Bericht zum Informationstag „IT-Sicherheit in der Marktforschung“

Am 10. Juni 2016 haben TeleTrust, ADM, DGOF und VMÖ gemeinsam in Wien den Informationstag „IT-Sicherheit in der Marktforschung“ mit freundlicher Unterstützung der Wirtschaftskammer Wien veranstaltet. Im Folgenden finden Sie eine kurze Zusammenfassung der dort gehaltenen Vorträge.

Harald Neustetter (GfK Austria):
Entwicklung der Informationssicherheit in den Marktforschungsinstituten

Das Eingangsreferat hielt Harald Neustetter (GFK Austria). Er beschrieb die Anforderungen an IT Sicherheit in der Vergangenheit, der Gegenwart und in nächster Zukunft. Anhand von plakativen Beispielen zeigte er die aktuellen Sicherheitsrisiken in der IT auf. Aufklärung der eigenen Mitarbeiter im Umgang mit den Gefahren steht für ihn im Vordergrund der notwendigen Maßnahmen seitens der IT Leitung.
Zu Beginn seines Vortrages erinnerte Neustetter an die Zeit der ersten Computerviren. Der erste Computer Virus wurde 1982 von einem 15-jährigen Schüler programmiert. Dieser Virus war noch nicht ausgerichtet, Schäden zu verursachen, sondern sollte nur Aufmerksamkeit erregen.

In den Folgejahren wuchs durch die rasche Verbreitung des Internets das Schadenspotenzial durch Viren, Würmer und Trojaner rasant an. Die Kosten für Prävention stiegen an und Schutz vor Cyberkriminalität wurde zur Aufgabe der IT-Abteilungen.

Der Vortragende zeigte anhand von aktuellen Beispiel des letzten Jahres, welche Schäden Cyberkriminalität in Unternehmen anrichten konnte. Ein neuer Trend sind Ransom-Viren, die den Zugriff auf die eigenen Dateien verhindern. Man kann diese Dateien retten, wenn man ein Lösegeld an den Täter überweist. Wie auch bei „Offline-Erpressungen“ scheiden sich die Geister, ob man den Lösegeldforderungen Folge leisten soll.

Ein weiteres Thema der Cyberkriminalität sind Datenbetrug und Datendiebstahl. Phishing Mails wurden in den letzten Jahren von kriminellen Programmierern laufend verbessert und neue Methoden (z.B. Voicephishing) entwickelt. Im „Dark Web“ findet man zusätzlich unzähligen Passwörter, die durch den sorglosen Umgang von Usern auf seriösen Webseiten preisgegeben wurden.

Dadurch verschaffen sich Cyberkriminelle Zugang zu Unternehmen und deren Daten. Eine deutliche Zunahme von Datendiebstahl und Betriebsspionage ist die Folge. Es entstehen Schwarzmärkte für gestohlen Daten.

Kriminelle Cyberattacken auf Unternehmen können in diversen Ländern gebucht werden, um unbequeme Mitbewerber lahm zu legen.

Eine weitere Möglichkeit andere Unternehmen zu schädigen sind DDoS Attacken. Dabei werden durch künstliche Belastungen die Übertragungsbandbreiten der Unternehmen geschwächt beziehungsweise vollständig blockiert. Ein zumindest phasenweiser Ausfall der Übertragungsmöglichkeiten ist die Folge.

Auch in Zukunft kann mit der weiteren Verbreitung der Cyberkriminalität gerechnet werden. Durch die rasche Verbreitung von Smartphones steigt auch die Anzahl der mobilen Schädlinge. Der mobile Datenverkehr schafft neue Herausforderungen für die IT Sicherheit.

Clouddienste sind in vielen Fällen ein weiterer Unsicherheitsfaktor. Bigdata und Smartdata sind für die Marktforscher zwar ein interessantes neues Geschäftsfeld, jedoch auch hier stellen sich Fragen zur IT

Sicherheit. Die Entstehung eines „Internet-Of-Things“ wird eine Kontrolle des Datenverkehrs zudem vor neue neue Herausforderungen stellen.

