Cyber Security / Resilience

Wer BIM sagt, muss sich schützen

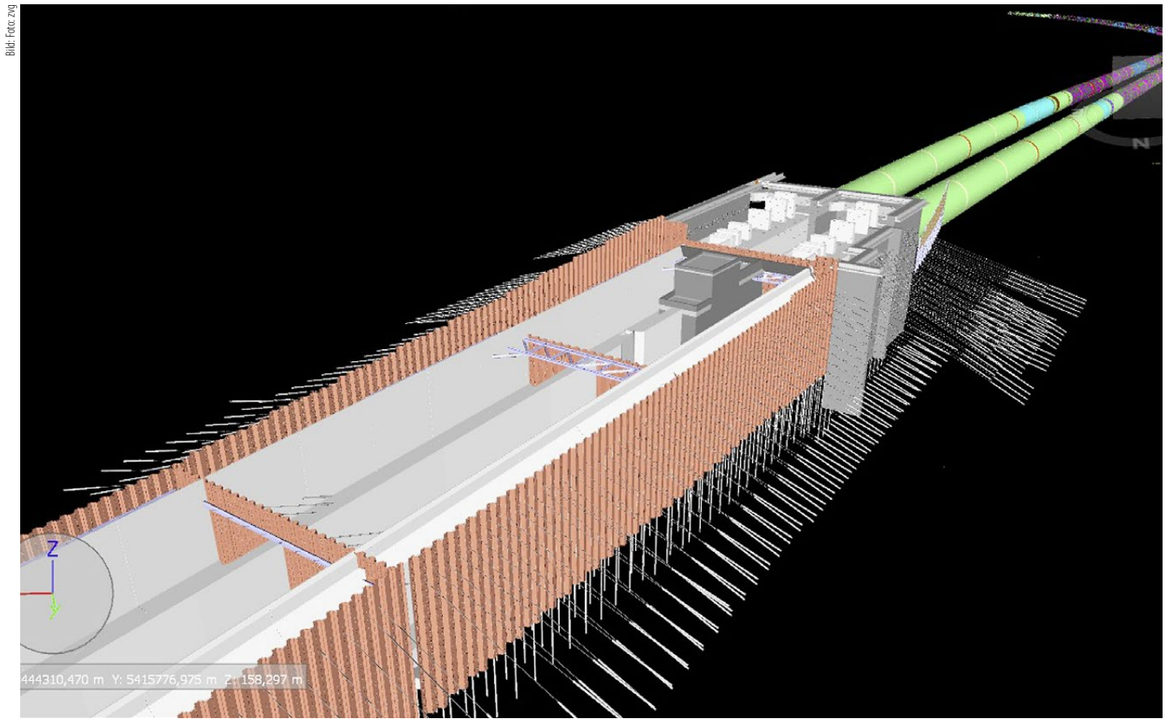
An BIM führt in der Baubranche bald kein Weg mehr vorbei. Doch rund um BIM und Digitalisierung ist kaum von den Bedrohungen die Rede, die im Netz lauern: Schutz vor Internet-Gangstern ist zentral, und die wirksamste Massnahme heisst Vorbeugung.

Von Ben Kron

Ob Immobilienbesitzer, Architekt, Baumeister, Fachplaner oder Handwerksbetrieb: Die Digitalisierung hat als eine der letzten auch die Baubranche erreicht. Digitalisierung und Building Information Modeling heissen die Schlüsselbegriffe. Wer sein Unternehmen für die Zukunft rüsten will, muss sich mit BIM auseinandersetzen und den Stufenplan Digitalisierung von Bauen digital Schweiz zur Hand nehmen. Ansonsten ist man bei zukünftigen Bauprojekten nur noch Zuschauer: Immer öfter wird in der Ausführung BIM verlangt, zunehmend werden Projekte sogar digital ausgeschrieben.

