CYBERVERSICHERUNG

Cyberrisiken...

Foto: Ken Schluchtmann, diephotodesigner.de

...für Ingenieure

Allgegenwärtig ist dieser Zeit das Thema Cyber. Ob in Verbindung mit aktuellen Geschehnissen in und um die Ukraine-Krise oder als generelles Risiko auch für Ingenieure. Geschichten über Phishing, Hacking und die Verschlüsselung von Daten finden sich in nahezu unendlicher Masse im Internet und immer häufiger auch im Kreis der Bekannten. Das Bundesamt für Sicherheit und Informationstechnologie (BSI) gibt für das Jahr 2021 die Anzahl von 144 Millionen neuen Schadprogrammen an und unterstreicht damit auch die aktuelle Bedeutung von Cyber-Risiken. Aber was sind die häufigsten Einfallstore der Hacker? Wie kann man sich schützen und absichern?

Nahezu alle Branchen, insbesondere auch das Bau- und Planungswesen durch z.B. den Einzug von BIM, fußen mehr und mehr auf digitalen Prozessen. Daher rücken diese Fragestellungen zur Cybersicherheit auch bei Architekten und Ingenieuren mehr und mehr in den Fokus.

Das Cyber-Risiko birgt vielfältige Angriffsszenarien

Die Einschätzung der aktuellen Bedrohungslage gehört im Cyber-Kontext zu einer der wichtigsten Aufgaben. Hier lohnt sich ein Blick in die Daten des BSI, welches jährlich einen Bericht zur Lage der IT-Sicherheit in Deutschland veröffentlicht. So ist im Bericht für das Jahr 2021 neben den bereits erwähnten 144 Millionen neuen Schadprogramm auch aufgeführt, dass durch das Ausnutzen von Schwachstellen die Cyber-Erpressung das größte Sicherheitsrisiko darstellt. Skizzenhaft lässt sich ein solcher Fall wie folgt darstellen: durch das Anklicken eines ungeprüften Inhaltes einer Phishing-Mail wird eine sogenannte Ransomware auf die eigenen Systeme gespielt. Ransomware als solches ist die Bezeichnung für Schadprogramme, mit deren Hilfe Angreifer Zugang zu den Systemen des Ange-griffenen Unternehmens bekommen. Ist diese Ransomware auf den Systemen haben Angreifer neben der Verschlüsselung beispielsweise auch die Möglichkeit sensible Daten aus dem Unter-nehmen herauszuziehen und zu verwenden. In beiden Fällen schließen sich häufig Erpresser-schreiben an, die eine Freigabe der Daten oder aber den Verzicht auf das Veröffentlichen abgezogener Daten gegen Bezahlung anbieten. Eine Weiterführung des Geschäftsbetriebes ist dann meist nicht mehr möglich, da z.B. auf Planungsdaten nicht mehr zugegriffen werden kann. Sind personenbezogene Daten betroffen, können weitere rechtliche Verpflichtungen, z.B. eine Meldung binnen 72 Stunden an den Landesdatenschutzbeauftragten vorzunehmen, auf die Unternehmen zukommen.

Neben dem beschriebenen Phishing-Szenario gibt es allerdings weitere Wege in die Systeme von Unternehmen zu gelangen. Neben dem Social Engineering, einer Beeinflussung von Personen, um (Zugangs-)Daten zu entlocken, gibt es auch immer wieder Sicherheitslücken in weit verbreiteten Softwares oder Systemkomponenten. Die bekannteste Schwachstelle aus dem Jahr 2021 ist laut BSI in Verbindung mit der Software Microsoft Exchange festgestellt worden. Dabei wurde bekannt, dass bei bestimmten Versionen der Software eine Lücke in der Sicherheitsinfrastruktur des Programmes aufzufinden ist, die Angreifer nutzen können, um direkten Zugriff auf die E-Mail-Server des Unternehmens zu bekommen. Der Hersteller stellte hier innerhalb von vier Tagen ein Update zum Schließen der Sicherheitslücke und

ein Analysetool zur Ermittlung der Kompromitierung der Systeme bereit. Hier war zu beobachten, dass es Fälle gab, bei denen die Schwachstelle zwar ausgenutzt wurde, um externe Software auf die Systeme der betroffenen zu bringen, diese aber noch nicht aktiv geworden ist. Auch dies ist eine häufig in der Praxis anzutreffende Situation. Die Kompromitierung eines Systems findet dabei deutlich früher statt als das aktive Nutzen von zuvor eingespielten Schadprogrammen.