Um nun die IT-Sicherheit zu gewährleisten, gibt es keine 100 % wirkungsvollen Patentrezepte. Ein wichtiger Baustein ist die Schaffung von Awareness für das Thema bei den Mitarbeitern: Regelmäßige Information und Schulungen sollen dazu dienen, die Sorglosigkeit der Mitarbeiter im Umgang mit der IT zu beseitigen. Verschlüsselungen bei E-Mails, eingeschränkte Verwendung von USB Sticks, regelmäßiges Ändern von Passwörtern und laufende Backups sind einfache und jedem bewusste Maßnahmen. Jedoch sollten diese auch tatsächlich beachtet werden. Daher muss darauf seitens der IT Verantwortlichen immer wieder hingewiesen werden.

MMag. Robert Sobotka (VMÖ)

Andreas Schütz (Taylor Wessing):
Rechtliche Aspekte der Informationssicherheit in der Markt- und Sozialforschung

Zum Thema „Rechtliche Aspekte der Informationssicherheit in der Markt- und Sozialforschung“ referierte Andreas Schütz (Taylor Wessing). Sein Vortrag war in drei Bereiche gegliedert: Erstens die rechtlichen Vorgaben im Informationssicherheitsbereich, zweitens die Datensicherheit nach dem Österreichischen Bundesgesetz zum Schutz personenbezogener Daten (Datenschutzgesetz 2000) und drittens die Europäische Datenschutz-Grundverordnung (EU-DSGVO).

Die rechtlichen Aspekte der Informationssicherheit reichen von der Geschäftsführerhaftung über das Arbeitsrecht und die Verbandsverantwortlichkeit bis hin zum Datenschutzrecht, das sowohl auf der nationalen Ebene (in Österreich durch das Bundesgesetz zum Schutz personenbezogener Daten) als auch auf der europäischen Ebene (durch die Europäische Datenschutz-Grundverordnung, die ab dem 25. Mai 2018 in den Mitgliedsstaaten der Europäischen Union als nationales Recht unmittelbar Anwendung findet) kodifiziert ist.

Im österreichischen Datenschutzgesetz 2000 sind insbesondere die §§ 14 und 24 für die Datensicherheit relevant. In § 14 DSG sind die verschiedenen Maßnahmen normiert, die zur Gewährleistung der Datensicherheit zu treffen sind. Die Informationspflichten bei Verletzungen der Datensicherheit sind in § 24 DSG geregelt.

Die Ziele der Datensicherheit betreffen den Schutz vor zufälliger oder bewusster Zerstörung, vor Verlust, vor nicht ordnungsgemäßer Verwendung und vor unbefugtem Zugang. Dazu sind auf der Grundlage einer Risikobewertung nach der Art der Daten, dem Umfang und Zweck der Verwendung, den technischen Möglichkeiten und der wirtschaftlichen Vertretbarkeit geeignete Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dazu gehören im einzelnen Unternehmen die Festlegung von Aufgaben und Kompetenzen, die Regelung der Zugriffs- und Zutrittsberechtigungen, die Belehrung, Schulung und Verpflichtung der Mitarbeiter sowie die Dokumentation aller Maßnahmen der Datensicherheit als Beweissicherung.

Die Pflicht zur Information der Betroffenen bei Verletzungen der Datensicherheit ist begrenzt auf systematische und schwerwiegende Verletzungen und wenn den Betroffenen ein Schaden droht. Die Information muss – ohne dass das DSG dazu konkrete Vorgaben macht, unverzüglich und in geeigneter Form erfolgen.

