



CYBERVERSICHERUNG

Cyberpraxis: Sicherheitsaspekte ...

Foto: Ken Schluchtmann, diephotodesigner.de

... im Building Information Management (BIM)

Einleitung: Building Information Management (BIM) hat sich als kooperative Arbeitsmethodik in der Architektur- und Ingenieursbranche entwickelt. Durch die Möglichkeit, alle relevanten Daten eines Bauprojekts in einem digitalen Modell zu verwalten und zu visualisieren, können Effizienz und Kommunikation verbessert werden. Allerdings bringt die Verwendung von BIM auch neue Herausforderungen mit sich, insbesondere in Bezug auf die Datensicherheit..

Um die Datensicherheit im Building Information Management (BIM) zu gewährleisten, gilt es von den BIM-Beteiligten mehrere Aspekte zu beachten (z.B. Schadsoftware, Softwarefehler, Kollision der Fachmodelle, mangelhafte Hard- und Software, Haftung für übernommene Softwareobjekte können „drohen“). Diese Aspekte können möglicherweise zu Sicherheitsrisiken führen, weshalb eine regelmäßige Datensicherung von großer Bedeutung ist.

WAS IST BIM?

Building Information Management (BIM) ist ein umfassender digitaler Ansatz zur Planung, dem Bau und dem Betrieb von Gebäuden. Es ermöglicht Architekten, Ingenieuren und anderen Beteiligten, Informationen über ein Bauprojekt in Echtzeit zu teilen und zusammenzuarbeiten. Das BIM-Modell enthält geometrische Daten, Materialien, technische Informationen, Kosten und Zeitpläne. Dadurch können Entscheidungen fundierter getroffen und Konflikte frühzeitig erkannt werden.

Um diese Risiken zu minimieren, sollten Sie sicherstellen, dass nur autorisierte Personen Zugriff auf die BIM-Daten haben. Implementieren Sie robuste Zugriffsrechte und verlangen Sie starke Authentifizierungsmethoden wie Passwörter und Zwei-Faktor-Authentifizierung. Dadurch wird eine angemessene Informationssicherheit gewährleistet.

Verschlüsseln Sie die BIM-Daten, um den unbefugten Zugriff oder die Manipulation durch Dritte zu verhindern. Verwenden Sie starke Verschlüsselungsprotokolle, um die Vertraulichkeit der Informationen zu gewährleisten.

Regelmäßige Backups sind unerlässlich, um gegen Datenverlust oder -beschädigung durch Hardwarefehler, Cyberangriffe oder menschliche Fehler gewappnet zu sein. Stellen Sie sicher, dass es effektive Mechanismen zur Wiederherstellung der Daten gibt. Diese sollten auch regelmäßig auf Komplikationen beim Wiedereinspielen getestet werden.

Verwenden Sie sichere Netzwerkprotokolle, um die Kommunikation zwischen den BIM-Teilnehmern zu schützen. Aktualisieren Sie regelmäßig Ihre Software und halten Sie Ihre Netzwerkinfrastruktur gut geschützt.

Mitarbeiter sollten für die Bedeutung der Informationssicherheit und Best Practices sensibilisiert werden. Sorgen Sie dafür, dass alle BIM-Teilnehmenden über die Risiken von Phishing, Malware und anderen Sicherheitsbedrohungen informiert sind.

In einer Zeit, in der digitale Technologien die Architektur- und Ingenieursbranche weiter vorantreiben, ist die Datensicherheit im Building Information Management (BIM) von größter Bedeutung. Mit klaren Verträgen, einer robusten Sicherheitsinfrastruktur und geschultem Personal können BIM-Beteiligte potenzielle Sicherheitsrisiken minimieren und das volle Potenzial dieser bahnbrechenden Technologie ausschöpfen.



Autor



Peter Bertram

Peter Bertram
Produktmanagement & Underwriting Cyber
HDI Versicherung AG
Hannover

Als Schutzschirm ergänzt eine Cyberversicherung das Unternehmenseigene Risikomanagement und hilft im Schadenfall mit einem umfassenden Expertennetzwerk, auch bei Datenschutzverstößen oder dem finanziellen Ausgleich einer Betriebsunterbrechung. Die Tätigkeiten im Rahmen von BIM-Projekten sind grundsätzlich vom Deckungsumfang erfasst.

TIPP

Die HDI Cyberversicherung hilft zusätzlich auf dem Weg zu mehr Informationssicherheit, da sie einen kostenlosen Zugang zu der Perseus Premium Präventionsplattform bietet. Diese unterstützt die Kunden mit Awareness-Schulungen für die Mitarbeiter, einem Richtliniengenerator oder einem Notfallplan.



Foto: Ken Schluchtmann, diephotodesigner.de