

untermStrich[®] × **CAIA**[®]

Live Webinar

Resilienz im digitalen Büroalltag.

Wie Architektur- und Planungsbüros Cyber-Risiken erkennen und sicher begegnen.

Agenda

01

Vorstellung der Referenten

Lernen Sie unsere heutigen Experten kennen.

02

Sicherheitsfallen & Versicherungsschutz

Wie Cyber-Vorfälle entstehen, sich auswirken und Sie sich absichern.

03

Organisatorische Maßnahmen

Was Sie im Büroalltag tun können und wie Software Sie unterstützt.

04

Fragen & Antworten

Stellen Sie Ihre Fragen, die Experten antworten.

Die Referenten



Diana Kurbitz

Underwriter
AIA AG

[Kontakt](#)



Steve Davidovic

Customer Success Manager
untermStrich

[Kontakt](#)

02

Sicherheitsfallen & Versicherungsschutz

Wie Cyber-Vorfälle entstehen, sich auswirken und Sie sich absichern.

Die MAF-Gruppe

Langjährige Expertise

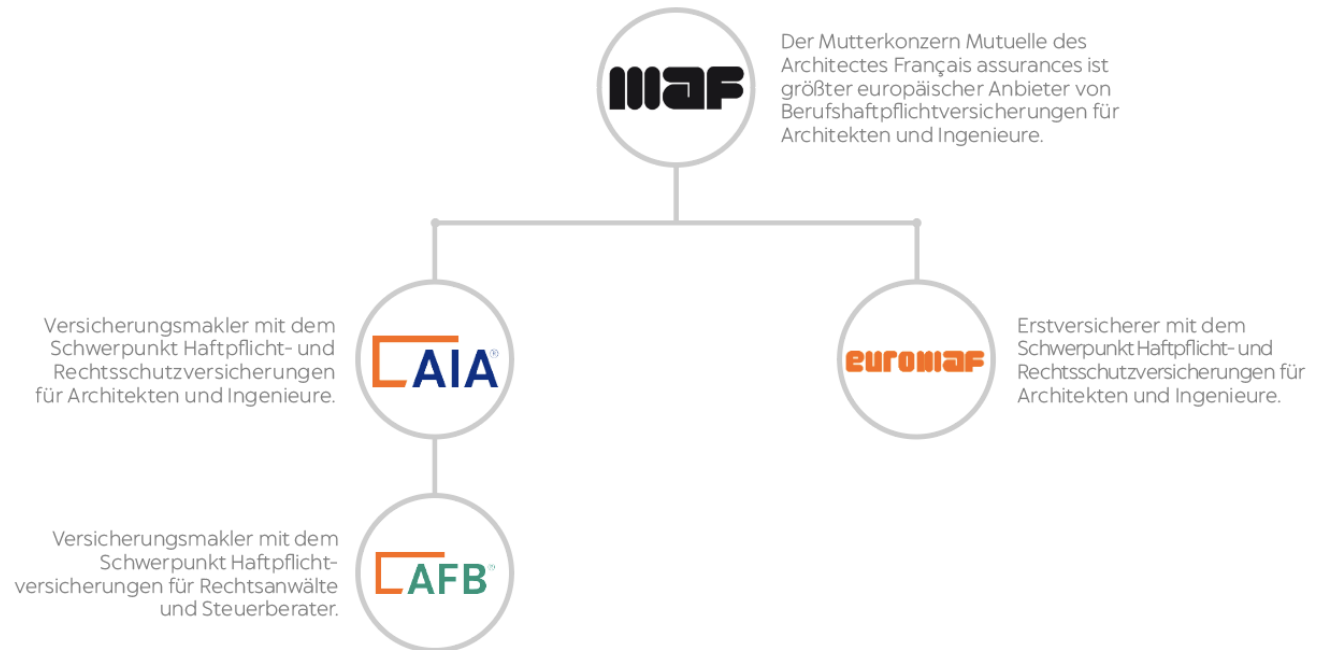
Über 90 Jahre Erfahrung in der Versicherung von bauplanenden Berufen.

100% berufsständisch

Von Architekten für Architekten und Ingenieure.

