KURATORIUM SICHERES ÖSTERREICH

Kuratorium Sicheres Österreich

Der Rechts-und Technologie-Dialog des KSÖ zum Cyber-Sicherheitsgesetz

Dr. Alexander Janda
KSÖ Generalsekretär

WKO E-Day 2016

KURATORIUM SICHERES ÖSTERREICH

Das Kuratorium Sicheres Österreich

Vorstellung des KSÖ

- Gemeinnütziger und unabhängiger Verein
- Die nationale Vernetzungs- und Informationsplattform für Themen der Inneren Sicherheit
- Aufgaben des KSÖ
  - Awareness in der Bevölkerung erhöhen
  - Stake-Holder in Staat, Wirtschaft, Wissenschaft und Gesellschaft einbinden
  - Gemeinsame Arbeit und Verantwortung für öffentliche Sicherheit in Österreich fördern

KURATORIUM SICHERES ÖSTERREICH

KSÖ Cybersecurity Forum

KURATORIUM SICHERES ÖSTERREICH

Der Rechts- und Technologiedialog

Rahmenbedingungen

- Regierungsprogramm
  - Erstellung eines „Cyber-Sicherheitsgesetzes“
- Österreichische Strategie für Cyber-Sicherheit
  - Arbeitsgruppe „Ordnungspolitischer Rahmen“
- Rechtsthemen der KSÖ Cyber-Security Initiative
  - Selbstorganisation
  - Datenschutz bei Planspielen
  - Informationsaustausch im Cyber-Security Forum
- NIS Richtlinie der Europäischen Union

KURATORIUM SICHERES ÖSTERREICH

Verlauf des Dialogs

KURATORIUM SICHERES ÖSTERREICH

Leitthemen des Dialogs

8 Leitthemenblöcke

- Grundsatzaspekte
- Schutzziele
- Informationsgewinnung und Datenschutz
- Ereignisbezogener Informationsaustausch – Meldepflicht
- Gefährdungsunabhängiger (Freiwilliger) Informationsaustausch
- Organisation der Cybersicherheit im Ereignisfall
- Beschaffung und Vergabe
- Haftung

KURATORIUM SICHERES ÖSTERREICH

Kernthemen und Ergebnisse

Meldepflicht

- Grobdefinition durch NIS Richtlinie
  - Branchen
  - Meldegrund („significant impact“, „cross-border effect“)
  - Meldestelle
- Feinabstimmungsbedarf auf nationaler Ebene
  - Schwellenwerte für Meldungen
  - Sanktionen bei Nicht-Meldung
  - Anonymität
  - Inhalt der Meldungen
  - Mitspracherecht der Unternehmen bei Verwendung der Meldungen

KURATORIUM SICHERES ÖSTERREICH

Kernthemen und Ergebnisse

Freiwilliger Informationsaustausch

- Rechtssicherheit schaffen
  - **Austausch von personenbezogenen Daten** durch Definition der Art der austauschbaren Daten um dem DSG Genüge zu tun
  - Ermöglichung des Datenaustausches in **SLAs mit Kunden** über einen Verweis auf das Gesetz **rechtlich absichern**
  - **Übertragung von Verschwiegenheitsverpflichtungen** ohne Abschluss eigener Vertraulichkeitsverträge
  - Verpflichtung der Unternehmen zur **Dokumentation** der an andere Unternehmen, CERTs etc. übermittelten Daten
  - Gesetzliche **Definition der Empfänger** (z.B. CERTs) und Vorgabe von Rechten und Pflichten dieser Empfänger (z.B. Datenaufbewahrung, Löschung, etc.)

KURATORIUM SICHERES ÖSTERREICH

Kernthemen und Ergebnisse

Freiwilliger Informationsaustausch

- Mögliche Hindernisse
  - Datenschutz (insbesondere: IP-Adressen als personenbezogene Daten)
  - Datenschutz Grundverordnung
  - Offizialprinzip
  - Andere Rechtsmaterien (Kartellrecht, Urheberrecht, Bankwesengesetz, etc.) und damit andere Zuständigkeiten
  - Ausschluss der Behörden aus freiwilligem Informationskreislauf
- Mögliche Realisierungen
  - Definition von Delikten als Offizial- bzw. Nicht-Offizialdelikt; Ermächtigungsdelikte oder Privatanklagedelikte über das Cyber-Sicherheitsgesetz
  - Rechtliche Definition eines „Melderechtes“ mit Einbindung des Staates

KURATORIUM SICHERES ÖSTERREICH

Weitere Themen

Grundsatzaspekte

- Stärkung der Rolle des CISO durch gesetzlich verpflichtende Besetzung und Bekanntmachung dieser Rolle
- Risikomanagement als Chance, Definition durch PPP-Prozess und Standardisierung durch staatlich akkreditierte Zertifizierer
- NIS Behörde als Garant für branchenübergreifende Abstimmung

Informationsgewinnung und Datenschutz

- Ermöglichung der Datenerfassung zur Erkennung und Abwehr eines Cyberangriffes, der Beseitigung der Schäden und der Herstellung des Normalbetriebes

Ereignisbewältigung

- Erlaubte Gegenmaßnahmen, Haftungsfragen, Konkretisierung und Festschreibung von Notwehr- und Nothilfemaßnahmen im Cyber-Sicherheitsgesetz

KURATORIUM SICHERES ÖSTERREICH

Weitere Themen

Beschaffung, Vergabe und Haftung

- Diskutiert wurden Themen wie z.B.
  - Verpflichtende Nachweise von Authentizität und Integrität von Produkten durch die Hersteller
  - Sicherheitsüberprüfung als Vergabekriterium
  - Verpflichtung der Hersteller zur Lieferung von Patches und Update
- Erwartete Auswirkungen
  - Wettbewerbsnachteile
  - Verteuerung der Produkten
  - Isolierung des Marktes Österreich
- Vergaberechtlich sollte die Beauftragung von nationalen Sicherheitsdienstleistern (z.B. für CERTs) ermöglicht werden

KURATORIUM SICHERES ÖSTERREICH

Weitere Schritte

Finalisierung des Whitepapers

- KSÖ Cybersecurity Forum und Steering Board
- Veröffentlichung

Weitere Begleitung der Gesetzeserstellung

- Expertise des Dialogs und des Cybersecurity Forums
- Berücksichtigung von NIS RL und Datenschutz-Grundverordnung

Vorstellung der Dialogergebnisse und Diskussion

- Z.B. im Anschluss an diese Präsentation

KURATORIUM SICHERES ÖSTERREICH

Kuratorium Sicheres Österreich

Der Rechts-und Technologie-Dialog des KSÖ zum Cyber-Sicherheitsgesetz

Dr. Alexander Janda
KSÖ Generalsekretär
eMail: janda@kuratorium-sicheres-oesterreich.at