War BIM anfangs vor allem ein erweitertes 3D-Planungstool, findet es heute immer mehr auch auf der Baustelle selbst integrierte Anwendung und reicht bald bis in den Betrieb und die Bewirtschaftung des Gebäudes: Ausführende können Pläne und Infos aus einer Cloud beziehen, wo alle Beteiligten am selben Datenmodell, beziehungsweise am «digitalen Zwilling» des Projekts arbeiten. Facility Manager nutzen später dieselben Daten, um die Gebäudetechnik zu steuern und den Unterhalt zu planen. Und genau in diesem gemeinsamen Zugriff liegt das Problem, weiss IT-Experte Fridel Rickenbacher *(siehe Box «Zur Person»)*.

Bild: Fotoz.zng



BIM-Planung für ein Tiefbauprojekt: Die digitale Methode birgt für die Baubranche enorme Chancen zur Effizienzsteigerung, daneben aber auch erhebliche Risiken, ins Visier von Cyber-Kriminellen zu geraten.

Sicherheitsvorkehrungen treffen

«An Diskussionen oder BIM-Kongressen zum Beispiel wird viel vom Common Data Environment gesprochen, von App- und Datenbank-Clouds, auf die alle von überall aus Zugriff haben. Aber niemand fragt nach der Integrität, Datensicherheit und dem Datenschutz der Daten. Oder was passiert, wenn diese BIM-Cloud mehrere Tage ausfällt.» Man begnüge sich meist mit der meist naiven Annahme, dass der Software-Entwickler und/oder Anbieter, beziehungsweise Betreiber der Cloud die nötigen Sicherheitsvorkehrungen gemäss «Stand der Technik» getroffen hat.

Tatsächlich aber schaffen solche Cloud-Lösungen ebenso umfassende Einfallstore für Akteure von CyberCrime. «China ist bedeutender Hersteller von Software und Hardware. Die im aufsehenerregenden ‹Big Hack› im Jahre 2018 in weltweit verwendeten Serverkomponenten eingepflanzten Chips – fähig, die kompletten Unternehmensdaten auszuspionieren – wurden höchstwahrscheinlich vom chinesischen Staat stillschweigend toleriert», sagt Rickenbacher. Er nennt neben China auch Russland, Nordkorea und die USA, wenn es um Staatsspionage geht. «Zudem ist die Frage nicht, ob etwas passiert, sondern, wie oft es schon passiert ist.»

Trojaner legen alles lahm

Ein Präzedenzfall für die Branche ereignete sich im Juli letzten Jahres: Die IT-Infrastruktur des Gebäudetechnikspezialisten Meier Tobler wurde durch einen Cyberangriff lahmgelegt. Das Fachmagazin «inside IT» führt die Details auf: Blockiert waren SAP-System, Lagerleitsystem, Telefonie, Website und alle E-Mailadressen: Ein eingeschleppter Trojaner hatte das gesamte System verschlüsselt, keiner der weltweit 1400 Mitarbeitenden hatte mehr Zugriff. Eingeschleppt wurde die Schadsoftware über die Hotelbuchung eines Mitarbeitenden, über welche die Hacker ins System des Unternehmens gelangten.

Das Unternehmen konnte eine Woche lang keine Auslieferungen vornehmen, der unmittelbare Schaden belief sich auf fünf Millionen Franken. Nicht zu beziffern sind der Ärger der Kunden, der Stress für die Mitarbeitenden und der Imageschaden fürs Unternehmen, das aus seiner Not eine Tugend gemacht hat und offen über den Vorfall kommunizierte. So hat es vor wenigen Tagen bekannt gegeben, dass der Vorfall einen zusätzlichen Umsatzverlust in ähnlicher Grössenordnung verursacht habe, unter zwar im Wärmeerzeugungsgeschäft aufgrund der mangelnden Verfügbarkeit der Informatiksysteme.

Auch Fridel Rickenbacker lobt das Haustechnikunternehmen: «Die Reaktion war vorbildlich: Man ist sofort proaktiv und professionell an die Öffentlichkeit gegangen, hat über den Angriff und die Gegenmassnahmen informiert. Zudem wurde die Schwachstelle erkannt und beseitigt.»

Bild: Fotolia

Cyberkriminelle tragen im richtigen Leben zwar wohl kaum Sturmmasken, sind aber in Netz äusserst aktiv. In Deutschland zählte die Telecom bis zu 46 Millionen Attacken von Hackern auf Firmen, und das jeden Tag.