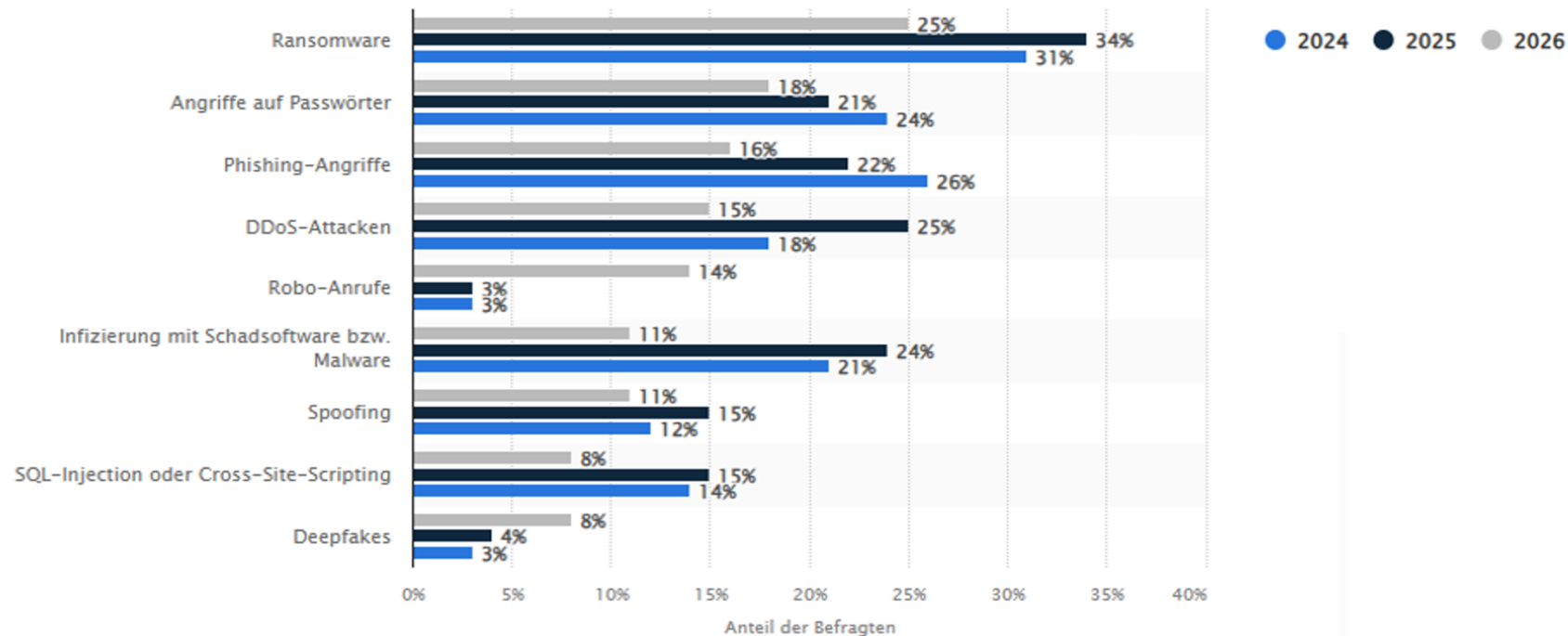
Spezialisierte Lösungen

Ein Bedingungsnetzwerk, speziell zugeschnitten auf die Berufsgruppen.



