VVB magazin

6/2020
Erscheint 6 x im Jahr
Einzelheft € 5,-
55. Jahrgang
15. Dezember 2020

Angriff auf Smart Cities

Welchen IoT-Bedrohungen sie ausgesetzt sind und wie Versicherer darauf reagieren können

Seite 164

Online-MV 2020

Ein Nachbericht von einer denkwürdigen Mitgliederversammlung

Fachkreise

Kosteneffizienz und Kundenbindung in der privaten Krankenversicherung

Treffpunkte

Bericht zur Podiumsdiskussion Versicherbarkeit von Pandemierisiken

VVBspezial

Mitglieder erzählen: Vom Beruf zur Berufung
Weihnachts-Spezial

Liebe Mitglieder, Förderer und Freunde unserer VVB,

wie in jedem Jahr, so möchte ich mich auch in diesem als Vorstandsvorsitzender unserer Vereinigung mit einem kurzen Rückblick an Sie/Euch wenden. Aber ist dieses Jahr wirklich wie jedes Jahr?

Das VVB-Jahr 2020 begann in gewohnter Weise mit dem Neujahrsempfang am IVW und den finalen Planungen für unsere Mitgliederversammlung im Mai in Hannover. Doch im Februar verdichteten sich nach und nach die Informationen über ein neuartiges Virus Corona / SARS-CoV2. Was zunächst aussah wie eine beherrschbare Thematik in weiter Ferne, bestimmt seither unser Leben und das in einer Weise, wie wir es uns alle sicher nicht hätten erträumen können oder wollen. So kam es denn, dass wir im Rahmen des 1. (!) Lockdowns unsere von unserem Treffpunktleiter Hannover, Frank Wente, mit anderen Mitstreitern sehr gut organisierte MV absagen mussten. Doch nicht nur das: Bis heute und sicher auch bis in das neue Jahr hinein mussten und müssen wir sämtliche Präsenz-Veranstaltungen – sei es von Fachkreisen oder Treffpunkten – absagen. Stattdessen sind die meisten von uns mehr oder weniger freiwillig zu Online-Meeting-Profis geworden. So auch bei der VVB mit Online-Vorstandssitzungen, der Online-Beiratssitzung Ende Oktober oder auch der ersten Online-Mitgliederversammlung in der Geschichte der VVB am 14.11.2020. Auch in anderen Bereichen, sei es im beruflichen Alltag oder sogar im Kontakt mit Freunden haben Online-Tools schnell Einzug gehalten. So gut aber auch die verschiedenen technischen Tools funktionieren, ich denke wir sind uns alle einig, dass diese dauerhaft nicht den persönlichen Kontakt ersetzen können. Und gerade dieser persönliche Kontakt ist ja zentraler Bestandteil unserer Vereinigung.

Was ist sonst noch im Jahr 2020 passiert?

Neben der nicht so sichtbaren Änderung unserer Finanzbuchhaltung ist dem einen oder anderen sicher die Neugestaltung unserer Website aufgefallen. Dank der tatkräftigen Unterstützung von Frank Ackermann, Christian Capitain und dem Grafikhaus ist diese sehr gut gelungen. Sicher ist aber die offensichtlichste Neuerung das etwas verkleinerte Format unseres VVBmagazin – oder ist Ihnen das doch nicht aufgefallen? Diese und weitere Anstrengungen haben dazu geführt, dass unsere Finanzen wieder in deutlich besserem Licht erscheinen.

Aber auch im Vorstand hat es Veränderungen gegeben, wenn auch ungewollte: So hat Franz-Peter Wirtz sein Vorstandsamt für die fachliche Organisation (Fachkreise) krankheitsbedingt Mitte des Jahres an Christian Czempiel-Mentrak übergeben. Wir wünschen Franz-Peter Wirtz alles Gute für seine Gesundheit und Christian Czempiel-Mentrak viel Erfolg in seinem neuen Amt. Auf der Mitgliederversammlung im November hat uns dann unsere langjährige Schatzmeisterin Karola Kurtze darüber informiert, dass sie ihr Amt zum Ende des Jahres nach über 28-jähriger Tätigkeit niederlegen will, um so zu einer weiteren Verjüngung im Vorstand beizutragen. Für ihr außerordentliches Engagement für die VVB sind wir ihr zu großem Dank verpflichtet, was wir dann auf der nächsten MV noch persönlich zum Ausdruck bringen werden.

Neben all diesen Dingen ist gerade in den jetzigen Zeiten die gute und vertrauensvolle Zusammenarbeit mit den Professoren des ivwKöln und der Fachschaft für alle Beteiligten sehr wichtig. Diese beiden Bereiche haben gerade in diesem Jahr mit vielfältigen Aktivitäten dazu beigetragen, den Kontakt zu den Studierenden zu halten und diese nach Kräften zu unterstützen. Dafür und für die wirklich sehr gute Zusammenarbeit, die mir persönlich sehr viel Freude bereitet hat, möchte ich mich an dieser Stelle ganz ausdrücklich bedanken.