Quelle: BSI – Die Lage zur IT-Sicherheit in Deutschland 2021

BIM und Cyberversicherungsschutz

Schon seit langem werden einzelne Planungs- und Ausführungsprozesse im Bauwesen digital unterstützt. BIM bietet die Möglichkeit, diese einzelnen Planungsschritte zu vernetzen und die Zusammenarbeit an einem Projekt effektiv zu gestalten. Alle Informationen und Planungsdaten werden erfasst und zentral verwaltet, sodass sie den Beteiligten zur weiteren Ausführung zur Verfügung stehen.

Immer mehr Projekte sollen und werden mit der BIM Methode umgesetzt. Aber was bedeutet das für den Cyberversicherungsschutz? Was muss ein BIM Beteiligter beachten?

Aus Sicht der Cyberversicherung handelt es sich bei einer BIM Software, auf die andere Beteiligte zugreifen oftmals um eine Cloudanwendung, bzw. aus Sicht der Beteiligten nicht um ein eigenes IT-System. Vereinfacht gesagt wird den Beteiligten ein Zugang zur BIM-fähigen Software zur Verfügung gestellt. Oftmals erfolgt die werkvertraglich geschuldete Leistung der Planung in den eigenen IT-Systemen der Fachplaner (BIM-Beteiligten). Nehmen wir das Beispiel der technischen Gebäudeausrüstung. Im Zuge eines BIM-Projektes erhält ein TGA den Auftrag, für einen Bürokomplex die Heizungsanlage zu planen. Die Planung erfolgt in eigenen Systemen des Planers. Hier greift jederzeit seine eigene Cyberversicherung, sollte es zu einer Informationssicherheitsverletzung in seinen Systemen kommen. Eine Cyberversicherung bezieht sich auf die eigenen IT-Systeme. Sollte eine Weiterverbreitung z. B. eines Virus auf die anderen Beteiligten über die Systeme des TGA erfolgen, wäre dieses auch über die Cyberversicherung gedeckt. Sollte der TGA gehacked werden, hilft das HDI Expertennetzwerk, die Gefahr ab zu wehren oder Schäden zu beheben, sodass möglichst schnell weitergearbeitet werden kann. Der TGA ist für seine Daten, bzw. die Daten in seinen IT-Systemen verantwortlich. Sollte die BIM-Software z. B. aufgrund eines Hackerangriffes nicht mehr erreichbar sein, so ist der Dienstleister, der die Software stellt für die Verfügbarkeit und Sicherheit verantwortlich. Bereits hoch geladene Daten sind nun allerdings ggf. nicht mehr für den TGA erreichbar, da die Software nicht mehr zur Verfügung steht. Die dadurch entstehende Betriebsunterbrechung kann mit einem optionalen Zusatzbaustein, Betriebsunterbrechung durch Cloud-Ausfall, gedeckt werden.

Bereits bei objektiven Umständen, die auf einen Versicherungsfall schließen lassen, leistet die HDI Cyberversicherung z. B. mit der Soforthilfe und einer 24/7 Notfallhotline, sodass jeder Zeit ein Netzwerk aus Experten hinzugezogen werden kann.

Kurzum, die Beteiligung bei BIM-Projekten hat keinen negativen Einfluss auf den Cyberversicherungsschutz. Durch die starke Vernetzung kann sich ggf. die Angriffsfläche auf die eigenen IT-Systeme erhöhen. Hier hilft, auch innerhalb von BIM-Projekten, die eigene Cyberversicherung.

Möglichkeiten zur Prävention

Welche Möglichkeiten bieten sich Unternehmen, um sich bestmöglich gegen die aktuelle Bedrohungslage zu wappnen und zu schützen? Zunächst sollten Einfallsvektoren bestimmt werden, welche man gezielt verbessern kann, um das Risiko für sich selbst zu minimieren.