Schwachstelle Mitarbeiter

Noch schlimmer traf es die Swisswindows AG, die Ende Februar dieses Jahres ihre Insolvenz erklären musste. Bei der Begründung dieser Massnahme heisst es: «Eine massive Cyberattacke auf unsere Systeme führte im Mai 2019 zu einem herben Rückschlag für unser Unternehmen. Die Folge war ein Produktionsausfall von über einem Monat, begleitet von massiven Folgekosten. Dieser Vorfall und die zu diesem Zeitpunkt nur begrenzten finanziellen Mittel, reichten aus um das Unternehmen in arge Bedrängnis zu bringen.»

Der Angriff auf Swisswindows wie derjenige auf Meyer Tobler erfolgte mit einem klassischen Verschlüsselungs-Trojaner und war auch ansonsten exemplarisch: Beide Male erfolgte der Zugriff aufs System nicht direkt, sondern über einen Mitarbeitenden der Firma. «Die bedeutendste Schwachstelle im Bereich der IT-Sicherheit ist und bleibt der Mensch. Bei unglaublichen rund 95 Prozent aller Angriffe hilft der Anwender, sprich Mitarbeiter, aktiv unbewusst mit, dem Täter ein Erfolgserlebnis zu verschaffen.» Meist ist es ein zu schneller unbedachter, reflexartiger Klick auf einen Link, einen potentiell gefährlichen Anhang oder aber auch ein zu schwaches Passwort ohne weitergehende Schutzmassnahmen, was fatale Folgen hat.

FORTSETZUNG AUF SEITE 50

Unsicherer Internetzugang

Der IT-Securityexperte schildert das Dilemma: «Keine Digitalisierung ohne Cloud, hier ist die kollaborierende Schnittstelle zwischen den Baubeteiligten. Und ebenso aus der Cloud bezieht man heutzutage nötige Funktionalitäten für umfassende Sicherheitssysteme, die regelmässig aktualisiert und aus der Cloud überwacht werden müssen. Zugleich begibt man sich dafür aber ins grundsätzlich unsichere Internet, das ist das Paradoxum.»

Der Bauunternehmer, der seine Firma digital transformieren und neu aufstellen will, muss sich also dringend um die Sicherheit seiner Mitarbeiter, Systeme und Daten kümmern. Aber wie macht man sein Unternehmen eigentlich fit für BIM? Rickenbacher setzt auf Konfrontation: «Das kann ein kritischer Fragendialog sein, dem man sich aussetzt. Oder ein aufklärender Schockmoment durch eine regelrechte Druckladung in Form eines Impulsreferats, das die Gefahren drastisch vor Augen führt.»

Wo muss gehandelt werden?

So müssen sich spätestens dann die Verantwortlichen diverse Fragen stellen wie: Wie lange können wir ohne E-mail arbeiten? Wie verhalten wir uns, wenn das Internet ausfällt? Was tun, wenn kein Zugang mehr auf die CAD-Umgebung oder sonstige auftragsrelevante Daten besteht? Wie lange und wie kann man solche Unterbrüche oder Einschränkungen überbrücken? Ab wann müssen Vertragspartner informiert werden, weil die Verbindlichkeiten im Werkvertrag kritisch werden?

«Mittels solcher Fragen lässt sich ermitteln, wo das Unternehmen schon resilient ist, also widerstandsfähig, und wo gehandelt werden muss. Ich erhalte rote und grüne Flaggen, je nach Eintrittswahrscheinlichkeit und Qualität des Schadenspotenzials.» *(siehe auch Box, Seite 52)*

Zugleich lässt sich abschätzen, inwieweit die firmeneigene IT diese Fragen beantworten und abdecken kann. Die Verantwortlichen des Unternehmen können dann abschätzen, ob sie sich externe Unterstützung holen müssen oder aber das Thema intern angehen können. Ist die Führungsetage schon bei der Evaluation der Massnahmen mit an Bord, vermeidet man ein anderes Problem: Für IT-Fachkräfte und Support-Organisationen ist es oft schwierig, solche konkreten Massnahmen für eine verbesserte Resilienz ihren Vorgesetzten zu verkaufen, da es sich auch um budgetbelastende Posten handelt.