Zum Jahresende gilt unser Dank aber auch allen anderen ehrenamtlichen Mitstreitern. Bedanken möchte ich mich dieses Mal insbesondere bei unseren „potentiellen" Gastgebern in Hannover, der HDI-Versicherung und der VGH-Versicherung, wie auch den zugesagten Referenten. Ich hoffe sehr, dass wir auf die Angebote zu einem späteren Zeitpunkt zurückkommen können. Ganz besonderer Dank an die vielen Autoren für die gelungenen Artikel in unserem VVBmagazin. Durch ihren Einsatz und den unseres Redaktionsteams ist es trotz der fehlenden Fachartikel von Fachkreisveranstaltungen gelungen, die sechs Ausgaben in gewohnt hoher Qualität mit interessanten und aktuellen Artikeln zu füllen. Das würde ich gerne wieder für den Appell nutzen, dass Sie weiter viele Beiträge schreiben – aktuelle Themen aus der Versicherungswirtschaft oder aber Fachbeiträge aus dem eigenen Arbeitsgebiet. Neben dem Redaktionsteam für das klassische Medium VVBmagazin möchte ich mich auch bei unserem Social-Media-Team ausdrücklich bedanken. Dieses sorgt für regelmäßige Veröffentlichungen auf den Plattformen XING, LinkedIn und Facebook, was gerade in der jetzigen Zeit eine gute Möglichkeit ist, um sichtbar zu bleiben!

Deshalb und damit Sie die VVB auch in Ihrem Alltag nicht vergessen, haben wir uns in diesem Jahr etwas Besonderes einfallen lassen: Im eingeklebten Umschlag auf der Seite 181 finden Sie einen VVB-Mund-Nasen-Schutz (nachhaltig & waschbar). Dies ist unser Beitrag, Ihnen nah zu sein und damit Sie gesund bleiben!

Nun wünsche ich Ihnen allen, auch im Namen meiner Vorstandskollegen, frohe Weihnachtstage und einen entspannten Jahreswechsel. Schöpfen Sie Kraft für das hoffentlich glückliche und friedliche Jahr 2021! Bleiben Sie gesund und positiv gestimmt! Ich freue mich auf ein Wiedersehen spätestens im Mai in Köln zu unserer 70. Mitgliederversammlung, in der Hoffnung, dass die Corona-Situation es dann zulassen wird!

Ihr Markus Metzler
Vorsitzender des Vorstands der VVB

INHALT

FACHTHEMEN

164 Titel: Angriff auf Smart Cities
170 Instant Payments – Versicherungen unter Zugzwang?
172 Sichtbar bleiben! Effektives Netzwerken in Zeiten von Corona
173 Studie zu Homeoffice in der Versicherungswirtschaft

FACHKREISE

174 Fachkreis Kranken: Die Tarifwechsel Prophylaxe

TREFFPUNKTE

182 Bericht zur Podiumsdiskussion Versicherbarkeit von Pandemierisiken

MV 2020

184 Eindrücke von unserer Online- Mitgliederversammlung 2020

ivwKöln

186 Bildungskongress der Versicherungswirtschaft
189 Online Webinar der Kölner Forschungsstelle Rückversicherung zu der RMT-Initiative von EIOPA

VVBspezial

190 Mitglieder erzählen: Vom Beruf zur Berufung
196 Weihnachts-Spezial

VVB intern + RUBRIKEN

173 Impressum
177 Fachkreisleiter
196 Geburtstage
198 Lehrgang „R": Erneutes Treffen in der Elbmetropole

Angriff auf Smart Cities:

Welchen IoT-Bedrohungen sie ausgesetzt sind und wie Versicherer darauf reagieren können

von PIRMIN SCHÄFER (kor. M.)

Gab es 2018 weltweit schon sieben Milliarden vernetzte Geräte, stieg diese Zahl in diesem Jahr bereits auf 31 Milliarden. Bis 2025 wird sich diese Zahl auf schätzungsweise 64 Milliarden vernetzte Geräte mehr als verdoppeln, so die übereinstimmende Einschätzung von Business Insider, IoT Analytics, Gartner und Intel. [1)]

Der Einsatz des „Internet of Things" (IoT) manifestiert sich längst in erfolgreich umgesetzten Projekten und Konzepten aus den Bereichen Industrie 4.0, Smart Home, autonomes Fahren oder Smart Health bzw. Wearables. Nun ziehen auch immer mehr Städte und Gemeinden nach und setzen auf die erfolgversprechenden Möglichkeiten, die ihnen durch die Transformation zu einer „Smart City" in Aussicht gestellt werden. (Abb. 1)