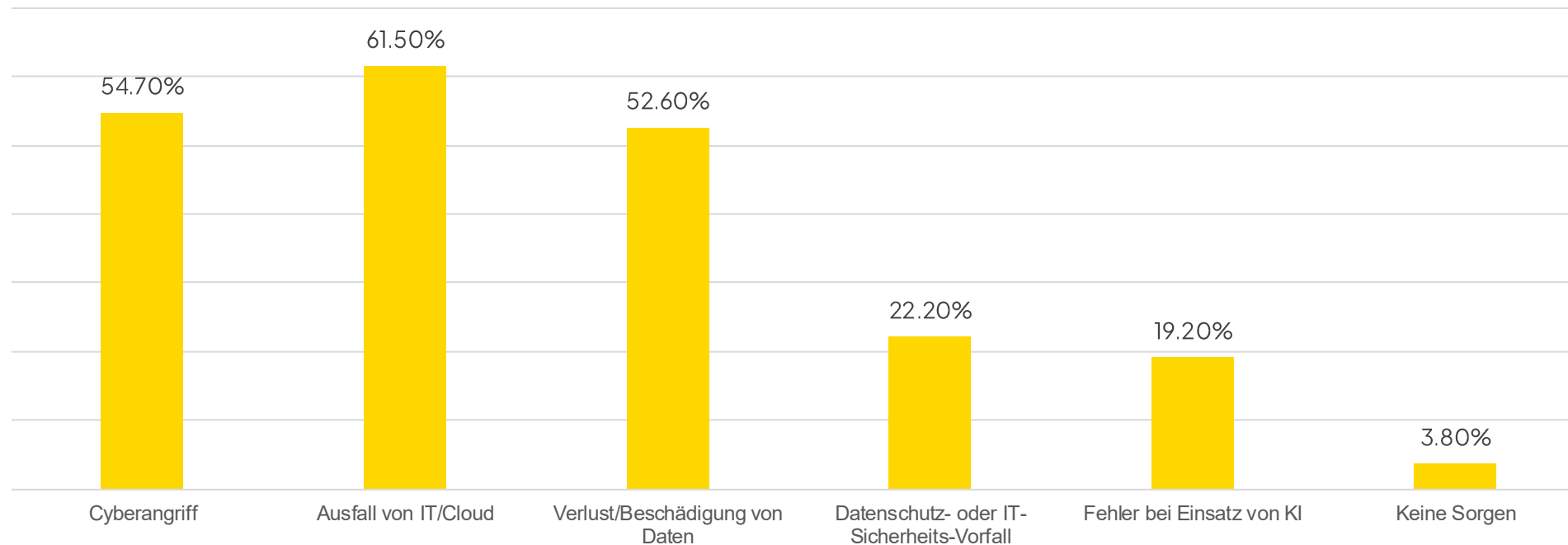
Wahrnehmung Cyber-Sicherheit

Welche der Arten von Cyberangriffen haben in den letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



Wahrnehmung Cyber-Sicherheit

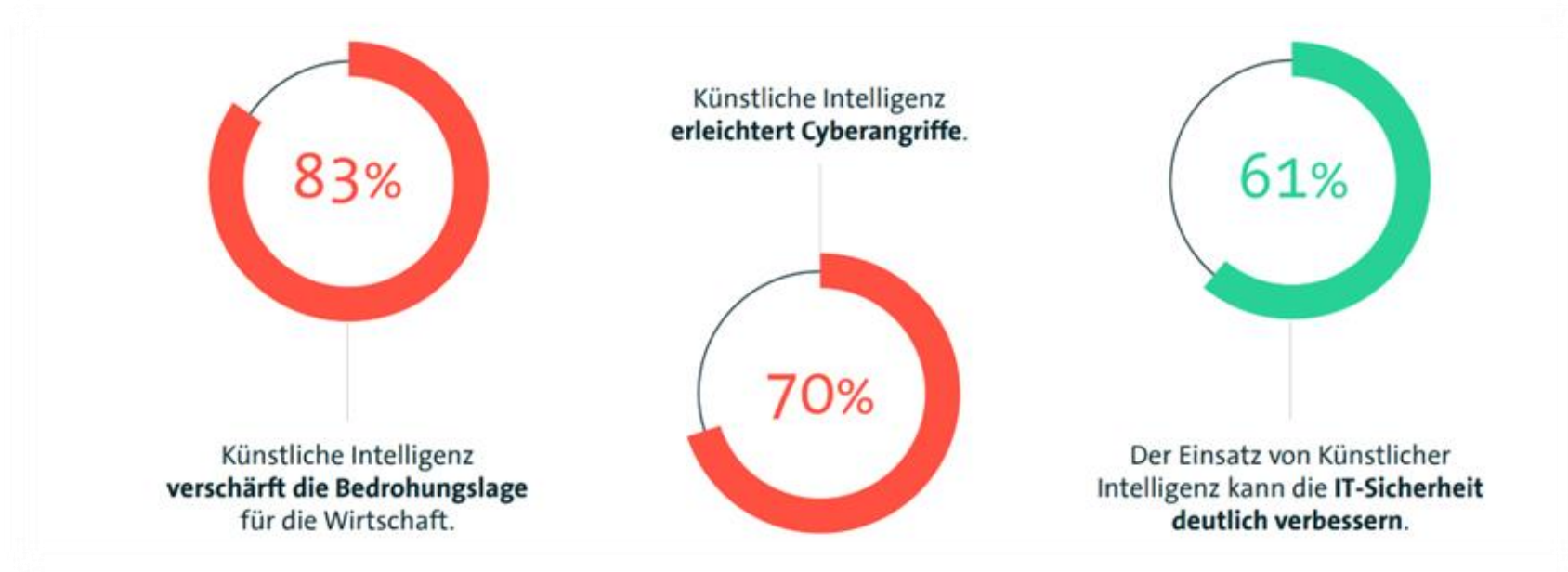
Welche digitalen Risiken bereiten Ihnen aktuell die größten Sorgen?



Wahrnehmung Cyber-Sicherheit

KI gilt als Gefahr für IT-Sicherheit – aber auch als Chance

Inwieweit treffen die folgenden Aussagen zu?





Risiken erkennen und minimieren

Typische Bedrohungen in Planungsbüros:

- Phishing-Mails mit Bezug zu Ausschreibungen oder Projektpartnern
- Malware durch infizierte Anhänge von Subunternehmern
- Ransomware-Angriffe mit Erpressungsszenarien
- Manipulierte Baupläne oder Leistungsverzeichnisse durch Dritte

Digitale Sicherheit ist
wie Statik: Man sieht sie
nicht – aber ohne sie
bricht alles zusammen.



