thínkproject

Die Bausteine der Informationssicherheit

So schaffen Sie sichere Grundlagen für sich und Ihre Anbieter

Inhalt

Milliardenschwere Investitionen in Informationssicherheit und Datenschutz in ganz Europa

Datenschutz und Informationssicherheit sind nicht nur in aller Munde, sondern auch eine wichtige Strategie, mit der Unternehmen ihre wertvollen Informationswerte schützen.

Der Bericht von Kroll 2021[1] zu den Trends bei Datenschutzverletzungen zeigt, dass der Bausektor zwischen 2019 und 2021 im Vergleich zum Durchschnittswert von

133%

in anderen Branchen eine Zunahme der Datenschutzverletzungen von

800%

verzeichnet hat.

Ausschlaggebende Faktoren waren hierfür unter anderem Schwierigkeiten von Unternehmen bei der Zusammenarbeit im Bereich der Datenverwaltung, die Kontrolle von Vermögenswerten in einem geografisch verstreuten Umfeld (inklusive Remote-Arbeit) sowie eine Zunahme von IoT-basierten Bedrohungen im Zuge von Innovationen in der Branche. Diese Herausforderungen haben IoT- und Compliance-Vorreitern vor Augen geführt, wie wichtig es ist, dass sie diesen mit ihren Digitalisierungs- und Sicherheitsstrategien effektiv begegnen können.

1 www.kroll.com

Investitionen in Informationssicherheit gehen nicht zurück

Laut der IDC (International Data Corporation) wurden für 2022 europaweite IT-Ausgaben von etwa

47 Milliarden € vorausgesagt;

eine Fünfjahresprognose geht sogar von mehr als

66 Milliarden €

bis 2026 aus.[2]

Das Management von Informations- und Cyberrisiken wird nun auch in Branchen wichtiger, die traditionell nicht zu den größten Investoren in diesem Bereich gehören. Die Digitalisierung von Bauabläufen und der Umstieg auf DfMA (Design for Manufacturing and Assembly), mit dem die Baubranche in den Bereich des Fertigungssektors greift, erhöht den Druck auf die Investitionen.

2 www.idc.com

Datenschutz ist nun in jedem Unternehmen ein Muss.

Im engen Zusammenhang mit den oben genannten Aspekten steht der Schutz personenbezogener Daten. Jedes Unternehmen in der EU ist mittlerweile mit der Datenschutz-Grundverordnung (DSGVO oder GDPR im Englischen) vertraut. Mit dieser Verordnung wurden strenge Vorgaben rund um den Datenschutz eingeführt – sowohl aus Sicht der Kunden als auch aus Sicht der Unternehmen. Der Datenschutz dient dem Schutz der (personenbezogenen) Daten Ihres eigenen Unternehmens und sorgt dafür, dass Sie die (personenbezogenen) Daten Ihrer Kunden, Lieferketten und aller Beteiligten schützen.

Darüber hinaus definiert die Network and Information Systems Directive (NIS-Direktive) Maßnahmen, mit denen ein hohes Maß an Sicherheit für Netzwerke und Informationssysteme in der EU gewährleistet wird. Die NIS-Direktive legte einen einheitlichen Rechtsrahmen für die EU-weite Entwicklung nationaler Cybersicherheitsmaßnahmen, die engere Zusammenarbeit zwischen den Mitgliedstaaten der EU und ein Mindestmaß an Sicherheitsanforderungen und Meldepflichten für kritische Infrastrukturen sowie für bestimmte Anbieter digitaler Services wie Cloud-Dienste und Online-Marktplätze fest.

Egal ob DSGVO oder NIS – beide Richtlinien haben erheblich zu einer bewussteren Wahrnehmung und vertieften Diskussionen rund um die Themen Datenschutz und Informationssicherheit in den einzelnen Unternehmen beigetragen.

Arten von Sicherheits-bedrohungen, für die Nutzer besonders gefährdet sind

Regelmäßige Schulungen der Mitarbeiter zur Informationssicherheit reduzieren das Risiko erfolgreicher Angriffe

Malware

Diese Schadsoftware hat das Ziel, Computersysteme und Netzwerke zu schädigen. Malware kann in unterschiedlichen Formen auftreten, von Viren bis hin zu Spyware usw.

Unternehmen können für Angriffe dieser Art gefährdet sein, da Malware z. B. hinter einem E-Mail-Link versteckt sein kann, wodurch unaufmerksame Nutzer getäuscht werden.

Ransomware

Ransomware kann besonders katastrophale Folgen haben, da sie wichtige Daten sperren und Zahlungen verlangen kann, um wieder Zugriff zu erhalten.

Jedes Unternehmen hat wertvolle Daten, auf die Cyberkriminelle zugreifen möchten, und Ransomware kann sich schnell in einem Netzwerk verbreiten und alle Aspekte eines Geschäfts beeinträchtigen.

Phishing

Phishing-Kriminelle geben sich als vertrauenswürdige Kollegen aus, um Zugriff auf Ihr Netzwerk zu erlangen. Dies geschieht häufig beim Zurücksetzen von Kennwörtern oder Klicken auf Links.

Haben sie erst einmal Zugriff, können sie Ransomware oder Schadsoftware auf dem System installieren oder Daten stehlen.

Advanced Persistent Threat

Ein Advanced Persistent Threat (APT) liegt dann vor, wenn ein gut ausgebildeter, typischerweise staatlich gesteuerter Angreifer zum Zweck der Spionage oder Sabotage über einen längeren Zeitraum hinweg sehr gezielt ein Netzwerk oder System angreift, sich unter Umständen darin bewegt und/oder ausbreitet und so Informationen sammelt oder Manipulationen vornimmt.

Social Engineering

Social Engineering bezeichnet alle Techniken, mit deren Hilfe die Kommunikation mit dem Ziel aufgenommen wird, bestimmte Informationen zu erlangen oder eine bestimmte unrechtmäßig Aktion durchzuführen.

Es gibt zahlreiche gut dokumentierte Angriffstechniken, die häufig auch kombiniert eingesetzt werden, um ein Unternehmen zu gefährden:

Denial of Service (DoS) und Distributed Denial of Service (DDoS)

Große Datenmengen bombardieren eine Website oder Anwendung mit dem Ziel, die gesamte verfügbare Bandbreite oderVerarbeitungskapazität des Systems zu nutzen, um es lahmzulegen. DDoS-Angriffe können zwar für erhebliche Unterbrechungen sorgen, sind aber in der Regel von kurzer Dauer und verursachen nur selten dauerhaften Schaden. Sie werden jedoch häufig als Ablenkungstaktik verwendet, um von gleichzeitig stattfindenden, schwerwiegenderen Angriffen abzulenken.

Man-in-the-Middle Angriff (MitM)

Man-in-the-Middle-Angriffe können knifflig sein. Sind sie jedoch erfolgreich, ermöglichen sie dem Angreifer normalerweise, verschlüsselte Daten im Textformat zu lesen (z. B. Kennwörter, Projektdaten und E-Mails). Zudem können die Angreifer gesendete Daten manipulieren.

