sure[secure]

CYBERSECURITY IN DER BAUBRANCHE

Warum Bau systemrelevant ist und gerade jetzt besonders.

Die Baubranche ist kein Nischensektor. Sie erwirtschaftet 193 Milliarden Euro Bruttowertschöpfung (4,9 % der deutschen Wirtschaftsleistung) — rechnet man Zulieferer, Planer und Hersteller mit, steigt das Gewicht auf 7,5 % (HDB/Destatis). 2025 waren 923.000 Personen allein im Bauhauptgewerbe beschäftigt, Tendenz steigend. Jede Milliarde Euro Baunachfrage erzeugt einen gesamtwirtschaftlichen Multiplikatoreffekt von 2,4 Milliarden Euro.

193 Mrd. €
Bruttowert-
schöpfung 2024

7,5 %
BWS inkl.
Vorleistungsverbund

923.000
Beschäftigte
Bauhauptgew. 2025

x 2,4
Wirtschaftl.
Multiplikator

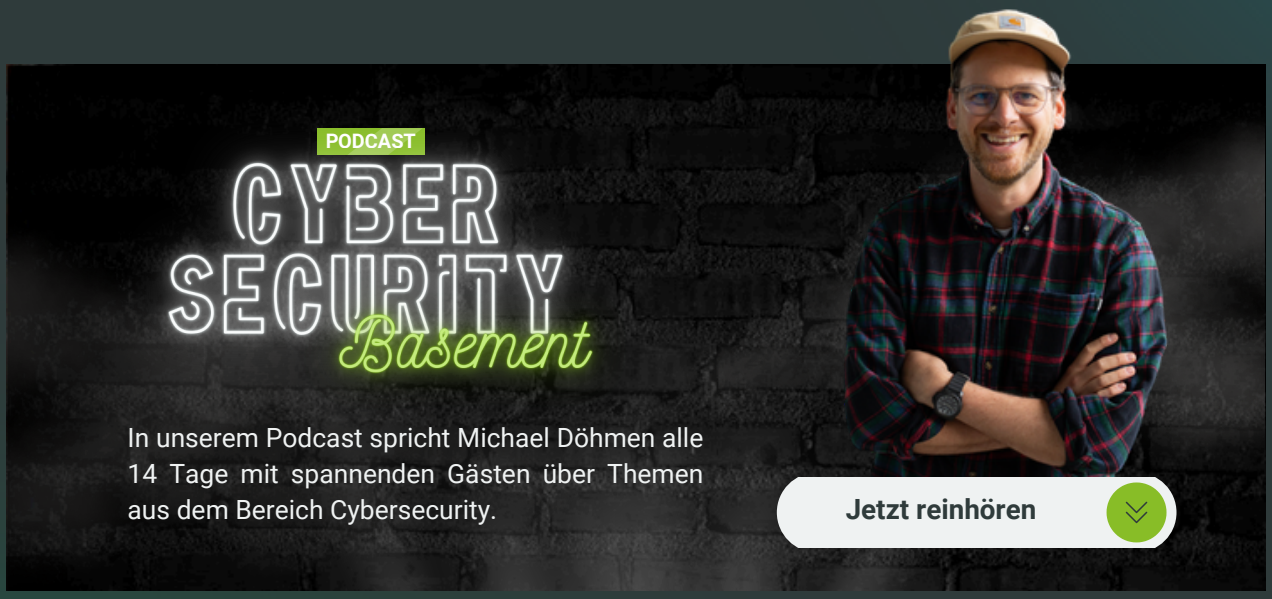
DAS 500-MILLIARDEN-SONDERVERMÖGEN

Historischer Bauboom und neue Zielscheibe

Im März 2025 beschloss der Bundestag das Sondervermögen Infrastruktur und Klimaneutralität: 500 Milliarden Euro über zwölf Jahre, davon 300 Mrd. für den Bund, 100 Mrd. für Länder und Kommunen. Allein für Verkehrsinfrastruktur sind 166 Milliarden Euro vorgesehen, das größte Infrastrukturprogramm der Bundesgeschichte (Bundesregierung 2025).

Für die Deutsche Bahn fließen bis 2029 über 100 Milliarden Euro; DB InfraGO plant 2026 allein mit 28.000 aktiven Baustellen im Schienennetz. Hinzu kommt das Bundeswehr-Infrastrukturprogramm: 26 Milliarden Euro bis 2035, über 100 Milliarden bis 2045.

