Magazin für Kommunen Ausgabe 3/2025

EnBW

KommPlus

Schwerpunktausgabe
Cybersicherheit

Das Schweigen der Server

Wie sich Kommunen gegen Cyberangriffe wehren können

Wenn der Himmel liefert …

… schießt er manchmal auch übers Ziel hinaus. Sommergewitter über Offshore-Windkraftanlagen wie hier über dem Baufeld des EnBW-Windparks He Dreiht kommen häufig vor. Die Blitzschutzsysteme der Anlagen sind jedoch dafür ausgelegt, den Blitzstrom sicher und schadlos abzuleiten.

Schwerpunkt Cybersicherheit

In dieser Ausgabe widmen wir uns ab Seite 4 ausschließlich dem Thema Cybersicherheit, das durch die zunehmende Bedrohungslage immer wichtiger wird. Allerdings gibt es wirksame Wege, sich zu schützen und möglichen Gefahren vorzubeugen.

Energiewissen tanken

Sie möchten tiefer in kommunale Energiethemen eintauchen oder Ihr Wissen auffrischen? In der EnBW Energiewelt decken leicht verständliche Videos von „Erneuerbare Energien“ über „Kommunale Wärmeplanung“ bis hin zu „Wasserversorgung“ ein breites Spektrum ab. Registrieren Sie sich einfach auf www.enbw-energiewelt.de oder über den QR-Code.

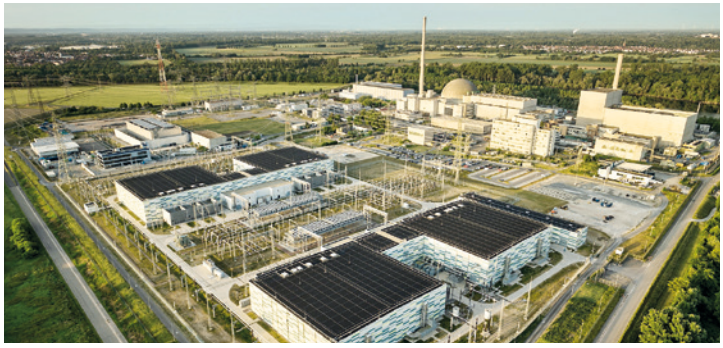
Sie sind gefragt!

In der KommPlus wollen wir komplexes Energiewissen verständlich aufbereiten und mit echten Beispielen zeigen, wie Kommunen Energiefragen angehen. Was denken Sie:

Welche Rolle können Kommunen dabei spielen, die Energiewende greifbarer zu machen? Welche Herausforderungen begegnen Ihnen bei der Umsetzung von Klimaschutzmaßnahmen? Welche erfolgreichen Projekte oder Ansätze aus Ihrer Kommune könnten als Vorbild für andere Regionen dienen, um die Energiewende zu fördern?

Schreiben Sie uns an redaktion@enbw.com.

Philippsburg: Standort im Wandel



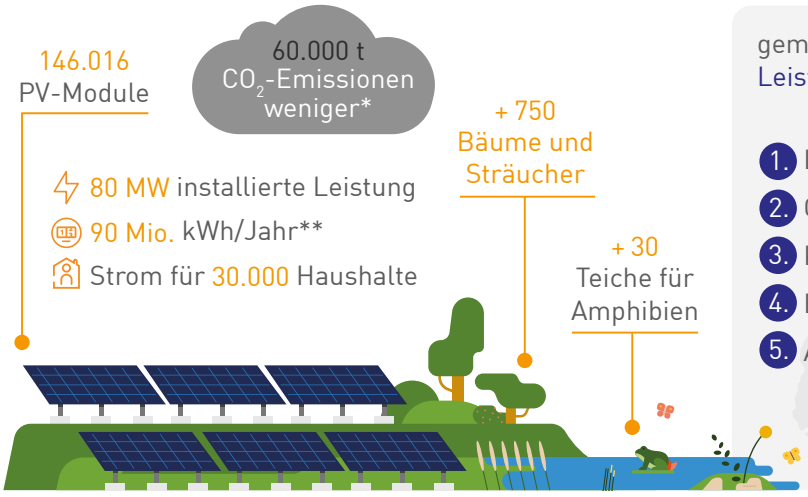
„Philippsburg ist seit einem halben Jahrhundert einer der wichtigsten Energiestandorte Deutschlands – und diese Rolle soll unsere Gemeinde auch in Zukunft behalten: als Ankerpunkt und riesiger Speicher für nachhaltige Stromerzeugung“, begrüßt Bürgermeister Stefan Martus die Pläne für Deutschlands größten Batteriespeicher.