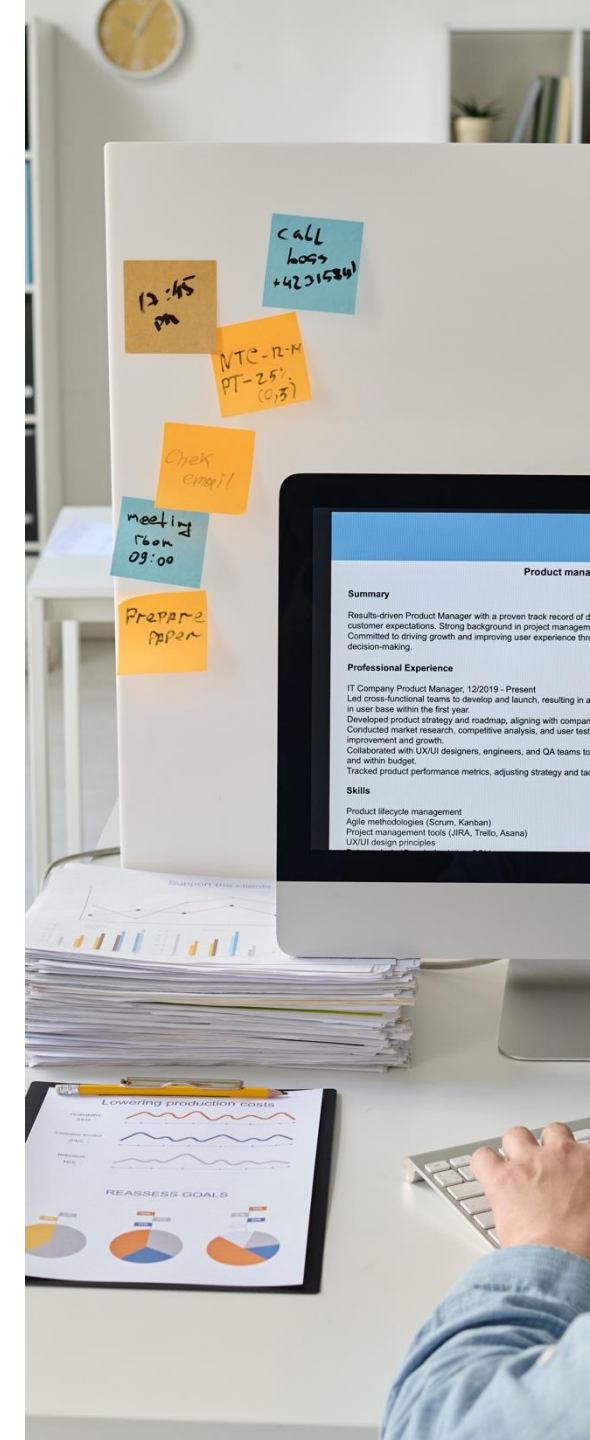
Fallbeispiel 1: Angriff auf Berliner Senatsverwaltung

- Eine kriminelle Angreifergruppe hat sich Zugriff auf das digitale Netzwerk der Berliner Verwaltung verschafft, Datenbestände kopiert und diese am 4. September 2026 im Darknet veröffentlicht.
- Betroffen waren vor allem die Senatsverwaltung für Stadtentwicklung, Bauen und Wohnen sowie die für Mobilität, Verkehr, Klimaschutz und Umwelt.
- Zuvor hatte die Tätergruppe das Land Berlin erpresst und damit gedroht, die entwendeten Daten zu veröffentlichen, sollte nicht gezahlt werden.
- Das Land Berlin ist auf diese Erpressung nicht eingegangen.



Fallbeispiel 2: Bewerbungsmail mit Schadsoftware

- Cyberangriff mit gefälschten Bewerbungsunterlagen sind eine heimtückische Form des Social Engineering.
- Kriminelle versenden täuschend echte E-Mails an Unternehmen und Personalabteilungen, um Schadsoftware zu verbreiten oder Daten zu stehlen.



