September 2017 Ausgabe Nr. 5
iddiw Hefte zur deutschen Immobilienwirtschaft

iddiw DENKANSTÖSSE

SICHERHEIT

- Cyber Sicherheit als Prozess-Enabler
- Gebäudesicherheit als Faktor im Asset Management
- Ohne Cybersicherheit keine sichere Projektentwicklung
- Smarte Objektsicherung zahlt sich aus
- Smart Home sicher gestalten
- So oder so – Sicherheit hat ihren Preis

Inhalt

Vorwort

Dr. Thomas Herr
Präsident iddiw

Dr. Thomas Herr Präsident iddiw

Sehr geehrte Leserinnen und Leser,

vor Ihnen liegt die neueste Ausgabe der „Denkanstöße – iddiw Hefte zur deutschen Immobilienwirtschaft“, die wir als Institut der Deutschen Immobilienwirtschaft e.V. herausgeben. Der Anspruch unseres Institutes ist es, die Entscheidungsträger aus Immobilienwirtschaft, Wissenschaft und Politik zu verbinden und einen fachlichen Austausch auf Augenhöhe zu organisieren. Dies erreichen wir durch unsere Discovery Foren, die Politischen Salons und durch die Publikation „Denkanstöße“.

In dieser Ausgabe widmen wir uns dem Thema Immobilie und Sicherheit. Wie das letzte Discovery Forum gezeigt hat, sind Sicherheitsaspekte für die Immobilienbranche nicht nur von theoretischer Relevanz. Viele Immobilienunternehmen setzen sich Tag für Tag mit einer sich ändernden Sicherheitslage auseinander. Wie schnell neue Themen auf die Tagesordnung gelangen können, haben die Ausschreitungen beim G20 Gipfel in Hamburg deutlich gezeigt. Deshalb ist es uns wichtig, das Thema Sicherheit in den „Denkanstößen“ noch einmal vertiefend zu behandeln. Hans-Wilhelm Dünn vom Cybersicherheitsrat, Dr. Christian Bogatu, Geschäftsführer des Startups KIWIKI, Johannes Eichelberger vom Asset Manager TRIUVA, Carsten Rutz, Vorstand bei der Deutschen Reihenhaus, Carsten Linde von Camelot Europe und Ingmar Behrens, Leiter Public Affairs German Council of Shopping Centers, haben ihre Schlussfolgerungen für uns zusammengefasst. Wir bedanken uns ganz herzlich bei den Autoren für Ihre Sicht auf das Zusammenspiel von Immobilie und Sicherheit.

Was wollen wir mit dem Heft erreichen? Die „Denkanstöße“ ermöglichen Ihnen, sich rasch und gleichzeitig umfassend zu einem branchenrelevanten Thema zu informieren. Gleichzeitig laden wir Sie herzlich dazu ein, mit uns zu diskutieren. Teilen Sie uns Ihre Einschätzung mit oder schenken Sie uns Ihre Ideen und Anregungen. Wir freuen uns auf den gegenseitigen Austausch.

Herzliche Grüße und Danke für Ihr Interesse
Ihr

Dr. Thomas Herr
Präsident

Cyber-Sicherheit als Prozess-Enabler der digitalisierten Immobilienwirtschaft

Hans-Wilhelm Dünn
Generalsekretär Cyber-Sicherheitsrat Deutschland e.V.

Die digitale Transformation hat das Individuum, die Gesellschaft, Wirtschaft und Staat gleichermaßen erfasst. In der Immobilienwirtschaft schlägt sich diese Entwicklung in Form von smart buildings, smart cities und der Expansion des Internet of Things nieder. Das Potential der Vernetzung von intelligenten Messsystemen (smart meter) mit Strom- und Versorgungsnetzen oder urbaner Gebäudekomplexe ist groß: Der Energie- und Wasserverbrauch, aber auch Müllentsorgungssysteme können so effizienter gestaltet werden.

Gleichwohl gehen mit der fortschreitenden Digitalisierung nicht nur Chancen, sondern auch Gefahren einher. Grundsätzlich stellt jedes vernetzte Objekt (smart item) ein potentielles Ziel für Cyber-Kriminelle dar. Realität ist bereits die Integration von smart items in Botnetze. Ein Botnetz ist ein Netzwerk aus gekaperten und somit fremdgesteuerten Rechnern und smart items. Das Datenvolumen des gesamten Botnetzes dient dann Cyber-Kriminellen als IT-Infrastruktur für weitere Angriffe. Eine erfolgreiche Distributed-Denial-of-Service-Attacke (DDoS) auf US-Internet-Dienstleister DYN wurde z.B. über das Botnetz Mirai ausgeführt, in Folge dessen Seiten wie Amazon, Twitter oder Netflix vorübergehend nicht erreichbar waren. Vernetzte Haushaltsgeräte wie Kühlschränke oder digitale Videorekorder waren dabei ein elementarer Bestandteil von Mirai.

Vernetzte Geräte können darüber hinaus nicht nur in Botnetze integriert, sondern auch selbst gehackt werden. Eine Kontrollübernahme beziehungsweise die Manipulation der Funktionsweise durch Hacker kann ernstzunehmende Folgen haben. Cyberkriminelle können zum Beispiel die Wechselrichter von Solaranlagen umprogrammieren und so Hausbrände auslösen. Ein solcher Vorfall stellt bereits auf der Ebene von einzelnen Haushalten eine ernstzunehmende Bedrohung dar. Überträgt man dieses Szenario auf ganze Wohnblöcke wird deutlich, dass eine IT-Sicherheitsarchitektur von smart buildings kritisch für die Sicherheit ganzer Städte sein kann.

Cyber-Sicherheit muss deswegen auch in der Immobilienwirtschaft als Prozess-Enabler der Digitalisierung verstanden werden. In erster Linie ist es daher notwendig, Hersteller von intelligenten Objekten wie smart metern in die Pflicht zu nehmen und IT-Sicherheitsstandards, Verschlüsselung, Datenschutz und Updates per Gesetz vorzuschreiben. Das Internet of Things ist ein großer Wachstumsmarkt, innerhalb dessen die Stakeholder der Cyber-Sicherheit jedoch eine untergeordnete Rolle zuschreiben. Entgegen dieser Fehlwahrnehmung sollte allerdings das Prinzip Secure by Design, also die vom ersten Schritt an auf Sicherheit ausgerichtete Entwicklung, Anwendung finden. Anreize für höhere Sicherheitsstandards könnten beispielsweise Gütesiegel schaffen. Es wäre

auch denkbar, bei mangelnden Sicherheitsstandards mit dem Entzug des Verkaufsrechts zu drohen.

Darüber hinaus sollten aber nicht nur die Objekte an sich, sondern auch die durch die smart items gesammelten Daten der Nutzer geschützt werden. Anhand dieser können zum Beispiel Alltagsabläufe rekonstruiert werden, was für Cyber- als auch „klassische" Kriminelle von Interesse ist.

Letztendlich liegt es aber auch an dem Verbraucher selbst, welche Daten und smart items dem Risiko eines Hacks ausgesetzt werden sollen. Ein gesundes Risikobewusstsein und die Anwendung von Cyber-Hygiene, also ein Cyber-Sicherheit konformes Verhalten, können Cyber-Angriffe effektiv vorbeugen.

