stelle steht. Wenden Sie sich an Expert*innen mit erprobten Hardware- und Softwarelösungen, die extern in einem sicheren Rechenzentrum gehostet werden.
- Datensicherheit:** Suchen Sie sich IT-Expert*innen, die Ihren hohen Ansprüchen gerecht werden und bewahren Sie sich Ihre digitale Souveränität.
- Entlastung und Transparenz:** Behalten Sie Ihre Kosten im Blick. Vertraglich vereinbarte Leistungsentgelte und Servicequalität geben Planungssicherheit und schützen vor bösen finanziellen Überraschungen. Bauen Sie auf eine Lösung, die Sie nicht nur von aufwendigen und teuren Aufgaben im IT-Bereich entlastet.
- So individuell wie Ihre Kommune:** Idealerweise vertrauen Sie auf eine Lösung, die an Ihre Bedürfnisse anpassbar ist. So stellen Sie sicher, dass Sie nur das erhalten, was Sie wirklich brauchen.



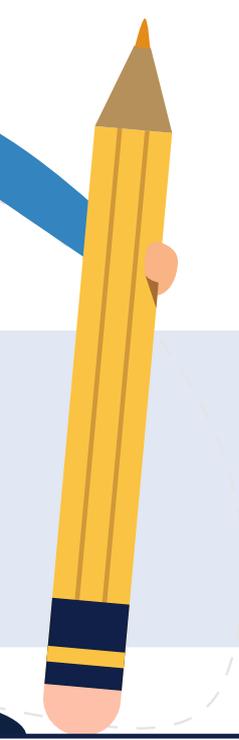


dITBetrieb – die optimale Lösung für Ihr IT-System

Ganz gleich, um welches eingesetzte Fachverfahren es sich handelt, mit dITBetrieb bekommt jede Kommune eine individuelle auf sie angepasste Lösung. dITBetrieb ist modular aufgebaut und umfasst immer genau das, was Kommunen brauchen und wollen: von der Beschaffung und Einrichtung von Endgeräten über den sicheren Betrieb von Fachanwendungen bis hin zum Virenschutz. Darüber hinaus ist auch das vollständige Auslagern des IT-Betriebes möglich – bei transparenten und planbaren Kosten und höchster IT-Kompetenz.

Was bietet dITBetrieb?

- Betrieb von Fachanwendungen – immer auf dem aktuellen Stand bezogen auf den IT-Datenschutz und der IT-Datensicherheit – im BSI-zertifizierten Rechenzentrum
- Beschaffung und Betreuung von Arbeitsplätzen sowie Zubehör
- Beschaffung und Betreuung der Netzwerktechnik
- Entlastung um IT-technische und administrative Tätigkeiten
- Individuell anpassbar: Von der einzelnen IT-Komponente und Dienstleistung bis zum vollständigen Outsourcing



Erfahren Sie jetzt mehr zum sicheren und flexiblen IT-Betrieb aus einer Hand!

Wir helfen gern. Einfach den QR-Code scannen:





Dataport.kommunal begleitet Kommunen und Regionen bei allen Digitalisierungsvorhaben und unterstützt seine Kund*innen dabei, die Attraktivität und Wirtschaftskraft für Menschen und Unternehmen vor Ort zu steigern. Dafür arbeitet der IT-Dienstleister für die kommunale öffentliche Hand mit Anbietern aus der Region zusammen, fördert kommunale IT-Kooperationen und kombiniert das notwendige Fachwissen mit kommunaler Verwaltungskompetenz.

Dataport.kommunal ist eine Marke von Dataport und baut seine Leistungsfähigkeit auf den Kompetenzen und Angeboten des IT-Dienstleisters auf. Träger der Anstalt öffentlichen Rechts sind die Länder Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Sachsen-Anhalt und Schleswig-Holstein sowie der kommunale „IT-Verbund Schleswig-Holstein“.

Dataport hat 5.500 Mitarbeiterinnen und Mitarbeiter und erzielte 2023 einen Umsatz von 1,36 Milliarden Euro.

Mehr Informationen unter
www.dataport-kommunal.de



dataport.kommunal

Anstalt des öffentlichen Rechts
Altenholzer Straße 10-14
24161 Altenholz

Telefon: 0431 3295-0

Telefax: 0431 3295-6410

E-Mail: info@dataport-kommunal.de