Investitionsbereich	KRITIS-Sektor
Schiene, Straße, Binnenwasserstraßen	Verkehr
Stromnetze, Energie- und Wärmenetze	Energie
Breitband, Digitalisierung der Verwaltung	Informationstechnik
Krankenhäuser, Bildungseinrichtungen	Öffentliche Versorgung
Bundeswehr-Liegenschaften & Anlagen	Verteidigung / Sicherheit



Die Konsequenz:
Mehr KRITIS-Baustellen als je zuvor.

Wer an diesen Projekten baut, ist nicht mehr nur Auftragnehmer. Er ist Teil der Angriffsoberfläche kritischer Infrastruktur, mit regulatorischer Mitverantwortung durch NIS2, KRITIS-Dachgesetz und CRA. Was früher ein IT-Thema war, ist heute Chefsache.

EXECUTIVE SUMMARY

Das Risiko kommt nicht durch die Vordertür.

Es kommt durch den Bagger. Durch den Sensor am Kran. Durch den Subunternehmer, der seinen Laptop ohne VPN ins WLAN hängt. Moderne Baustellen sind längst digitale Systeme, nur denken die wenigsten Bauunternehmen nicht darüber nach.

Dieses Whitepaper zeigt: Wer heute baut, ist Teil einer Angriffsfläche, die staatliche Hacker, Ransomware-Gruppen und organisierte Cyberkriminalität täglich ins Visier nehmen. Wer an kritischer Infrastruktur baut, trägt darüber hinaus regulatorische Mitverantwortung - ob er es weiß oder nicht.

Die drei Kernbefunde:

- Die Baubranche ist laut NordLocker der weltweit meistangegriffene Sektor. Noch vor Healthcare, Manufacturing und Tech/IT.
- Moderne Baustellen schaffen durch IoT, BIM und Cloud-Plattformen neue Angriffsflächen, für die kaum Schutzkonzepte existieren: Laut PwC-Baustudie 2025 sehen 62 % der Bauunternehmen großes Potenzial in IoT - aber nur 10 % haben die Kompetenz, es sicher zu betreiben.
- Wer an KRITIS-Projekten baut, ist regulatorisch betroffen, durch NIS2, KRITIS-Dachgesetz und CRA. Die Schonfrist ist vorbei.

Die neue Baustelle und ihr blinder Fleck

Noch vor zehn Jahren war eine Baustelle weitgehend analog. Heute läuft fast jedes Großprojekt über cloudbasierte Projektmanagementsysteme, Building Information Modeling (BIM), IoT-Sensoren an Maschinen und vernetzte Geräte auf der gesamten Fläche. Das ist gut für Effizienz, Planung und Kostenkontrolle.
Das Problem: Die Sicherheitsinfrastruktur ist nicht mitgewachsen. Die Baubranche digitalisiert, aber ohne die Fähigkeit, das abzusichern. PwC hat das 2025 schwarz auf weiß belegt: Die Lücke zwischen dem, was Technologie verspricht, und dem, was Unternehmen tatsächlich beherrschen, wächst in der Baubranche von Jahr zu Jahr. Besonders drastisch bei IoT und BIM, genau den Technologien, die neue Angriffsflächen schaffen.

Digitalisierung ohne Sicherheitsstrategie: Die Zahlen

Laut PwC-Baustudie 2026 bremsen explizit Cyber-Risiken die digitale Transformation der Baubranche. Lediglich 13 % der Befragten geben an, bei KI-Anwendungen starke Fähigkeiten zu haben, während 80 % das Potenzial als hoch einschätzen. Bei IoT auf der Baustelle sehen 62 % Chancen, aber nur 10 % sind wirklich kompetent. Das bedeutet: Technologie wird eingeführt, bevor die Sicherheitsfrage gestellt wird.

Dazu kommt ein strukturelles Problem: Auf Großbaustellen mit vielen Beteiligten treffen unterschiedlichste IT-Standards und Sicherheitskulturen aufeinander. Der Generalunternehmer hat vielleicht eine Firewall. Der Elektro-Sub nicht. Und genau dort liegt das Einfallstor.