Durch die Digitalisierung werden immer mehr Alltagsgegenstände vernetzt, die scheinbar nur eine geringe Auswirkung auf unser Leben haben. Mit der fortschreitenden Vernetzung entsteht aus einzelnen Objekten jedoch ein enges Geflecht, welches den Alltag unsichtbar begleitet und mitgestaltet. Dieses Netzwerk umfasst nicht nur Smartphones und Smartwatches, sondern eben auch smart meter, smart TVs oder mit dem Internet vernetzte Hausalarmanlagen. Die Einflussnahme durch Cyber-Kriminelle auf dieses individuelle Netzwerk sollte also unbedingt verhindert werden. Der Grundsatz eines Sicherheitsschlosses sollte demnach auch bei der Benutzung von Soft- und Hardware im smart home Bereich Anwendung finden.

Gebäudesicherheit als Faktor im Asset Management

Ein Interview mit
Johannes Eichelberger
Director Technical Asset Management TRIUVA.

Herr Eichelberger, nehmen Sie in Ihrem Geschäftsalltag eine geänderte Sicherheitslage in Deutschland wahr? Verfügen Sie über Statistiken zur tatsächlichen Sicherheitslage, z.B. aus dem Versicherungsbereich?
Innerhalb unseres europäischen Portfolios bei TRIUVA sind Sachbeschädigungen (böswillige Beschädigung, Einbruch, Diebstahl und Raub) auf einem langfristig niedrigen Stand und nahmen innerhalb der letzten drei Jahre nochmals stetig ab. Es ist jedoch anzumerken, dass der Immobilieneigentümer bei Einbrüchen lediglich in puncto Sachbeschädigung der Gebäudehülle betroffen ist und die eigentlichen Ziele des Diebstahls üblicherweise den Mieter betreffen.

Welche Auswirkungen haben Terror und Kriminalität auf die Immobilienwirtschaft? Wurden diese Themen früher anders bewertet bzw. waren sie mehr oder weniger präsent? Stellen Mieter heute neue Anforderungen?
Bei besonders exponierten Lagen, Nutzungsarten und Gebäudeklassen, beispielsweise Bahnhöfen, Flughäfen und Hochhäusern sowie bei speziellen Mietern wie Banken, Behörden und Ministerien besteht nach wie vor ein unverändert hohes Gefährdungspotential und somit der Bedarf an entsprechende Vorkehrungsmaßnahmen durch die Eigentümer. Beispielsweise besitzt THE SQUAIRE am Frankfurter Flughafen seit Fertigstellung ein gemeinsam mit Bundespolizei, Landespolizei, Feuerwehr, Flughafen und Bahn erarbeitetes Sicherheitskonzept. Zentrale Einheit dieses Sicherheitskonzeptes ist die ständig besetzte Notfall-Serviceleitstelle, welche im Regelbetrieb das Gebäude steuert, überwacht und Sicherheitsmitarbeiter sowie die hauseigene Feuerwehr koordiniert. In einem Notfall-Szenario wie Bombendrohung, Brand, Explosion oder Amok ist die Leitstelle ausgerüstet, um für die Einsatzleitung als Krisenzentrale zu fungieren.

Bei Gebäuden, die weder von der Lage, noch von der Nutzungsart einer besonderen Gefährdung unterliegen, stellen wir seitens unserer Mieterschaft keine erhöhten Anforderungen aufgrund aktueller Vorfälle fest. Als einzige neue Entwicklung lässt sich ein Hinterfragen der Fluchtkonzepte, die in jedem Notfall nach außen führen, feststellen. Neue Konzepte sollen zwischen Gefahren innerhalb des Gebäudes und Angriffen von außen unterscheiden und die Fluchtrichtung entsprechend steuern.

Welchen Beitrag kann die Immobilienwirtschaft leisten, um die Sicherheit von Menschen und Sachwerten in Gebäuden zu gewährleisten? Ist hier ggf. auch die Politik gefordert? Brauchen Immobilienunternehmen heute einen Sicherheitsbeauftragten?
Der Beitrag der Immobilienwirtschaft zur Sicherheit von Menschen und Sachwerten liegt sowohl in baulichen als auch in organisatorischen Schutzmaßnahmen.

Durch streng reglementierte Bauvorschriften insbesondere beim Brandschutz ergibt sich bereits ein flächendeckend hoher Standard bezüglich der bei Notfall-Szenarien relevanten Aspekte wie Feuerwiderstand und sichere Entfluchtung. Besondere bauliche Sicherungselemente wie z.B. schusssichere oder sprenghemmende Fassaden, welche schon seit vielen Jahren zum Einsatz kommen, werden lediglich von einer kleinen Klientel abgefragt. Eine erhöhte Nachfrage aufgrund aktueller Ereignisse ist hier nicht festzustellen.

Müssen wir unsere Freiheit einschränken, um in unseren Gebäuden sicherer zu sein? Was bewirken Ereignisse die Terroranschläge in Paris, Istanbul, München oder Berlin?
Jedes Sicherheitskonzept schränkt Freiheiten auf die ein oder andere Art und Weise ein. In unserem Portfolio sind wir insbesondere im hochwertigen Bürosegment regelmäßig mit diesem Konflikt konfrontiert.
Mehr Sicherheit bedeutet grundsätzlich mehr Kontrolle und damit ein höherer Zeitaufwand bei Zugangstüren und Aufzügen und hierdurch weniger Benutzungskomfort und weniger Effizienz.
Insbesondere bei Ankäufen von Projektentwicklungen machen wir die Erfahrung, dass eine frühzeitige und detaillierte Abstimmung der Sicherheitskonzepte mit den Mietern immens wichtig ist. Nicht kommunizierte Einschränkungen führen leicht zu Mieter-Unzufriedenheit und spätere Änderungen sind mit hohen Kosten verbunden.

Welche neuen Geschäftsmodelle ergeben sich aus der tatsächlichen oder gefühlt erhöhten Bedrohungslage?
Insgesamt lässt sich feststellen, dass durch gesetzliche Vorschriften und gezielte Nachfrage der Mieter bereits ein hoher Sicherheitsstandard besteht. Dieser Standard wird sich in Abhängigkeit von Bauvorschriften und der Nachfrage stetig weiterentwickeln.

Herr Eichelberger, nehmen Sie in Ihrem Geschäftsalltag eine geänderte Sicherheitslage in Deutschland wahr? Verfügen Sie über Statistiken zur tatsächlichen Sicherheitslage, z.B. aus dem Versicherungsbereich?
Innerhalb unseres europäischen Portfolios bei TRIUVA sind Sachbeschädigungen (böswillige Beschädigung, Einbruch, Diebstahl und Raub) auf einem langfristig niedrigen Stand und nahmen innerhalb der letzten drei Jahre nochmals stetig ab. Es ist jedoch anzumerken, dass der Immobilieneigentümer bei Einbrüchen lediglich in puncto Sachbeschädigung der Gebäudehülle betroffen ist und die eigentlichen Ziele des Diebstahls üblicherweise den Mieter betreffen.