Die Europäische Datenschutz-Grundverordnung ist ab dem 25. Mai 2018 in den Mitgliedsstaaten der Europäischen Union als nationales Recht unmittelbar anzuwenden. An verschiedenen Stellen der EU-DSGVO sind sogenannte Öffnungsklauseln vorgesehen, die den Mitgliedsstaaten einen gewissen Spielraum

bei der Umsetzung der gesetzlichen Bestimmungen der EU-DSGVO einräumen. Diese Spielräume werden allerdings überschätzt. Ziel jeder Verordnung der Europäischen Union ist, im Gegensatz zu den Richtlinien der EU, die europaweit einheitliche Rechtsdurchsetzung.

Ein Eckpfeiler der EU-DSGVO ist die informierte Einwilligung der Betroffenen in die Verarbeitung (einschließlich der Erhebung) ihrer personenbezogenen Daten. Darüber hinaus setzt die EU-DSGVO unter anderem auf eine datenschutzkonforme Technikgestaltung durch „privacy by design“ und „privacy by default“ sowie bei Verstößen gegen datenschutzrechtliche Bestimmungen auf Sanktionen auf der Grundlage eines harten Strafrahmens.

Weiterhin letztlich ungeklärt ist die Frage, ob die Garantien und Ausnahmen des Artikels 89 EU-DSGVO für Zwecke historischer und wissenschaftlicher Forschung und für statistische Zwecke auch auf die Markt-, Meinungs- und Sozialforschung Anwendung finden. Damit verbunden ist eine im Vergleich zur nationalen Datenschutzgesetzgebung höhere Rechtsunsicherheit.

Erich Wiegand (ADM)

Adrian Altrhein (TÜViT):
Management und Zertifizierung der Informationssicherheit in den Marktforschungsinstituten

Adrian Altrhein (TÜViT) referierte zu "Zertifizierung der Informationssicherheit in Marktforschungs-instituten". Er gab einen Überblick über Normen, insbesondere generische ISO-Normen, die für Marktforschungsinstitute relevant sind - vor allem, wenn die Institute ihre Dienstleistungen IT-gestützt erbringen.

Die Betrachtungen führten notwendigerweise zum Thema IT-Sicherheitsmanagementsystem.

Viel ist heute von Informationssicherheit die Rede: vom Schutz der Daten vor unbefugten Zugriffen und dem Schutz vor simplen technischen Defekten. Unternehmen kann das in eine prekäre Lage bringen. Ausreichende Informationssicherheit ist mehr denn je eine wichtige Basis für Wettbewerbsfähigkeit und unabdingbar für langfristigen Erfolg. Wobei es auf das richtige Maß ankommt, denn zu wenig Sicherheit ist fahrlässig, zu viel Sicherheit ist unwirtschaftlich. In jedem Fall berührt IT-Sicherheit das Grundkapital der Marktforschung, das Vertrauen der Kunden.

Mit dem Schutz von Unternehmensdaten und Informationen werden Compliance Manager, Sicherheitsbeauftragte, Datenschutzbeauftragte und Risikomanager betraut. Bei allen Bemühungen dieser Verantwortlichen erreichten aber Informationen über mögliche Gefahren und Risiken und die implementierten Schutzmaßnahmen oft nicht die Unternehmensführung. Die Einführung und nachhaltige Umsetzung von Compliance-Anforderungen zur Informationssicherheit und eines wirksamen Risikomanagements sind in allen größeren Unternehmen komplexe Aufgabenstellungen. Dabei reiche es bei Weitem nicht aus, nur die technische Infrastruktur abzusichern, vielmehr muss ein funktionierendes Managementsystem die gesamte Organisation einbeziehen, auch in Bezug auf menschliches Verhalten und Geschäftsprozesse.

Altrhein wies darauf hin, dass Auftraggeber vermehrt Nachweise über etablierte IT-Sicherheitsmaßnahmen verlangen. Ein naheliegender Nachweis ist dabei die Zertifizierung durch eine objektive und unabhängige Zertifizierungsstelle nach gängigen Normen. Beispiele hierfür sind die Zertifizierungen nach ISO 27001 (Information security management system), aber auch nach ISO 20252 (Market, opinion and social research) oder ISO 26362 (Access Panels).