Bedrohungen durch Insider

Eine Bedrohung durch Insider liegt vor, wenn eine Person, die im Unternehmen über bestimmte Berechtigungen verfügt, so handelt, dass ein Sicherheitsverstoß vorliegt. Der Verstoß kann böswillig oder unbeabsichtigt sein, jedoch ist das Risiko für ein Unternehmen aufgrund des Zugangs zu Daten und Systemen, über die es bereits verfügt, erhöht.

SQL-Injection

Angreifer nutzen Schwachstellen für SQL-Injections, um Daten aus einer Anwendung ohne entsprechende Berechtigung zu manipulieren, zu löschen oder zu extrahieren. Dies kann zu umfassenden Datendiebstählen und Systemschädigungen führen.

Cross-Site Scripting (XSS)

Schädliche Skripts können in Websites umgewandelt werden, die die Browseraktivitäten eines Nutzers ohne sein Wissen ausspionieren. Angreifer versuchen, das Ziel den schädlichen Code ausführen zu lassen, indem es über eine vertrauenswürdige Website bedient wird. Zahlreiche Schwachstellen begünstigen XSS-Angriffe. Sie können schwer aufzuhalten sein, da der Webbrowser des Opfers glaubt, dass das Skript von einer vertrauenswürdigen Website stammt.

Passwortangriffe

Ein solcher Angriff kann auf unterschiedliche Weise umgesetzt werden, z. B. durch das Knacken von Kennwörtern, um Zugriff auf Kennwörter zu erhalten, die in der Folge verändert oder dekodiert werden können. Bei ausreichend Zeit können Kennwörter erraten werden. Dabei machen sich Kriminelle die Neigung der Nutzer zunutze, das gleiche Kennwort an vielen Stellen wiederzuverwenden. Sie testen Benutzernamen und Kennwörter von öffentlich bekanntgewordenen Datenschutzverletzungen, um sich bei anderenWebsites und Systemen anzumelden. In den letzten Jahren war dies eine sehr erfolgreiche Technik.

Zero-Day Attacken

Wenn ein Angreifer eine unbekannte Schwachstelle ausnutzt, können Sicherheitsteams die Bedrohung deutlich schlechter erkennen und darauf reagieren. Wird sie erkannt, dauert es in der Regel einige Tage, bis die Softwareanbieter einen Patch für den Angriff programmiert haben. Ein solcher Angriff wird „Zero-Day“ genannt, weil er seit null Tagen bekannt ist.

Malware

Spyware | Würmer

Trojaner | Viren

Ransomware

Netzwerk basiert

Dos | DDos

MitM

Web-Anwendung

XXS

SQL-Injection

Social Engineering

Phishing

Bedrohungen durch Insider

Zero-Day Attacken

Angriffe auf unerkannte Schwachstellen

Authentifizierung

Passwortangriffe

Der Bausektor ist nicht immun gegen Verletzungen der Informationssicherheit.

Die Digitalisierung der Baubranche hat bereits große Fortschritte gemacht. Der Einsatz von Automatisierung, KI und digitalen Methoden wie Building Information Modelling (BIM) macht Software erforderlich, die sich durch eine Qualitätsverbesserung bei gleichzeitiger Zeit- und Kostenersparnis günstig auf die Bauprojekte auswirkt, und Einblicke in und Analysen von Daten aus der Vergangenheit ermöglicht. Für die in puncto Digitalisierung eher als rückständig geltende Baubranche sind dies sehr positive Schritte. Doch mit der verstärkten digitalen Präsenz geht immer auch die Gefahr böswilliger Absichten einher.

Warum ist die Baubranche ein beliebtes Ziel?

Die Auswirkungen einer Verletzung der Informationssicherheit auf ein Unternehmen

Stellen Sie sich folgendes Szenario vor: Cyberkriminelle senden eine Phishing-E-Mail an einen Mitarbeiter eines internationalen Bauunternehmens. Dieser öffnet einen in der E-Mail enthaltenen Link und erhält darüber Ransomware, die dem Vertragspartner den Zugriff auf die Projektdaten verweigert und gleichzeitig verschiedene Projektstandorte lahmlegt.

Die Hacker erhalten nicht nur Zugriff auf die personenbezogenen Daten von Mitarbeitern und Kunden sowie auf vertrauliche Informationen zu Bauprojekten wie z.B. Baupläne für Regierungsgebäude auf der ganzen Welt, sondern der Cyberangriff zieht darüber hinaus massive Auswirkungen auf das Geschäft, die Beteiligten, die Lieferkette und die Kunden nach sich. Ist ein Unternehmen nicht in der Lage, auf Projektdaten zuzugreifen und die Arbeit planmäßig fortzuführen, hat dies große Auswirkungen auf den gesamten Zeitplan und kann potenziell Strafen für verspätete Lieferung nach sich ziehen und zu großen Produktivitätseinbußen führen. Insgesamt kann der Schaden für die Finanzen und den Ruf des Unternehmens erheblich sein – ganz zu schweigen von den monetären Folgewirkungen.

Das Unternehmen ist dann verantwortlich für anfällige Gerichtskosten, Kosten für die Behebung des Schadens und hohe Strafzahlungen. Das mühsam erarbeitete Vertrauen in das Unternehmen muss zudem mit erheblichem Aufwand, zahlreichen Ressourcen und viel Geld wieder aufgebaut werden. Für Branchen mit sensiblen Daten, wie der Atomsektor oder kritische Infrastrukturen, bei denen potenzielle Probleme landes- oder weltweite Auswirkungen haben können, ist das Risiko, sich von einem solchen Angriff zu erholen, eventuell noch höher.

Das Unternehmen hat dieses Risiko durch eine Informationssicherheitsstrategie gemindert, mit der ein wiederholter Angriff ausgeschlossen wird. Zu den entsprechenden Maßnahmen zählen Multifaktor-Authentifizierung, Mitarbeiterschulungen zur Erkennung von Phishing-Angriffen, die Stärkung der Netzwerksicherheit und die Verbesserung der Reaktionsverfahren bei Vorfällen. Darüber hinaus hat das Unternehmen eine Richtlinie für rigorose Sicherheitsüberprüfungen für externe Anbieter eingerichtet, mit denen es arbeitet. Damit ist sichergestellt, dass die gesamte Lieferkette mit ähnlichen Verfahren arbeitet. Diese Schritte stellen sicher, dass die Organisation im Fall eines weiteren erfolgreichen Angriffs vorbereitet ist und damit das Risiko minimiert wird.

In diesem Beispiel werden die Risiken deutlich, denen Bauunternehmen ausgesetzt sind. Zudem zeigt es, welche langfristigen Vorteile die Priorisierung von Informationssicherheit hat. Noch mehr steht auf dem Spiel, wenn Cyberkriminelle sensible Projekte wie kritische Infrastrukturen[3] oder Atomkraftwerke treffen wollen. Im Jahr 2021 meldeten 56% der Energieanlagen in den USA Angriffsversuche, die zu einer Unterbrechung des Betriebs führten. Dabei entstanden pro Angriff schätzungsweise 100 Milliarden US-Dollar Kosten für die Wiederherstellung[4]. Die Reichweite der Auswirkungen solcher Angriffe auf Infrastruktureinrichtungen wie in der Wasserversorgung oder der Wärme- und Stromversorgung von Gebäuden kann enorm sein.