Die EnBW hat dem Gemeinderat ein zukunftsträchtiges Projektvorhaben vorgestellt. Auf dem Gelände des Energieparks Philippsburg soll einer der größten Batteriespeicher Deutschlands entstehen: Mit 400 Megawatt Leistung und 800 Megawattstunden Kapazität könnte er den Strombedarf von rund 100.000 Haushalten decken sowie überschüssigen Wind- oder Solarstrom speichern und ins Netz einspeisen.

Der Wandel der deutschen Energieversorgung zeigt sich am Standort Philippsburg besonders deutlich: Seit 2017 und 2020 werden die beiden Kernkraftwerksblöcke zurückgebaut. Auf einem benachbarten Abschnitt hat die TransnetBW ein Gleichstrom-Umspannwerk errichtet, das als Teil der neuen Gleichstromverbindung ULTRANET Windstrom aus Norddeutschland nach Süddeutschland bringen soll.

Baden-Württembergs größter Solarpark

EnBW Solarpark Langenenslingen



* ggü. konventioneller Erzeugung; ** Prognose

Die 5 größten Solarparks in BW

gemessen an der Leistung (in MWp)

1.	Langenenslingen	80,3
2.	Gundelsheim	58,0
3.	Külsheim	29,7
4.	Emmingen-Liptingen	17,3
5.	Allmendingen	12,9

Zielscheibe Kommune

Die Zahl der Cyberangriffe auf Städte und Gemeinden steigt. Dabei wenden die Täter immer geschicktere Methoden an. Doch viele Kommunen scheinen in Sachen IT-Sicherheit überfordert. Ohne Hilfe von außen sind sie oft wehrlos.

Cyberangriffe gehören längst zum Alltag von Behörden und Kommunen. Mit einfachen Maßnahmen können sich Städte und Gemeinden jedoch effektiv schützen.

Den 24. April 2025 wird die Stadt Ellwangen wohl nicht so schnell vergessen. An diesem Tag treten zunächst Unregelmäßigkeiten in der IT auf. Dann werden die Verantwortlichen nervös. Denn schnell steht fest: Ursache ist ein Cyberangriff. Besonders betroffen ist das Netzwerk der staatlichen Schulen. Die Kommune lässt das auffällige System sofort abstellen und bildet einen Krisenstab. Es wird Monate dauern, bis die Schulen wieder Zugriff auf alle ihre Programme haben.

Die Stadt hat Glück im Unglück. Sensible Daten werden nicht gestohlen und offensichtlich ist sie auch kein Opfer organisierter Kriminalität geworden. Die Polizei verdächtigt kurz darauf einen ehemaligen Schüler, die Tat begangen zu haben. „So glimpflich gehen solche Attacken aber selten aus", sagt Experte Robin Dold, der für die EnBW Cyber Security GmbH (ECS) Kommunen in Sachen IT-Sicherheit berät.

Angriffe auf die IT gehören mittlerweile zum Alltag in der Behördenwelt. Nach einer Befragung des Deutschen Städte- und Gemeindebunds war von 2023 bis 2024 rund ein Viertel aller deutschen Kommunen Ziel einer Cyberattacke. Knapp die Hälfte der Fälle betraf große Städte. Doch kleinere Gemeinden standen ebenfalls im Fokus. Von den Kommunen mit weniger als 10.000 Einwohnern wurden 17 Prozent attackiert.

Die Zahl der Cyberangriffe steigt. Und neben Firmen stehen auch Kommunen immer häufiger im Visier der Kriminellen. Allein in Baden-Württemberg hat sich die Zahl der Delikte seit 2016 verdoppelt. Das ist nur die Spitze des Eisbergs, denn die meisten Opfer bemerken den Angriff nicht oder verschweigen ihn. Laut Bundeskriminalamt liegen neun von zehn Taten im Dunkelfeld.

IT-Wildwuchs erhöht das Risiko

Hacker sehen Kommunen zunehmend als lohnendes Angriffsziel. Viele kommunale IT-Systeme sind veraltet oder die Sicherheitsmaßnahmen sind unzureichend. Manche Verwaltung ist überfordert, wenn es darum geht, Eintrittspforten für Cyberkriminelle zu identifizieren. In kleineren Gemeinden fehlt das Geld für Fachpersonal. Außerdem besitzen zahlreiche Kommunen keine einheitliche IT-Landschaft. „Schulen oder Kindergärten arbeiten oft mit anderen Systemen als das Rathaus am Ort", sagt Cyberexperte Dold.