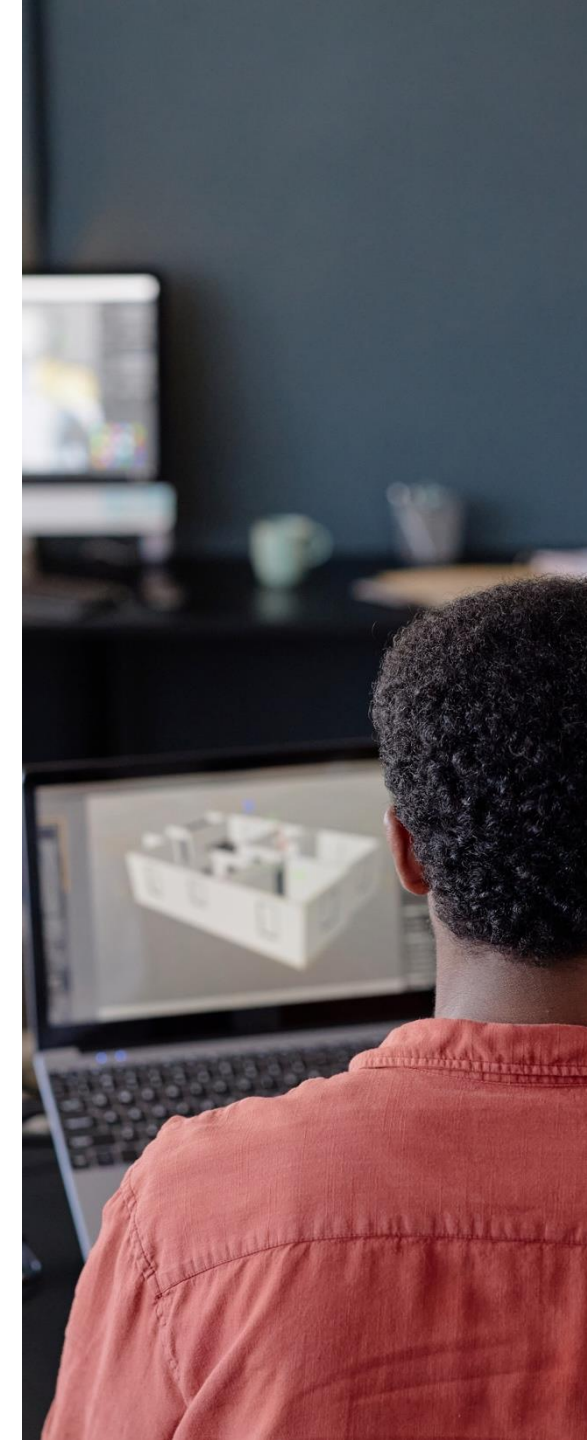
Fallbeispiel 3: Manipulierte digitale Rechnungen im Umlauf

- Rechnungen für tatsächlich erbrachte Leistungen, die digital per Mail versendet wurden, werden abgefangen und die Kontodaten des Rechnungssteller durch Kontodaten der Betrüger ausgetauscht.
- Die gefälschte Rechnung landet mit der originalen E-Mail des tatsächlichen Rechnungsstellers beim Empfänger im E-Mail-Postfach.
- Die E-Mailadresse und die E-Mail selbst bleiben unverändert. Für den Verbraucher ist nicht zu erkennen, dass die beigefügten Unterlagen gefälscht sind. Es wird lediglich das PDF-Dokument (die Rechnung) manipuliert.



Fallbeispiel 4: Manipulierte Planungsparameter

- Ein Architekturbüro mit BIM-Software arbeitete an der Planung eines Bauprojekts.
- Durch eine Sicherheitslücke in der Software manipulierten Angreifer einzelne Planungsparameter in den Projektdateien, um den Bau zu sabotieren.
- Die betroffenen Daten blieben zunächst unbemerkt und weiterhin Teil der Planung. Auf dieser Grundlage wurden Bauteile geplant und später umgesetzt.
- Im weiteren Projektverlauf fiel auf, dass bestimmte Ausführungen nicht den tatsächlichen Anforderungen entsprachen.
- Nach langer Ursachenforschung konnte man die Fehler auf die manipulierten Planungsdaten zurückführen.





Sensibilisierung der Mitarbeitenden



Minimierung von Risiken durch Mitarbeitenden-Trainings

Online-Trainings rund um die Themen Cybersicherheit, Datenschutz und Phishing



Team-Bewusstsein stärken mit realitätsnahen Phishing-Tests

Realitätsnahe Phishing-Simulationen für maximalen und nachhaltigen Nutzen



Cyberprävention durch Gefahrenwarnungen

Praktische Leitfäden, aktuelle Gefahrenwarnungen und umfassendes Cyberlexikon



Versicherungsschutz

Finanzielle Absicherung



Cyber- und Dateneigenschaden

Beschädigung, Zerstörung, Veränderung, Blockierung, Löschung oder der Missbrauch der IT-Systeme der Versicherten.



Cyber-Betriebsunterbrechung

Unterbrechung oder Beeinträchtigung des versicherten Geschäftsbetriebs der Versicherten infolge eines Cyber- und Dateneigenschaden.