Neben der naheliegenden, technischen Verbesserung von IT-Systemen, sind es allerdings auch organisatorische Maßnahmen, die einen großen Einfluss auf die Risikominimierung haben. Mit dem Verfassen einer IT-Sicherheits- und einer Datenschutzrichtlinie, legen Unternehmen die Rahmenbedingungen fest. So können Prozesse klar definiert und etabliert werden, während man gleichzeitig eine bessere Rückverfolgung der Sicherheitslücke im Schadenfall gewährleisten kann. Auch können im Rahmen dieser Richtlinien die technischen Prozesse niedergeschrieben werden. Betrachtet man in diesem Zusammenhang das Patchmanagement, kann innerhalb der IT-Sicherheitsrichtlinie die Dokumentation und der Ablauf zur Einspielung von Patches geregelt sein. Gleiches gilt auch für das Datensicherungs-

Foto: Ken Schluchtmann, diephotodesigner.de

Foto: Ken Schluchtmann, diephotodesigner.de

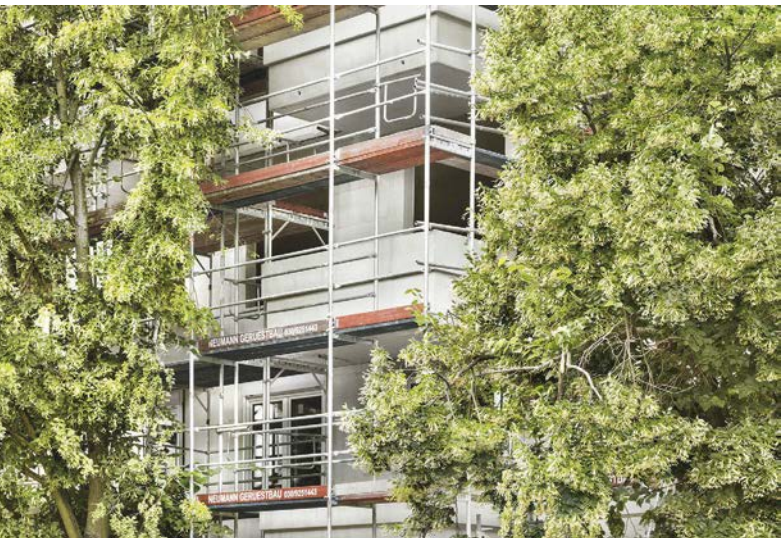


Foto: Ken Schluchtmann, diephotodesigner.de

konzept, welches ebenfalls im Rahmen eines Prozesses niedergeschrieben werden sollte. Zusammenfassend betrachtet, hilft die organisatorische Ordnung vorhandener technischer Prozesse dabei zu jeder Zeit einen Überblick über die aktuellen Abläufe zu bekommen, was wiederum im Schadenfall eine erhebliche Zeitersparnis in der Analyse der Situation bedeuten kann.

Nicht nur die Verbesserung der reinen technischen und organisatorischen Situation ist ausschlag-gebend für die IT-Sicherheit. Ein mindestens genauso wichtiger Faktor ist der Mensch. Mitarbeitende sollten regelmäßig zu Themen rund um den Arbeitsalltag mit der IT geschult werden. Gleichzeitig sollten aber auch Informationen rund um die aktuelle Bedrohungslage an die Belegschaft geleitet werden. Um diese Maßnahmen auch überprüfen zu können, gibt es die Möglichkeit Phishing-Mails zu fingieren und diese dann testweise an die Mitarbeitenden zu versenden, um einen Überblick über die Effektivität der eigenen Schulungsmaßnahmen zu erhalten. Ihre HDI Cyberversicherung unterstützt Sie hierbei. Mit der Awarenessplattform, welche wir durch unseren Partner Perseus Technologies GmbH bereitstellen, erhalten Sie die Möglichkeit Schulungen, Informationen und Phishingtests zu nutzen.