ANGRIFFSVEKTOREN

Wo es auf der Baustelle brennt

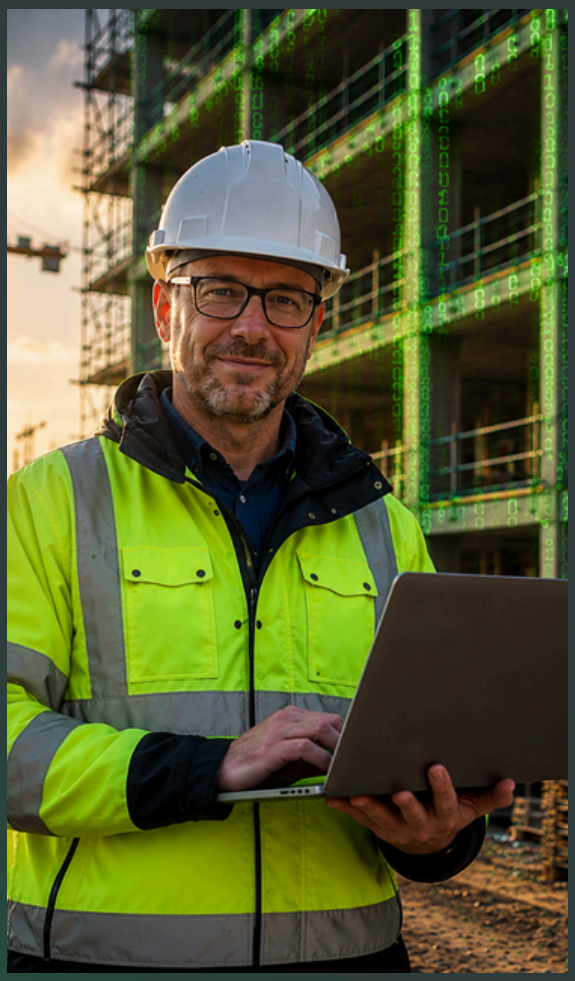
Cyberangriffe auf Bauunternehmen folgen keinem Zufallsprinzip. Sie nutzen strukturelle Schwächen und die Baubranche hat davon mehr als genug. Laut Mittelstand-Digital Zentrum Bau sind die zwei größten Einfallstore: Phishing sowie veraltete, schlecht gesicherte IT-Infrastrukturen.

Vektor 1 - IoT und vernetzte Maschinen

Sensoren, Steuerungseinheiten und Maschinentelemetrie kommunizieren in Echtzeit, oft über ungesicherte Protokolle. Wer auf einer modernen Baustelle ein IoT-Gerät kompromittiert, sitzt im Netzwerk. Und von dort aus führt der Weg zu allem anderen.

Vektor 2 - BIM-Daten und Cloud-Plattformen

Baupläne, Statiken, Ausschreibungsunterlagen. Sie liegen in der Cloud und sind wertvoller als viele Unternehmen ahnen. Insbesondere für staatliche Akteure oder auch den Wettbewerb. Und Ransomware-Gruppen wissen: Wer eine Ausschreibung verliert, weil seine Daten im Darknet auftauchen, zahlt lieber Lösegeld als mit dem Schaden an die Öffentlichkeit zu gehen.



Vektor 3 - Subunternehmer und Lieferkette

Der gefährlichste Angriff kommt selten vom Hauptauftragnehmer, er kommt von dessen schwächstem Glied. Supply-Chain-Angriffe sind 2025 einer der dominierenden Trends: Angreifer kompromittieren nicht das Ziel selbst, sondern dessen Dienstleister. Auf Baustellen ist das strukturell vorprogrammiert. Jeder zusätzliche Subunternehmer ist potenziell ein offenes Tor.

Vektor 4 - Der Mensch

KI-gestützte Phishing-Mails sind heute kaum noch von echter Unternehmenskommunikation zu unterscheiden. Laut TÜV Cybersecurity-Studie 2025 halten sich 91 % der Unternehmen für gut geschützt. Tatsächlich weisen nur 30 % eine gute oder sehr gute Cyber-Resilienz auf. In einer Branche, in der Mitarbeiterschulungen selten stattfinden, ist das ein gefährliches Selbstbild.