Hinzu kommt, dass die rechtlichen Vorgaben für Kommunen schwer zu durchblicken sind. Es gibt Leitlinien wie das IT-Grundschutzprofil und andere Sicherheitsdokumentationen. Insgesamt sollten Städte und Gemeinden rund 600 Anforderungen erfüllen. „Ohne fachliche Hilfe lässt sich das kaum umsetzen", sagt Dold. Zwar handelt es sich um Empfehlungen – sie zu ignorieren, könnte aber im schlimmsten Fall als grob fahrlässig angesehen werden.

Cybergrüße aus Moskau

Dabei können sich Kommunen mit einfachen Maßnahmen schon gegen eine Reihe von Angriffen schützen. Denn es sind nicht immer geniale Cybergangster, die sich durch die digitalen Schranken arbeiten. Mit Software, die im Internet bestellt werden kann, verschaffen sie sich Zugang zu Systemen, die sie kompromittieren wollen.

In vielen Fällen passiert das über E-Mail-Anhänge, die unvorsichtige Mitarbeitende öffnen. Klicken sie auf den Link, geht der Ärger los. Das IT-System wird blockiert, manchmal fordern die Täter Geld, um die Sperre aufzuheben. In anderen Fällen wollen sie der Kommune einfach nur schaden. Laut Verfassungsschutz verüben Staaten wie Russland, China, Iran oder Nordkorea Cyberangriffe in Deutschland, um kritische Infrastruktur wie Energieversorgung, Wasserwirtschaft oder Verkehrssysteme zu stören.
Eine Vielzahl der Attacken lässt sich mit einfachen Mitteln vermeiden. „Schutz vor Hackern fängt bei den Mitarbeitenden an", sagt Dold. Um sensibler

auf Gefahren zu reagieren, müssen sie geschult werden. Wie erkenne ich verdächtige Nachrichten? Wie vermeide ich es, einem dubiosen Anrufer auf den Leim zu gehen? Und wie muss ich Passwörter wählen, damit sie wirklich schützen? Sind solche und ähnliche Fragen geklärt, haben es Hacker schon schwerer.

Vorsicht vor dem Pizzamann

Natürlich versuchen es die Täter mit immer neuen Tricks. Beispiel: Ein als Pizzabote verkleideter Hacker verschafft sich Zugang zu einem Unternehmen. In seiner Tasche trägt er aber keine Speisen, sondern einen USB-Stick mit Schadsoftware. An einem unbewachten Arbeitsplatz steckt er ihn in den Rechner. Klingt wie im Thriller, ist aber so passiert.

Die Stimme des Chefs am Telefon perfekt nachzuahmen, ist im Zeitalter der künstlichen Intelligenz eine weitere Masche von Cybergangstern. So überzeugen sie ihr Gegenüber, Geld zu überweisen oder Zugangsdaten preiszugeben. Deshalb sollte auch in Behörden der Grundsatz gelten: Keine vertraulichen Informationen per Telefon oder Video.

Vor Cyberangriffen ist niemand geschützt. Selbst die Vorsichtigsten sind mal unachtsam. Ist der Schaden da, muss die IT allerdings sofort handeln. Sie braucht einen Notfallplan, der genau regelt, wer zu verständigen ist und was in welcher Reihenfolge unternommen werden soll. Dieser Plan muss immer greifbar sein – natürlich nicht als digitale Datei auf dem Server, sondern auf einer einfachen externen Festplatte oder, wie früher ausgedruckt und abgeheftet.

EnBW Cyber Security: Angebot für Kommunen

- Phishing-Simulation und weitere Sensibilisierung
- Cyber-Rating – Risiken umgehend bewerten.
- Interne Schwachstellensuche mit automatisierten Scans
- Penetrationstests – wie verwundbar ist die IT?
- Sicherheitsüberwachung für IT und Prozessleittechnik
- Informationssicherheitsberatung (z. B. für die Umsetzung des Grundschutzprofils)
- Notfallmanagement – Planen und Üben

Weitere Informationen finden Sie unter www.enbw.com/cyber-security

Cyberabwehr: Erste Hilfe für Städte und Gemeinden

Um Kommunen vor IT-Gangstern zu schützen, arbeitet die EnBW mit der Cybersicherheitsagentur Baden-Württemberg (CSBW) zusammen. Deren Präsidentin Nicole Matthöfer erklärt die Aufgaben ihrer Behörde.