3 www.allianz.com

4 www.firstpoint-mg.com

Dieses E-Book zur Informationssicherheit liefert Informationen zu aktuellen Best Practices, wichtigen Punkten, auf die Sie bei der Zusammenarbeit mit externen Anbietern achten sollten und dazu, wie Sie sich und Ihr Unternehmen schützen können.

In einfachen Worten Informationssicherheit verständlich erklärt:

Das Thema Informationssicherheit beinhaltet viele Abkürzungen und Fachbegriffe. In unserem Leitfaden finden Sie Erläuterungen zu den wichtigsten Begriffen, die Sie kennen sollten.

BCP
Der Business Continuity Plan (Betriebskontinuitätsplan) wird entwickelt und tritt bei einem Notfall in Kraft. Er definiert die Reaktionen und Wiederherstellungsschritte, die Geschäftskontinuität in einer Krise gewährleisten.

Bedrohung
Alle Aktionen, die Schaden verursachen können.

BIA
Die Business Impact Analysis (Analyse der Geschäftsauswirkungen) quantifiziert die potenziellen Auswirkungen einer Bedrohung auf den Geschäftsbetrieb. Dies ist ein wichtiger Schritt bei der Definition geeigneter Kontrollen, mit denen die Risiken auf ein annehmbares Niveau reduziert werden.

CIA Triade
Ein häufig verwendetes Drei-Punkte-Modell mit den Faktoren Vertrauen (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability), den drei Hauptprinzipien der Informationssicherheit.

CISO
Der Chief Information Security Officer ist ein Mitarbeiter, der dafür verantwortlich ist, das Informationssicherheitsprogramm eines Unternehmens zu steuern und zu verwalten. Die primäre Aufgabe ist der Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Informationswerte der Organisation.

Firewall
Eine Vorrichtung, die den Datenfluss zwischen Netzwerken kontrolliert.

Informationssicherheit
Der Schutz der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen (siehe: CIA-Triade) sowie die Maßnahmen, die zur Schadensverhinderung ergriffen werden. Dazu gehört die Umsetzung von Maßnahmen und die Einführung von bewährten Verfahren. Sie umfasst Computernetzwerke, lokale Gebäude und alle Einrichtungen, in denen Informationen zu finden sind.

ISMS
Das Information Security Management System (Informationssicherheits-Managementsystem) umfasst Richtlinien, Prozesse und Kontrollen zum Schutz der sensiblen Informationen einer Organisation und zur Abwehr von Angriffen auf diese.

ISO 27001
Weltweit anerkannte und für ISMS angewendete Norm. Die ISO hat einen robusten Rahmen festgelegt, mit dessen Hilfe Unternehmen maximalen Schutz sicherstellen und akkreditiert werden können, wenn sie die Kriterien erfüllen.

Patching
Die Anwendung von Software- oder Firmware-Updates, die Schwachstellen aus Ihren Assets eliminieren.

Reaktion auf Störungen (Incident Response)
Störungsmanagement ist der Prozess zur Identifizierung, Eindämmung und Eliminierung von Sicherheitsbedrohungen und der Wiederherstellung eines Normalzustands.

Risiko
Wenn eine Schwachstelle und eine Bedrohung aufeinandertreffen.

Risikobewertung
Ein Mechanismus, der zur Bewertung von Risiken und deren Schweregrad herangezogen wird.

VPN
Ein Virtual Private Network sichert die Kommunikation zwischen zwei Netzwerken oder einem Nutzergerät und dem Unternehmensnetzwerk, indem die Daten über einen verschlüsselten Tunnel gesendet werden. Ein VPN arbeitet mit Verschlüsselung, damit identifizierbare Informationen für potenzielle Bedrohungen blockiert werden. Die Verschlüsselung wird in der Regel beim Zugriff auf das Internet angewendet.

Zugriffskontrolle
Dieses Verfahren stellt sicher, dass Einzelpersonen nur Zugriff auf Daten haben, die sie benötigen und für die sie eine Berechtigung haben. Die Zugriffskontrolle ist ein wichtiges Instrument zur Minimierung von Datenschutzverletzungen.

Grundbegriffe zum Datenschutz

Effektiver Datenschutz beginnt mit dem Verständnis dieser häufig verwendeten Begriffe:

Daten-minimierung
Die Beschränkung der Sammlung personenbezogener Daten auf das für die Durchführung der Verarbeitungstätigkeit erforderliche Maß.

Datenschutz
Kontrolle über den Zugang und die Nutzung von Daten.

Datenschutz-beauftragter
Der Datenschutzbeauftragte ist eine Rolle, die in der DSGVO festgehalten ist. Die primäre Aufgabe des Datenschutzbeauftragten besteht darin sicherzustellen, dass die Organisation, für die der Datenschutzbeauftragte ernannt wurde, die personenbezogenen Daten ihrer Mitarbeiter, Kunden, Anbieter oder anderen Personen (auch als Datensubjekte bezeichnet) in Übereinstimmung mit den geltenden Datenschutzregeln verarbeitet.

Daten-schutzverletzung
Ein Sicherheitsvorfall, bei dem unberechtigte Parteien Zugriff auf sensible Daten oder vertrauliche Informationen wie personenbezogene Daten oder Unternehmensdaten erlangen.

Daten-verantwortlicher
Eine natürliche oder juristische Person, Behörde, Agentur oder andere Einrichtung, die den Zweck und die Mittel der Verarbeitung personenbezogener Daten allein oder gemeinsam mit anderen festlegt.

Daten-verarbeiter
Eine Einheit, die personenbezogene Daten im Namen eines Datenverantwortlichen verarbeitet.

Daten-verarbeitung
Datenverarbeitung ist die Sammlung, Analyse und Transformation von Daten, um bedeutsame Informationen zu erlangen und die Entscheidungsfindung zu erleichtern. Sie spielt in zahlreichen Bereichen, z. B. Wirtschaft, Forschung und Technologie, eine wichtige Rolle, da sie Unternehmen befähigt, Daten für die betriebliche Effizienz, Strategieplanung und Innovation zu nutzen.

Datensubjekt
Alle Personen, die anhand der über sie erfassten Daten als natürliche Personen identifizierbar sind.

DPIA
Die Data Protection Impact Assessment (Datenschutzfolgenabschätzung) ist ein Prozess, mit dem Risiken und Auswirkungen der Verarbeitung und Speicherung von Daten zu einer Person identifiziert werden. Die Datenschutzfolgenabschätzung wird in der Regel bei der Verarbeitung bestimmter Datenkategorien oder für Datenverarbeitungen mit hohem Umfang oder hohem Risiko angewendet.

DSGVO
DSGVO steht für „Datenschutz-Grundverordnung".