Angriff

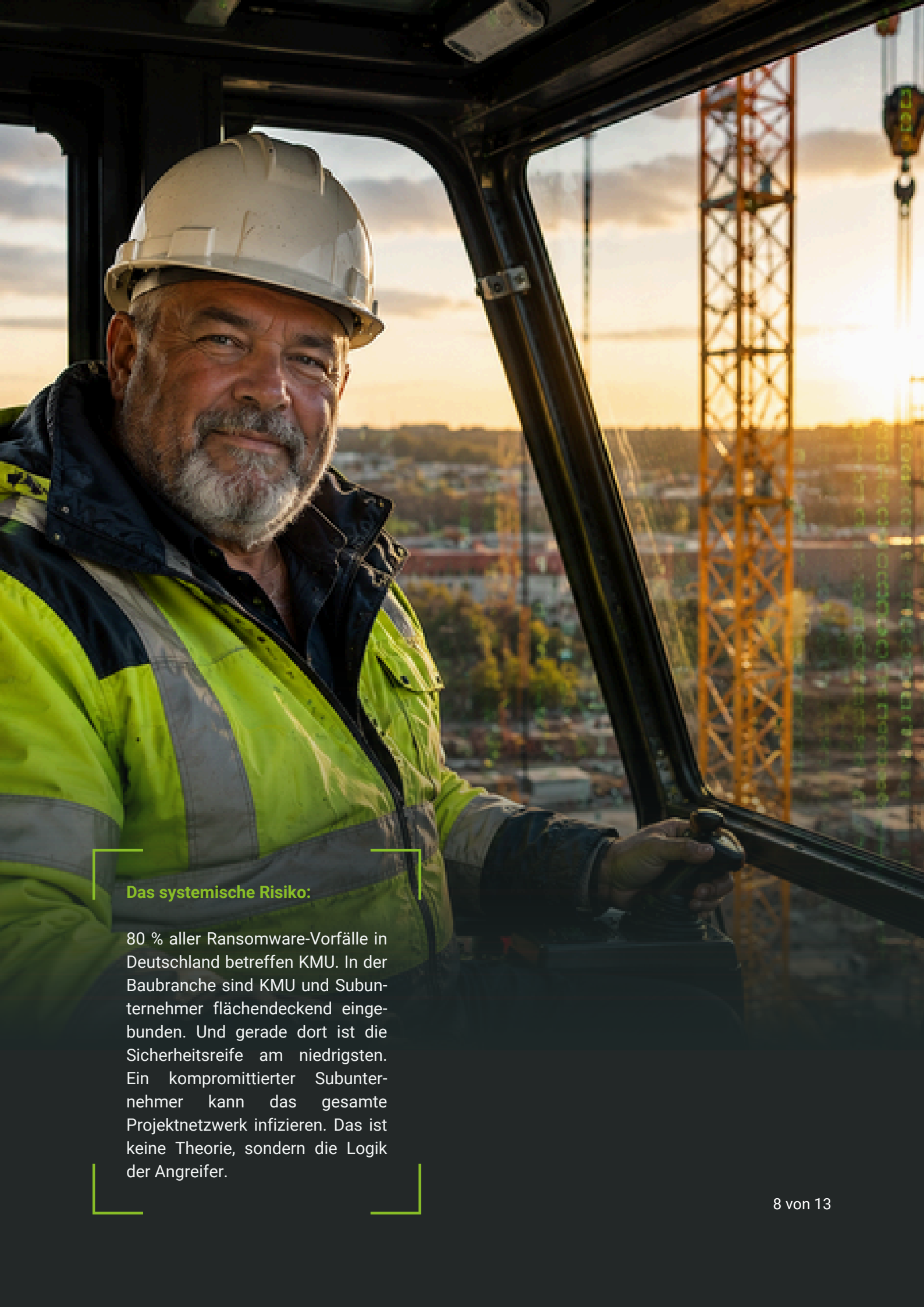
Ransomware

Unternehmen betroffen (Verbreitung DE 2025)

34 %

Trend ↑ vs. 2022

3× faster



Das systemische Risiko:

80 % aller Ransomware-Vorfälle in Deutschland betreffen KMU. In der Baubranche sind KMU und Subunternehmer flächendeckend eingebunden. Und gerade dort ist die Sicherheitsreife am niedrigsten. Ein kompromittierter Subunternehmer kann das gesamte Projektnetzwerk infizieren. Das ist keine Theorie, sondern die Logik der Angreifer.