Wie sieht Ihre Zusammenarbeit mit der EnBW aus?
Matthöfer: Das Land Baden-Württemberg und die EnBW arbeiten seit 2020 zusammen. Ziel ist die Verbesserung der Cybersicherheit von Kommunen, Wirtschaft und Gesellschaft sowie Stadtwerke und das Gesundheitswesen. Als CSBW tragen wir dazu bei, indem wir unter anderem die Aus- und Fortbildung von Cybersicherheitsfachleuten stärken, zum Beispiel durch die gemeinsame Betreuung von Studierenden der Dualen Hochschule Baden-Württemberg. Einmal im Quartal tauschen sich die Kooperationspartner zu aktuellen Themen und Projekten der Vereinbarung aus.

Wo sehen Sie die größten Sicherheitslücken der Kommunen?
Matthöfer: Bei insgesamt 1.101 Kommunen im Land greifen allgemeingültige Aussagen zu kurz. Je nach Größe und Ausstattung haben wir es mit unterschiedlichen Risiken zu tun. Grundsätzlich spielen technische Sicherheitslücken eine große Rolle. Kriminelle scannen die IT-Infrastrukturen großflächig und automatisiert auf Schwachstellen ab. Und natürlich ist auch der Faktor Mensch eine wichtige Größe.

Wie helfen Sie Kommunen bei einem Sicherheitsvorfall?
Matthöfer: Wir bieten Kommunen eine Cyber-Ersthilfe an und sind rund um die Uhr erreichbar. Meldungen von Betroffenen werten wir umgehend aus. Bewahrheitet sich ein Verdachtsfall, unterstützen wir bei der Analyse und guten Bewältigung. Auch können wir helfen, Systeme wiederherzustellen.

Schwachstelle Mensch

Mit ausgefallenen Methoden testet die Firma whitemacs, ob Behörden und Firmen ausreichend gegen Cyberattacken geschützt sind. Dabei liegt der Schwerpunkt auf menschlichen Verhaltensweisen.

Die Geschäftsidee entstand, als Tobias Weiß bei einem Autozulieferer in Baden-Württemberg arbeitete. „Dort sind mir die webbased Trainings zum Thema IT-Sicherheit ziemlich auf die Nerven gegangen“, sagt der gelernte Software-Entwickler. Er und seine Kollegen hätten die Aufgaben so schnell wie möglich durchgeklickt, der Lerneffekt sei gleich null gewesen. „Ich dachte mir, das können wir besser.“

Im Oktober 2023 gründete er seine Firma whitemacs. Ihr Ziel ist es, das Bewusstsein für IT-Sicherheit in Unternehmen und Behörden zu schulen. Die Mitarbeitenden müssen keine Online-Aufgaben lösen, sondern reagieren auf simulierte Cyberattacken. Die beginnen meistens mit einer Phishing-E-Mail. Das Kunstwort Phishing steht für „Password Fishing“, also den Versuch, Menschen so zu manipulieren, dass sie sensible Daten preisgeben.

Mittlerweile haben Cyberkriminelle einen ganzen Werkzeugkasten an Tricks, um an sensible Informationen zu kommen. „Das geht weit über den Versand von E-Mails mit Schadsoftware hinaus“, sagt Weiß. Ein Beispiel ist die Stadt Dülmen in Nordrhein-Westfalen. Die Kommune hatte zwei neue Feuerwehrautos in Auftrag gegeben, die Betrüger wussten offensichtlich davon, spionierten den Hersteller aus und schickten eine täuschend echte Rechnung. Die Stadt zahlte 400.000 Euro. Das Geld ging auf ein Konto im Ausland – und ist futsch.

Menschen zu manipulieren, um digitale Daten zu erbeuten, kann auf vielfache Weise geschehen. Durch einen Anruf, einen geschriebenen Brief oder eine Person, die den Pförtner überlistet und sich Zugang zu den Büros verschafft. Rund 90 Prozent alle Cyberattacken beginnen mit dieser Art von Täuschung. Sie werden unter dem Begriff „Social Engineering“ zusammengefasst.

Whitemacs hat es sich zur Aufgabe gemacht, bestimmte Einfallstore zu erproben, damit die überlisteten Personen aus den Vorfällen lernen können. „Wir nutzen den Schrecken des Augenblicks, wenn jemand merkt, dass er einen Fehler begangen hat“,

Langwierige E-Learnings zu IT-Sicherheit bringen nichts, ist Tobias Weiß überzeugt. Er setzt stattdessen auf realistische Simulationen, um Menschen für die Gefahren von Social Engineering zu sensibilisieren.

sagt der 32-jährige Gründer. Auch die EnBW Cyber Security arbeitet mit whitemacs zusammen, um ihre Kunden zu sensibilisieren.

