STANDPUNKT.

IRE|BS Immobilienakademie
International Real Estate Business School
Universität Regensburg

Ausgabe 80 | 26. August 2019

Cyber Sicherheit - Wichtig für eine erfolgreiche Digitale Transformation

Viktor Weber, Gründer - Future Real Estate Institute

Bruce Schneier, einer der profiliertesten Cyber Security Experten, ist der Meinung, dass die zunehmende Komplexität der digitalen Welt der schlimmste Feind von Sicherheit ist. Unsere Systeme, Unternehmen und Prozesse werden digitaler und somit komplexer, was wiederum bedeutet, dass die Sicherheit abnimmt. Hier müssen wir gegensteuern und dabei möchte ich Ihnen in diesem IREBS Standpunkt helfen. Wie bereits in meinem diesjährigen IREBS Standpunkt 73 „Blockchain bekömmlich erklärt – Hype vs. Realität“ habe ich Fragen gesammelt, die mir häufig in der Beratung oder nach Vorträgen auf Veranstaltungen gestellt werden; und auf diese Fragen gebe ich hier kurz Antwort.

Ist das Thema Cyber Sicherheit für die Immobilienbranche überhaupt relevant?

Auf unsere Branche kommt das Thema Cyber Sicherheit sogar in besonderer Komplexität zu: Zum einen müssen sich die Unternehmen ihre eigenen Daten und Systeme sichern, was gerade im Zuge der digitalen Transformation notwendig wird. Zum anderen müssen vernetzte und computerisierte Gebäude abgesichert werden.

Ersteres ist den meisten Entscheiderinnen und Entscheidern bewusst, da dies für alle Unternehmen in der digitalen Welt gilt. Vernachlässigt wird aber, dass Immobilien auf Objektebene ein besonderes digitales Schutzbedürfnis haben, da wir circa 80% unserer Lebenszeit in Gebäuden verbringen, dort eine große Menge an Daten erzeugen und eine Schließanlage, Wachpersonal sowie Kameras nicht mehr zum Schutz ausreichen, da die Nutzung von Gebäuden sehr elementare Schutzbedürfnisse weckt. Sind unsere Gebäude nicht sicher, ist unsere Privatsphäre, mitunter sogar unser Leben gefährdet.

Immobilien aller Assetklassen, seien es Industrieanlagen, Wohnungen oder Büros, werden immer stärker technisch aufgerüstet. Das macht eine Immobilie zu einer Art Computer, in dem man wohnen oder arbeiten kann. Diese Erkenntnis sollte sich in der Branche etablieren, vom Trainee bis zur Geschäftsführung.

Folglich sollte man Immobilien genauso sichern wie ein Laptop, auf dem wichtige Daten gespeichert sind. Man sollte nur Komponenten von vertrauenswürdigen Firmen verbauen, überprüfen ob die betroffene Hard- und Software mit regelmäßigen Updates über den gesamten Lebenszyklus versorgt wird, es sollte auf Virenschutz geachtet werden, die Daten sollten verschlüsselt werden etc. All diese Selbstverständlichkeiten, die jeder private Internetnutzer beachten sollte, gelten auch in der computerisierten umbauten Welt.

Daher ist es erstaunlich, dass gerade im Kontext von Smart Home und Smart City diese grundlegenden Prinzipien oftmals außer Acht gelassen werden, indem beispielsweise die

verbauten Komponenten gar nicht gesichert werden oder es keine Updates/Patches auf Komponentenebene gibt.[1]

Was bedeutet das konkret für einzelne Assetklassen?

Wohnimmobilien sollten zukünftig, trotz mobiler Geräte, verbauten Sensoren, Netzwerktechnik und anderen Internet of Things-Komponenten (IoT), unsere individuelle Privatsphäre schützen. Der Erhalt der Privatsphäre ist dabei ein klassisches Schutzziel aus der Informationssicherheit, dort bekannt unter den Begriffen der Vertraulichkeit bzw. Confidentiality.

Technisierte Infrastruktur, Krankenhäuser, Kraftwerke, Serverfarmen, militärische Einrichtungen und viele weitere Sonder- bzw. Spezialimmobilien dürfen in ihrer Funktionalität trotz möglicher Cyber-Angriffe nicht in ihrer Funktionalität gestört werden können. Dieses Schutzziel wird als Verfügbarkeit bzw. Availability bezeichnet.

Gleiches gilt für gewerbliche Objekte, in denen geistiges Eigentum entwickelt wird, physische Wertgegenstände lagern oder andere vertrauliche Informationen verarbeitet werden; z.B. Gebäude, in denen Banken, Versicherungen, Anwaltssozietäten, Wirtschaftsprüfungs-gesellschaften etc. arbeiten.

