DENICs ISMS-Ansatz überzeugt beim 14. Deutschen IT-Sicherheitskongress

Seit gut drei Jahrzehnten setzt sich der Deutsche IT-Sicherheitskongress auf nationaler Ebene für eine intensive Kooperation von Staat, Wirtschaft und Wissenschaft ein – in der Überzeugung, dass sich informationstechnischen Bedrohungen durch die Bündelung von Wissen und den daraus gewonnenen Erkenntnissen gemeinsam besser begegnen lässt.

Ausgerichtet vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als ziviler oberer Bundesbehörde mit Zuständigkeit für Fragen der IT-Sicherheit, fand die inzwischen 14. Auflage der Veranstaltung vom 19. bis 21. Mai 2015 unter dem Motto „Risiken kennen, Herausforderungen annehmen, Lösungen gestalten“ statt. Die Eröffnungs-Keynote über die künftigen Herausforderungen, die die IT-Sicherheit an Staat, Wirtschaft und Gesellschaft stellt, hielt Bundesinnenminister Thomas de Maizière, zu dessen Geschäftsbereich das BSI gehört.

DENIC unter ausgewählten Rednern: Exzellente Visitenkarte abgegeben

Im Rahmen des Kongresses sprach auch DENICs Chief Information Security Officer Boban Kršić gemeinsam mit Alexander Koderman, Abteilungsleiter Certification and Audits der SerNet GmbH (DENIC-235). Ihr Vortrag am 21. Mai 2015, der vom Programmkomitee als einer von 50 aus über 300 Einreichungen ausgewählt worden war, beschäftigte sich mit dem Informationssicherheits-Managementsystem der deutschen TLD-Registry als Prävention gegen Cyber-Bedrohungen. Im Fokus standen dabei vor allem die speziell für den Betrieb einer zentralen Internet-Infrastruktur notwendigen Schritte beim Aufbau des erforderlichen Risikobehandlungsmodells, das aus den strategischen Geschäftszielen abgeleitet wurde, sowie dessen Steuerung mit Hilfe diverser Key-Performance-Indikatoren (KPI); daneben wurde aber auch das Modell als generische Referenz für andere Organisationen diskutiert.

Im Detail ging Boban Kršić darauf ein, wie das DENIC-Modell erarbeitet wurde, um das ISMS basierend auf regelmäßig durchgeführten Risikoanalysen mit Beteiligung aller Verantwortungsträger im Unternehmen kontinuierlich an die sich verändernde Bedrohungslage anzupassen. Ebenfalls zur Sprache kam, wie äußere Bedrohungen, die beispielsweise über den Deutschen CERT-Verbund und externe Kooperationen (UP KRITIS, DNS-OARC, CENTR …) erfasst werden, dabei ebenso Berücksichtigung finden wie operative Risiken als Ergebnis aus Risk Assessment Workshops und dem internen Incident- und Problem-Management.

Einen Schwerpunkt des Vortrags stellten die zum Einsatz kommenden Methoden und Werkzeuge dar: Denn wie sich bei der 2011 begonnenen Modellierung des DENIC-ISMS schnell herauskristallisierte, können die gängigen vorhandenen Bewertungsmodelle wie etwa SPICE (Software Process Improvement and Capability Determination), mit dessen Hilfe sich der Reifegrad von Geschäftsprozessen anhand des Erfüllungsgrades der jeweiligen relevanten Attribute bewerten lässt, lediglich anteilig zu einem umfassenden, integrierten ISMS beitragen. Erst durch die Einbeziehung von Inhalten einer Vielzahl sich ergänzender Standards, so arbeitete der Vortrag klar heraus, lässt sich das Ziel einer ganzheitlichen Betrachtung umsetzen. Hierzu zählen vor allem:

- ein risikoorientiertes ISMS im Sinne der normativen Vorgaben der ISO/IEC 27001,
- eine an der Balanced Scorecard angelehnte Methodik zur Ausrichtung aller Aktivitäten des ISMS auf gemeinsame Ziele relevanter Interessengruppen,
- eine Ausrichtung des ISMS an den Geschäftszielen und den Anforderungen des Geschäftszweckes (Business Alignment) unter Verwendung von COBIT5,
- ein Asset Management, das gemäß den normativen Anforderungen als Basis für ein Risiko- und Business Continuity Management einer Organisation gilt.

An dieser Stelle kam Co-Referent Alexander Koderman ins Spiel: Weil der gesamte Risikograph mit seiner Vielzahl von Beziehungen sich mit herkömmlichen Office-Tools nämlich nicht mehr abbilden ließ, setzt DENIC seit 2013 auf verinice. Das von SerNet entwickelte Open-Source-Tool eignet sich zur Implementierung von BSI IT-Grundschutz genauso wie für den komplexen Betrieb eines ISMS nach der internationalen Norm ISO/IEC 27001. Alexander Koderman, der bei SerNet verinice als Projektleiter federführend betreut, erläuterte, wie die mit seiner Unterstützung entstandene, an DENICs Erfordernisse angepasste Software-Lösung in der Lage ist, nicht nur das gesamte ISMS zu modellieren, sondern zugleich auch das Risikomanagement mit abzubilden und dadurch die Aufbereitung und Präsentation der Ergebnisse für die Entscheidungsträger im Unternehmen zu ermöglichen.

Dass die DENIC-Präsentation und die darin aufgezeigten Verfahrensweisen beim Publikum – rund 300 Sicherheitsverantwortliche aus der öffentlichen Verwaltung, dem universitären Umfeld und der Wirtschaft – auf großes Interesse stieß, zeigten die zahlreichen Rückfragen aus dem Forum ebenso wie verschiedene Vortragsanfragen im Nachgang für weitere ähnliche Fachveranstaltungen. Eine schöne Bestätigung dessen, was auch schon die Auditoren des TÜV Nord im Oktober 2014 überzeugte, als sie DENICs ISMS nach dem Standard ISO/IEC 27001:2013 zertifizierten: Die hohe Zahl von „Best Practices“ hat Vorzeigecharakter und kann Anderen als Vorbild dienen. Somit konnte DENIC bei diesem wichtigen, in Fachkreisen viel beachteten Kongress eine exzellente Visitenkarte abgeben.

Über den Deutschen IT-Sicherheitskongress

Der alle zwei Jahre in Bonn stattfindende IT-Sicherheitskongress ist eine feste Größe im Veranstaltungskalender der nationalen und internationalen IT-Sicherheitsbranche. Eine Teilnahme ist für alle Interessierten möglich. Ziel des Kongresses, der in der Regel um die 600 Fachbesucher verzeichnen kann, ist es, aktuelle Trends und Technologien im Bereich der IT-Sicherheit aus unterschiedlichen Perspektiven zu beleuchten und zu diskutieren sowie Lösungsansätze vorzustellen und weiterzuentwickeln. Zu den Rednern zählen Vertreter aus Unternehmen und Forschungseinrichtungen ebenso wie aus Behörden und anderen Institutionen.

Neben dem Management von Informationssicherheit sowie den entsprechenden Standards und Prüfverfahren beschäftigte sich der diesjährige Kongress mit den verschiedensten Aspekten rund um die Sicherheit von Plattformen, Netzen und mobiler Kommunikation, Cloud Computing, Identitäten und Datenschutz sowie diversen rechtlichen Fragen im IT-Kontext. Das Gesamtprogramm des Kongresses sowie die Themenpräsentationen jener Referenten, die einer Veröffentlichung ihrer Folien zugestimmt haben, stehen auf den Webseiten des BSI zum Download zur Verfügung.