Welche Auswirkungen haben Terror und Kriminalität auf die Immobilienwirtschaft? Wurden diese Themen früher anders bewertet bzw. waren sie mehr oder weniger präsent? Stellen Mieter heute neue Anforderungen?
Bei besonders exponierten Lagen, Nutzungsarten und Gebäudeklassen, beispielsweise Bahnhöfen, Flughäfen und Hochhäusern) sowie bei speziellen Mietern wie Banken, Behörden und Ministerien besteht nach wie vor ein unverändert hohes Gefährdungspotential und somit der Bedarf an entsprechende Vorkehrungsmaßnahmen durch die Eigentümer. Beispielsweise besitzt The Squaire am Frankfurter Flughafen seit Fertigstellung ein gemeinsam mit Bundespolizei, Landespolizei, Feuerwehr, Flughafen und Bahn erarbeitetes Sicherheitskonzept. Zentrale Einheit dieses Sicherheitskonzeptes ist die ständig besetzte Notfall-Serviceleitstelle, welche im Regelbetrieb das Gebäude steuert, überwacht und Sicherheitsmitarbeiter sowie die hauseigene Feuerwehr koordiniert. In einem Notfall-Szenario wie Bombendrohung, Brand, Explosion oder Amok ist die Leitstelle ausgerüstet, um für die Einsatzleitung als Krisenzentrale zu fungieren.

Bei Gebäuden, die weder von der Lage, noch von der Nutzungsart einer besonderen Gefährdung unterliegen, stellen wir seitens unserer Mieterschaft keine erhöhten Anforderungen aufgrund aktueller Vorfälle fest. Als einzige neue Entwicklung lässt sich ein Hinterfragen der Fluchtkonzepte, die in jedem Notfall nach außen führen, feststellen. Neue Konzepte sollen zwischen Gefahren innerhalb des Gebäudes und Angriffen von außen unterscheiden und die Fluchtrichtung entsprechend steuern.

Welchen Beitrag kann die Immobilienwirtschaft leisten, um die Sicherheit von Menschen und Sachwerten in Gebäuden zu gewährleisten? Ist hier ggf. auch die Politik gefordert? Brauchen Immobilienunternehmen heute einen Sicherheitsbeauftragten?
Der Beitrag der Immobilienwirtschaft zur Sicherheit von Menschen und Sachwerten liegt sowohl in baulichen als auch in organisatorischen Schutzmaßnahmen.

Durch streng reglementierte Bauvorschriften insbesondere beim Brandschutz ergibt sich bereits ein flächendeckend hoher Standard bezüglich der bei Notfall-Szenarien relevanten Aspekte wie Feuerwiderstand und sichere Entfluchtung. Besondere bauliche Sicherungselemente wie z.B. schusssichere oder sprenghemmende Fassaden, welche schon seit vielen Jahren zum Einsatz kommen, werden lediglich von einer kleinen Klientel abgefragt. Eine erhöhte Nachfrage aufgrund aktueller Ereignisse ist hier nicht festzustellen.

Müssen wir unsere Freiheit einschränken, um in unseren Gebäuden sicherer zu sein? Was bewirken Ereignisse die Terroranschläge in Paris, Istanbul, München oder Berlin?
Jedes Sicherheitskonzept schränkt Freiheiten auf die ein oder andere Art und Weise ein. In unserem Portfolio sind wir insbesondere im hochwertigen Bürosegment regelmäßig mit diesem Konflikt konfrontiert.
Mehr Sicherheit bedeutet grundsätzlich mehr Kontrolle und damit ein höherer Zeitaufwand bei Zugangstüren und Aufzügen und hierdurch weniger Benutzungskomfort und weniger Effizienz.
Insbesondere bei Ankäufen von Projektentwicklungen machen wir die Erfahrung, dass eine frühzeitige und detaillierte Abstimmung der Sicherheitskonzepte mit den Mietern immens wichtig ist. Nicht kommunizierte Einschränkungen führen leicht zu Mieter-Unzufriedenheit und spätere Änderungen sind mit hohen Kosten verbunden.

Welche neuen Geschäftsmodelle ergeben sich aus der tatsächlichen oder gefühlt erhöhten Bedrohungslage?
Insgesamt lässt sich feststellen, dass durch gesetzliche Vorschriften und gezielte Nachfrage der Mieter bereits ein hoher Sicherheitsstandard besteht. Dieser Standard wird sich in Abhängigkeit von Bauvorschriften und der Nachfrage stetig weiterentwickeln.

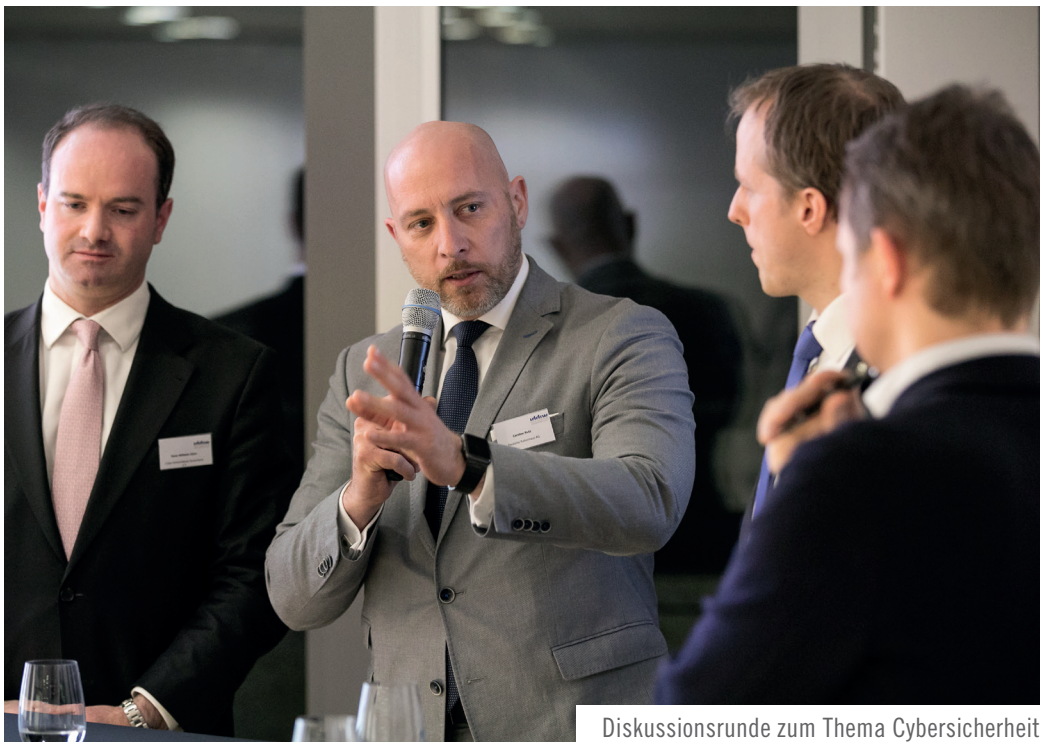
Ohne Cybersicherheit keine sichere Projektentwicklung

Carsten Rutz Vorstand Deutsche Reihenhaus AG

Die elektronische Dateninfrastruktur ist heute das Fundament für das Überleben der gesamten Gesellschaft. Wie sehr das Thema uns alle betrifft, sehen wir gerade in diesen Tagen. Hacker legen mit gezielten Angriffen ganze Behörden und Unternehmen lahm. Scheinbar einziger Ausweg aus einer Erpressung ist die Bezahlung mit virtuellem Geld – den Bitcoins. Die Angreifer sind damit nicht einmal mehr identifizierbar. Gewaltige Summen fließen in der Hoffnung, der Angriff möge damit abgewehrt sein. Doch es trifft auch vermehrt – und genauso taktisch geschickt – Privatmenschen. Da kommt eine E-Mail in den Posteingang mit dem Hinweis, man habe wohl die Begleichung einer Rechnung vergessen und man möge den Betrag von 20 Euro doch bitte schnell begleichen, bevor die Sache zum Anwalt geht. Und manch einer drückt eben schnell auf „Jetzt bezahlen!“ bevor sich das zu einem riesigen Ärgernis ausweitet. Für die Verbrecher zahlt sich diese Methode aus: Kleinvieh macht eben auch Mist.