Eine **Smart City** ist ein Ökosystem in einem urbanen Raum, das eine Reihe von ganzheitlichen Richtlinien und **Strategien** umsetzt, bei denen unter Einsatz von **Informations- und Kommunikationstechnologien** intelligente Anwendungsmöglichkeiten entwickelt und ausgebaut werden, die danach streben,

1. die **Entscheidungsfindung** und die **operative Effizienz** bzgl. der städtischen Vermögenswerte, Ressourcen (Finanzen) und Dienstleistungen zu optimieren,
2. ökologisch **nachhaltig** zu wirtschaften und dabei parallel
3. die Lebensqualität der Bürger zu steigern.[2)]

Abb. 1

Im VVBmagazin 6/2018 wurde bereits auf den personenbezogenen Datenschutz im Smart Home und die Marktchancen für die Versicherungsbranche eingegangen. Der vorliegende Beitrag legt den Fokus ergänzend dazu auf die technisch orientierte IT-Security von Smart Cities und wie Versicherer hier in ihrer Rolle als zuverlässiger Partner unterstützen und begleiten können.

Aktuelle Lage und Projekte smarter Städte in Deutschland

Im Smart City Index 2020 des Bitkom[3)] rangieren derzeit die nebenstehend aufgeführten deutschen Städte auf den vordersten zehn Plätzen.

Begutachtet wurden die Städte in den Kategorien Verwaltung, IT und Telekommunikation, Energie, Mobilität, Gesellschaft sowie in einer übergreifen-

Platz	Tendenz	Stadt	Index
1	→ 0	Hamburg	79.2
2	↗ +3	München	74.4
3	↗ +5	Köln	73.0
4	↑ +6	Darmstadt	71.7
5	↘ -3	Karlsruhe	70.0
6	↘ -3	Stuttgart	69.1
7	↘ -3	Berlin	68.8
8	↑ +23	Osnabrück	66.0
9	↗ +2	Aachen	65.9
10	↘ -4	Heidelberg	65.7

den Gesamtwertung (siehe Abbildung zum Smart City Index 2020). Im Rahmen der „Modellprojekte Smart Cities“ der Bundesregierung[4] sollen neben Großstädten auch kleinere Städte und Mittelzentren in Deutschland die Chance erhalten, sich die neuen Möglichkeiten digitaler Technologien zunutze zu machen.

Bereits seit einigen Jahren sind auf internationaler Ebene Metropolen wie Chicago, Singapur, Wien oder auch die südkoreanische Planstadt Songdo südwestlich von Seoul dabei, den Aufenthalt in ihrer Stadt komfortabler, effizienter und sicherer zu machen.[5] In Anlehnung an die Kategorien aus dem Smart City Index 2020 des Bitkom haben sich dabei diverse Handlungsfelder herauskristallisiert, auf denen die Kommunen tätig werden. (Abb. 2)

In den genannten Sektoren werden umfangreiche Maßnahmen ergriffen:

- Open Data mit öffentlich zugänglichen Informationen und Datenauswertungen, z.B. für Heat Maps
- digitale Bürgerservices (Ausweise, Bescheinigungen, Genehmigungen, etc.) als Teil einer „eGovernment“-Strategie
- sichere, robuste und breitbandige Telekommunikationsnetze
- Überwachung und Steuerung von Umweltdaten, z.B. Temperatur, Wind, Lärm, Luftverschmutzung, Sonneneinstrahlung, Pegelstände von Gewässern, UV-Strahlung
- Einsatz von Smart Grids und Smart Metern: dezentrale Energieerzeugung aus erneuerbaren Energien, Netzlast kontrollieren, automatisch ermittelte und verarbeitete Verbrauchsdaten von Wasser, Strom, Gas etc.
- Förderung von Urban Gardening auf Flachdächern und Brachflächen
- optimiertes Abfallentsorgungsmanagement mit Hilfe von Smart Bins und intelligenter Routenplanung
- angepasste Straßenbeleuchtung zur Vermeidung von Lichtverschmutzung
- Predictive Maintenance für die kommunale Infrastruktur (Strom-, Wasser- und Telekommunikationsleitungen, Brücken, Straßen, Kanäle)
- integrierte Ladesysteme für die innerstädtische Elektro-Mobilität
- optisch unterstützte, anonymisierte Verkehrsüberwachung (Videokameras, Sensoren, Bodenschwellen) und Ampelsteuerung (grüne Welle)
- optimiertes Parkplatzmanagement
- Steuerung autonomer Fahrzeuge, Flottenmanagement, Car Sharing
- leistungsfähiges öffentliches Nahverkehrssystem
- digitales Klassenzimmer oder auch eine „Bildungscloud“ mit datenschutzfreundlichen Anwendungen für Schüler, Lehrer und Eltern
- schnellstmögliche medizinische Notfallversorgung, sicheres Krankenhausmanagement
- Videoüberwachung neuralgischer Punkte im öffentlichen Raum zur Vermeidung von Vandalismus, Kriminalität oder auch Missbrauch von Einrichtungen

