qSkills Security Summit 2015

Der Mensch als Risiko, der Mensch als Chance

Just am 5. Oktober 2015, dem Tag des 8. qSkills Security Summit, veröffentlichte das Handelsblatt einen Beitrag zu „Digitale Fallen". Darin erläutert der Autor, dass „arglose Mitarbeiter, die fremde USB-Sticks an ihre Rechner anschließen" ein hohes Risiko darstellen, „denn die Geräte können mit Schadsoftware ausgestattet sein". Und der Beitrag resümiert mit Bezug auf eine aktuelle Sicherheitsstudie unter anderem: „Nur jedes vierte befragte Unternehmen bereitet seine Mitarbeiter in Schulungen auf solche Gefahren vor." Eine wichtige Aussage in Zeiten permanenter Hackerangriffe und Spionagevorfälle. Denn Tatsache ist, dass der Mensch der Schlüssel zu einem qualitativen Mehr an Informationssicherheit ist. Für Prof. Dr. Dr. Franz Josef Radermacher, Institut für Datenbanken und Künstliche Intelligenz, Universität Ulm und Mitglied im Club of Rome ist der Mensch gleichzeitig auch die Schwachstelle Nummer eins. Der Mensch hat Gefühle oder „Qualia", Wünsche und Neigungen. Seine Evolutionserfahrungen wie der Wunsch nach Nähe, die Reaktion auf andere oder Mitleid nehmen Einfluss auf das Verhalten des Menschen. Und damit wird er angreifbar. Dementsprechend müssen sich Unternehmen und ihre Mitarbeiter darauf vorbereiten. Radermacher nennt das Beispiel „Race" als das Rennen zwischen Education und Technology. Sprich, die Ausbildung ist ein wesentlicher Faktor für den Erfolg von Unternehmen. Radermacher, Keynote Speaker des qSkills Security Summit, empfiehlt, dass jeder in diesem Rennen vorne dabei ist. „Egal wie schlimm es wird, mehr zu verstehen als die anderen ist in diesem Prozess wichtig, sowohl für das Unternehmen als auch jeden einzelnen", resümiert Radermacher.

Digitalisierung, Cyberrisiken und Social Engineering

Mit den Auswirkungen der Digitalisierung auf die Geschäftsmodelle von Unternehmen beschäftigte sich Prof. Dr. Stefan Stoll, Leiter des Studienganges Wirtschaftsinformatik an der Dualen Hochschule Baden-Württemberg. Entscheidend ist im Kontext der Digitalisierung, dass man sein Denken ändern muss, „denn die Digitalisierung passiert mit oder ohne uns", so Stoll. Man müsse sich vom alten Denken verabschieden. Nicht alte Geschäftsmodelle werden die Zukunft prägen, sondern die von Google & Co. Denn wer Big Data und Algorithmen beherrscht und für sein Geschäftsmodell nu nutzen versteht, wird zukünftig profitieren. Als Beispiel nannte Stoll den Sportartikelhersteller Nike. Das Unternehmen habe als eines der ersten mit einem Chip im Laufschuh gearbeitet, um Daten seiner Kundschaft auszuwerten. Eine der großen Herausforderungen bestehe nach den Worten Stolls darin, sich vom linearen Denken zu verabschieden. Es geht um Daten und Datensätze sowie deren Verknüpfung und Auswertung in Datenbanken. Unternehmen, die mit dieser Digitalisierung gehen, werden zu den Marktgewinnern gehören. Unternehmen, die an alten Geschäftsmodellen festhalten, werden vom Markt verschwinden.

Vom Verschwinden in einem anderen Kontext geht es beim Verlust von Informationen durch Datendiebstahl, Sabotage oder Hacking – verursacht von Menschen. Die Fakten sprechen für sich. Der „Allianz Risk Barometer“ von 2015 kommt zu dem Ergebnis, dass Cyberrisiken mit 29 Prozent das größte Risikopotenzial darstellen, auf die Unternehmen am schlechtesten vorbereitet sind.

Eine aktuelle Befragung des Digitalverbands Bitkom zeigt: 52 Prozent der Taten in den Bereichen digitale Wirtschaftsspionage und Datendiebstahl gingen in den letzten beiden Jahren von aktuellen oder ehemaligen Mitarbeitern aus. Und Thomas Kraus, Experte zum Thema Social Engineering, präsentierte im Rahmen des qSkills Security Summit: „Nach aktuellen Zahlen von BITCOM und Kaspersky ist belegt, dass Daten aus Unternehmen wie folgt abfließen: circa 20 Prozent durch gezielte technische Angriffe und circa 80 Prozent durch direkte menschliche Eingriffe.“ Für Kraus ist Social Engineering „die Kunst, andere Menschen zur Herausgabe von sensiblen und geschützten Daten zu bewegen“. Das perfide an solchen Angriffen ist das Ausnutzen der Gutgläubigkeit und Hilfsbereitschaft von Menschen. Zudem ist Social Engineering die effektivste Methode, um Opfer zu Mittätern zu machen.