Gerade Projektentwickler stehen in meinen Augen vor einer besonderen Herausforderung innerhalb der Industrie. Denn sie gestalten ein Produkt, dass in der unmittelbaren Lebenswelt des Menschen steht: Immobilien. Der Großteil von uns arbeitet jeden Tag in ihnen. Und ein noch wesentlich höherer Prozentsatz lebt in einem Haus. Dabei hat der physische Einbruch heute dieselbe Bedrohungsqualität wie der virtuelle.

An unsere Branche bestehen zwei Erwartungen: Die Cybersicherheit in den Unternehmen muss gewährleistet sein. Von den Preisverhandlungen, Kaufvertragsgestaltungen bis hin zur Planung und zum Bau der Immobilien ist heute ein Unternehmen ohne IT nicht mehr konkurrenzfähig. Wenn die Daten in schlecht gesicherten Systemen für Hacker zugänglich sind, können Immobilien durch Eingriffe in Planungen im wahrsten Sinne des Wortes auf



Diskussionsrunde zum Thema Cybersicherheit

einem wackligen Fundament stehen. Wie wird wohl der Projektentwickler handeln, der am Abend vor der feierlichen Eröffnung des Einkaufzentrums mit Politik und Verwaltung eine E-Mail bekommt, die voraussagt, dass man die Planungen seiner Immobilie manipuliert hat?

Damit dieses Szenario nicht eintreten kann, müssen absolute Experten mit der Datensicherung beschäftigt werden. Und in die muss investiert werden. Denn diese werden nicht nur von der Immobilienbranche nachgefragt, sondern von nahezu allen Unternehmen. Der Markt ist knapp – gute Mitarbeiter demzufolge schwer verfügbar. Die Personalentwicklung geht in meinen Augen den gleichen Weg, wie die der Unternehmenskommunikation in den vergangenen Jahren. Auch da haben sich vorausschauende Immobilienunternehmen Experten ins Haus geholt, die nichts mit Immobilien zu tun haben müssen. Ihre Aufgabe war es, die gewachsenen Anforderungen der Kunden und Geschäftspartner an interne und externe Kommunikation – hier vor allem die Dialogkommunikation – bewältigen zu können. Die zweite Welle von Spezialisten von außen sind heute die IT-Experten, die mit ihrem Können eben auch die Kommunikation sichern.

Gerade die Entwickler von Wohnimmobilien haben in meinen Augen eine ganz besondere Aufgabe: Es muss sichergestellt bleiben, dass die eigenen vier Wände weiterhin eine sichere Burg für die Bewohner bleiben. Menschen müssen sich darauf verlassen können, dass ein Bauträger ein einwandfreies Produkt gestaltet, dass einen stabilen Lebensmittelpunkt garantiert. Datensicherheit beim Bauträger spielt dabei in der gesamten Wertschöpfungskette eine wichtige Qualität. Es muss aber ebenso gewährleistet werden, dass nach Übergabe des Hauses an den Käufer oder Mieter der virtuelle Einbrecher nicht zum klassischen Einbrecher wird. Zwei Komponenten sorgen für Schutz: Die Sicherheit der persönlichen Daten des Hauskäufers innerhalb der IT des Bauträgers muss garantiert sein. Ebenso sicher sein muss die smarte Elektronik, mit der immer mehr Häuser gesteuert werden. Der moderne Einbrecher kann auf sein Brecheisen verzichten, wenn er ganz leicht die Funkfrequenz für die Öffnung der Garage abfangen und einbrechen kann, weil die Daten nicht geschützt sind.

Kommen wir auf die zahlreichen arglos geöffneten E-Mail-Anhänge zurück, die in so manchen privat wie auch geschäftlich genutzten Computern ein Virus freigesetzt haben. Sie belegen, dass das Thema Cybersicherheit gesamtgesellschaftlich nicht ausreichend angekommen ist. Ein Mitarbeiter, der für das Thema privat nicht sensibilisiert ist, wird am Unternehmenscomputer nicht bedächtiger handeln.

„Unsere Gesellschaft ist stärker als zuvor durch Computerversagen, -missbrauch oder -sabotage bedroht. Bisher kann nicht ausreichend sichergestellt werden, dass die Informationstechnik das tut, was sie soll, und nichts tut, was sie nicht soll.“ Dieses Zitat stammt aus der selbst formulierten Aufgabe des Bundesamts für Sicherheit in der Informationstechnik. Ich frage mich: Ja, wer soll das denn sicherstellen? Ich sage: Es ist auch eine Aufgabe der Politik! Das BSI biete Initiativen, Aktionsbündnisse und Handlungsempfehlungen an, die den Unternehmen im Lande die Cybersicherheit näherbringen. Allerdings fehlt mir oft der Bezug zur Realität aller Menschen. Ich sehe hier die staatlichen Institutionen in der Pflicht, das Thema Cybersicherheit deutlicher zu positionieren. Nur wenn das gesamtgesellschaftliche Wissen über die Bedrohungen der Cyberkriminalität wächst, kann das in den Unternehmen auch effektiv an die Menschen weitergegeben werden. Die Entwicklung darf in keinem Falle dazu führen, dass sich nur ein kleiner Kreis innerhalb der Führungsebenen und der IT-Abteilung mit der Problematik auseinandersetzt. Dieses Wissen ist wertvoll und werterhaltend für alle.

Gerade für uns Projektentwickler heißt es deshalb: In unserer hochsensiblen Branche dürfen wir keine Kosten und Mühen scheuen, dass Thema Cybersicherheit voranzutreiben und dafür zu sensibilisieren. Denn wir tragen schließlich die besondere Verantwortung für die Menschen, die in Immobilien leben und arbeiten. Ein staatliches Informationsangebot ist schön – das Abholen der Inhalte und die Einbindung in die Organisation liegt in unserer Verantwortung.

Smarte Objektsicherung zahlt sich aus

Karsten Linde Business Development Director, Camelot Europe

Immobilienbesitzer behandeln die Phasen am Rande des Immobilienzyklus – Neubau und Leerstand – oft stiefmütterlich. Dabei stellen sich gerade in diesen Phasen mit Blick auf Gefahren wie Vandalismus, Diebstahl, Bauverzögerung oder Wertverlust ganz akute Sicherheitsfragen. Durch innovative Konzepte lassen sich diese Herausforderungen nach dem Motto „kleine Ursache, große Wirkung" intelligent bewältigen. Mit gut gesicherten Objekten leistet die Immobilienbranche zugleich einen Beitrag zur allgemeinen Sicherheit.

Es muss nicht gleich der Wachdienst sein

Vandalen treibt die pure Lust an der Zerstörung, Diebe haben es auf wertvolle Werkzeuge, Maschinen oder Materialien abgesehen: Beide Arten von Eindringlingen auf Baustellen können kostspielig für Immobilienbesitzer bzw. Bauherren werden. Weil es durch die Schäden, die kriminelle Eindringlinge anrichten, oft auch noch zu Verzögerungen im Bauterminplan kommt, wird es schnell doppelt teuer.