Dr. Holger Mühlbauer (TeleTrusT)

Dr. Stefan Oglesby (LINK Institut):
Informationssicherheit 4.0 in der Markt- und Sozialforschung

Das Referat von Dr. Stefan Oglesby vom LINK Institut in der Schweiz veranschaulicht die Bedeutung der digitalen Transformation für die Marktforschung und die mit ihr verbundenen Herausforderungen in der Sicherung der erhobenen Daten und Systeme.

Die Verknüpfung von Verhaltensdaten, die durch technische Messungen erhoben wurden, mit Befragungsdaten, werden das zukünftige Rüstzeug der Marktforschung sein, wenn es darum geht, die Fragestellungen der Wirtschaft, der Verbände und Institutionen zu beantworten.

Die digitalen Technologien der sozialen Medien, mobilen Kommunikation und Mobile Business sind längst in unseren privaten wie geschäftlichen Alltag integriert und verändern die wirtschaftlichen Prozesse. Die digitale Revolution drängt in die meisten Branchen und fordert Unternehmen dazu auf, ihre Prozesse kundenzentrierter auszurichten, den Service zu verbessern und auch neue Märkte und Produkte ins Leben zu rufen, um wettbewerbsfähig zu bleiben. Der Service um ein Produkt wird zunehmend wichtiger als das Produkt selbst.

Will die Marktforschung auch zukünftig relevante Antworten auf die Forschungsfragen ihrer Kunden liefern, muss sie ihr Portfolio selber einer digitalen Transformation unterziehen. Wie sie dies tut veranschaulichten die Beispiele des Vortrags zur Mobilitätsmessung mit dem Einsatz von Beacons, die neuen Wege in der Werbemittelforschung durch den Einsatz von Cookietrackings oder die Optimierung von Shoppingkonzepten durch die Aufzeichnung der Shopper Journey und POS Trackings. Und das ist erst der Anfang – das Internet of Things bietet durch die Dokumentation der Kommunikation der Geräte z.B. eines Haushalts sehr viel tiefere und umfassender Einblicke in das Verbraucherverhalten, die Alltagsroutinen und die Bedürfnisse der Menschen als dies vorher je möglich war. Die Analyse dieser Daten entlang präziser Fragestellungen verbunden mit dem Anreichern mit Befragungsdaten, ermöglichen es zu relevanten Insights zu kommen. Dies ist zugleich das Zukunftsmodell der Marktforschung und ihre größte Herausforderung. Die Kommunikation verschiedener Geräte untereinander und das Sammeln großer Datenmengen mit der Verknüpfung von Befragungsdaten vergrößert die Herausforderung, Vorsorge zu leisten, um die personenbezogenen Daten zu schützen und an allen Stellen der Messung, Erhebung, Verarbeitung und Speicherung der Daten die Schutzmaßnahmen einer sich stetig verändernden Technik anzupassen. Zudem müssen die internen Systeme einer kontinuierlichen Überprüfung unterzogen werden, ob sie dem aktuellen technischen Stand noch angemessen sind.

Die digitale Transformation ist damit nicht nur eine Herausforderung das eigene Geschäftsmodell darauf auszurichten, sondern auch die internen Ressourcen bereitzustellen, um die eigenen Sicherheitsmaßnahmen kontinuierlich auf den Prüfstand zu stellen.

Erfolgt dies nicht, kann dies den Verlust des Vertrauens der Verbraucher in die Sicherstellung der Anonymität der von Ihnen gemachten Angaben und die Sicherheit der von ihnen zur Verfügung gestellten Daten zur Folge haben. In der Konsequenz würde sich dies negativ auf die Möglichkeit auswirken, repräsentative Daten erheben zu können. Daher muss der Daten- und Informationssicherheit oberste Priorität im Rahmen der digitalen Transformation zukommen.

Alexandra Wachenfeld-Schell (DGOF)