Ist das nicht alles etwas übertrieben?

Das IP-Telefon im Büro, Ihr privates Mobiltelefon, die verwandte Software oder App, die IP-Kamera im Foyer oder der Drucker, können bereits heute eine hinreichende Schwachstelle bieten, um Angreifern einen unbeschränkten Zugang zu allen Unternehmensdaten zu gewähren.

Man misstraut Huawei bei der Ausrüstung mit 5G-Technologien, kauft aber im wahrsten Sinne des Wortes tonnenweise IoT-Komponenten wie IP-Kameras aus ungeprüften Quellen.

Die Crux an der Sache ist, dass die schwächste oder am schlechtesten gesicherte Komponente bereits einen systemrelevanten Angriff ermöglichen kann. Eine solch anfällige Komponente ist jedoch nicht nur eine Workstation, sondern theoretisch jede Hardware und vor allem jedes installierte Softwarepaket inklusive extern verlinkter Softwarequellen, von denen ein Nutzer in der Regel nichts weiß.

Das heißt, dass Sie unter Umständen eine vermeintlich sichere Software von einer etablierten Firma nutzen, die aber, ohne Ihr Wissen, Codes aus einer externen Quelle nutzt, um eine gewisse Aufgabe im Programm zu erledigen. Das ist nicht unüblich, da das die Programmierung spürbar beschleunigt und damit vergünstigt. Man muss schließlich das Rad nicht immer wieder neu erfinden. Problematisch wird es dann, wenn die verwandte Software

[1] Mehr zum Thema finden Sie in meinem Artikel „Is your smart home as safe as you think?“ für die World Economic Forum Agenda.

nicht sicher entwickelt wurde. Eine einzige Zeile eines unsicheren Codes aus einer Million Zeilen kann dann ausreichen, um die Kontrolle über Ihre Firmen-IT zu erlangen. Das ist zwar etwas reißerisch formuliert, aber leider dennoch korrekt.

Wie schätzen Sie den Stand der IT-Sicherheit in der Immobilienbranche ein?

Schlecht. Das klingt hart, jedoch habe ich schon bei etablierten Technologieunternehmen im Rahmen meiner beruflichen Tätigkeit hinter den Vorhang blicken dürfen, sodass ich aus eigener Erfahrungen und Gesprächen mit Verantwortlichen aus dem Security-Bereich berichten kann, dass auch dort, wo man sich intensiv mit IT-Sicherheit beschäftigt, nicht alles Gold ist, was glänzt.

Das ist auch der Grund, weshalb die durch Hacks verursachten Datenleaks immer größer werden und deren Frequenz zunimmt. Denken Sie nur an den Capital One, Equifax und viele andere Hacks, die medial präsent waren. Im Falle des Finanzdienstleisters Capital One wurden über 100 Millionen Kundendatensätze gestohlen, was vermutlich durch eine Schwachstelle in der Konfiguration der Webapplikation ermöglicht wurde. Bei Equifax wurden mehr als 140 Millionen personenbezogene Daten über eine Schwachstelle in deren Website entwendet.

Was sollte das Ziel einer guten Informationssicherheitsstrategie sein?

Das wohl bekannteste Modell zur Zieldefinition ist die CIA-Triad mit den drei Zielen „Confidentiality", „Integrity" und „Availability", also Vertraulichkeit, Integrität und Verfügbarkeit. Diese habe ich eingangs schon erwähnt. Jenseits dieses einfachen Dreiklangs gibt es viel umfangreichere Orientierungshilfen, wenn es um die Definition einer Informations-sicherheitsstrategie geht. Tatsächlich empfehle ich Entscheiderinnen und Entscheidern, sich mit der ISO/IEC 27000 auseinanderzusetzen (Hier ein Überblick). Dort werden die Schutzziele der CIA-Triad aufgegriffen, jedoch in den Kontext einer Gesamtstrategie gesetzt. Besonders interessant ist der Anhang A des Dokuments, da dort 114 Kontrollen ausformuliert sind, die einem Unternehmen zeigen worauf man im Themenkomplex „Sicherheit" achten sollte.

Doch für diesen Einstieg reicht erst einmal die CIA-Triad: Die Vertraulichkeit beschreibt, dass Daten nur von autorisierten Nutzern eingesehen werden können. Unternehmen können zum Beispiel unberechtigte Zugriffe auf Daten durch das Prinzip der minimalen Rechte (Principle of Least Privilege) minimieren und sollten alle relevanten Daten durch Verschlüsselung schützen.