Klarheit für Jedermann

Ein anderes Thema ist die technologische «Flughöhe» dieser Chefetage. Fridel Rickenbacher muss sein Anliegen oft gegenüber Entscheidungsträgern erläutern, die selber keine IT-Fachleute sind. «Ich versuche natürlich, mich einfach auszudrücken, aber gewisse Fachausdrücke sind unvermeidlich. Es ist deshalb wichtig, dass sich auch die Leute in der Chefetage in gewissem Mass mit der Materie befassen und versuchen, mit dem rasant sich entwickelnden Stand der Technik mitzuhalten.»

Daneben versucht er, den Leuten gewisse Ängste vor der Digitalisierung zu nehmen. «Wenn von BIM die Rede ist, sprechen alle im Stil von irgendwelchen Methoden und schöngeistig anmutenden Hochglanzprospekten. Das weckt auch gewisse Ängste und Skepsis, die ich den Leuten nehmen will. Deshalb spricht er nicht nur von Digitalisierung, sondern mehr von Effizienzsteigerung. «Das ist ein Thema, das jeden Bauunternehmer interessiert. BIM und letztlich die Digitalisierung kann und muss Effizienz herbeiführen und das möglichst sicher und umfassend.»

Orientierung an «Best Practices»

Für die konkrete Umsetzung der Digitalisierung und der begleitenden IT-Security gibt es eine Reihe von «Best Practices», auch von Bauen digital Schweiz, an denen man sich orientieren kann. Umsetzen sollte man die grosse Entwicklung in sogenannten «Baby Steps», rät Rickenbacher. «Man darf den Leuten nicht alles mittels einer «Druckladung» als Zwang überstülpen. Die Organisation soll schrittweise Erfahrungen sammeln, über möglichst viele messbaren «Use Cases» im Rahmen der Transformation und Innovation.

So lässt sich die Digitalisierung schrittweise implementieren und die betroffenen Mitarbeitenden können Erfahrungen sammeln und werden Teil der Transformation. Die Digitalisierung und Transformation ist keine lineare Leiter, sondern viel mehr eine Kletterwand mit unterschiedlichen Pfaden zum Ziel zum höheren Level. Und bei diesem iterativen Prozess wird die IT-Sicherheit von selbst ein wichtiges Thema und integraler Bestandteil der gesamten Transformation und Entwicklung.

Dabei braucht es eine ganze Reihe von Massnahmen auf technologischer und prozessualer Ebene, um sich möglichst umfassend gegen Angriffe zu schützen. Früher befand sich der ICT-Security-Perimeter im geschützteren Firmenumfeld. Da aber die Mitarbeitenden als «mobile liquid Workforce» standort- oder gar geräteunabhängig arbeiten sollen, hat sich dieser Perimeter längst verschoben: Herkömmliche Sicherheitsmassnahmen wie etwa eine Internet Firewall, VPN (Virtual Private Network), Security-Gateways, klassischer Virenschutz oder Backups reichen längst nicht mehr.

Komplexe Sicherheitssysteme nötig

Im Internet und speziell in den Social Media sind die Leute und Firmen ausgeklügelten Angriffsvektoren wie Social Engineering, Phishing oder gar APT (Advanced Persistent Threat) ausgesetzt. «Hier ist ein sogenanntes ‹verhaltens- / cloud-basiertes› und möglichst automatisiertes Gesamt-Sicherheitssystem die einzige effektive Chance, komplexe Angriffe und Sicherheitslücken möglichst frühzeitig zu erkennen und deren Risiken und Schadenspotential proaktiv zu minimieren, zugunsten der maximierten Angriffs- und Betriebssicherheit. Nur durch solche, mehrschichtig orchestrierte Systeme kann eine ausgewogene Cyber Security-Resilienz aufgebaut und aufrecht erhalten werden und damit die heute unumgängliche Widerstandsfähigkeit.»