Pirmin Schäfer (geb. 1987) ist Wirtschaftsinformatiker und als Senior Consultant für die DYNACON GmbH tätig. Nach seinem dualen Studium der Wirtschaftsinformatik (Bachelor) nahm er einige Jahre später ein weiteres berufsbegleitendes Studium im Fach IT-Management (Master) auf, das er zum Herbst 2018 cum laude abschloss. Als Teil des interdisziplinären Beraterteams der DYNACON GmbH vereint er Knowhow in Business und IT, Expertise in Data Analytics und Umsetzungsstärke.

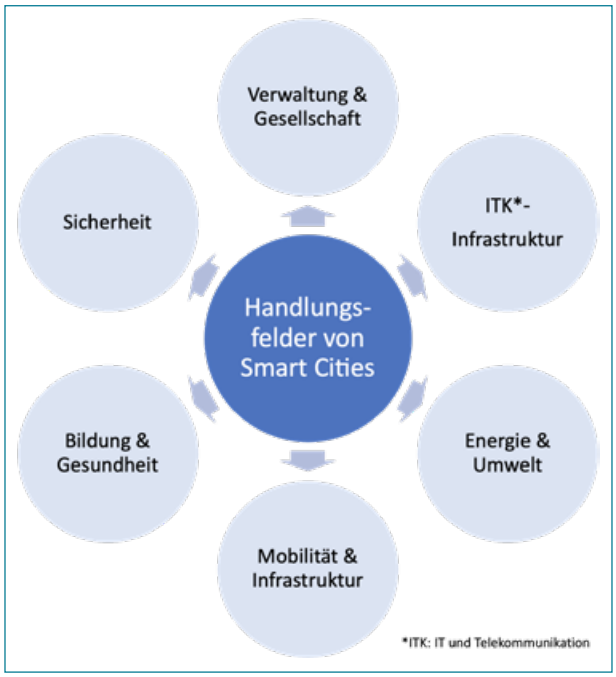

Abb. 2

Bedrohungen für die Infrastruktur

Ein derartig weit gespanntes Netz von Angeboten und Dienstleistungen, das die wirtschaftliche, soziale und ökologische Grundlage für kommunalen Austausch und Handel darstellt und von dem u. U. eine große Anzahl an Menschen profitiert oder abhängig ist, weckt auch das Interesse von Cyberkriminellen. So ist nicht nur die Gesamtmenge an verbreiteter Malware in den letzten Jahren an sich gewachsen[6]. Auch das ausbeuterische Hacken von Systemen und der Diebstahl wertvoller Daten aus unerlaubt zugänglich gemachten Quellen hat sich international zunehmend professionalisiert, sodass die finanziellen Schäden durch Cyberkriminalität immer wieder neue Höchststände erreichen. (Abb. 3)

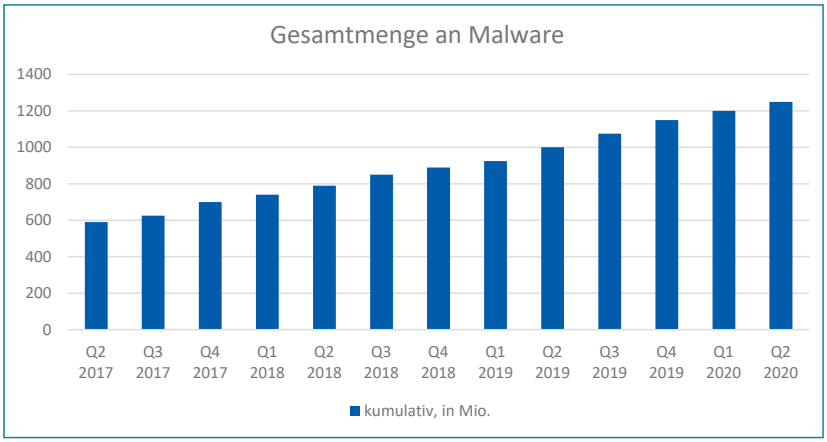

Abb. 3

Unterdessen herrscht unter Cyberkriminellen eine strikte Arbeitsteilung. Diese erschwert das Aufspüren und Verurteilen der Drahtzieher und Beteiligten durch die Exekutive und weitere Sicherheitsbehörden, wie der folgende exemplarische Ablauf zeigt:

1. Ein Hacker, der sich etwas dazu verdienen möchte, sucht systematisch nach Schwachstellen in bekannten Softwareprodukten. Um dafür eine Prämie vom Hersteller (Bug-Bounty-Programm) oder eine Zahlung von Dritten zu erhalten, überlegt er sich dazu auch eine Art Anleitung (Exploit), wie die Sicherheitslücke ausgenutzt werden kann. Je nach eigener Motivation und ausgeprägter krimineller Energie wird zwischen White Hats (suchen, um aufzuzeigen und zu korrigieren), Grey Hats (verstoßen gegen Gesetze, handeln aber aus guter Überzeugung) oder Black Hats (suchen, um auszunutzen) unterschieden.
2. Falls der Hersteller oder ein Admin der Software die (bekannte) Sicherheitslücke (Vulnerability) nicht zeitnah schließt (Patchen) oder nicht schließen kann, weil sie ihm nicht bekannt ist (dies wird Zero Days genannt), kann ein anderer Programmierer nach solchen angebotenen Exploits suchen und sie anonym erwerben. Auf Basis der mitgelieferten Anleitung zum Ausnutzen der Lücke schreibt er eine Software, um sie methodisch zugänglich zu machen (z.B. mit einer Malware, einem Trojaner oder über Phishing).
3. Ein oder mehrere andere Akteure kaufen dem Hacker diese Software ebenfalls völlig anonym ab, z. B. im Darknet im Tausch gegen Bitcoins oder andere Kryptowährungen.
4. Die gekaufte Späh-Software wird nun von den Käufern dazu eingesetzt, Zugang zu dem im Fadenkreuz stehenden System zu erhalten.
   a. Entweder werden dort dann umgehend in großem Stil Daten illegal heruntergeladen, um damit die Eigentümer zu erpressen, oder absichtlich softwaretechnische (Bugs) oder physische Schäden (an der Hardware) angerichtet, um den Eigentümer des Systems gezielt zu schwächen. Denkbar ist auch, den gesamten Datenbestand mit einem Crypto-Trojaner zu verschlüsseln, um mit dieser sogenannten Ransomware dann Geld zu erpressen.
   b. Aus Sicht der Kriminellen ist es jedoch oft langfristig cleverer, sich zunächst in Ruhe auf dem fremden System umzuschauen, das System zu überwachen und dabei möglichst keine Spuren in Logdateien zu hinterlassen. Wenn genügend Informationen zum inneren Aufbau des Systems vorliegen, kann dort mit einer weiteren Schadsoftware (Wurm oder Bot) ein für das Opfer zunächst unsichtbares Programm installiert werden, das automatisiert unauffällig Systemdaten mitschreibt und gegebenfalls auf externe Server kopiert. Auf diesem Weg entstehen mit der Zeit gigantische Schattendatenbanken auf fremden Servern, die von den Angreifern administriert werden (Beispiel für Advanced Persistent Threat).
5. Wurde wie im Fall 4b) eine Schattendatenbank auf einem fremden Server aufgebaut, wächst der erbeutete „Datenschatz" im Laufe der Zeit. Den Zugang zu diesen Informationen kann der Programmierer dann wiederum an ein oder mehrere andere Bieter auf anonyme Weise verkaufen, die wiederum dem ursprünglichen Eigentümer dann finanziellen Schaden oder eine Schädigung seiner Reputation zufügen können.

Beunruhigend ist hier vor allem, wie sich die Bedrohungslandschaft über die Zeit gewandelt hat. Attacken kommen zunehmend aus Kreisen, die

DYNACON

Unternehmen wie die DYNACON GmbH mit Sitz in München und Köln begleiten Versicherungen und andere Unternehmen auf ihrem Weg zur Digitalisierung mit dem nötigen Knowhow und maßgeschneiderten Umsetzungsstrategien.

von Staaten finanziert werden und mit Hilfe derer politische oder industrielle Spionage betrieben wird (Cyber Warfare). (Abb. 4)

Smart Cities als lohnendes Ziel für Hacker

Führt man sich vor Augen, dass die über 600 Smart Cities weltweit inzwischen einen Markt im Volumen von etwa 400 Milliarden USD darstellen[7], Tendenz steigend, wird auch klar, warum dieses Ziel auch für Hacker immer interessanter wird. Besonders die als unzureichend geschützt geltenden IoT-Systeme verzeichnen hohe Zuwächse von Angriffen von außen, oft unabhängig vom Sektor oder der vermuteten Größe des Netzwerks.

Dabei nutzen „Cyberkriminelle [...] zunehmend die Tatsache aus, dass viele Unternehmen [und die öffentliche Hand] der Komplexität ihrer eigenen IT-Landschaft nicht mehr gewachsen sind. Wer den Überblick verliert, kann Attacken nicht umgehend analysieren, abwehren und Folgeschäden beseitigen.“, so Christian Milde, General Manager DACH bei Kaspersky[8].