Teuer ist direkt auch das Stichwort: Viele Eigentümer sehen zwar die Probleme, scheuen aber die scheinbar hohen Kosten. Klassische Lösungen wie Wachdienste haben ihren Preis, die Kosten summieren sich im Bauverlauf erheblich. Die gute Nachricht: Es gibt innovative Sicherheitssysteme, die mit wenig Aufwand viel Sicherheit schaffen. So existieren heute Videoüberwachungslösungen, die auf die Baustellensicherheit zugeschnitten sind. Camelot selbst hat zum Beispiel das System des „WatchTower" entwickelt. Hierbei handelt es sich um einen bis zu sieben Meter hohen Mast mit drei nachtsichtfähigen 360°-Grad Kameras, die in Full HD aufzeichnen. Schon die abschreckende Wirkung ist nicht zu unterschätzen. Der Erfassungsbereich des Towers erstreckt sich auf bis 20.000 m² und kann individuell festgelegt werden. In diesem Bereich entsteht ein „virtueller Zaun" – wird dieser überschritten, entdeckt das System den Eindringling und nimmt ihn auf. Zeitgleich wird die Leitstelle informiert. Von dort kann ein Mitarbeiter über eine optionale Lautsprecheransprache oder zuschaltbare gleißend helle Lichtstrahler den oder die Unbefugten vertreiben. Gleichzeitig wird ein angeschlossener Wachdienst oder die Polizei informiert, im Idealfall können Täter so direkt gefasst werden. Für die spätere Strafverfolgung schafft die Full-HD-Aufzeichnungen gute Voraussetzungen.

Systeme wie der WatchTower lassen sich idealerweise in kurzer Zeit in Betrieb nehmen. Sie schlagen einen Bogen von der Abschreckung bis hin zur Strafverfolgung und ersparen zu einem geringen Preis viel Ärger und Kosten. Die Baustelle mit ihren Werten ist auf wirkungsvolle Weise überwacht, gleichzeitig übernimmt der Eigentümer Verantwortung für die Sicherheit in seinem Verfügungsbereich.

Damit aus Leerstand keine Einladung an Eindringlinge wird

Vor einer Umnutzung oder zwischen zwei Nutzungsphasen von Immobilien kann es zu Leerstand kommen. Je länger diese Phasen dauern, desto stärker können Immobilien von Wertverfall bedroht sein. Gleichzeitig wirkt sichtbarer Leerstand geradezu wie eine Einladung für Vandalen oder Eindringlinge. Eingeworfene Fensterscheiben sind hierfür nur eines der klassischen Zeichen. Für den Eigentümer stellt sich hier die Frage, wie er sein leerstehendes Objekt sichert – auch weil Versicherungsrisiken und steuerliche Konsequenzen drohen können.

Auch hier schrecken viele wieder vor den Kosten eines professionellen Wachdienstes zurück. Ein interessante Alternative ist das Hauswächter-Konzept, das sich als „Bewachung durch Bewohnung" beschreiben lässt. Hier leben so lange wie nötig oder gewünscht so genannte Hauswächter in Teilen des Objekts. Die Immobilie wirkt bewohnt und dadurch sofort alles andere als einladend für Unbefugte. Angenehmer Nebeneffekt: Schäden – wie z.B. ein Rohrbruch – werden durch die Hauswächter eher entdeckt und können behoben werden, bevor es richtig teuer wird.

Darüber hinaus kann Leerstand auch aktiv zwischengenutzt werden, z.B. in dem befristet Workspaces geschaffen werden oder das Objekt als Filmkulisse angeboten wird. Sicherungswirkung inklusive. Die Möglichkeiten und Chancen sind vielfältig – wenn man sich mit den ungeliebten Phasen des Leerstands aktiv und professionell beschäftigt.

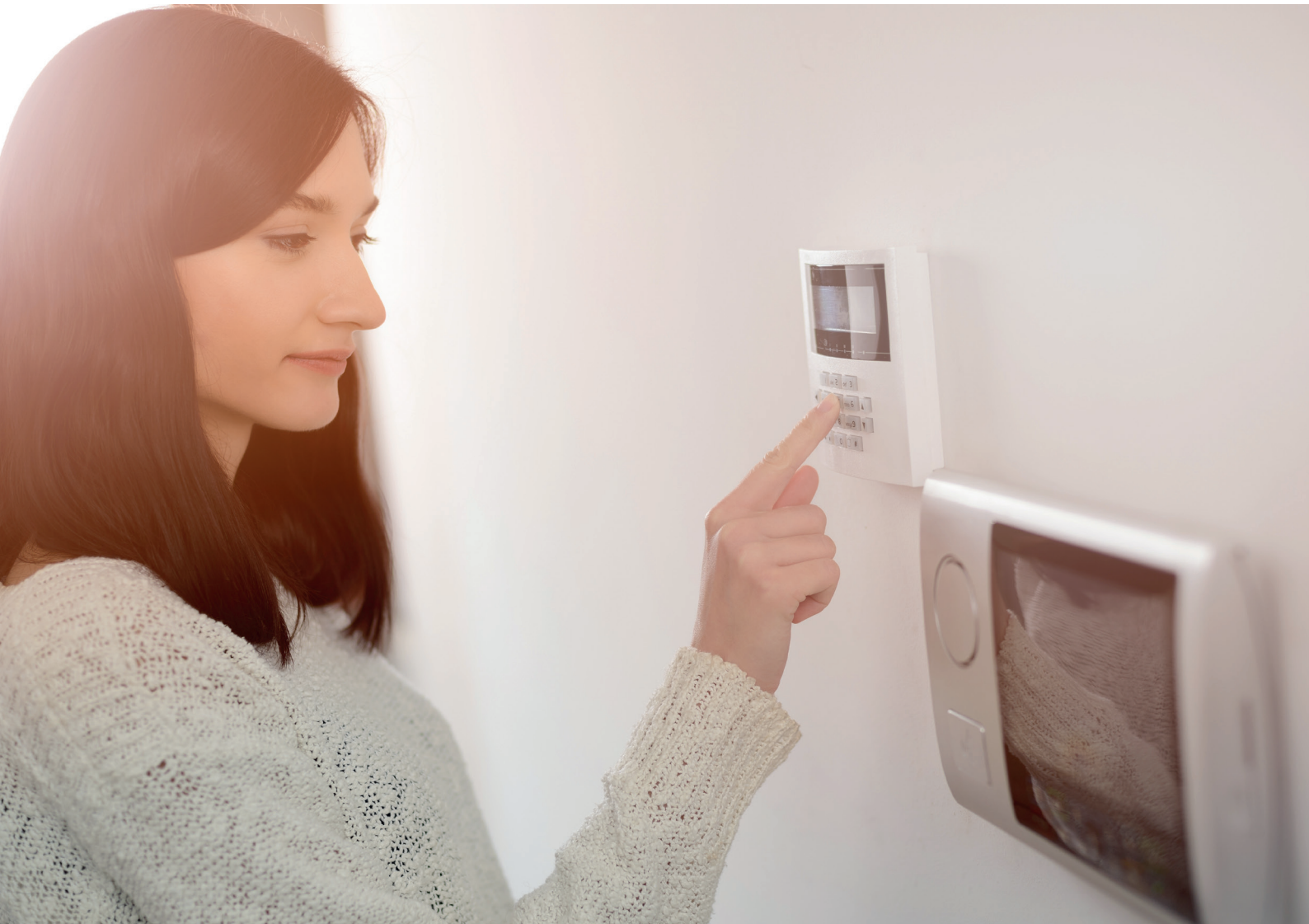
Sicherheit von Immobilien – ein Beitrag zur allgemeinen Sicherheit?