Die Integrität besagt, dass Daten nicht unautorisiert modifiziert werden können, weder bewusst noch unbewusst. Auch dies lässt sich durch gutes Berechtigungsmanagement und Kryptographie gewährleisten.

Das Ziel der Verfügbarkeit definiert, dass berechtigte Nutzer ihre Handlungen wie geplant abhalten können und Systeme eben immer verfügbar sind, wenn sie gebraucht werden.

Schlussendlich sollte man sich bewusst sein, dass es nie 100% Sicherheit geben wird. Man kann sich ökonomisch-vertretbar und relativ leicht grundlegend schützen; dies reicht häufig aus, da Angreifer unter Umständen auf leichtere Ziele ausweichen, außer Ihr Unternehmen wird gezielt angegriffen. Daher ist das relative Schutzniveau ebenfalls von Bedeutung.

Neben der CIA-Triad ist die Resilienz der Systeme wichtig, also das Verhindern, Absorbieren, Adaptieren und Erholen von bzw. nach externen Schocks (z.B. einer Wirtschaftskrise, einer Cyberattacke oder einer Naturkatastrophe). Sie sollten in Ihren Unternehmen also Strategien für den Fall eines Angriffs haben, regelmäßig Backups machen und Trainings durchführen, um für den Ernstfall vorbereitet zu sein.

Muss man nicht ein Superhacker sein, um wirklich gefährlich zu sein?

Leider nein. Es gibt heute unzählige Softwaretools und Anleitungen, die einen interessierten Laien zu einem Script-Kiddy[2] werden lassen. Das können sogar besonders gefährliche Angreifer sein, da diese oftmals nicht verstehen, welche Tools sie nutzen und welchen Schaden sie im Extremfall anrichten können.

Aber das ist doch trotzdem extrem kompliziert, oder etwa nicht?

Man muss anerkennen, dass es extrem leicht ist, in der Cyberwelt Schaden anzurichten. Man muss kein Hacker wie in der Serie Mr. Robot sein, Zero-Day Schwachstellen[3] finden und eigene Exploits[4] entwickeln, sondern kann es sich deutlich einfacher machen:

Man kann heute Schwachstellen in einigen kostenlosen oder kostenpflichtigen Datenbanken finden. Dort sind die Schwachstellen in der Regel nach dem Common Vulnerability Scoring System (CVSS) klassifiziert, sodass man direkt sieht, was immanent gefährlich werden kann und dringlich behoben werden muss. Jedoch unterscheidet sich oftmals die Qualität und Genauigkeit der Meldungen, sodass eine eigene Bewertung relevanter Meldungen notwendig ist.

Durch Plattformen wie Shodan oder eigene Systemerkundung, können Angreifer herausfinden, wie und womit im Unternehmen kommuniziert wird. Das heißt, dass Hacker relativ leicht Informationen über Ihre IT samt Konfiguration sammeln können.

Da die meisten Unternehmen in der Praxis nur unzureichendes Schwachstellenmonitoring betreiben und diese Schwachstellen selten bei Entdeckung direkt durch Updates/Patches schließen, kann es passieren, dass ein System über Monate, gar Jahre relativ leicht angreifbar bleibt.

[2] Angreifer, die existierende Angriffssoftware, also ein Skript, nutzen, welches sie nicht programmiert haben und unter Umständen nicht einmal verstehen.
[3] Eine Zero-Day Schwachstelle ist eine kritische Lücke, die von den Findern zurückgehalten wird, um sie an Tag 0, zum Beispiel bei einem Cyberkrieg auszunutzen und verheerenden Schaden anzurichten.
[4] Ein Exploit ist ein Programm, mit dem eine Schwachstelle ausgenutzt wird.

Im Umkehrschluss sollten Unternehmen diese Schwachstellenveröffentlichungen genaustens beobachten und eigene Lücken zügig schließen. Je mehr Soft- & Hardware in der Immobilienbranche verwandt wird, desto wichtiger wird also auch der Aufbau einer guten IT-Sicherheitsabteilung im Unternehmen, die dann auch die Schwachstellenbeobachtung und -schließung umfasst.

Lauert die Gefahr dann hauptsächlich im Cyberspace?

Das kann und sollte man in der Immobilienbranche beziehungsweise der gebauten Welt nicht sagen, denn auch offline lauern Gefahren: Sensoren lassen sich oft leicht manipulieren, sodass die aufgezeichneten und übermittelten Daten falsch sind, was unter Umständen zu malignen Folgehandlungen führen kann. Stellen Sie sich beispielsweise intelligente Thermostate in einer Lebensmittelfabrik oder einer Apotheke vor, die eine zu niedrige Ist-Temperatur signalisieren. Die Folge könnte sein, dass die Temperatur zu stark erhöht wird, die Kühlkette würde unterbrochen und die Nahrungsmittelcharge oder Arzneimittel wären unbrauchbar – ohne dass der Nutzer dies bemerken würde, denn die Temperaturanzeige signalisiert ja hinreichende Kühlung.

