Nachlese qSkills Security Summit

Vom freiwilligen Geben und dem verbotenen Nehmen

Ganz gleich ob Menschen, Industrieanlagen oder Regierungseinrichtungen – Wirtschaftsspione und Hacker kennen keine Grenzen. Ihre Methoden sind perfide und sie verfolgen in der Mehrzahl klare Ziele, namentlich Wirtschaftsspionage, Sabotage und Erpressung. Dies ist eines der Ergebnisse des diesjährigen qSkills Security Summit. Das Entscheiderforum, das am 6. Oktober in Nürnberg stattfand, verdeutlichte den rund 100 Teilnehmern aus Wirtschaft und Wissenschaft, wie wichtig ein präventiver Schutz für die Informationssicherheit ist und welche Vorreiterrolle ein zukunftsgewandtes Risikomanagement besitzt.

Menschen für sich gewinnen – als Strategie

Nach aktuellen Ergebnissen des „IBM Cyber Security Intelligence Index" wurden 2013 zwölf Prozent mehr Sicherheitsvorfälle als im Vorjahr aufgedeckt. Das entspricht 91 Millionen Vorfällen, wobei 95 Prozent der Angriffe menschliches Fehlverhalten einschließen. Und auf die Karte des menschlichen Verhaltens setzen Agenten vielfach bei ihrer Arbeit. Einblicke gewährte der Ex-Geheimdienstmitarbeiter Leo Martin in seinem Vortrag zu „Geheimwaffen der Kommunikation". Martin: „Menschen für sich gewinnen" heißt im Agentenumfeld die Devise und dabei setzen die Spezialisten auf eine klar strukturierte Vorgehensweise, um an Informationen zu gelangen oder seinen Gegenüber zu manipulieren. Leo Martin präsentierte hierzu die „007-Formel", um Vertrauen aufzubauen. Diese gliedert sich in einzelne und aufeinander aufbauende Schritte: Von der Vorbereitung und Kontaktaufnahme über die Charakterisierungsphase, der Belohnung durch Anerkennung bis zum Nehmen von Widerständen und Ängsten. Nach Leo Martins Worten werden mit dieser Formel Spionierende hart an ihre Grenzen gehen und ahnungslose Menschen manipulieren. Oder anders ausgedrückt: „So werden auch wildfremde Menschen unter schwierigsten Bedingungen zu Verbündeten."

Sabotage und Vandalismus 2.0

„Von der Spitze des Eisberges" sprach Holger Junker, Referatsleiter Cyber-Sicherheit beim BSI, in seinem Vortrag. Der Sicherheitsexperte zielte in seinen Ausführungen auf das Thema von Industrieanlagen ab, die im Fokus gezielter Angriffe lägen. Als Beispiel nannte er den Computerwurm „Stuxnet", der 2010 bekannt wurde und für viel Aufregung in der Öffentlichkeit sorgte. Vor allem Experten zeigten sich zu jener Zeit erstaunt über die Professionalität, mit der Stuxnet programmiert wurde. Das Ziel sind industrielle Steuerungskomponenten, die mithilfe des Sabotagewurms außer Kraft gesetzt oder manipuliert werden. Betroffen war zu jener Zeit das iranische Atomprogramm, Absender die USA und Israel. Junker spricht in diesem Zusammenhang von „Vandalismus 2.0". Denn es gehe in diesen Fällen nicht um Informationsbeschaffung, sondern um Sabotage und Chaos.

Dass solche hochkomplexen und professionell programmierten Würmer und Trojaner keine Einzelfälle sind, sondern eben nur die eingangs erwähnte Spitze des Eisberges bedeuten, zeigt das jüngste Beispiel: der „Super-Trojaner" mit dem Namen „Regin". Die Schadsoftware soll nach Informationen von Spiegel-Online „über Jahre Unternehmen, Behörden und Forschungseinrichtungen vor allem in Russland und Saudi-Arabien ausgespäht" haben. Regin sei von der Programmierung so aufwendig, dass dahinter nur Staaten stehen könnten. Dies ist ein Mosaikstein im Cyberwar und gleichzeitig ist die Bandbreite möglicher Angriffsszenarien viel umfangreicher. Gerade weil dahinter das nackte Kalkül von Staaten und Organisationen im Wettrennen um Macht, Einfluss oder Marktvorteile steht.

Weitere Themen bildeten die Felder Governance, Risk und Compliance, interne Ermittlungen in Organisationen sowie Application Security, IT-Netzwerke und deren Komplexität und risikogerechte Bewertungen von Unternehmen samt Strategien.

Für Birgit Jacobs, Mitglied der Geschäftsleitung beim Trainingsanbieter qSkills, liegt gerade aufgrund der Brisanz der Sicherheitsthemen ein großer Fokus auf der Qualität der Vorträge. „Wir setzen mit dem Security Summit einen hohen Anspruch an unsere Referenten und Inhalte, um ein Maximum an Wissen zu vermitteln“, erklärt Jacobs. Und Sie ergänzt: „Das Summit hat sich in den vergangenen Jahren als das Entscheiderforum für die Themen Informationssicherheit und Risikomanagement etabliert.“ Ein gewichtiger Grund sei dabei der mehrwertstiftende Nutzen der Inhalte für alle Teilnehmer in Theorie und Praxis.

Der kommende qSkills Security Summit findet am 5. Oktober 2015 in Nürnberg statt.