Dazu lautet seine pragmatische Devise als Mindestanforderung «Backup, Backup, Backup». Plus der Aufruf an alle Akteure in der Firma gegen den Angriffsvektor «Social Engineering» und Phishing Mails: «Start thinking! Stop clicking!». «Ein Backup im Betrieb, eines offline ausserhalb des Firmengeländes und eine weitere verschlüsselte, zusätzlich abgesicherte Sicherheitskopie in der Cloud sind das Minimum wenn man von ‹Stand der Technik› spricht. Diese Kombination ergibt ein gutes, erstes Schutzniveau gegen kriminelle Erpressung im Netz.»

Grundsätzlich solle man Cloud-Lösungen vertrauen, denn die dort herrschenden Sicherheitsvorkehrungen kann sich kein Einzelunternehmen einfach mehr so leisten geschweige denn auf gleichem Niveau rund um die Uhr betreiben. «Und letztlich

Zur Person

Bild: Fridel Rickenbacher

IT-Experte Fridel Rickenbacher

IT-Experte Fridel Rickenbacher (46) ist Senior Consultant der Execure AG, Member of Swiss IT Security Group. Dank seiner langjährigen Erfahrungen berät und begleitet er Firmen sowohl bei der Digitalisierung und bei der Vorbeugung und Gegenmassnahmen von Cyber-Attacken im IT-Bereich, wie auch bei «Incident Response» Aktivitäten.

Ein weiterer Bereich seiner Arbeit ist die Beratung von Fachverbänden und Expertengruppen, unter anderem im Informatiksteuerungsorgan des Bundes «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS1 und NCS2)». Bei Bauen Digital Schweiz ist er Projektleiter für «BIM ICT-Architektur- / Security- / Audit-Framework > Security minded building information modelling». *(bk)*

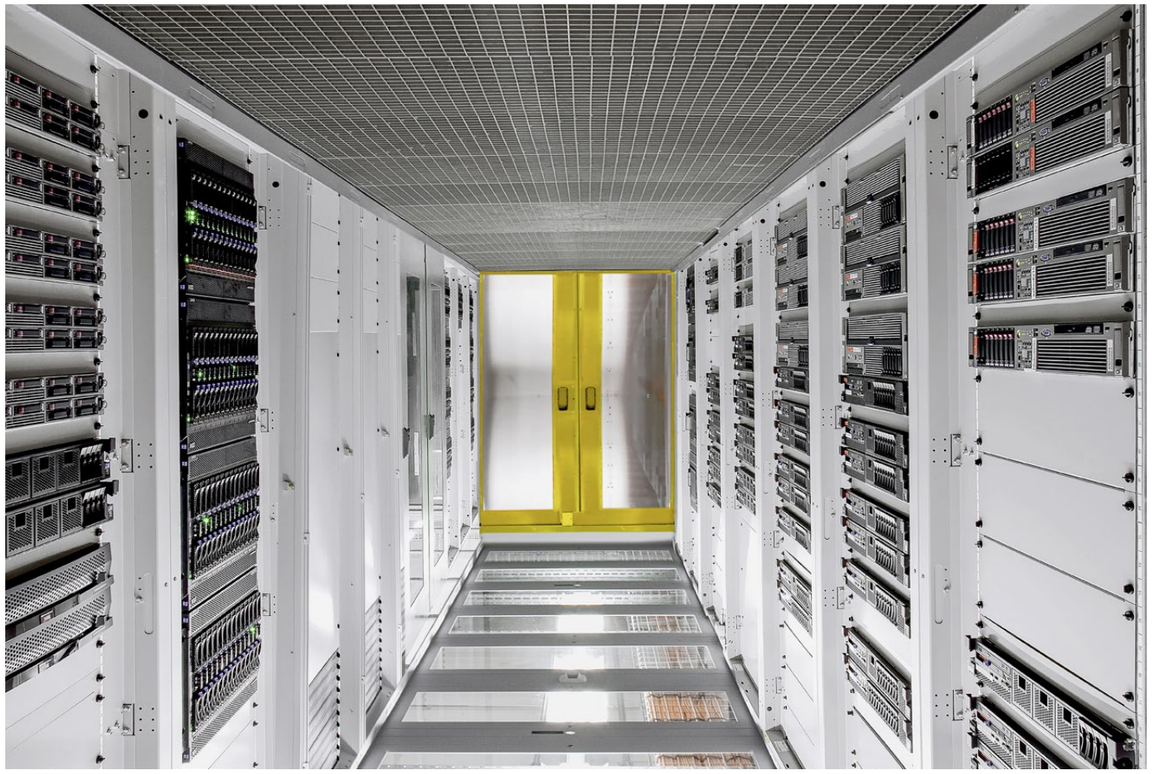


Bild: Stadt Zürich

Serverraum eines Cloud-Anbieters: Wer mit BIM arbeitet, nutzt solche Internet-gestützten Lösungen als gemeinsame digitale Arbeitsplattform.