Dabei versuchen Weiß und sein neunköpfiges Team, auf den Kenntnisstand jedes Einzelnen einzugehen. „Wer noch nicht viel Erfahrung hat, bekommt eine einfache Phishing-E-Mail zugesandt.“ Wird der Anhang geöffnet, erscheint eine Warnung, die darauf hinweist, dass dies eine Cyberattacke hätte sein können. Dann werden die wichtigsten Sicherheitsmaßnahmen erklärt.

Wer schon mehr Erfahrung hat, muss sich anspruchsvolleren Prüfungen unterziehen. An einen Kunden versandte Weiß vor Kurzem eine manipulierte Rechnung per Fax. Die Forderung wurde prompt bezahlt. Das Geld landete auf einem Konto von whitemacs – und wurde natürlich zurücküberwiesen.

Wenn die Polizei ins Netz geht

Auf den Anstieg digitaler Attacken stellt sich auch die Kripo ein. In Baden-Württemberg unterstützt die Zentrale Ansprechstelle Cybercrime (ZAC) Behörden und Unternehmen, um Angriffe abzuwehren. Torsten Seeberg vom Landeskriminalamt (LKA) spricht über Vorsorge, Ermittlungen und Festnahmen.

Wie reagieren Sie, wenn Unternehmen oder Behörden einen Cyberangriff melden?
Seeberg: Wir lassen uns den Sachverhalt schildern und bewerten ihn. Daraus leiten wir eine Gefahrenprognose ab und helfen den Betroffenen, den Schaden zu minimieren. In vielen Fällen ist das dank unserer langen Erfahrung ohne aufwendige forensische Untersuchung möglich. Vor einiger Zeit teilte uns zum Beispiel ein Geschädigter mit, dass die Täter immer noch auf sein Netzwerk zugreifen und seine Wiederherstellungsmaßnahmen sabotieren. Den Schilderungen konnten wir entnehmen, dass es im System noch eine offene Hintertür gab. Als sie geschlossen wurde, gaben die Täter auf.

Was müssen Kommunen tun, wenn sie Ziel einer Cyberattacke werden?
Seeberg: Sie sollten sich sofort bei uns melden. Wir empfehlen Maßnahmen und nehmen die Strafanzeige auf. Allerdings beraten wir auch präventiv, damit es gar nicht erst zu einem Angriff kommt. Unser Angebot kommt bei Behörden und Firmen gut an. Im Jahr 2023 zählten wir 1.395 Kontaktaufnahmen, Beratungen und Anzeigeneingänge, 2024 waren es bereits 1.745.

Zur Person

Torsten Seeberg begann seine Karriere 1997 mit der klassischen Polizeiausbildung. Nach einigen Jahren als Mitglied der Motorradstaffel zwang ihn ein Unfall zu einer längeren Pause. Anschließend absolvierte er ein Studium an der Hochschule für Polizei und wechselte er zum Landeskriminalamt. Er ist seit 2017 in der ZAC tätig.

Rücken Sie auch mal mit einem ganzen Team aus, um einen Cyberangriff aufzuklären?
Seeberg: Das machen wir etwa, wenn kritische Infrastruktur betroffen ist. Dann gehen wir mit unseren Fachleuten direkt in die Rechenzentren. Wichtig für die Betroffenen: Wir beschlagnahmen die kompromittierten Systeme in der Regel nicht, denn wir wissen, dass Unternehmen und Behörden schnell wieder arbeitsfähig sein müssen. Die Polizei soll hier nicht als Störfaktor wahrgenommen werden.

Aber wie klären Sie die Vorfälle dann auf?
Seeberg: Wir machen ein Abbild des Systems und speichern es auf unseren eigenen Modulen. Diese Kopien werten wir in der Dienststelle aus, um Spuren von den Tätern zu finden und Ansätze für die Ermittlung zu entwickeln. Ein wesentliches Ziel besteht darin, den Angriffsweg nachzuvollziehen und die Sicherheitslücke zu erkennen. Das System wiederherzustellen, ist Aufgabe der Betroffenen. Wir unterstützen sie aber gern dabei, künftig Angriffe zu verhindern und teilen erkannte Schwachstellen mit.

Wie oft gelingt es Ihnen, Kriminelle zu identifizieren?
Seeberg: Grundsätzlich sind Cybercrime-Verfahren herausfordernd. Internationale Bezüge kommen häufig vor und dabei handelt es sich oft um Länder, in denen sich die Kooperation mit Behörden schwierig gestaltet. Auch die Täter nutzen alle Möglichkeiten, ihr Handeln zu verschleiern. Aber immerhin liegt die Aufklärungsquote von Cybercrime-Straftatbeständen in Baden-Württemberg bei 36 Prozent. Vergangenes Jahr ist es uns beispielsweise gelungen, nach mehrjährigen Ermittlungen ein führendes Bandenmitglied einer cyberkriminellen Gruppierung im europäischen Ausland festzunehmen. Jetzt läuft das Verfahren vor dem Landgericht Stuttgart.