Cyber-Erpressung

Geld- oder Warenforderung durch Dritte im Zusammenhang mit angedrohter oder bereits erfolgtem Cyber- und Dateneigenschaden.



Cyber-Haftpflicht

Haftpflichtansprüche privatrechtlichen Inhalts für einen Vermögensschaden, sofern der Schadensersatzanspruch auf einem Cyberverstoß beruht.

Versicherungsschutz

Anforderungen Zugang Versicherungsschutz

- Verwenden Sie Betriebssysteme und Programme einschließlich Antivirensoftware und Firewalls, für die vom Hersteller Updates bereitgestellt werden, und installieren Sie diese Updates unverzüglich auf Ihren IT-Systemen?
- Führen Sie mindestens einmal wöchentlich eine Datenvollsicherung (Backup) durch und lagern diese getrennt vom System?
- Besteht eine Zugangskontrolle für Ihre IT-Systeme durch Benutzerkennungen mit Passwörtern?
- Informieren Sie Ihre Mitarbeiter regelmäßig über Cyber-Risiken bei der Nutzung der IT-Systeme und des Internets?



Versicherungsschutz

Konzepte für Architekten und Ingenieure

- Honorar 1 Mio. Euro p. a.
 - VS: 500.000 Euro, SB: 500 Euro
 - Beitrag: 957 Euro inkl. VSt. p. a.
- Honorar 250.000 Euro p. a.
 - VS: 500.000 Euro, SB: 500 Euro
 - Beitrag: 675 Euro inkl. VSt. p. a.

Jeweils inklusive:

- Sensibilisierung der Mitarbeiter
- Erstellung eines Notfallplans
- Soforthilfe im Schadenfall
- Finanzielle Absicherung



03

Organisatorische Maßnahmen

Was Sie im Büroalltag tun können und wie Software unterstützt.

3 Säulen der digitalen Sicherheit



Tool- und IT-
Sicherheit



Sensibilisierung



Versicherungs-
schutz



Wer plant, baut Verantwortung – das gilt auch für die eigene digitale Infrastruktur

Tool- und IT-Sicherheit

Aktuelle Systeme

- HTTPS/TLS aktiv und korrekt konfiguriert: schützt Daten während der Übertragung zwischen Browser und Server.
- Systeme und Tools aktuell halten: Updates zeitnah und gemäß den Herstellerempfehlungen einspielen.
- Updates geplant durchführen: Zuständigkeit festlegen, Updates testen und anschließend den Betrieb prüfen.



Tool- und IT-Sicherheit

Datensicherung

- Wichtige Unternehmensdaten sichern – nicht nur Dokumente, sondern auch Datenbanken.
- Sicherung getrennt vom Produktivsystem aufbewahren – möglichst verschlüsselt und offline oder gegen Veränderung geschützt.

Interessant dabei:

- 21,5 % der EU-Unternehmen mit mindestens 10 Beschäftigten meldeten für 2023 Folgen durch ICT-Sicherheitsvorfälle – darunter nicht verfügbare IT-Dienste, beschädigte oder zerstörte Daten oder die Offenlegung vertraulicher Daten.