Wenn es passiert…

Es ist Mai 2026. Ein mittelständisches Bauunternehmen mit 1.300 Mitarbeitenden, internationalem Geschäft und erklärten IT-Sicherheitsstandards wird früh morgens Opfer eines Cyberangriffs. Der Vorfall wird bestätigt. Mehr Details gibt es nicht. Kein Angriffsvektor, kein Schadensausmaß, kein Ergebnis.
Viele Cyberangriffe auf Bauunternehmen werden nicht kommuniziert. Aus Angst vor Reputationsschaden, Vertragsstrafen oder Projekt- bzw. Kundenverlust. Das BKA geht bei Ransomware-Vorfällen von einer hohen Dunkelziffer aus. Was bekannt wird, ist die Spitze des Eisbergs.

Das Muster hinter den Vorfällen:

NordLocker dokumentiert die Baubranche in zwei von drei Jahren als meistangegriffenen Sektor weltweit. 87 % der deutschen Unternehmen wurden laut Bitkom 2025 innerhalb eines Jahres Opfer einer Cyberattacke. Fast jedes fünfte KMU, das getroffen wird, muss Insolvenz anmelden oder schließen. Die Frage ist nicht ob, sondern wann. Und ob du dann vorbereitet bist.

Drei Fragen, die jedes Bauunternehmen beantworten sollte.

1. **Wer hat Zugang zu welchen Systemen, und ist das lückenlos dokumentiert?**

   Auf Baustellen mit Dutzenden Subunternehmern, BYOD-Geräten und Cloud-Zugriffen quer durch das Projektteam ist die Antwort fast nie befriedigend. Was nicht inventarisiert ist, kann nicht geschützt werden.

2. **Wie lange dauert es, bis ein Angriff bemerkt wird?**

   Im Branchendurchschnitt vergehen Monate zwischen Infiltration und Entdeckung, auch bei Unternehmen, die sich für gut geschützt halten. Laut BSI erschwert vor allem das Fehlen von Logging- und Monitoring-Mechanismen die frühzeitige Erkennung. Ein Angreifer, der unbemerkt im Netz sitzt, richtet mehr Schaden an als einer, der sofort entdeckt wird.

3. **Gibt es einen Notfallplan und wurde er jemals geprobt?**

   Laut Bitkom 2025 haben 39 % der deutschen Unternehmen kein Notfallmanagement. In der Baubranche dürfte der Anteil noch höher liegen. Wer den Ernstfall nicht geprobt hat, improvisiert ihn. Auf Kosten des Betriebs, der Projekte und der Kunden.

WAS JETZT ZU TUN IST:

Konkret, nicht theoretisch

Cybersicherheit ist kein Einmal-Projekt. Es ist ein Betriebszustand. Hier sind die fünf Maßnahmen mit dem größten Wirkungsgrad, priorisiert nach Relevanz für die Baubranche.

Angriffsfläche inventarisieren

Was nicht bekannt ist, kann nicht geschützt werden. Alle Assets, Zugänge und IoT-Geräte, auch die der Subunternehmer.

Patch-Management als Pflicht

Über 90 % erfolgreicher Angriffe nutzen bekannte, bereits gepatchte Schwachstellen. Updates sind kein IT-Thema. Sie sind Chefsache.

Security Awareness schulen

Phishing und Social Engineering bleiben das Haupteinfallstor. KI macht Angriffe täuschend echt. Wer nicht schult, zahlt doppelt.