So kann man es nicht nur, aber auch, in Zeiten der Bedrohung durch Terror durchaus sehen. Welcher Eigentümer möchte es riskieren, dass ein entwendetes Baustellenfahrzeug für ein Verbrechen benutzt wird? Wer möchte Kriminellen in einem leerstehenden Gebäude unwissentlich Unterschlupf ermöglichen? Mit intelligenten Sicherungslösungen vertreten Eigentümer nicht nur ihre wie Diebstahlschutz und Werterhalt, sie übernehmen Verantwortung für ihren Verfügungsbereich und können automatisch auch einen Beitrag zur allgemeinen Sicherheit leisten.

Smart Home sicher gestalten

Dr.-Ing. Christian Bogatu Mitgründer und Beirat der KIWI.KI GmbH

Ob schlüssellose Zugangssysteme oder Komfortsysteme für Senioren – Smart Home Produkte verbreiten sich in unseren Immobilien immer stärker. Da die Geräte am intimsten Platz in unsere Leben angebracht werden – unserem Zuhause – braucht es hohe Standards in Sachen Sicherheit. Einheitliche Standards existieren heute jedoch nur eingeschränkt. Die Folge: Sicherheitstechnisch unausgereifte Produkte gelangen auf den Markt, immer wieder berichten Medien über Schwachstellen und Gefahren von Smart Home Geräten. Vereinzelte Negativbeispiele schaden so dem Ruf der ganzen Branche und schmälern das Vertrauen der Kunden. Oft kann der Verbraucher die Sicherheit einzelner Systeme auf Grund der Komplexität der Thematik schlecht einschätzen. Einheitliche, nachvollziehbare aber auch erreichbare und angemessene Regeln sind daher wichtig.



Weil Sicherheit und Datenschutz neben Komfort und Effizienzsteigerung bei KIWI die wichtigsten Faktoren sind, setzen wir auf strenge regelmäßige Testroutinen. Mit sogenannten Attack-Tests können wir das System von Cryptoexperten testen lassen. Wir arbeiten mit White-Hat-Hackern, also Hackern, die professionelle Sicherheitstest durchführen, zusammen, um sicherzustellen, dass unser System Angriffen von außen standhält. Zudem legen wir die sicherheits- und datenschutzrelevanten Algorithmen offen, um maximale Transparenz zu erzielen. Standards bringen dem Verbraucher nichts, wenn sie nicht offengelegt werden. Es wäre sinnvoll, die Einhaltung dieser Anforderungen vor dem Verkauf zu kommunizieren.

Sicherheit sollte von Unternehmen nicht nur als notwendiges Übel, sondern als Fundament für langfristig erfolgreiche Smart Home Produkte gesehen werden. Ist die Sicherheit nicht gewährleistet, muss daran als erstes gearbeitet werden, schließlich geht es bei Smart Home um Lösungen für das Zuhause. Damit einher geht auch der Datenschutz. Schließlich darf die Privatsphäre unter keinen Umständen leiden. Das Gebot an dieser Stelle ist der sparsame Umgang mit Daten. Dabei gilt: Die sichersten Nutzerdaten sind die, die nie erhoben werden.

Digitale Todsünden identifizieren

Jedes Produkt, das mit dem Internet verknüpfbar und für Smart Home einsetzbar ist, sollte gewisse Mindestanforderungen erfüllen. Im Rahmen eines kürzlich von KIWI geführten Interviews mit Richter Ulf Beuermeyer entwickelte sich die Bezeichnung „digitale Todsünden“, welche unbedingt zu vermeiden sind. Ein minimaler Standard kann schon mit wenig Aufwand erreicht werden. Optimaler Weise sollte es gesetzliche Grundlagen geben, um eine ausnahmslose Durchführung zu sichern. Es darf kein Wettbewerbsvorteil sein, wenn Unternehmen zur Kostensenkung an Herstellungskosten sparen. Im Augenblick können Produzenten ihr Produkt zu einem für Kunden attraktiveren Preis auf den Markt bringen, ohne dass mangelhafte Sicherheitsstandards gekennzeichnet würden. Daher fordere ich, dass für jedes Produkt sinnvolle und angemessene Mindestanforderungen formuliert werden, bevor es eine Verbindung zum Internet herstellen kann. Eben einen Katalog der digitalen Todsünden.

Beispielhaft für derartige digitale Todsünden sind Standard-Passwörter, die sich auch Außenstehende leicht erschließen können, oder keine Möglichkeit für spätere Sicherheitsupdates. Nur durch regelmäßige Updates können Geräte immer auf dem neuesten Stand der Sicherheitstechnik bleiben, ohne direkt ausgetauscht werden zu müssen. Das macht Smart Home nicht nur deutlich sicherer und günstiger, sondern auch nachhaltig. Neben Sicherheit sollten wir schließlich auch an die Umwelt denken. Massive Sicherheitslücken lassen sich so vermeiden. Außerdem ist die Prävention eine deutlich sinnvollere Strategie als die bisher praktizierte: Wir jagen Cyber-Kriminellen hinterher, was in der Regel wenig Erfolg verspricht, anstatt die Technologien sicherer zu machen.

Smart Home als Zukunftsthema für die Immobilienbranche

Smart Home ist ein wichtiges Thema für die Immobilienbranche. Unternehmen, die zukunftsorientiert arbeiten, sollten die Digitalisierung nicht links liegen lassen. Nicht zuletzt, weil sie sich selber den Arbeitsalltag erleichtern können. Ein kontinuierlicher Blick auf das Thema Cybersicherheit bleibt jedoch die Voraussetzung für die weitere Digitalisierung.

Zum Schluss noch ein grundlegender Denkanstoß speziell für die Immobilienbranche: Verteilen Sie keine herkömmlichen Schlüssel mehr. Das traditionelle Schlüsselmanagement birgt große Sicherheitslücken. Metallschlüssel gehen verloren oder können nachgemacht werden. Keiner kann sich sicher sein, wie viele Schlüssel in Umlauf sind. Das ist ein großer Risikofaktor. Die Immobilienbranche muss die Schlüsselhoheit behalten. Das ist nicht nur unter Sicherheitsaspekten, sondern auch unter Kostenpunkten zu bedenken.

Mehr über KIWI auf www.kiwi.ki

So oder so – Sicherheit hat Ihren Preis

Ingmar Behrens Leiter Public Affairs German Council of Shopping Centers

Manche Dinge ändern sich so schnell, dass man zum Zeitpunkt der Veränderung noch nicht absehen kann, welche Wirkung in den nächsten Stunden, Wochen und Jahren daraus entstehen wird. Eines der denkwürdigsten Ereignisse im 21. Jahrhundert ist „9/11“, der Terroranschlag in New York. Die Bilder im Kopf habend, dürfte jeder noch wissen, wo er war, als er von den Anschlägen am Dienstagvormittag (Ortszeit NY) erfahren hat und diese auch in der Liveberichterstattung mit brutaler Härte und unbeschreiblichen Details quasi „miterleben“ musste.