Verschaffen sich kriminelle Hacker Zugang zu Systemen einer Smart City, bedroht dies unmittelbar die Sicherheit der Bewohner. Die folgenden (teils schon eingetretenen) Szenarien veranschaulichen die Gefahr:

1. Der Datenverkehr in einem Netzwerk wird abgehört. Mit Hilfe einer falschen GSM-Basisstation werden durch Unbefugte Mess- sowie technische Daten zwischen intelligenten Zählern und dem Zentralsystem erfasst. Dadurch lassen sich Abrechnungsdaten von Smart Metern manipulieren, wodurch die Vertraulichkeit des Systems verletzt wird.
2. Ein Distributed-Denial-of-Service (DDoS)-Angriff auf den Hauptserver eines Smart Grids führt zur Überlastung und zum partiellen oder totalen Ausfall des Stromnetzes. Die Verbraucher können die Webseite des Anbieters nicht erreichen. Smart-Grid-Komponenten können nicht kommunizieren, sodass unklar ist, wo und wie die Störung behoben werden kann.
3. Funkfrequenzen für Einsatzfahrzeuge (Polizei, Feuerwehr) werden gestört, sodass das Herbeirufen der Rettungskräfte verzögert oder gar verhindert wird.
4. Durch eine Schwachstelle bei einer externen Software-Schnittstelle in der Verkehrsleitzentrale können die Ampelschaltungen manipuliert werden. Die Störung führt zu Staus, Verzögerungen, Unfällen sowie fehlender Orientierung der Verkehrsteilnehmer durch ausgefallene Leitsysteme.
5. Videokameras werden gehackt, sodass sie nur noch Standbilder statt Livebilder zeigen. Müll oder Unrat, der im Sichtbereich abgelagert wird, wieder freiwerdende Parkplätze oder Kriminalität werden nicht registriert.
6. Die Steuerung autonom fahrender Autos, Straßenbahnen oder anderer Fahrzeuge wird übernommen und es passieren Unfälle, bei denen Menschen zu Schaden kommen.
7. Eine europäische Ransomware-Hackergruppe griff während der Pandemie das US-amerikanische Krankenhausnetzwerk an, was dort zu größeren Systemausfällen führte. Die Attacke löste Warnungen durch das Department of Homeland Security und das FBI aus, die weitere Attacken während der Pandemie erwarteten. [9]
8. Auch das Düsseldorfer Universitätskrankenhaus wurde tatsächlich Opfer einer Ransomware-Attacke durch erzwungene Verschlüsselung der Daten im eigenen Verwaltungssystem. Der Angriff führte dazu, dass geplante und neu anstehende Behandlungen von Patienten nicht mehr ausgeführt werden konnten. Ein Notfallpatient im herannahenden Krankenwagen musste daher in ein Wuppertaler Krankenhaus umgeleitet werden. Durch die um eine Stunde verzögerte Behandlung verstarb der Patient wenig später. [10]