Wie baut man ein Informationssicherheitsmanagementsystem (ISMS) auf?

Das kommt auf Ihr Unternehmen an und ist in der Regel Bestandteil einer entsprechenden Beratung. Jedoch wäre es sinnvoll, ein Assetinventar anzulegen, welches alle Informationswerte auflistet, die in Ihrem Unternehmen sowie den Objekten vorhanden sind. Jedem Asset im Inventar können dann ein oder mehrere Schutzbedürfnisse zugeordnet werden, die man im Rahmen einer Schutzbedarfsanalyse bestimmt. Zum Beispiel könnten Sie sagen, dass die nicht auf der Website stehenden personenbezogenen Daten der Mitarbeiter besonderer Vertraulichkeit bedürfen. Im Idealfall hinterlegt man im Anschluss jedes Asset noch mit einem Geldwert, um zu bestimmen, ob eine Schutzmaßnahme im Verhältnis zum Wert steht oder nicht.

Auch müssen die jeweiligen Risiken realistisch eingeschätzt werden. Dies umfasst nicht nur die technischen Schwachstellen, sondern auch böswillige Mitarbeiter oder den Wasserschaden im Serverraum.

Man sollte auch realistische Erwartungen an das ISMS haben, denn es wird mit Sicherheit nicht sofort perfekt funktionieren. Es sollte kontinuierlich und iterativ verbessert werden.

Verhindert die DSGVO datengetriebene Geschäftsmodelle?

Es kommt dabei auf den konkreten Anwendungsfall sowie die heranzuziehenden Daten an. Im Zweifel sollte man sich hier anwaltlich beraten lassen, um nicht gegen die DSGVO zu verstoßen. Grundsätzlich gilt bei personenbezogenen Daten die Zweckbindung, sodass beispielsweise ein Wohnungsverwalter nicht die individuelle Prognose zur Zahlungsbereitschaft modellieren darf. Gleichwohl darf man aber mit anonymisierten oder pseudonymisierten Daten arbeiten. Jedoch sollte man sich bewusst sein, dass es möglich ist, pseudonymisierte oder anonymisierte Daten wieder einer Person zuzuordnen. Daher ist es

ratsam, die gespeicherten Daten gut zu sichern. Fakt ist jedoch, dass die bis dato verhängten Strafen bei Verstößen gegen die DSGVO nicht sonderlich abschreckend waren, sodass der Erziehungscharakter der Richtlinie gemindert wird. Es sei insbesondere davor gewarnt, gespeicherte Daten aufgrund der Auskunftspflicht unachtsam an vermeintlich Berechtigte zu übermitteln, da genau diese Lücke von Angreifern im großen Stil ausgenutzt worden ist.

Appell für eine sichere digitale Transformation

Ziel unserer Branche sollte es nicht sein, sich möglichst rasch und fehlerbesetzt digital zu transformieren, sondern langfristig und nachhaltig Erfolge zu erzielen. Es ist daher zwingend erforderlich, mehr digitales Fachwissen über aktuelle Technologien, Datenverarbeitung, und Informationssicherheit aufzubauen. Die IT-Abteilung sollte nicht mehr als Kostenstelle, sondern als zukunftsweisender Wettbewerbsvorteil gesehen werden. Kleinere Unternehmen und Einzelunternehmer/innen können sich ebenso durch die gewissenhafte Auswahl von Soft- & Hardware sowie regelmäßigen Updates/Patches relativ kostengünstig sichern.

Vor allem müssen unsere Kommunen mehr Personal zu fairen Gehältern einstellen, um unsere Infrastruktur und Lebensräume zukünftig vor Cyberattacken zu schützen. Wir können keine smarten Städte entwickeln, wenn wir dadurch die Einwohner gefährden.

Viktor Weber

Future Real Estate Institute
Thomas-Dehler Weg 4
93051 Regensburg
E-Mail: contact@fre-institute.com
www.fre-institute.com

Viktor Weber (Gründer - Future Real Estate Institute) berät Unternehmen bei deren digitaler Transformation, publiziert international zu Zukunftsthemen und spricht auf Konferenzen über innovative Technologien, holistische digitale Transformation, Smart Cities sowie gesellschaftliche Aspekte des digitalen Wandels.