Viele Cybercrime-Attacken ließen sich vermeiden, wenn geeignete Vorkehrungen getroffen würden, weiß Torsten Seeberg. Ob für große Städte, kleine Kommunen, Konzerne oder Familienunternehmen: Die grundsätzlichen Handlungsempfehlungen unterscheiden sich nicht wesentlich und sind öffentlich zugänglich.

Welche Art von Cyberangriffen stellen Sie am häufigsten fest?

Seeberg: In den meisten Fällen sind finanzielle Interessen ausschlaggebend. Täter schleusen zum Beispiel Schadsoftware ein und blockieren den Systemzugriff so lange, bis Lösegeld fließt. Manche täuschen auch eine andere Identität vor und senden per E-Mail gefälschte Rechnungen mit Bitte um Zahlung auf ein von ihnen kontrolliertes Konto. Diese Variante lässt sich mit einfachen Mitteln abwehren – zum Beispiel, indem Mitarbeitende vor einer hohen Überweisung zum Telefon greifen und sich die Kontonummer bestätigen lassen.

Wie stellt sich die Polizei auf die Zunahme der Cyberkriminalität ein?

Seeberg: Die Fallzahlen steigen steil an. Deshalb rüsten wir personell auf. In unseren Fachstellen sind 400 Mitarbeiter tätig, darunter Experten für Kriminalistik, Informatik oder Mathematik. In Baden-Württemberg steht extern ausgebildeten Fachleuten die Sonderlaufbahn Cyberkriminalität offen. Sie arbeiten beim LKA sowie bei den 13 Cybercrime-Fachstellen im Land. Baden-Württemberg ist wegen seiner vielen Unternehmen ein beliebtes Angriffsziel. Und die Täter brauchen heute nicht mal mehr IT-Fachkenntnisse. Sie setzen zugekaufte Software als Angriffswerkzeuge ein oder verschaffen sich von anderen Tätergruppen unbemerkt eingerichtete Zugänge in IT-Netzwerke oder E-Mail-Konten. Dafür gibt es mittlerweile einen eigenen Fachbegriff: „Cybercrime-as-a-service“.

Handlungsempfehlungen des LKA gegen Ransomware finden Sie unter https://lka.polizei-bw.de/handlungsempfehlungen-gegen-ransomware

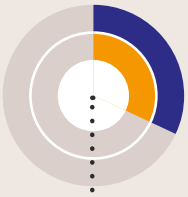
Haltet den Datendieb!

Spionage, Sabotage, Datenraub: Cyberangriffe zielen verstärkt auf öffentliche Verwaltung und kritische Infrastruktur. Ein Blick auf die Lage – und wo die größten Gefahren für Kommunen lauern.

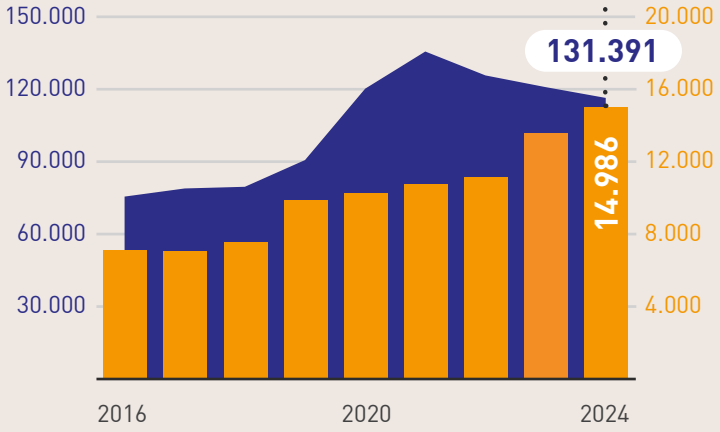
Die Lage

Cyberkriminalitätsdelikte

Deutschland Baden-Württemberg



Aufklärungsquote 2024
je 32 %

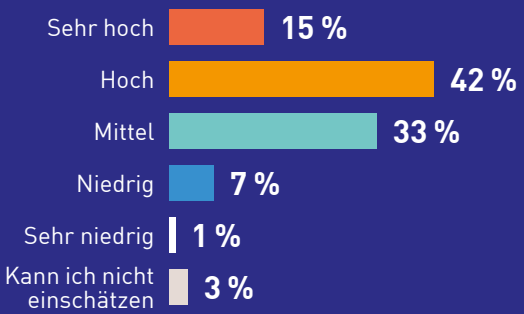


Doch: **90 % aller Taten** liegen laut BKA im Dunkelfeld und werden gar nicht erfasst.