GDPR
Die General Data Protection Regulation (deutsch: DSGVO) ist das Datenschutzgesetz der EU, durch das ein konsolidierter Rechtsrahmen für den Datenschutz für alle Mitgliedstaaten der Europäischen Union (EU) sowie Island, Liechtenstein, Norwegen und die Schweiz – diese Länder gehören zum Binnenmarkt des Europäischen Wirtschaftsraums (EWA) – festgelegt wurde. GDPR trat im Mai 2018 in Kraft und gilt für die Verarbeitung von personenbezogenen Daten der Bürger der EU – unabhängig davon, ob die Verarbeitung in der EU oder außerhalb der EU stattfindet.

Personenbezo-gene Daten
Alle Informationen über eine identifizierte oder identifizierbare Person (Namen, E-Mail-Adressen, IDs usw.)

PII
Personal Identifying Information (Persönliche Identifikationsdaten) sind alle Arten von Daten, die zur Identifizierung einer Person verwendet werden können, z. B. die Telefonnummer, Ausweisdaten und Sozialversicherungsnummern.

SAR
Ein Subject Access Request (Antrag auf Offenlegung der gespeicherten Daten) ist ein Mechanismus, mit dem Einzelpersonen eine Kopie der Daten anfordern können, die eine Organisation über sie speichert. Mit dem Antrag können Einzelpersonen außerdem ihre Rechte geltend machen, z. B. das Recht auf Berichtigung oder das Recht auf Vergessen.

Grundbegriffe zum Datenschutz

Sieben Hauptprinzipien

Die DSGVO (englisch GDPR) folgt sieben Hauptprinzipien: Rechtmäßigkeit, Fairness und Transparenz, Zweckgebundenheit, Datenminimierung, Genauigkeit, eingeschränkte Speicherung, Integrität und Vertraulichkeit und Rechenschaftspflicht.

Sonderdaten-kategorien

Eine genau definierte Untergruppe personenbezogener Daten, die als sensibel betrachtet werden, z. B. Herkunft, ethnische Herkunft, Sexualität oder politische Überzeugungen. Die Verarbeitung dieser Daten unterliegt zusätzlichen Anforderungen.

UK Data Protection Act (2018)

Das Datenschutzgesetz des Vereinigten Königreichs gilt für Einwohner des Vereinigten Königreichs und kombiniert die DSGVO mit umfassenderen Datenschutzthemen.

Verschlüsselte Daten

Diese Daten werden in einen Geheimcode chiffriert, der nur durch einen eindeutigen digitalen Schlüssel entsperrt werden kann. Mithilfe von Verschlüsselung wird verhindert, dass die Daten von unberechtigten Personen gelesen, gestohlen, verändert oder angegriffen werden können. Es handelt sich um eine besonders wirkungsvolle Kontrolle im Fall eines Datenverlusts oder -diebstahls.

Sie haben eine digitale Strategie, könnten beim Thema Informationssicherheit aber noch Unterstützung brauchen?

In den letzten Jahren haben sich die digitale Transformation und Veränderungen von Geschäftsprozessen in der AECO-Branche (Architecture, Engineering, Construction and Operations) erheblich beschleunigt.

Die Digitalisierung, Construction 4.0 und KI-Technologien haben während der Pandemie im Jahr 2020 einen wahren Boom erfahren. Unternehmen erkennen zunehmend, welche Vorteile intelligentes Bauen hat und wie es für höhere Effizienz und Produktivität sowie mehr Nachhaltigkeit, Gesundheit und Sicherheit sorgt.

Die Konzentration auf eine digitale Strategie kann viele verschiedene Softwarekomponenten wie BIM- und CDE-Plattformen umfassen und stellt ein sehr nützliches Toolkit für den gesamten Lebenszyklus eines Bauprojekts dar. Neben den Zeit- und Kosteneinsparungen zeigt sich immer mehr, dass durch die Daten und Analysen, die nun erfasst werden können und die wichtige Erkenntnisse für bessere zukünftige Projekte liefern, ein großer Mehrwert entsteht.

Digitalisierung ist wichtig, aber achten Sie auf die Schwachstellen

Im Rahmen der Digitalisierung werden immer größere Mengen an Daten erfasst, verarbeitet und gespeichert. Zu diesen Daten gehören häufig sensible Kunden-, Finanz- und personenbezogene Daten sowie geistiges Eigentum und kommerziell sensible Informationen. Die Tiefe der gespeicherten Daten hat das Profil von AECO-Organisationen und ihrer Lieferkette für Cyberkriminelle besonders interessant gemacht. Damit ist das Risiko, von einer Reihe krimineller Akteure, von Ransomware-Gruppen bis hin zu gesponserten Advanced Persistent Threats (APTs), angegriffen zu werden, gestiegen.

Damit eine Bedrohung Erfolg hat, muss sie eine Schwäche ausnutzen – sei es eine technische Schwachstelle wie ein Softwarebug, eine Schwachstelle im Prozedere wie das Kopieren von unverschlüsselten Daten auf ein USB-Laufwerk oder eine menschliche Schwäche wie z. B. eine Person, die auf eine Scam-E-Mail hereinfällt.

Für den Schutz vor Angriffen ist traditionell eine Informationssicherheitsstrategie erforderlich, die sicherstellt, dass digitale Systeme über ihren gesamten Lebenszyklus gewartet, erneuert, überwacht, gesichert und mit Ressourcen ausgestattet werden. Darüber hinaus werden strenge technische und Compliance-Normen (ISO27001, SOC2, NIST-800, Cyber Essentials Plus usw.) angewendet. Das Personal muss Schulungen zu den Prozessen erhalten und für Cyberbedrohungen sensibilisiert werden. Die Bedrohungen müssen erkannt und schnell behoben werden, damit die Angreifer keine Zeit haben, das Netzwerk zu schädigen. All dies erfordert nicht nur ein hohes Engagement für Informationssicherheit und Datenschutz seitens des Unternehmens, sondern auch erhebliche Investitionen.

Dies sind jedoch nicht die einzigen großen Herausforderungen für die AECO-Branche. Darüber hinaus müssen der Datenzugriff in einer unternehmensübergreifenden kollaborativen Umgebung mit Nutzern aus unterschiedlichen Organisationen verwaltet, Sicherheitsstandards und -richtlinien entwickelt und eingehalten und gleichzeitig die Anforderungen des Kunden erfüllt werden. Die dazu verwendeten Werkzeuge müssen flexibel sein und die Durchsetzung von Sicherheitskontrollen gewährleisten, deren Pflege nicht von einer einzelnen Organisation abhängt.

Aus Beispielen für Verstöße gegen die Informationssicherheit haben wir gelernt: Cyberangriffe führen zu enormen Unterbrechungen, finanziellen Verlusten und Reputationsschäden. Hinzu kommt der für Bauunternehmen besonders wichtige Aspekt,dass wertvolle Daten in die falschen Hände gelangen können. Bausoftware verarbeitet sehr viele sensible Informationen von Bauplänen, Entwürfen und Plänen bis hin zu Daten zu Schwachstellen in Gebäuden oder anderen Mängeln, die ausgenutzt werden könnten. Diese sensiblen Informationen werden benötigt, um qualitativ hochwertige Projekte zu erstellen; sie können sich jedoch auch gegen ein Unternehmen richten, wenn sich Hacker Zugang verschaffen.