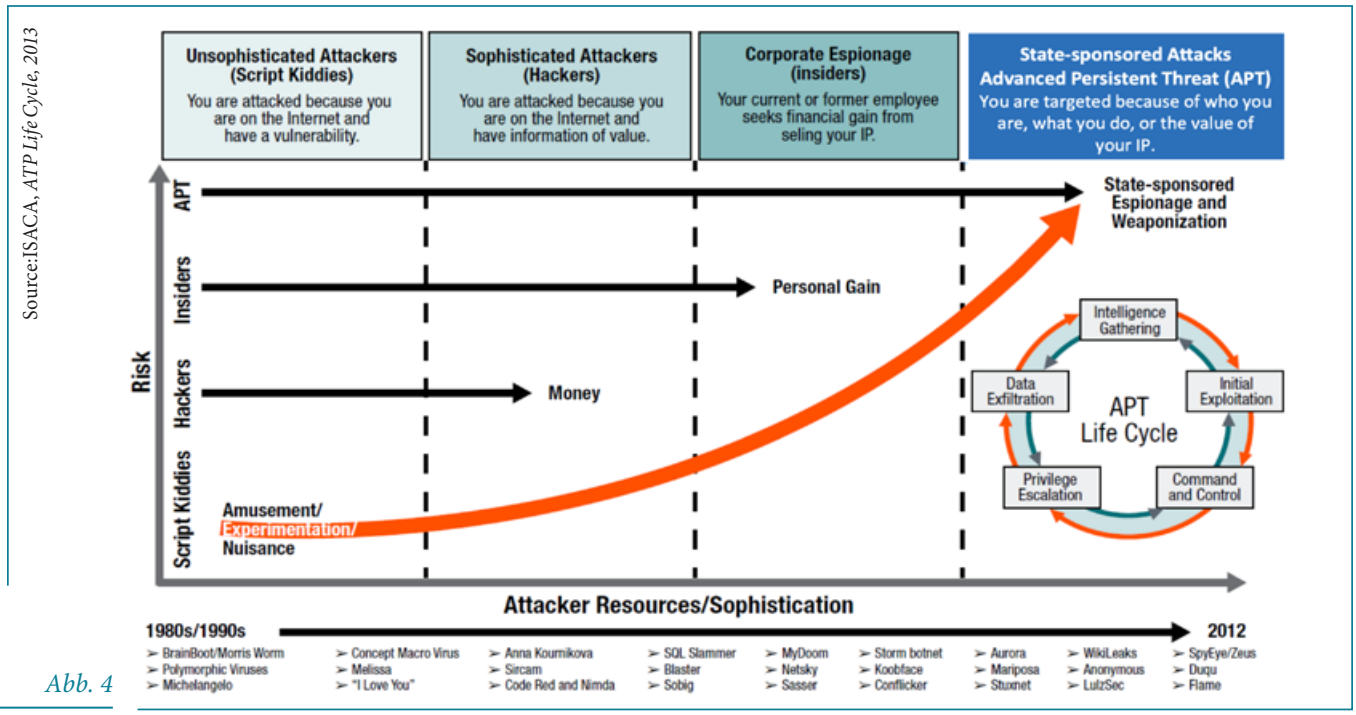

Abb. 4

Mögliche Lösungswege zur Abwehr und Entschärfung

Städte, Behörden und Nutzer der smarten Infrastruktur sind diesem böswilligen Treiben jedoch nicht hilflos ausgeliefert. Die allgemeingültigen IT-Security-Ziele Vertraulichkeit, Integrität, Verfügbarkeit und Zuverlässigkeit kommunaler Dienstleistungen und der Notfallvorsorge sind bereits in der Planung nach dem Prinzip „Security by Design" zu berücksichtigen. So muss bei energetischen und datentechnischen Verknüpfungen garantiert werden, dass Teilsysteme bei Störungen funktionsfähig bleiben. Für die Kernkomponenten der technischen Infrastrukturen (Server, Router, Netzwerksteuerung) sind technische Redundanzen vorzusehen. Für die Kommunikation der Rettungsdienste, die Trinkwasserversorgung, das Gesundheitswesen und weitere unverzichtbare Versorgungsdienste sind auch analoge Redundanzen vorzuhalten.[11)]

Dies alles ist im Rahmen einer ganzheitlichen IT-Security-Strategie einzufordern, umzusetzen und aktuell zu halten. Auf diese Weise ist es möglich, sich systematisch und je nach Wichtigkeit des zu schützenden Assets effektiv und zielgerichtet zu wappnen. Zahlreiche Firmen aus der IT-Strategie- und IT-Sicherheit-Branche füllen mit ihren Angeboten und Dienstleistungen äußerst erfolgreich diese Nische. Typische Inhalte davon sind[12)]:

1. **Identifizieren**, d.h. Risikoanalyse durchführen
   - Assets identifizieren, die geschützt werden sollen
   - Bedrohungslage möglicher Angriffe aktuell im Auge behalten
   - IT-Governance aufbauen, bei der Verantwortlichkeiten klar definiert sind
2. **Schützen**, d.h. Sicherungsmaßnahmen durchführen
   - Netzwerksicherheit gewährleisten (u.a. Firewalls, Netzwerksegmentierung, Zugriffskontrollen, Cloud Security, Systeme zur Verhinderung von Eindringlingen, Security Information und Event Management (SIEM), Web Security, Wireless Security, etc.)
   - Sensibilisierung und Schulung von Mitarbeitern und Nutzern
   - Richtlinien, um Malware zu verhindern
   - Richtlinien für externe Speichermedien
   - Sicherheitsupdates für alle eingesetzten Systeme unmittelbar ausführen
   - Rechteverwaltung
   - Daten-Backups und Sicherungen von Konfigurationen
3. **Erkennen** von Angriffen, d.h. Überwachung von Netzwerkaktivitäten, Systemen sowie von verdächtigem Nutzerverhalten
4. **Reagieren**, d.h. Einrichtung eines Computer Security Incident Response-Teams (CSIRT), also eine Expertengruppe für sicherheitskritische Vorfälle
5. **Wiederherstellen**, d.h. Erstellung eines Desaster Recovery Plans (Notfallwiederherstellungsplan)
6. **Zusammenarbeiten**, d.h. mit Partnern Erfahrungen austauschen