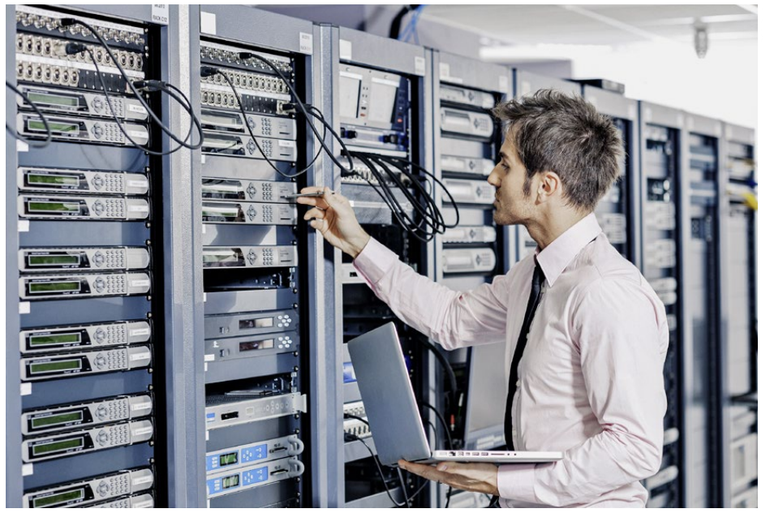


Bild: Bents

Wartungsarbeiten in einem Serverraum: Wie lange bleibt ein Unternehmen handlungsfähig, wenn die eigenen Computer gehackt werden und nicht mehr zugänglich sind?

basiert ebenso die gesamte Smartphone-Technologie seit Jahren auf komplexen Cloud-Lösungen.»

Aufklärung ist Vorbeugung

Zum anderen ist die Vorbeugung entscheidend. Fridel Rickenbacher wünscht sich Präventions-Kampagnen, wie sie die Suva mit Erfolg zur Bekämpfung von Arbeitsunfällen durchführt. «Ein Cyber-Unfall kann genau gleich radikal und gefährlich sein, hoffentlich nicht für Leben und Gesundheit von Menschen, aber für personen- und firmenbezogene Daten, für Betriebe, Firmen und Projekte.» Deshalb müssen alle Mitarbeiten ebenso darüber aufgeklärt werden, wie wichtig der Schutz der digitalen Identität und Zugangsdaten ist.

So besteht ein grundsätzliche Problem in der Mitgliedschaft auf diversen sozialen Socialmedia-Plattformen wie Facebook, Instragam oder Twitter. «Ich unterstelle mich automatisch deren Datenschutzrichtlinien und habe letztlich keinen Einfluss und 100 Prozent Kontrolle über meine Daten mehr, gebe meine digitale Identität aus der Hand zugunsten von auch ‹Social Engineering›-Angriffsvektoren.» Man muss einfach annehmen und hoffen, dass die Algorithmen im Bereich Cybercrime richtig funktionieren – doch wiederholte Meldungen über gehackte Konten wecken Zweifel.

Passwörter regelmässig wechseln

Und mit den so gewonnen Informationen können Cyberkriminelle arbeiten: «Ein grosser Prozentteil der gehackten Daten kann von den Kriminellen jeweils für den Zugang zu Firmensystem genutzt werden. Oder als Quelle für eine Social Engineering Attacke» Dies ist oft einfach, da Firmenanwender aus Bequemlichkeit überall dieselben Passwörter verwenden, auch privat. «Solche Fehler wirken sich knallhart aus, lassen sich aber vermeiden: Etwa durch Systeme, die einen regelmässigen Wechsel der Passwörter und bei diesen eine vorgegebene Komplexität erzwingen. Zudem sind Technologien wie Multi Factor Authentication effektive Hilfsmittel.»