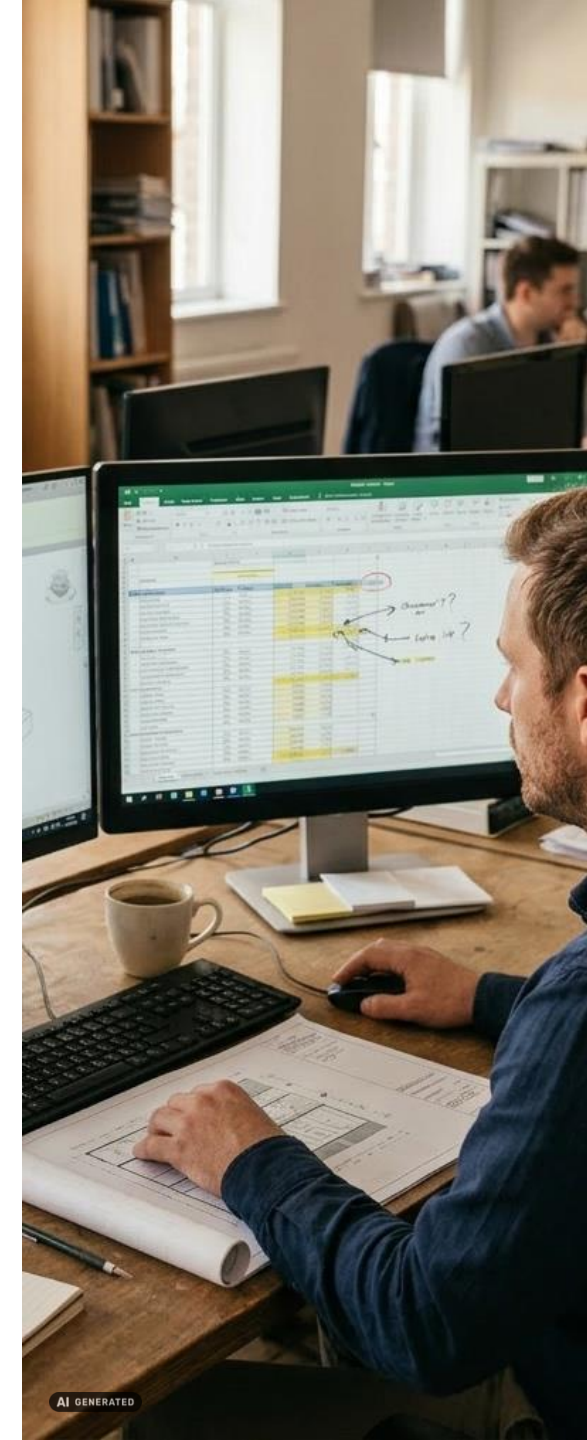
Tool- und IT-Sicherheit

MFA (Multi-Faktor-Authentifizierung):

- MFA ergänzt das Passwort um einen zweiten Nachweis – zum Beispiel App, Passkey oder Sicherheitsschlüssel.
- Hilfreich bei gestohlenen, erratenen oder wiederverwendeten Passwörtern.
- MFA schützt den Zugang, ist aber kein Schutz vor jedem Cyberangriff.

Interessant dabei:

- Microsoft-Studie: MFA verringerte das Risiko einer Kontoübernahme in der untersuchten Population um 99,22 %; bei bekannten geleakten Zugangsdaten um 98,56 %.



Tool- und IT-Sicherheit

Rechtebasierte Zugriffskontrolle:

- Mehrstufiges Sicherheitssystem
- Vertraulichkeit interner Kenngrößen, Honorare, Kalkulationen und Auswertungen
- Manipulationssichere Zeiterfassung: Granulare Einstellungen, wie lange Zeiten rückwirkend geändert werden können