Nicht zuletzt ist auch die Verpflichtung des Unternehmens zum Schutz der Daten seiner Mitarbeiter, Kunden und der gesamten Lieferkette von Bedeutung. Eine Verletzung personenbezogener Daten kann in endlosen Rechtsverfahren und mit hohen Strafen enden, ganz zu schweigen von der erheblichen Rufschädigung, von der sich ein Unternehmen möglicherweise nur mühsam wieder erholt.

Wie können Sie und alle Beteiligten wertvolle Daten schützen?

Die Digitalisierung führt zu einer stärkeren Vernetzung und Zusammenarbeit der unterschiedlichen Beteiligten an einem Bauprojekt wie Architekten, Ingenieure, Vertragspartner und Lieferanten. Diese zunehmende Vernetzung hat zahlreiche Vorteile, birgt jedoch auch das Risiko, dass sich Sicherheitsverstöße, die eine Partei betreffen, schnell im ganzen Ökosystem des Projekts ausbreiten und andere Beteiligte beeinträchtigen können.

Bauunternehmen müssen daher das Thema Informationssicherheit priorisieren und robuste Sicherheitsmaßnahmen wie Patchmanagement, Sicherheitsmonitoring, Zugriffskontrollen, Verschlüsselung und Netzwerksegmentierung einsetzen, um ihre Systeme und Daten vor Cyberbedrohungen zu schützen. Außerdem müssen sie sicherstellen, dass ihre Mitarbeiter in den bewährten Sicherheitspraktiken geschult werden und die Risiken von Cyberattacken kennen. Durch proaktive Maßnahmen zum Schutz der Systeme und Daten und ein gut informiertes Personal können die Angriffsrisiken minimiert und sichergestellt werden, dass die gesamte Lieferkette erfolgreich funktioniert und mithilfe digitaler Technologie die bestmöglichen Assets erzeugt.

Eine eigene Strategie für Informations-sicherheit entwickeln

Auf dem Papier sieht das alles recht einfach aus, aber welche wichtigen Punkte müssen bei der Planung einer Informationssicherheitsstrategie bedacht werden? Folgende Aspekte sollten Sie berücksichtigen:

- Ein klar definiertes Ziel sowie die konkreten Schritte, mit denen dieses erreicht werden kann. Dazu ist es unter anderem wichtig, das Vertrauen des Kundenstamms aufzubauen, einen Betriebskontinuitätsplan zu erstellen oder eine Zertifizierung nach einem anerkannten Standard für Informationssicherheit einzuführen.
- Eine sorgfältige Risikobewertung, mit der Schwachstellen bei der Speicherung und Verarbeitung von Daten erkannt werden. Idealerweise sollten Sie sich dabei zuerst auf die Bereiche mit dem höchsten Risiko konzentrieren.
- Einrichtung eines Information Security Management System (ISMS)-Teams, das für die Steuerung und Kontrollen verantwortlich ist, die für die Einhaltung konsequenter Datenschutzstandard erforderlich sind.
- Entwicklung von Vorfallreaktions- und Betriebskontinuitätsplänen, damit die Arbeit auch im Fall eines Sicherheitsverstoßes fortgeführt werden kann.
- Mithilfe festgelegter Rollen und Verantwortlichkeiten lässt sich Informationssicherheit nahtloser gewährleisten. Klare Entscheidungen und die Zuweisung von ausreichenden Ressourcen sorgen dafür, dass Sie in einemWorst-Case-Szenario das Schlimmste vermeiden.
- Prüfen und entwickeln Sie Richtlinien und Verfahren und organisieren Sie regelmäßige Vorfallüberprüfungen. Die besten Ergebnisse für alle Prozesse lassen sich in Zusammenarbeiten erzielen.
- Fördern Sie eine Kultur, in der jeder Verantwortung für den Datenschutz übernimmt. Mithilfe einer Kombination aus regelmäßigen Schulungen und Angriffssimulationen muss die Organisation sicherstellen, dass ihre Teams in puncto Gefahren durch Bedrohungen wie Phishing-Scams immer auf dem neuesten Stand sind.
- Bewertungen durch einen externen Anbieter. Eine solche Bewertung geht jedoch über das Abhaken von Kriterien und einen Badge für Ihre Website hinaus. Bei solchen externen Bewertungen können Lücken in Ihrem Sicherheitsplan erkannt werden, die für eine Person, die das Netzwerk täglich nutzt, möglicherweise nicht offensichtlich sind.

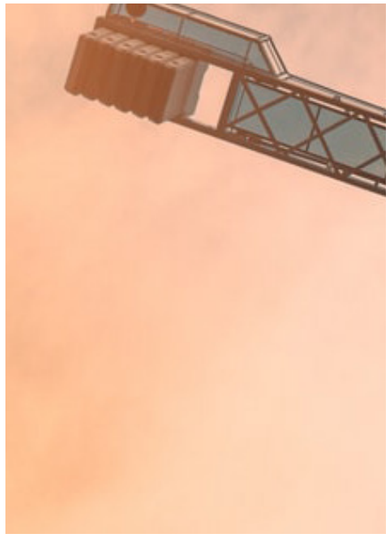
Arbeiten Sie mit Anbietern zusammen, die den Goldstandard in puncto Sicherheit erfüllen.

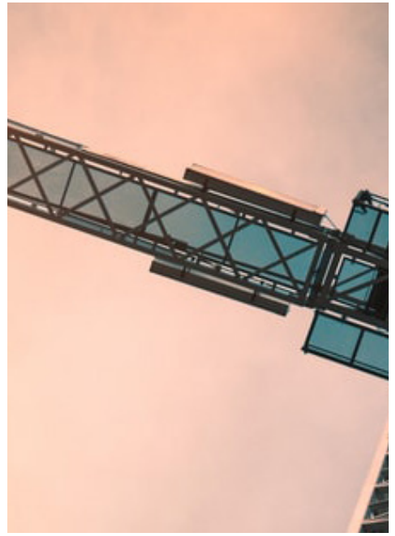
Schauen wir uns einmal näher an, was Sie von einem Softwareanbieter erwarten sollten, der sich um die Sicherheit Ihrer Daten kümmert.