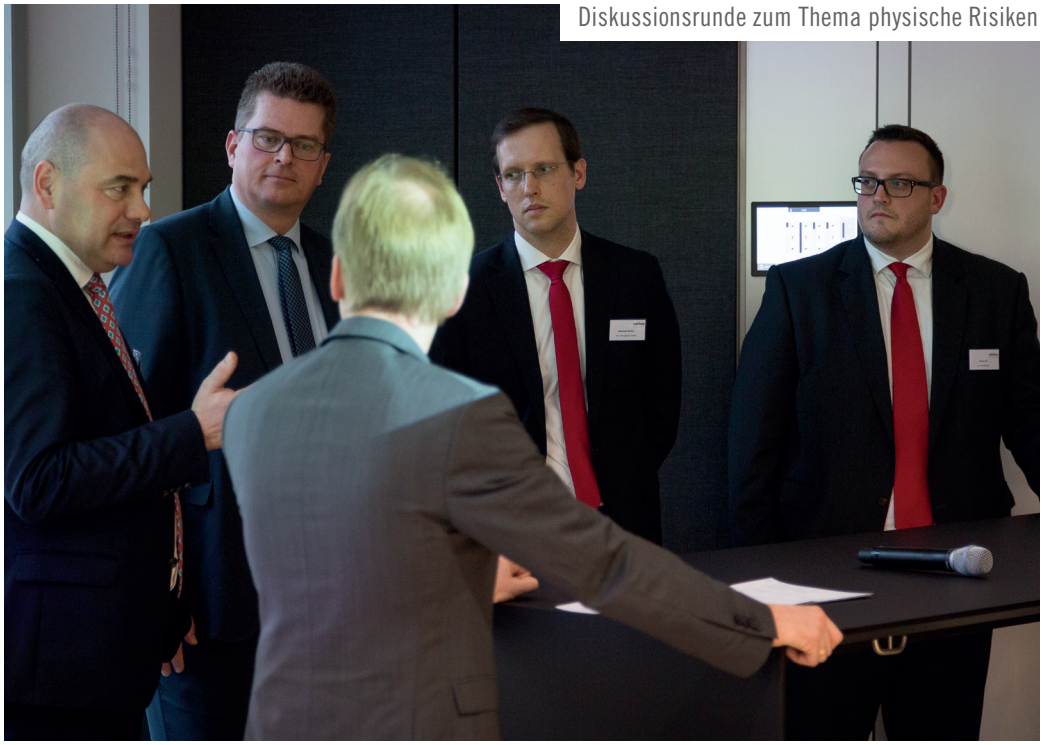
„9/11“ war eine Zäsur in der Geschichte des Terrorismus, es war eine neue grausame Dimension von fatalistischem und islamistischem Denken und Handeln. Die verehrende Bilanz: etwa 3.000 Todesopfer und ein noch nie eingetretener Schadensfall für die Versicherungsbranche. Die Folgen der immensen Schäden nur aus der Sicht der Versicherer belaufen sich bis heute auf rund 37,5 Milliarden US-Dollar, von denen rund 51 Prozent Sachschäden sind. Bis zu diesem Ereignis war „Terror“ undefiniert in allen Versicherungssachverträgen ohne Limit eingeschlossen.

Die Stadt New York bezifferte ein Jahr später die Gesamtschäden in Form zerstörter Gebäude, Gehalts- und Steuerausfällen sowie verloren gegangener Umsätze der betroffenen Unternehmen auf rund 95 Milliarden Dollar. Die Stadt verlor über 80.000 Arbeitsplätze, und ein zuvor erwarteter Stellenanstieg von 63.000 blieb aus. Es wurden rund 1,2 Millionen Quadratmeter Büroraum zerstört und etwa 1,6 Millionen Quadratmeter beschädigt. Die Kosten hierfür belaufen sich allein auf 21,8 Milliarden Dollar. Das durch den Anschlag nachhaltig eingebremste Wirtschaftswachstum hat in den Vereinigten Staaten schätzungsweise 750.000 Jobs gekostet.

In vielerlei Hinsicht stand die Welt seinerzeit Kopf. Die Neustrukturierung der „Terrorversicherung“ durch führende Versicherer und der Bundesrepublik Deutschland in der gemeinsamen Gesellschaft „Extremus AG“ ist ein Baustein in der neuen Sicherheitsarchitektur westlicher Gesellschaften. Die Terror-Ereignisse in Europa mit den Stichworten „Brüssel, Paris, Nizza, London und Berlin“ zeigen den aktuellen Stand der Dinge gut 16 Jahre später auf. All diese Terroranschläge wurden von Terroristen mit islamistischem Hintergrund sowie engster Verbindung zum Islamischen Staat geplant und ausgeführt. Den eigenen Tod in Kauf nehmend, fehlt jegliches westliche, christliche und menschliche Wertesystem bei diesen Menschen. Die Grausamkeit der Taten bezeugen dies vielfach.

Was heißt das für die Immobilienwirtschaft? Juristisch gesehen muss sich spätestens nach der Terrorwarnung durch das BKA jeder Geschäftsführer und Vorstand „enthaften“, indem er geeignete Maßnahmen zur Unversehrtheit seiner Mitarbeiter, Kunden und Mieter erarbeitet, diskutiert und umsetzt. Dies ergibt sich klar aus dem Arbeitsvertrag und in der Folge auch aus dem Mietvertrag und vielem mehr. Tut er dies nicht, haftet er im schlimmsten Falle persönlich, sofern fahrlässiges oder sogar vorsätzlich Verhalten festgestellt wird. Da der Autor kein ausgebildeter Jurist ist, sei folgender Hinweis erlaubt: Die Rücksprache zu diesem Themenfeld*

ist mit dem Hausjuristen, dem qualifiziertem Sicherheitsberater oder der geeigneten Kanzlei sicher individuell und fachlich am besten zu führen. Wichtigtuer und selbsternannte „Terrorexperten“ gehören nicht in diesen Kreis der Berater. Es ist daher immer zwingend notwendig sich nachvollziehbare und überprüfbare Referenzen vorab geben zu lassen und diese ggf. mit den zuständigen Behörden abzuklären.



Diskussionsrunde zum Thema physische Risiken

Die Immobilienwirtschaft steht im Themenfeld bei möglichen Terrorakten mittelbar und unmittelbar im Fokus. Die Auswirkungen der Anschläge „9/11“ zeigen den Wirkungsradius auf. Ein LKW, der mit Sprengstoff beladen in ein Bürogebäude rast, wird gewaltige Schäden im Umkreis mehrerer hundert Metern anrichten. Die Muster der vergangenen Anschläge haben immer die Schädigung größtmöglicher Menschenmengen bei gleichzeitig größter Aufmerksamkeit und Destabilisierung der Gesellschaft als Ziel verfolgt. Diese Strategie für Gegenwart und Zukunft vorausgesetzt, stellen alle Immobilien mit zentraler Bedeutungen wie Bahnhöfe, Flughäfen, Einkaufspassagen als potentielle Ziele dar. Das betrifft selbstverständlich auch Immobilien, in denen Unternehmen arbeiten, die international im Themenfokus des IS mit seinem radikalen Umfeld stehen. Die vergangenen Terroranschläge – Rucksackbombe bei Stadtfest und Axtangriff im Regionalzug – haben aber gezeigt, dass auch unprominente Ziele angegriffen werden. Daher ist aus dem Themenfeldmuster keine „Enthaftung“ für „Nebenlagen“ von Immobilien zu schließen. Das Vorbereiten auf mögliche Terror- und Amoklauf-Szenarien ist daher heute leider zum Pflichtprogramm der Immobilienwirtschaft geworden. Hierbei ist die Grundlage eines erfolgreichen Sicherheitskonzeptes ein fachliches, sachliches, besonnenes und professionelles Arbeiten.