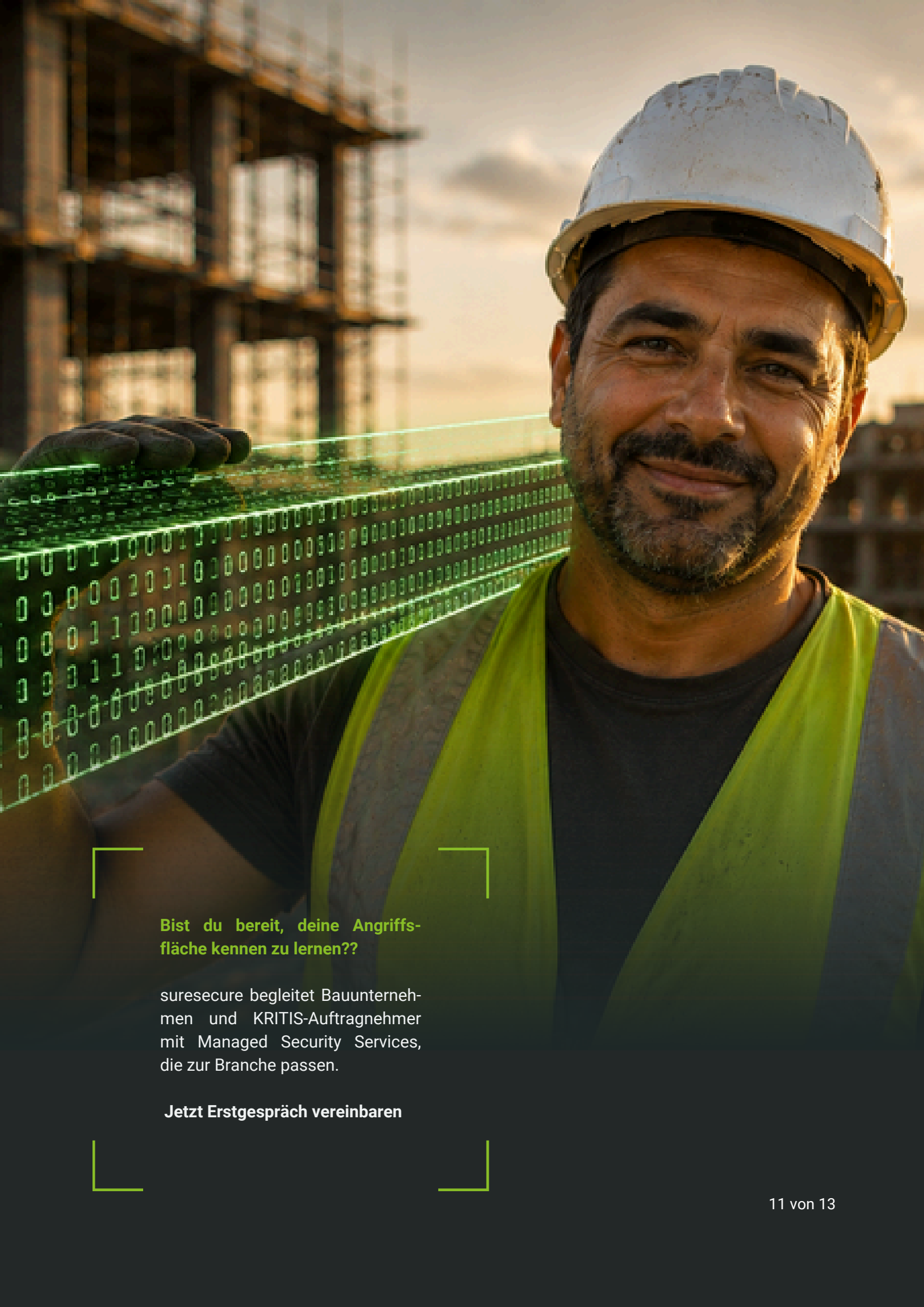
Subunternehmer-Standards definieren

Sicherheitsanforderungen in Verträge aufnehmen. Wer ins Projektnetz darf, muss Mindeststandards nachweisen.

Notfallplan etablieren

39 % der deutschen Unternehmen haben kein Notfallmanagement. Wer den Ernstfall nicht geprobt hat, improvisiert ihn.

Quellen: Bitkom Wirtschaftsschutz 2025 · BSI-Lagebericht 2025 · PwC Baustudie 2025/2026 · TÜV Cybersecurity-Studie 2025 · NordLocker Ransomware-Analyse (fortlaufend) · Mittelstand-Digital Zentrum Bau / FZI Karlsruhe 2025 · Die Rheinpfalz, 11.05.2026



Bist du bereit, deine Angriffs-fläche kennen zu lernen??

suresecure begleitet Bauunternehmen und KRITIS-Auftragnehmer mit Managed Security Services, die zur Branche passen.

Jetzt Erstgespräch vereinbaren

Quellen & Nachweise

Branchenstruktur & Wirtschaftsleistung

— Hauptverband der Deutschen Bauindustrie (HDB) / Destatis: Volkswirtschaftliche Bedeutung der Bauwirtschaft 2024. Bruttowertschöpfung 193 Mrd. Euro (4,9 % der deutschen Wirtschaftsleistung). Stand: Dezember 2025. www.bauindustrie.de

— Institut der deutschen Wirtschaft Köln (IW): Volkswirtschaftliche Bedeutung der Bauwirtschaft. Gutachten im Auftrag des HDB. Verbundeffekt 7,5 % der gesamtwirtschaftlichen Bruttowertschöpfung. Köln, Juni 2024. www.iwkoeln.de