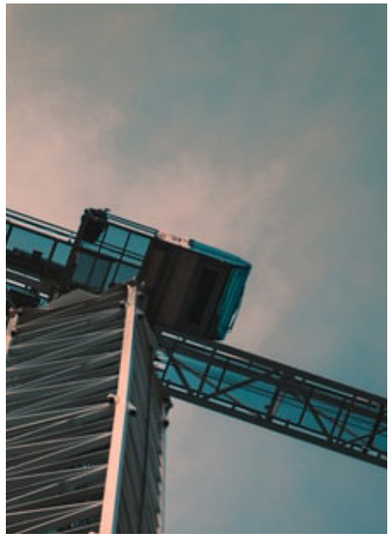
Sicherheitstyp	Was bedeutet das?	Bei Thinkproject
Sichere Entwicklungs-Praktiken	Entwicklungsteams sollten Werkzeuge nutzen, um ihre Arbeit und die Bereitstellung von neuem Code in einer Version zu strukturieren. Die Bereitstellung sollte Mechanismen enthalten, mit denen Schwachstellen auf Komponenten-oder Codeebene erkannt werden. Sie sollte die bewährten Praktiken der Codeentwicklung erfüllen und das Testen des Codes sollte möglichst automatisiert werden.	Thinkproject arbeitet mit einer definierten DevOps-Struktur unter Verwendung von CI/CD-Prinzipien (Continuous Integration/Continuous Delivery), um zu gewährleisten, dass zuverlässiger und ausführlich getesteter Code für die Produktion bereitgestellt wird. Während der Entwicklung werden Werkzeuge eingesetzt, die Schwachstellen in den Komponenten identifizieren und Codefehler in Echtzeit aufdecken. Während der Entwicklung werden Werkzeuge eingesetzt, die Schwachstellen in den Komponenten identifizieren und Codefehler in Echtzeit aufdecken.
Physische Sicherheit	Lokale und Remote-Büros müssen immer gegen unberechtigten Zugriff geschützt sein. Das kann z. B. durch Berechtigungskarten für den Zugang zu Gebäuden, einer An-/Abmelderichtlinie für Besucher und CCTV-Kameras bewerkstelligt werden.	Unsere Büros sind mithilfe von Zugangskarten geschützt und alle Mitarbeiter und Besucher müssen sich im Gebäude an- und abmelden. Darüber hinaus setzen wir auf CCTV-Kameraüberwachung, haben eine Politik des papierlosen Büros und auf sensible Informationen können nur berechtigte Personen zugreifen.
Netzwerksicherheit	Das Unternehmensnetzwerk muss über robuste Sicherheitsmaßnahmen und aktuelle Risiko- und Kontinuitätspläne verfügen. Netzwerksicherheit kann durch Firewalls, Antivirus-Software und Intrusionserkennungssysteme gewährleistet werden.	Unser sicheres Büronetzwerk und die sicheren Rechenzentren sind Teil unserer ISO27001-Akkreditierung und werden regelmäßig überprüft.
Mitarbeiter-schulungen	Jeder Mitarbeiter im Unternehmen sollte die Informationssicherheitsrichtlinien und -verfahren in regelmäßigen Schulungen genau kennenlernen. Die Mitarbeiter müssen gute Sicherheitsmaßnahmen umsetzen, wie z. B. Gerätesperre, Meldung von Phishing-Scams und sichere Kennwörter.	Alle unsere Mitarbeiter nehmen jedes Jahr verpflichtend an Schulungen zu unterschiedlichen Themen teil, z. B. Cybersicherheit und Datenschutz. Alle Richtlinien müssen von jedem Mitarbeiter anerkannt und bestätigt werden.
Einhaltung von Rechtsvorschriften (Compliance)	Das Unternehmen muss in Bezug auf die relevanten Sicherheitsvorschriften auf dem neuesten Stand sein. Die Einhaltung dieser Vorschriften zeugt von den aktiven Bemühungen zu einem Sicherheits-bewusstsein seitens des Unternehmens. Zu den Vorschriften gehören z. B. GDPR, ISO 27001 oder Cyber Essentials Plus.	Wir führen jährlich externe und interne Audits im Rahmen des ISMS-Auditprogramms durch, um die ISO27001-Zertifizierung zu erlangen. Darüber hinaus erhalten wir regionale Zertifizierungen.

Sicherheitstyp	Was bedeutet das?	Bei Thinkproject
Risiko durch Dritte	Das Unternehmen muss ein Lieferantenmanagementprogramm einrichten, damit auch Drittlieferanten angemessene Sicherheitsmaßnahmen ergreifen.	Wir verfügen über einen Lieferantenmanagementprozess, der unsere ISMS-Anforderungen erfüllt. Darunter fallen die Prüfung externer Lieferanten durch unser Compliance-Team, NDAs, DSGVO-Prüfungen und weitere Maßnahmen, mit denen wir die Einhaltung unserer Standards gewährleisten. Unsere Drittlieferanten werden regelmäßig im Hinblick auf die Einhaltung der Vorschriften bewertet.
Datenschutz	Sofern an Ihrem Standort anwendbar muss Ihr Lieferant die DSGVO erfüllen. Darüber hinaus muss das Unternehmen in der Lage sein, Ihnen alle Informationen zu seinen Datenschutzpraktiken vorzulegen und nachzuweisen, wie es Ihre Informationen schützt.	Die DSGVO-Compliance von Thinkproject-Unternehmen und ihren Produkten hat höchste Priorität. Für verschiedene juristische Einheiten von Thinkproject und Länder werden externe Datenschutzbeauftragte beauftragt wie z.B. thinkprojekt Deutschland GmbH und thinkproject Holding GmbH. In anderen Einheiten werden interne Datenschutzbeauftragte oder Datenschutzkoordinatoren ernannt, die Compliance mit den Datenschutzanforderungen der Gruppe sicherstellen. Regelmäßige Datenschutzaudits sind integraler Bestandteil unseres Datenschutzmanagementsystems. Alle unsere Mitarbeiter müssen jedes Jahr eine DSGVO-Schulung absolvieren. Wir halten uns an unsere konzernweiten, robusten Datenschutzrichtlinien.
Vorfallreaktion (Incident response)	Es ist wichtig, dass jeder Anbieter über Pläne verfügt, die im Fall einer Sicherheitsverletzung in Kraft treten. Dazu gehören Erkennungs-, Reaktions- und Wiederherstellungspläne sowie Maßnahmen, mit denen die Kunden in einem solchen Fall informiert werden.	Unser Vorfallmanagementverfahren ist in Kraft und wird regelmäßig getestet und bewertet, um sicherzustellen, dass es bei allen Vorfällen schnell reagiert. Unsere Mitarbeiter erhalten verständliche Schulungen dazu, wie sie Vorfälle über unser Whistleblower-Portal und unsere OneTrust-Plattform melden können.
Schwachstellen-management	Der Anbieter sollte seine Software regelmäßig aktualisieren, patchen und testen, um Angreifer zu hindern, etwaige Schwachstellen auszunutzen.	Im Rahmen unseres sicheren Rechenzentrumsbetriebs arbeiten wir mit Werkzeugen, die potenzielle Schwachstellen erkennen, sodass wir schnell handeln und potenzielle Bedrohungen abwehren können.