Potenziale für die Versicherungswirtschaft

Genau an dieser Stelle lohnt es sich auch für Versicherer, in diesen Milliardenmarkt einzusteigen. Einerseits steigt die Höhe der erpressten Geldsummen immer weiter, andererseits sind immer mehr Geräte und Dienstleistungen miteinander verknüpft. In dieser Komplexität muss sich eine kommunale Verwaltung nicht allein auf beauftragte Sicherheitsfirmen verlassen. Um ihrer Kernkompetenz, nämlich dem Planen, Steuern und Verwalten städtischer Angelegenheiten, uneingeschränkt nachkommen zu können, soll sich die Stadtverwaltung auf einen erfahrenen und vertrauensvollen Ansprechpartner verlassen können, der eine passende Cyber-Police für die Bedrohungslage der Kommune anbieten kann. Die Bausteine eines solchen Tarifes lassen sich aus den potenziellen Handlungsfeldern von Smart Cities ableiten. Wird die Kommune als Versicherungskunde bei der Erstellung einer ganzheitlichen IT-Security Strategie begleitet, können die im Zuge der Risikoanalyse identifizierten Vermögenswerte statistisch berechenbarer versichert werden.

Ähnlich wie bei einem Schaden am Auto, der über die Kaskoversicherung versichert ist, sollte sich eine kundenorientierte, moderne Versicherung um die vollumfängliche Abwicklung des Falles kümmern, ohne dass der Versicherungskunde zu sehr seine eigentlichen Aufgaben vernachlässigen muss. Die Versicherung spielt also die Rolle des Dirigenten bei der Prävention, Identifikation und im Notfall Abwehr von Angriffen auf die IT-Sicherheitsinfrastruktur einer Smart City. Schließlich sind Sicherheit, Vertrauen und Verlässlichkeit deren Kernkompetenzen.

Nebenbei gelingt es, einen Erfahrungsschatz aufzubauen und so mit der Zeit die eigenen Kunden noch besser betreuen und die Tarifprämien genauer kalkulieren zu können. Dabei hilft der Zugriff auf die in der Smart City erhobenen anonymisierten Daten auch bei der Kalkulation, Prävention und Abwicklung von Schäden aus anderen Versicherungssparten, wie z. B. Kfz-, Hausrat- oder Krankenversicherungen.

Quellennachweise

1. https://techjury.net/blog/internet-of-things-statistics/, https://www.businessinsider.com/internet-of-things-report
2. https://www.rolandberger.com/en/Point-of-View/How-the-Smart-City-can-build-itself.html, https://iot-analytics.com/product/smart-city-use-case-adoption-report-2020/
3. https://www.bitkom.org/Smart-City-Index
4. https://www.bmi.bund.de/DE/themen/bauen-wohnen/stadt-wohnen/stadtentwicklung/smart-cities/smart-cities-node.html
5. https://www.bbsr.bund.de/BBSR/DE/veroeffentlichungen/sonderveroeffentlichungen/2015/smart-cities-dl.pdf
6. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf
7. https://www.techrepublic.com/article/smart-cities-6-essential-technologies/
8. https://www.itsicherheit-online.com/media/archive/93/bb/4e/epaper-IT-SICHERHEIT_4-2020YwIPbmTSzqJtx/epaper/IT-SICHERHEIT_4-2020.pdf
9. https://www.cyberscoop.com/ransomware-hospitals-ryuk-fireeye/
10. https://www.bleepingcomputer.com/news/security/ransomware-attack-at-german-hospital-leads-to-death-of-patient/
11. vgl. S. 12f https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/bauen/wohnen/smart-city-charta-kurzfassung-de-und-en.pdf
12. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps

Sie möchten gerne weiterlesen?

Dann werden Sie jetzt Mitglied der VVB

Ihre Vorteile einer Mitgliedschaft

15 Fachkreise

Kern der fachlichen Weiterbildung innerhalb der VVB bilden die fünfzehn Fachkreise, deren Bedeutung sowohl in der Mitgliedschaft als auch in der Versicherungswirtschaft allgemein ständig wächst.

19 Treffpunkte

In 19 verschiedenen Städten sind unsere Treffpunkte vertreten. Hier finden regelmäßige ungezwungene Treffen der Mitglieder zum freundschaftlichen Erfahrungsaustausch statt.

Mitglieder-Netzwerk

Finden Sie über unsere Mitglieder-Suche Gleichgesinnte und tauschen Sie sich mit Ihnen über aktuelle Themen oder Studiengänge aus.

VVBmagazin

Erhalten Sie über den internen Bereich exklusiven Zugriff auf das gesamte VVBmagazin, auch auf Ausgaben vergangener Jahre!

Das VVBmagazin als Online-Ausgabe!

Lesen Sie jetzt überall bequem auf Ihrem Handy oder Tablet die aktuellen Themen aus dem VVB-magazin und tauschen Sie sich mit Mitgliedern darüber aus.

Jetzt Mitglied werden

www.vvb-alumni.de/vvb-mitglied-werden/