— Hauptverband der Deutschen Bauindustrie (HDB): Baukonjunkturelle Entwicklung in Deutschland. Beschäftigte Bauhauptgewerbe 2025: 923.000 Personen. Stand: März 2026. www.bauindustrie.de

— Zentralverband des Deutschen Baugewerbes (ZDB): Jahresergebnis 2025. Umsatzplus 2,5 % real. Berlin, März 2026. www.zdb.de

Infrastrukturprogramm & Sondervermögen

— Bundesregierung: Sondervermögen Infrastruktur und Klimaneutralität (500 Mrd. Euro). Grundgesetzänderung Artikel 143h, beschlossen 18. März 2025. www.bundesregierung.de

— Bundesministerium für Verkehr (BMV): Koalitionsausschuss 9. Oktober 2025. Investitionen Verkehrsinfrastruktur 166 Mrd. Euro in der Legislaturperiode. www.bayika.de/aktuelles

— Deutsche Bahn AG / DB InfraGO: Bilanz 2025 — mehr als 19 Milliarden Euro verbaut, 28.000 Baustellen im Schienennetz 2026. Stand: Dezember 2025. www.deutschebahn.com

— Bundeswehr / Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen (BAIUDBw): Jahresbilanz Infrastruktur Bundeswehr 2025. Bedarf bis 2035: 26 Mrd. Euro. Stand: Dezember 2025. www.bundeswehr.de

Cybersecurity — Gesamtlage Deutschland

— Bitkom e.V.: Wirtschaftsschutz 2025. Gesamtschaden Cyberkriminalität: 289,2 Mrd. Euro. 34 % der Unternehmen von Ransomware betroffen. Berlin, September 2025. www.bitkom.org

— Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2025. 119 neue Schwachstellen/Tag (+24 %), 950 KRITIS-Meldungen (+30 %). Bonn, November 2025. www.bsi.bund.de

— Bundeskriminalamt (BKA): Bundeslagebild Cybercrime 2024. 950 Ransomware-Fälle gemeldet, 80 % gegen KMU. Berlin, Mai 2025. www.bka.de

— Check Point Software Technologies: Cyber Security Report 2026. 1.223 Angriffe/Woche auf deutsche Unternehmen (+14 % ggn. Vorjahr). Tel Aviv, Januar 2026. www.checkpoint.com

Cybersecurity — Baubranche spezifisch

— PwC Deutschland: Bauindustrie unter Druck — Studie 2025 / 2026. 62 % sehen IoT-Potenzial, nur 10 % mit starken Fähigkeiten. Cyber-Risiken als Digitalisierungshemmnis. 100 bzw. 150 befragte Bauunternehmen. Düsseldorf, Februar 2025 / Mai 2026. www.pwc.de

— TÜV-Verband: TÜV Cybersecurity-Studie 2025. 15 % der Unternehmen 2024 von Angriff betroffen. 91 % halten sich für gut geschützt, nur 30 % weisen tatsächlich gute Resilienz auf. Berlin, Juni 2025. www.tuev-verband.de

— NordLocker / Nord Security: Ransomware-Analyse (fortlaufend, Basis 2020–2023). Baubranche in 2 von 3 Jahren meistangegriffener Sektor weltweit. www.nordlocker.com

— Mittelstand-Digital Zentrum Bau / FZI Forschungszentrum Informatik Karlsruhe: Cybersicherheit im Bauwesen. Phishing und veraltete IT als größte Einfallstore. Karlsruhe, November 2025. www.digitalzentrumbau.de

— Hiscox: Cyber Readiness Report 2025. KMU-Fokus, 5.750 befragte Unternehmen weltweit. 59 % erlitten 2025 einen Cyberangriff. www.hiscox.de

Fallbeispiel

— Die Rheinpfalz / Steffen Gierescher: Cyberangriff auf Baufirma Heberger, Schifferstadt. 11. Mai 2026. www.rheinpfalz.de

— Computer Weekly (Redaktion): Die Cyberangriffe der KW20/2026 im Überblick. Heberger GmbH & Co. KG, Angriff 7. Mai 2026. www.computerweekly.com

Alle Quellen wurden zuletzt im Juni 2026 geprüft. Trotz sorgfältiger Recherche übernimmt suresecure GmbH keine Haftung für die Vollständigkeit und Aktualität der verwendeten Daten.

suresecure gmbh
Dreischeibenhaus 1
40211 Düsseldorf

Phone: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
www.suresecure.de