Sicherheitstyp	Was bedeutet das?	Bei Thinkproject
Historie von Sicherheits-vorfällen	Der Blick auf vergangene Sicherheitsvorfälle ist eine gute Maßnahme zum Messen der Transparenz der Organisation. Der Anbieter muss in der Lage sein, Erkenntnisse darüber zu liefern, wie auf vergangene Erfahrungen reagiert wurde und welche Maßnahmen seit diesem Vorfall implementiert wurden.	Alle Vorfällen werden im OneTrust-Werkzeug nachverfolgt. Für jeden Vorfall werden gemäß unserem Vorfallmanagement-verfahren Ursachenanalysen durchgeführt und Erfahrungen gesammelt.







Einblicke von einem Experten

Dr. Ralf Hundhammer, CTO bei Thinkproject, legt seine Überlegungen zur Informationssicherheit dar.

Wir haben Dr. Ralf Hundhammer darum gebeten, seine Überlegungen zu einer Reihe von Fragen zum Thema Informationssicherheit darzulegen. Ralf blickt auf mehr als 20 Jahre Erfahrung in diesem Bereich zurück und hat wertvolle Erkenntnisse gesammelt.

Wenn Ihr Unternehmen mit dem Thema Informationssicherheit noch nicht vertraut wäre, wie würden Sie anfangen, Ihre Daten zu schützen und eine Informationssicherheitsstrategie einzurichten?

Eine Sicherheitsstrategie einzuführen ist keine leichte Aufgabe. Aber wie jeder Prozess kann auch dieser in kleine Schritte unterteilt werden, die sich zu einem großen Ganzen zusammensetzen. Zuerst ist es wichtig, einen Schritt zurückzugehen und die Daten kennenzulernen. Man muss verstehen, warum sie da sind und warum sie benötigt werden. Ist es wirklich nötig, diese Daten zu verarbeiten? Können sie verschlüsselt werden? Dies sind nur einige Fragen, über die man nachdenken muss. Wenn Sie verstehen, welche Daten in Ihrem Unternehmen verarbeitet werden, können Sie und Ihr Sicherheitsteam die entsprechenden Risiken bewerten und die Daten angemessen schützen.

Für das Sicherheitsteam ist eine kontinuierliche Weiterbildung extrem wichtig, damit es immer auf dem neuesten Stand ist. Regelmäßig kommen neue Bedrohungen auf und das Team muss sich dessen bewusst sein. Sie sollten viel Energie in die Entwicklung Ihres Sicherheitsteams investieren, da eine Datenschutzverletzung deutlich teurer wird. Das Gleiche gilt für das gesamte Personal: Das gesamte Unternehmen muss potenzielle Bedrohungen bewerten können, egal ob durch die regelmäßige Simulation von Phishing-Angriffen oder durch die regelmäßige Änderung von Kennwörtern. Denken Sie dabei auch an den physischen Raum. Bei Thinkproject leben wir z. B. die Politik des aufgeräumten Schreibtischs (clear desk policy) und des papierlosen Büros. Damit sind weniger Informationen offen zugänglich.

Wenn Sie diese Aspekte berücksichtigt haben, kommt der Rest häufig ganz von allein. Erstellen Sie eindeutige Informationssicherheitsrichtlinien, arbeiten Sie mit strengen Authentifzierungsmethoden und stellen Sie sicher, dass alles jederzeit aktualisiert wird. Bereiten Sie einen Vorfallreaktionsplan vor, führen Sie Audits durch und bauen Sie eine fundierte Wissensbasis auf, um eine Akkreditierung zu erhalten, anhand derer Ihre Kunden erkennen, dass Sie ein sicherheitsbewusstes Unternehmen sind.

Cyberangriffe werden immer ausgereifter. Was ist Ihrer Meinung nach das größte Risiko und wie sollte die AECO-Branche damit umgehen?

Eine der größten Sorgen sind potenzielle Angriffe auf wichtige Infrastruktur und sensible Projektdaten. Mit der Verbreitung von integrierten Systemen, Cloud-Plattformen und Internet of Things (IoT)-Geräten hat sich die Reichweite von Angriffen massiv vergrößert. Wenn Organisationen eine starke technische Abwehr mit geschulten Mitarbeitern kombinieren, können sie Cyberrisiken wirksam mindern und ihre kritischen Assets schützen.

In dem Maße, wie sich die Technologie weiterentwickelt, werden auch die Angriffe immer ausgeklügelter. Ihr ISMS muss regelmäßig überprüft werden und ausreichend flexibel sein, um an immer fortgeschrittenere Attacken angepasst zu werden. Es ist ein ständiger Balanceakt: Das Unternehmen muss anpassungsfähig sein und gleichzeitig eine strenge Roadmap einhalten, die das gesamte Unternehmen kennt.

Organisationen müssen die Zusammenarbeit und die Freigabe von Informationen zwischen Unternehmen priorisieren und mit Experten für Cybersicherheit zusammenarbeiten, damit die Branche dauerhaft so gut informiert ist wie nur möglich. Wenn alle zusammenarbeiten, können die Risiken minimiert werden, vor allem vor dem Hintergrund der vielen wertvolle Erfahrungen, die Unternehmen gesammelt haben.

Welche bewährten Praktiken wendet Thinkproject an, um seine Kunden zu schützen?

Datenschutz nehmen wir schon seit der Gründung unseres Geschäft sehr ernst. Als deutsches Unternehmen mit Sitz in Europa sind wir in puncto Datenschutz besonders gut ausgewiesen! Unser Compliance-Team unternimmt alles, was möglich ist, um sicherzustellen, dass alle Mitarbeiter regelmäßige Schulungen zu DGVO, ISMS und unseren Notfallplänen erhalten.

Wir sind stolz, robuste Maßnahmen zu haben, mit denen wir die Sicherheit unserer Kunden-, Mitarbeiter- und Geschäftsdaten gewährleisten. In unserem anschaulichen Diagramm sind unsere Maßnahmen dargestellt und es ist erkennbar, wie sie regelmäßig bewertet und aktualisiert werden.

Garantierte Sicherheit: Schützen Sie Ihre Informationswerte

Diese Tipps helfen Ihnen, Ihre Informations-sicherheit und Ihren Datenschutz in einem robusten, widerstandsfähigen System zu bündeln.