Rechte — Controlling

Stunden

Verwaltung

Unternehmer Plus

Unternehmer

✓ Verwaltung

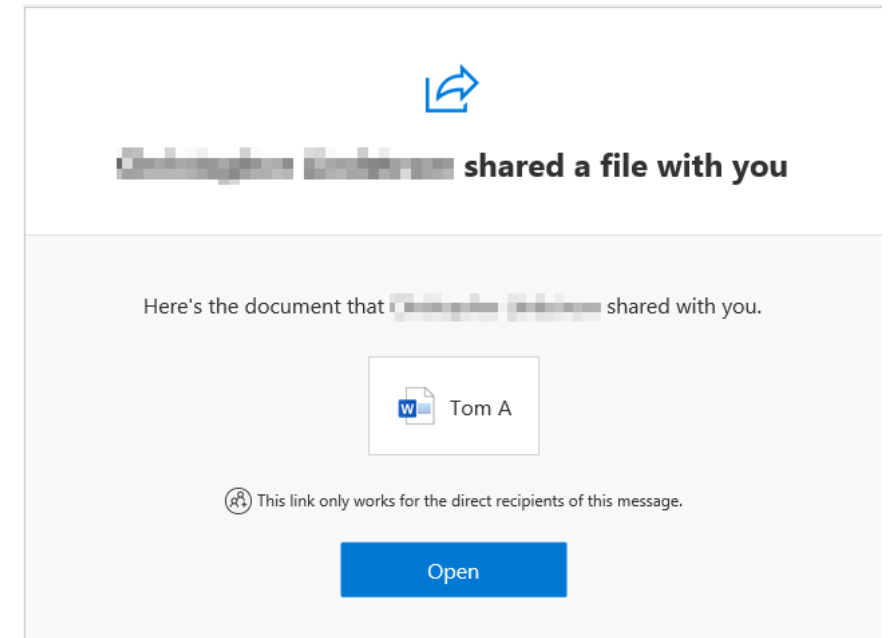
Mitarbeiter

Gesperrt

Tool- und IT-Sicherheit

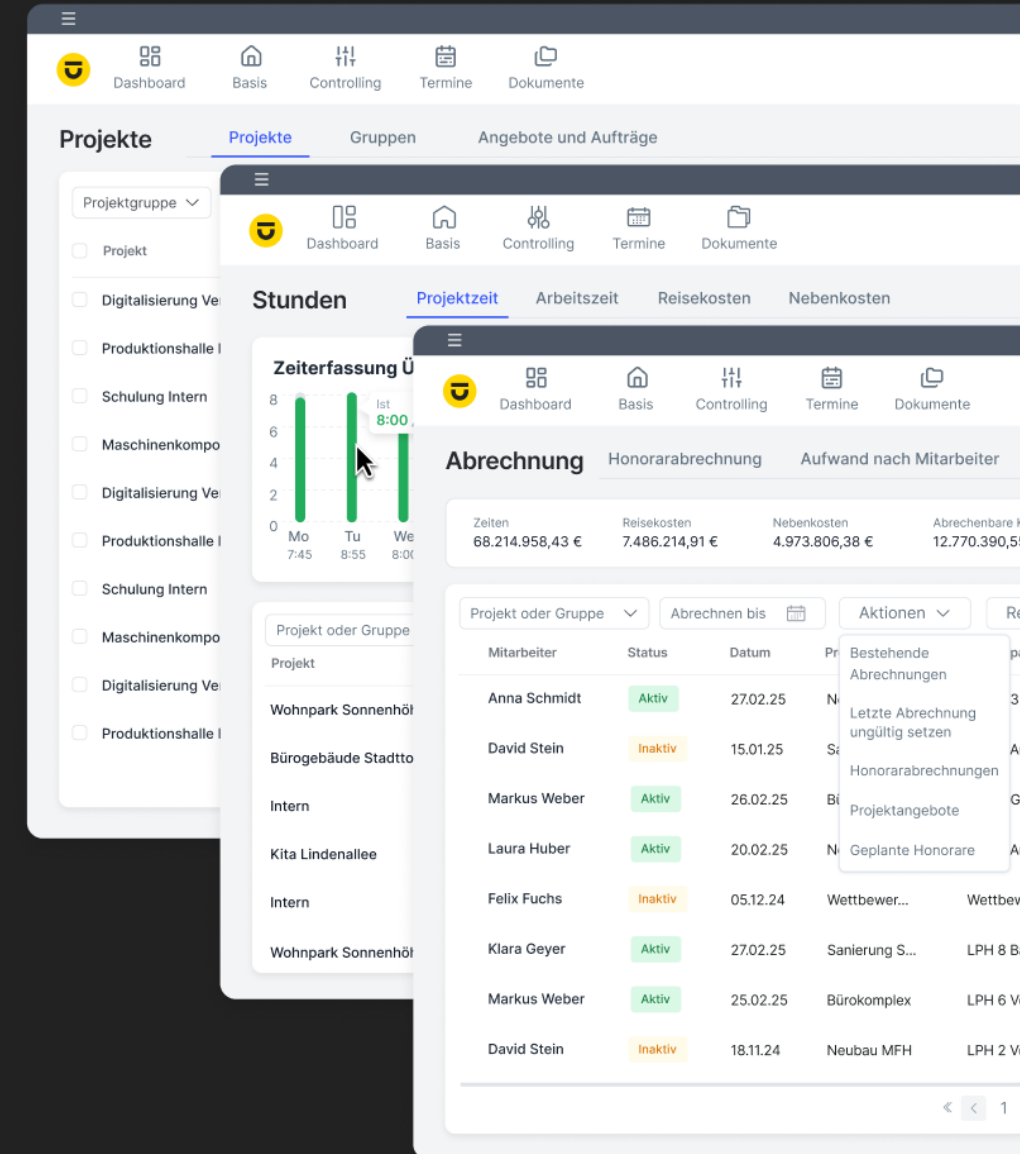
Wenn doch ein Vorfall passieren sollte:

- Ein einfacher Notfallplan
 - Zuständigkeiten und externe IT-Kontakte vorhalten
 - Vorgehen bei Phishing/Ransomware/Geräteverlust definieren
 - Kommunikationswege und Backup-Wiederherstellung festhalten
 - Benutzerkonten einführen.
- Kurz und regelmäßig schulen, statt nur einmal jährlich ein langes Pflichtmodul zu absolvieren.
- Merksatz: Innehalten – prüfen – melden.



untermStrich

- Bürosoftware für Architektur- und Planungsbüros
- Leistungen und Vorgänge nachvollziehbar dokumentieren – Honorarrisiken früh erkennen und im Streitfall handlungsfähig bleiben
- Zentrale Projektorganisation, Angebots- und Auftragsverwaltung im Projektkontext
- Basis für wirtschaftlich saubere Steuerung bis zur Abrechnung
- Entwickelt von Branchenexperten für die Herausforderungen der Branche



04

Fragen & Antworten

Ihre Fragen, direkt den Experten gestellt.

Exklusive Konditionen

Für AIA-Versicherte:

20 % auf untermStrich im 1. Vertragsjahr

[Link](#)



Für untermStrich-Kunden:

5 % auf Berufshaftpflichtkonzepte (dauerhaft)

[Link](#)