Die Gewaltenteilung in Deutschland stellt in hervorragender und engagierter Weise durch die Justiz und die Polizei vor Ort und als BKA und LKA´s sowie Verfassungsschutz und seit kurzen auch dem Bundesamt für Sicherheit in der Informationstechnik (Cyber-Sicherheit) in geübter Zusammenarbeit mit Feuerwehr und THW die Rahmenbedingungen für die Abwehr- und den Kampf im Thema „Terror“ sicher. Das Aufrüsten des zivilen Bürgers ist nicht die Aufgabe und das Ziel. Die Stichworte heißen vielmehr Bewusstseinsschaffung, Prävention und professionelles Üben von Handlungsabläufen während und nach dem Krisenfall.

Hierbei kommt es immer auf eine verlässliche, geübte und enge Verbindung zu den lokalen Polizeibehörden und anderer BOS Dienste (Behörden und Organisationen mit Sicherheitsaufgaben) an, da es diverse Schnittstellen der Informationsübergabe und Zusammenarbeit in der hier erforderlichen Praxis gibt.

In der Verantwortung der Immobilienwirtschaft liegt daher die aktive Auseinandersetzung mit der Bedrohungslage und der Abarbeitung des Fragenkataloges „Was heißt das für unser Unternehmen, unsere Mitarbeiter und Mieter?“ sowie „Welche Maßnahmen haben wir schon, wie sicher sind diese und welche brauchen wir noch bzw. könnten optional helfen, die benötigte Sicherheit in allen Verantwortungsbereichen herzustellen?“.

Diese Fragen führen nicht nur auf Themen wie Räumungsübungen im Terror- bzw. Amokfall, sondern ebenso auch in die „Investorenabteilung“ und dort zu den Fragen nach dem Risiko der Standorte und der Immobilien sowie der dagegenstehenden Versicherung und der finalen Frage: „Was unternimmt die Geschäftsleitung noch, um Risiken zu minimieren?“. Hierbei darf

der Imageschaden nicht unterschätzt werden, wenn im Krisenfall später herauskommt, dass der sparsame Finanzvorstand sich z.B. für das „Sicherheitskonzept light“ entschieden hat und daher nur wenige Mitarbeiter an Übungsszenarien zur Räumung teilgenommen haben.

Die deutsche Shopping Center- und Handelsimmobilien Branche gibt hier in der Praxis ein gutes Beispiel, da sie schon immer ein Vorreiter der technisch möglichen und rechtlich relevanten Maßnahmen gewesen ist, wenn es um das komplexe Thema Sicherheit ging. In keiner Assetklasse wird so akribisch auf die Einhaltung der regelmäßigen Brandschutzübungen, z.B. mit Räumungen im laufenden Tagesgeschäft, geachtet wie hier. Die Ereignisse im vergangenen Jahr, nach dem Amoklauf in München, haben die Branchen noch einmal stärker zusammengeschweißt. Basierend auf der Erkenntnis, dass keiner bei wahnsinnigen, religiös motivierten Taten eine 100-prozentige Sicherheit garantieren kann, ist es zu einem bislang bundesweit einmaligen Schulterschluss aller bedeutenden Marktakteure in Deutschland gekommen. In dem vom German Council of Shopping Center (GCSC) initiierten „Arbeitskreis Sicherheit“ engagieren sich seit dem Frühjahr 2016 die Mitgliedsunternehmen des GCSC ohne jeglichen Wettbewerbsgedanken und teilen ihr Wissen sowie ihre Erfahrungen und Konzepte – ein in der Branche einmaliger Vorgang.

Sicherheit in Shopping-Centern und Handelsimmobilien ist kein PR- und Marketingtool, diese Haltung gilt in dem Arbeitskreis und ebenso für alle Immobilien-Assetklassen.

Derzeit arbeitet das GCSC an einem Standardwerk zum Thema „Terror- und Amoklagen“ für die Branche und dem operativen Einsatz mit der professionelle Unterstützung der Rheinischen Fachhochschule und dem dazugehörigen „Kompetenzzentrum Internationale Sicherheit“ in Köln zu arbeiten. Im Herbst wird dieses streng kontrolliert den GCSC Mitglieder in einer ersten Version zur Verfügung gestellt. Der Verband sieht seine Aufgabe in der aktiven Unterstützung der Unternehmen bei der Bewältigung dieser sehr komplexen und menschlich emotionell extrem belastenden Herausforderung. Die Unternehmen können aber letzten Endes dem Staat nur ihre Hilfe im Rahmen ihrer Möglichkeiten und der rechtlichen Rahmenbedingungen anbieten. Umfangreichere Videoüberwachungen mit Schnittstellen zur Polizei werden sehr befürwortet. Die technische und rechtlich einwandfreie Umsetzung der Schnittstellen kann jedoch nicht in der Verantwortung der Unternehmen liegen.

Sicherheit ist etwas, das gemeinsam entsteht und besteht. Diese wichtige Erkenntnis gehört an den Anfang jeder Überlegung, wenn es darum geht, Unternehmen oder Immobilien, einem Sicherheitscheck vor dem Hintergrund der aktuellen Lage zu unterziehen. Als nächstes muss klar werden, dass es sich nicht um eine kurzzeitige Marktbeeinflussung handelt, sondern, dass nach Einschätzung der nationalen und internationalen Fachleute der BOS Dienste diese Bedrohungslage noch über Jahre bestehen bleiben wird. Es ist daher leider nicht die Frage ob etwas passiert, sondern nur wann und wo. Antizipation ist der Schlüssel zum Erfolg.

Wenn eine neue Qualität des Bewusstseins um diese Bedrohungslage zu durchdachten und ständig aktualisierten Präventionsmaßnahmen führt und diese in praktischen Übungen vor Ort mit „lesson learned“ Ergebnissen mündet, dann ist schon sehr viel getan und eine neue Dimension der Sicherheit erreicht. Ein Blick auf unser weltweit beachtetes und bewundertes System der Freiwilligen Feuerwehren sollten uns auch hier lehren: Oft hat eine kleinen Freiwillige Feuerwehr zehn Jahre keinen Einsatz und dann rettet sie in der Nacht ein Menschenleben, welches ohne das Sicherheitsnetz Freiwillige Feuerwehr, ein Todesopfer wäre. Zehn Jahre und mehr üben Männer und Frauen regelmäßig, wird Fahrzeug und Geschirr vorgehalten, um im Fall des Falles einmal helfen zu können.

Seien wir also froh wenn, keiner die neuen Techniken und Maßnahmen zum Schutz der uns anvertrauten Menschen und Wert jemals real einsetzen muss. Ein Schaden im Krisenfall ist sowieso ungleich teurer und menschlich unbeschreiblich schmerzhafter, als jeder Euro der langfristig in vernünftige Sicherheitskonzepte investiert wird. Und ja, am Ende ist dann echte und gelebte Sicherheit auch ein Wettbewerbsvorteil.

---

*der Begriff „Themenfeld“ meint die Tatsachen, die aus der Sicht der Terroristen ein potentielles Ziel darstellen. Das kann beispielsweise ein Mieter sein, der Geschäfte tätigt, die gegen „Regeln“ des IS verstoßen. Hierbei stellt der Immobilieneigentümer nicht das eigentliche Ziel dar, ist aber natürlich potentiell betroffen.