Für Fridel Rickenbacher sind solche Massnahmen zur Erhöhung der eigenen Sicherheit nicht nur ein wirtschaftliches Muss, sondern auch ein soziales: «Ein Unternehmen muss sich gegen solche Schäden wappnen. Untätigkeit ist für mich asoziales Verhalten, da es am Ende die Gesellschaft schädigt, die den Schaden immer mitträgt.» Unternehmen müssten durch ihre Verhalten dafür sorgen, dass die Resilienz innerhalb der Wirtschaft und Gesellschaft erhöht wird. «So kann man zum Beispiel gemeinsam dafür sorgen, dass ein Phishing Mail als Angriffsvektor wenig grossen Erfolg mehr hat.» In anderen sozialen Bereichen seien Massnahmen zur Verbrechensvorbeugung schliesslich ebenfalls eine Selbstverständlichkeit.

Sicherheit wird vernachlässigt

Während also BIM überall auf der Agenda steht, hat der Aspekt der Sicherheit und Widerstandskraft mittels Angriffs- und Betriebssicherheit für Fridel Rickenbacher noch nicht den gebührenden Stellenwert. Aber der IT-Experte sieht auch, dass bei den Firmen ein Umdenken beginnt. «Die Leute sind eher bereit, komplexe Texte zu lesen und ein paar Fachbegriffe im Internet nachschauen um gewisse Themen besser zu verstehen. Die Notwendigkeit ist bei immer mehr Entscheidungsträgern angekommen.»

Das ist gut so, denn die Digitalisierung ist nicht aufzuhalten, und damit auch die mit ihr verbundenen Risiken und Chancen. Das Bauunternehmen, das sich digital ausrichtet, muss neben aller Expertise im eigenen Fachbereich auch die Bereiche Computersicherheit und Widerstandsfähigkeit der ganzen Organisation berücksichtigen, also Cyber Security und Resilienz. Das Implementieren der nötigen Massnahmen und Tools in diesem Bereich sollte so selbstverständlich sein wie der Helm auf der Baustelle. ■

Fragen zu Cyber Security / Resilience

- Was für Auswirkungen und Massnahmen sind zu adressieren bei Betriebsunterbrüchen von einzelnen Stunden, einem halben oder ganzen Tag, mehreren Tagen?
- Sind kritisch klassifizierte Teilsysteme auf getrennten, unterschiedlichen Systemen genügend robust und resilient, um bei Teil-Ausfällen oder Total-Ausfällen einen Teil der Arbeit oder Produktion aufrechterhalten zu können?
- Sind weitergehende Redundanzen oder gar automatische Ausfall-Systeme nötig?
- Wie häufig pro Jahr werden Recovery-Tests geprüft von Backups, Daten oder ganzen Systemen?
- Ist die CyberSecurity-Sensibilisierung der Mitarbeiter («social engineering») und speziell der Führungsetage und Entscheider sichergestellt und trainiert?
- Sind technisch vorgegebene und erzwungene Kennwort-Komplexitäts-Regeln umgesetzt und in Betrieb?
- Sind Schutzmechanismen der digitalen Identität mittels MFA («multi factor authentication»), 2FA («2 factor authentication») oder Conditional Access (CA, Zugang nur bei Erfüllung von Bedingungen) geplant oder umgesetzt?
- Wie steht es mit der E-mail-Security (rund 90 Prozent der erfolgreichen Cyber-Attacken starten mit einem E-mail) bezüglich integrierter Spamfilterung und Schutzmechanismen wie Anti-Malware, Content Filterung, «threat protection», «data loss prevention», «safe links» oder «sand boxing»?
- Sind die Geräte wie PC, Notebooks, Tablets, Smartphones geschützt mittels «mobile device management» (MDM), «advanced threat protection» (ATP) und zentralisiert verwaltbaren Dashboards «security & compliance automation»?
- Braucht es eine externe Cyber-Security-Beratung, Audit, Penetration Test oder Zweitmeinung?