Prävention, Detektion, Reaktion

Solche Missstände sind an der Tagesordnung, Gefahren lauern in unserem digitalen Zeitalter in allen erdenklichen Formen und Ausprägungen. Umso wichtiger ist der Blick nach vorne, um die Chancen neuer Technologien für die eigene Organisation zu nutzen. So wie das Unternehmen Carl Zeiss. Dr. Michael Kaschke, CEO Carl Zeiss, formulierte es jüngst so: Für Zeiss ist Digitalisierung keine Option: Es ist ein absolutes Muss. Gleichzeitig bietet die Digitalisierung dem Unternehmen eine große Chance. Bei Zeiss müssen wir alle unsere technische Exzellenz nutzen und in die digitale Welt übertragen.“ Den Verantwortlichen des Unternehmens ist trotz aller „digitalen Euphorie“ bewusst, dass es in diesem Kontext eine klare Informationssicherheit braucht. In diesem Sinne brachte es Andreas Karl, Leiter SMT-B Information Security, Carl Zeiss SMT, im Rahmen seines Vortrags auf den einfachen Nenner: „Prävention, Detektion, Reaktion“. Hierzu gehören beispielsweise definierte Sicherheitszonen und minimierte Schnittstellen, den Traffic zu überwachen sowie ein Incident Response und PDCA. Im Zuge der zunehmenden Digitalisierung und der damit einhergehenden Gefahren müssen bewährte Sicherheitskonzepte regelmäßig geprüft und angepasst werden – inklusive einer Verschlüsselung vertraulicher Informationen.

Vom Rückspiegel zum Blick in die Zukunft

Um zu wissen, was wichtig ist, braucht es eine vorwärtsgewandte Sicht auf kommende Szenarien, potenzielle Risiken und Gefahren. Geschieht dies, sind Organisationen auf einem guten Weg. Geschieht dies nicht, sind sie reine Risikoverwalter. Denn sie schauen in den Rückspiegel und damit verpassen sie meist den Blick nach vorne und in die Zukunft.

Der Flughafen München hat dies als Risiko erkannt und ein zukunftsorientiertes Risikomanagement aufgebaut. Anlässlich des qSkills Security Summit stellte Olivier Rombach, Referent Konzernplanung und Controlling, Flughafen München GmbH, klar, dass es neben der Aufnahme zukünftig möglicher Risiken vor allem einen Kulturwandel innerhalb der Organisation braucht. Unterstützt wird der ganze Prozess durch „Coso ERM“ als Standard – auch um zu einer neuen Rolle des Risikomanagements inklusive eines besseren Workflows zu kommen. Das Ziel ist es von der Modellierung zur aktiven Steuerung des Risikomanagementprozesses zu gelangen.

Compliance oder die kleinen Ursachen mit großer Wirkung

Den Menschen in ein anderes Licht rückte Dr. Josef Scherer, Professor für Unternehmensrecht (Compliance), Risiko- und Krisenmanagement, Sanierungs- und Insolvenzrecht an der Technischen Hochschule Deggendorf, in seinem Vortrag. „Die Medien berichten täglich über unzählige Themen, bei denen scheinbar Egoismen, Gier und Macht … regieren. ... Die Ursache ist einfach zu finden: Dahinter stecken Menschen mit ihren menschlichen Schwächen.“

Und Scherer überträgt dies auf die Unternehmensführung: „Im Bereich der ordnungsgemäßen Unternehmensführung und -überwachung (Corporate Governance) und gewissenhaftem Management … stellen sich sehr ähnliche Fragen.“ Ein Beispiel bietet nach Scherers Worten die Dauerbaustelle des Hauptstadtflughafens BER, wo nach Medienberichten aktuell rund 600 neue Brandschutzwände erforderlich sind. Der Compliance- und Risikomanagementexperte brachte es auf den Punkt „Was in der Praxis alles nicht so klappt“ und zeigt auf, dass es vielfach kleine Ursachen sind, die eine große Wirkung entfalten. In diesem Kontext zeigt sich was passiert, wenn ein Großbäcker die von den Behörden monierten Hygienemängel missachtet: Insolvenz. Scherer stellte in seinem Vortrag die Frage: Verstehen Sie und Ihre Mitarbeiter die einschlägigen Handbücher, Konzernregelungen, Prozessbeschreibungen, etc.? Josef Scherer rät bei allen Überlegungen: „Bei unternehmerischen Entscheidungen von gewisser Tragweite ist stets an die Business Judgement Rule zu denken, das heißt dokumentierte Überlegungen bezüglich der Risiko- und Chancen-Auswirkungen und sachgerechte Abwägung schützen vor Haftung, falls das Ergebnis der Entscheidung Schäden und Verluste bringen sollte.“

„Wir stehen vor großen Umbrüchen und neuen Herausforderungen resümiert Birgit Jacobs, Initiatorin des qSkills Security Summit. Und sie ergänzt: „Durch die Vernetzung und Komplexität der Systeme und Prozesse kommen gravierende Veränderungen in der Arbeitswelt und Organisationsstrukturen auf uns zu Die fachliche Kompetenz und Qualifikation der Mitarbeiter trägt maßgeblich zum Erfolg oder Mißerfolg bei der Durchsetzung der zukünftigen Digitalisierungsmaßnahmen bei.“

In diesem Sinne bot die achte Auflage des qSkills Security Summit für die rund 80 Teilnehmer aus Wirtschaft und Wissenschaft eine optimale Basis, um Erfahrungen, Theorie und Best Practice auszutauschen – für das qualitative Mehr im Informationssicherheits- und Risikomanagement.

Das nächste qSkills Security Summit findet am 27. Oktober 2016 statt.