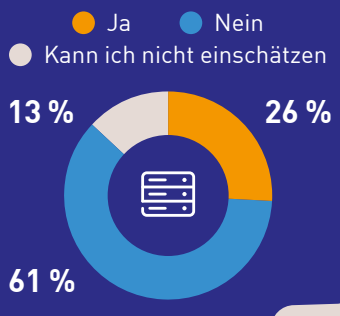
Quelle: BKA, Sicherheitsbericht Baden-Württemberg 2024

Die Perspektive der Kommunen

Wie hoch schätzen Sie die Bedrohung für Ihre Kommune durch Cyberangriffe ein?

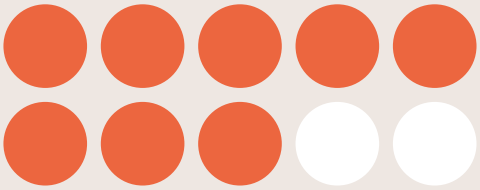


War Ihre Kommune in den vergangenen zwei Jahren Ziel eines Cyberangriffs?



Quelle: Zukunftsradar Digitale Kommune 2024, n = 1.067

Die Opfer

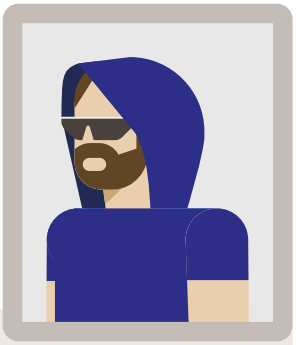


8 von 10
Unternehmen waren innerhalb eines Jahres betroffen.

Öffentliche Verwaltungen und kritische Infrastruktur (KRITIS) waren 2024 europaweit verstärkt Ziel von Cyberangriffen:

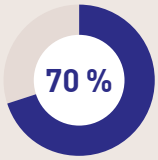
+ 31 % ggü. Vorjahr

Quelle: Bitkom Research, Myra Security

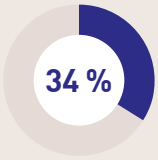


Die Täter

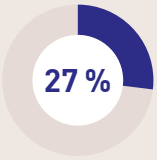
Auch Beschäftigte sind ein Risiko!