Regelmäßige Risikobewertungen durchführen

Potenzielle Schwachstellen aufdecken

Bedrohungen identifizieren

Bedrohungen bewerten und priorisieren

Erkenntnisse zur Entwicklung eines Risikomanagementplans verwenden

Eindeutige Sicherheitsrichtlinien einrichten

Bewährte Praktiken aufführen

Beratung zur Systemnutzung und zum Umgang mit Daten

Mitarbeiter über ihre Verantwortlichkeiten aufklären

Richtlinien und Verfahren regelmäßig prüfen

Mitarbeitern Wissen vermitteln

Regelmäßige Schulungen und Bewertungen durchführen

Mitarbeiter zu bewährten Praktiken (z. B. sicheren Kennwörtern) schulen

Erfahrungen zu Bedrohungen mit Mitarbeitern teilen

Strenge Zugriffskontrollen verwenden

Sicherstellen, dass nur berechtigte Personen auf die Daten zugreifen können, die sie benötigen

Authentifzierungsmetho-den für zusätzliche Sicherheit einrichten (z. B. Privileged Access Management)

Infrastruktur auf neuestem Stand halten

Alle Systeme regelmäßig aktualisieren und patchen

Firewalls nutzen, um Schäden abzuwehren

Netzwerke schützen, um unberechtigten Zugriff zu vermeiden

Top-Tipps

Tipps zur Hilfe
Fortsetzung

Vorschriften einhalten

Sicherstellen, dass nur berechtigte Personen auf die Daten zugreifen können, die sie benötigen

Authentifzierungsmethoden für zusätzliche Sicherheit einrichten (z. B. Privileged Access Management)

Sensible Daten verschlüsseln

Verschlüsselte Daten sind nicht lesbar, selbst wenn sie angegriffen wurden

DSGVO-Richtlinien sollten die Datenverschlüsselung umfassen

Vorfallreaktionsplan erstellen

Reaktionsplan entwickeln und regelmäßig testen, um sicherzustellen, dass aktuelle Faktoren berücksichtigt wurden

Rollen und Verantwortlichkeiten sowie eindeutige Kommunikationskanäle definieren

Zusammenarbeit und Informationsaustausch mit anderen Organisationen

Der Informationsaustausch mit Branchenkollegen ist eine gute Möglichkeit, die aktuelle Angriffslandschaft zu verstehen

Die Weitergabe bewährter Praktiken stellt sicher, dass sich jeder schützen kann

Häufige Bewertung von Lieferkette und Anbietern

Ihre Software- und Cloud-Anbieter sollten eigene Richtlinien zum Schutz der Daten Ihrer Organisation haben

Diese sollten mit Ihren eigenen Sicherheitsstandards übereinstimmen

Trends im Bereich Informations-sicherheit, die jedes Unternehmen im Jahr 2023 und darüber hinaus kennen sollte.

In der zunehmend digitalisierten Landschaft, die sich dauerhaft verändert, gibt es immer mehr Bewegung. Was vor einigen Jahren noch der Goldstandard der Informations-sicherheit war, kann heute schnell veraltet sein. Daher müssen Sie sich selbst regelmäßig zu den bewährten Praktiken auf dem Laufenden halten, damit Ihr Unternehmen bestmöglich geschützt ist.

Die wichtigsten Trends haben wir im Folgenden für Sie zusammengefasst.

Zero-Trust-Sicherheit

Wenn Ihre Website aufgrund eines Angriffs offline geht, ist das schon schlimm genug. Aber wenn Ihr gesamtes System durch eine Cyberbedrohung geschädigt wird, ist das eine Katastrophe für Ihr Unternehmen. Zero-Trust-Sicherheit ist ein Netzwerksicherheitsansatz, bei dem davon ausgegangen wird, dass der gesamte Datenverkehr potenziell feindlich ist. Daher müssen vor der Vergabe von Zugriffen Prüfungen durchgeführt werden, sodass Cyberbedrohungen ihre Ziele nur noch schwer erreichen können.

Multifaktor-Authentifizierung (MFA):

MFA kann das Risiko, dass Konten angegriffen werden und Sicherheitsverletzungen entstehen, deutlich reduzieren. Wenn mehr als eine Form der Authentifizierung (z. B. ein Kennwort und die Rücksendung eines auf ein Mobilgerät gesendeten Codes) erforderlich ist, hat es ein potenzieller Hacker viel schwerer, Zugriff auf Ihre Unternehmensdaten zu erhalten.

KI und Maschinelles Lernen:

Künstliche Intelligenz (KI) und Maschinelles Lernen (ML) bieten heute Möglichkeiten für eine deutlich bessere Sicherheit. Sowohl KI als auch ML werden für die Echtzeit-Analyse [5] riesiger Datenmengen eingesetzt, um Trends zu analysieren und ungewöhnliche Verhaltensweisen oder Aktivitäten zu erkennen.

Investitionen in Cyber-Sicherheits-Talente:

Da das Thema Cybersicherheit noch relativ jung ist, erleben wir derzeit weltweit einen Mangel an Talenten in diesem Bereich. Damit muss ein Unternehmen, das ein motiviertes Team für Informationssicherheit haben möchte, in Schulungen, Entwicklung und Weiterbildung vorhandener Mitarbeiter investieren. Darüber hinaus werden Praktika im Bereich Cybersicherheit immer beliebter, bei denen neue Talente Unternehmen suchen, in denen sie sich weiterentwickeln können.

Datenschutzvorschriften:

Mit der steigenden Bedeutung von Datenschutz müssen Unternehmen sicherstellen, dass sie die entsprechenden Vorschriften erfüllen, wie z. B. die DSGVO. Dazu müssen sie geeignete Sicherheitsmaßnahmen wie Datenverschlüsselung und Zugriffskontrollen einrichten und sicherstellen, dass sie über Richtlinien und Verfahren verfügen, mit denen sie die Daten ihrer Kunden schützen.

5 www.analyticsinsight.net

Sicherheitsbedrohungen proaktiv entgegentreten

Fazit: In der heutigen schnelllebigen digitalen Landschaft müssen Unternehmen ihre eigenen Daten und die Daten ihrer Kunden proaktiv vor Cyberbedrohungen schützen. Die Konsequenzen von Datenschutzverletzungen und Angriffen sind häufig sowohl für Unternehmen als auch für Einzelpersonen katastrophal.

Durch eine proaktive Denkweise und eine umfassende Sicherheitspolitik können Unternehmen Schwachstellen erkennen, Risiken bewerten und robuste Sicherheitsmaßnahmen einrichten, die dem Unternehmen (bei regelmäßiger Wartung) gute Dienste leisten können. Darüber hinaus müssen sie sich zu den Sicherheitstrends kontinuierlich auf dem Laufenden halten und Vorschriften einhalten. Dies sind wesentliche Komponenten eines proaktiven Informationssicherheitsansatzes und positive Zeichen, aufgrund derer Unternehmen – Kunden und Anbieter – bewertet werden.

Wenn Sie mehr darüber erfahren möchten, wie Thinkproject innovative Bausoftwarelösungen mit Sicherheit nach Goldstandard kombiniert, besuchen Sie unser Trust Center.

Thinkproject Trust Center

thínkproject

Thinkproject ist Europas führender SaaS-Anbieter für Common Data Environment, Asset-, BIM- und Field-Management sowie Projektcontrolling. Thinkproject digitalisiert Bauunternehmen, Bauherren, Projektsteurer und Planer seit mehr als 20 Jahren mit einer leistungsstarken, flexiblen Technologie in Kombination mit Beratungskompetenz aus einer Vielzahl komplexer Großprojekte.

Mit weltweit 650+ Mitarbeitenden bietet Thinkproject digitale Lösungen an, die den gesamten Lebenszyklus eines Bauprojekts abdecken.

75.000
PROJEKTE

300.000
ANWENDER

650+
KUNDENORIENTIERTE MITARBEITER/INNEN

3.250
KUNDEN

60
LÄNDER

23
NIEDERLASSUNGEN

Thinkproject.com