Die Basis für nachhaltige Cybersicherheit – Der Perseus Security Baseline Check

Für kleinere Unternehmen bietet unser Partner Perseus den Security Baseline Check an. Hierbei werden die technischen und organisatorischen Maßnahmen Ihrer IT-Sicherheit beleuchtet. Dies geschieht mit Hilfe eines Vorab-Fragebogens, sowie einer Live-Systemanalyse. Im Anschluss erfolgt die Dokumentation der Ergebnisse in Form eines Berichtes. Die Bewertung wird anhand einer Ampel-Logik vorgenommen. Sollten Punkte keinem aktuellen Standard entsprechen, werden Verbesserungsmöglichkeiten und Handlungsempfehlungen aufgezeigt.

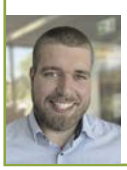
Worauf genau wird also geprüft?
Hier hat Perseus eine Teststruktur entwickelt die sich in die Blöcke *Account Validity, Password policy, Bring your own device (BYOD) policy, Antivirus, Firewall, Patch-Management und Backup-Concept* unterteilen lässt. Der Bereich Accound Validity befasst sich vor allem mit der Prüfung des Aufbaus der Nutzerrollen, der Berechtigungen und der technischen Umsetzung der Passwort-Richtlinie. Letzteres erfährt im Rahmen des Blocks *password policy* auch einen organisatorischen Check. Neben dem generellen Aufbau der Passwort-Richtlinie wird auch die Einhaltung mit Hilfe von Best Practices überprüft. Im Rahmen der *BYOD policy* wird hier ähnlich zur *password policy* der Aufbau und die Einhaltung des Prozesses zur Nutzung von privaten Geräten bewertet. Dies betrifft auch den Aufbau einer sicheren Verbindung in Ihr Unternehmensnetzwerk, wobei hier auch die Prüfungsblöcke *Antivirus* und *Firewall* Anwendung finden. So werden hier die Konfiguration und die Einbettung in das Unternehmensnetzwerk bewertet. Gleichzeitig erfolgt im Rahmen des *Patch-Managements* eine Bestandsaufnahme der Software-Aktualität und eine Prüfung des Prozesses zur Einführung neuester Patches und Updates für die eingesetzte Software. Im Rahmen des letzten Blockes wird das *Backup-Concept* Ihres Unternehmens bewertet. Sowohl technische als auch organisatorische Maßnahmen fließen in die Bewertung mit ein.

Ihre HDI Cyberversicherung honoriert die Durchführung eines Security Baseline Checks mit der Awarenessklausel. Durch diese Klausel besteht für Sie die Möglichkeit bei einer positiven Bewertung den Selbstbehalt im Schadenfall, um bis zu 75 % zu reduzieren. In Verbindung mit der Durchführung der Schulungsmaßnahmen auf der Awarenessplattform ist es sogar möglich, den Selbstbehalt im Schadenfall gänzlich zu reduzieren.

Fazit

Aufgrund des sehr dynamischen Risikos und der vielen beeinflussenden Faktoren kann und wird es keinen 100 % igen Cyberschutz geben. Aber organisatorische und technische Maßnahmen zur Cybersicherheit erhöhen das Sicherheitsniveau und bilden die Grundlage einer Unternehmens-Cyberstrategie. Das finanzielle Restrisiko kann über eine Cyberversicherung abgefangen werden. Daneben ergänzen Cyberversicherungen oftmals vor allem durch umfangreiche Assistanceleistungen und nicht zuletzt durch ein umfassendes Expertennetzwerk im Schadenfall. Mit einer Cyberversicherung sind die eigenen Daten auch bei der Teilnahme an BIM-Projekten geschützt, auch wenn diese nicht zwangsläufig in eigenen IT-Systemen gespeichert werden. In diesem Tätigkeitsbereich kann die HDI Cyberversicherung sinnvoll durch den optionalen Baustein Betriebsunterbrechung durch Cloudausfall ergänzt werden. So können eventuelle Deckungslücken geschlossen werden und die HDI Cyberversicherung stellt bei der Teilnahme an BIM-Projekten ihr volles Leistungsspektrum zur Verfügung.

Autor



Kevin Luhmann
Kevin Luhmann
Produktmanagement Cyber
HDI Versicherung AG
Hannover
kevin.luhmann@hdi.de