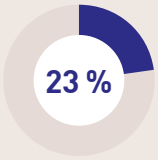
Organisierte Kriminalität/Banden



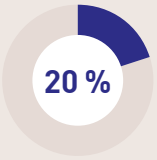
Privatpersonen



Vorsätzlich handelnde (ehemalige) Beschäftigte



Unabsichtlich handelnde (ehemalige) Beschäftigte



Ausländische Nachrichtendienste

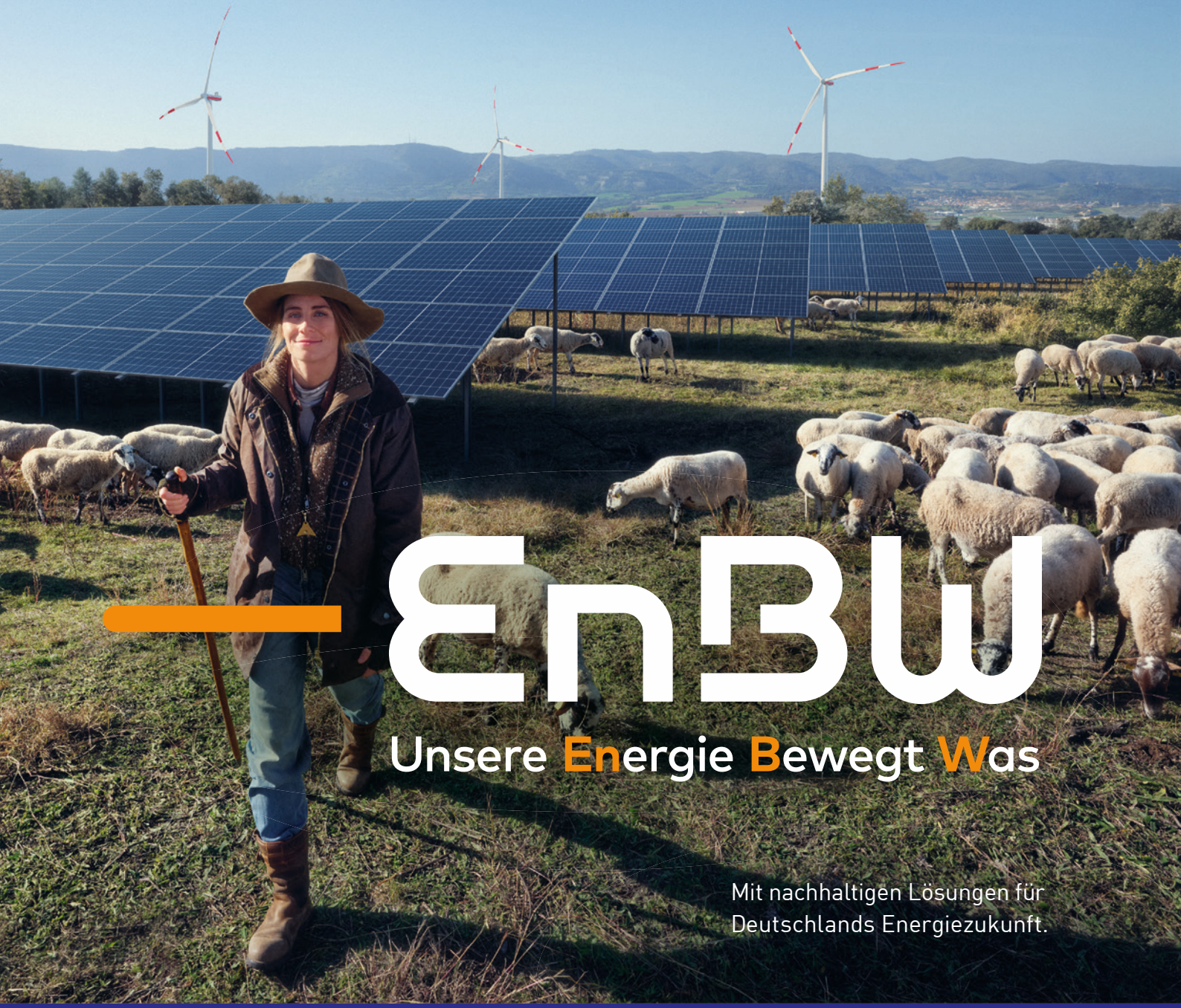
n = 1.003 befragte Unternehmen, Mehrfachnennung möglich, 2024
Quelle: Bitkom Research

Die Tricks

Top-5-Einfallstore für Cyberattacken in der öffentlichen Verwaltung laut BSI und BKA:

1. Phishing- und Spam-Mails (53 % Spam-Quote!)
2. Nicht gepatchte Software-Schwachstellen
3. Gestohlene und schwache Zugangsdaten und Passwörter
4. Kompromittierung durch IT- und andere Dienstleister
5. Ransomware (2 – 3 Fälle/Tag, Infektion meist via Punkte 1 und 2)

Quelle: BKA, Bundesamt für Sicherheit in der Informationstechnik



Impressum

Herausgeber: EnBW Energie Baden-Württemberg AG
Anschrift: Durlacher Allee 93, 76131 Karlsruhe
E-Mail: redaktion@enbw.com
Projektleitung: Eva Wulff, Christof Hafkemeyer (v. i. S. d. P.)
Redaktion: Heimo Fischer, Eva Wulff
Fotos: Adobe Stock, CSBW, EnBW, Leon Robson/Vestas
Layout: Miriam Elze, **Druck:** Systemedia

Datenschutzinformation
Wir haben die Netze BW GmbH – Kommunale Beziehungen, Schelmenwasenstr. 15, 70567 Stuttgart, mit dem Versand der KommPlus beauftragt. Die Verarbeitung Ihrer Daten erfolgt durch die Netze BW GmbH zu Zwecken von Einladungen, des Direktmarketings oder einer direkten Kontaktaufnahme, also eines berechtigten Interesses (Art. 6 Abs. 1 f) DSGVO). Wir speichern Ihre Daten, solange Sie Ihre Funktion innehaben oder wir aufgrund von gesetzlichen Aufbewahrungspflichten zur Speicherung verpflichtet sind. Sie können dem Bezug der KommPlus jederzeit widersprechen. Weitere Informationen zum Datenschutz und zu Ihrem Widerrufsrecht finden Sie unter: **www.netze-bw.de/datenschutz**. Unseren Datenschutzbeauftragten erreichen Sie unter: **datenschutz@netze-bw.de**.

KommPlus per E-Mail?

Wenn Sie das Magazin lieber als PDF erhalten möchten, senden Sie bitte eine E-Mail an kommunale-beziehungen@netze-bw.de.

Gedruckt auf 100 % Recyclingpapier
mit dem Gütesiegel „Der Blaue Engel“