ICANN Specific Reviews - Second Registration Directory Service Review (RDS-WHOIS2)
Recommendation SG.1 - Implementation Documentation

RDS-WHOIS2 Final Report
https://www.icann.org/en/system/files/files/resolutions-board-action-rds-whois2-final-recs-25feb20-en.pdf

Board resolution on RDS-WHOIS2 Final Report
https://www.icann.org/resources/board-material/resolutions-2020-02-25-en#1.a

- Recommendation submitted: September 2019
- Recommendation approved: February 2020
- Implementation completed: January 2024

See https://community.icann.org/display/WHO/Implementation for more information on RDS-WHOIS 2 implementation.

RDS-WHOIS2 Recommendation SG.1

The ICANN Board should require that the ICANN org, in consultation with data security and privacy expert(s), ensure that all contracts with contracted parties (to include Privacy/Proxy services when such contracts exist) include uniform and strong requirements for the protection of registrant data and for ICANN to be notified in the event of any data breach. The data security expert(s) should also consider and advise on what level or magnitude of breach warrants such notification. In carrying out this review, the data security and privacy expert(s) should consider to what extent GDPR regulations, which many but not all ICANN contracted parties are subject to, could or should be used as a basis for ICANN requirements. The ICANN Board should initiate action intended to effect such changes. The ICANN Board should consider whether and to what extent notifications of breaches that it receives should be publicly disclosed.

Board Action on SG.1

The Board approves this recommendation, and directs this item to be included in the next round of contractual negotiations with the Contracted Parties, insofar as it relates to ICANN receiving notification of data breaches in circumstances that threaten to undermine the stability, security, and resiliency of the Internet's DNS. The Board cannot require or guarantee any negotiation outcomes.

Final Implementation Report

Recommendation SG.1 calls for agreements with contracted parties to include protection requirements for registrant data. The Board directed ICANN org to include this in the next round of contract negotiations, insofar as it relates to ICANN receiving notification of data breaches in circumstances that threaten to undermine the stability, security, and resiliency of the Internet's DNS.

To inform discussions with contracted parties, ICANN org conducted a gap analysis of the contracts and due diligence in considering how the recommended requirements differ from existing requirements and how any differences can be presented and positioned in negotiations and ultimately added, as appropriate, in a way that is most beneficial to all parties.

Analysis:

To meet the objectives of this recommendation, contracts should require gTLD registry operators and accredited registrars to notify ICANN org of data breaches concerning registration data, registrant account information, or those impacting registry systems. Such breaches could threaten to undermine the stability, security, and resiliency of the Internet's DNS.

The gTLD Registry Agreement (RA) does not have a requirement for security incident notifications to ICANN. While ICANN org could seek legal expert advice concerning the level or magnitude of security incident that would warrant a breach notification to ICANN organization, this may not require new or original research by ICANN to determine. This determination could, for example, be informed by an understanding of laws applicable to ICANN and industry best practices as they relate to ICANN's mission.

The security breach notice requirement in the Registrar Accreditation Agreement (RAA) requires registrars to notify ICANN of any unauthorized access to or disclosure of registrant account information or registration data (see RAA at Section 3.20). The RAA breach notice requirement is not contingent on a breach or magnitude threshold to preserve the stability, security, and resiliency of the Internet's DNS. Specifically, the RAA requires registrars to include in such notice "a detailed description of the type of unauthorized access, how it occurred, the number of registrants affected, and any action taken by Registrar in response."

To implement this recommendation, as informed by this analysis of the existing requirements in the RAA, ICANN org can propose changes to the RA during its next bilateral negotiation with the Registries Stakeholder Group. As set out above, these changes would require the registry operators to notify ICANN in the event of a security incident, and ICANN Contractual Compliance would have the ability under the agreement to take enforcement action against a registry operator that does not comply with the breach notice requirement.

Based on the above, in January 2024, ICANN org added recommendation SG.1 to the queue of potential contract amendments topics for future negotiation and consideration by the registry operators.

The ICANN org team developing an updated RA for use with the next Round of gTLDs has added the RDS-WHOIS2 Recommendation SG.1 for consideration. It will be considered by the IRT and community when a draft becomes available later in 2024.

Rationale

Adding the RDS-WHOIS2 recommendation to the list of proposed contract amendments and for consideration in the Next Round of applications for new gTLDs satisfies the Board direction.

Timeline

Expected implementation date: December 2023

Final implementation date: January 2024

Milestones

- April-September 2023: Completion of gap analysis and assessment
- January 2024: Inclusion into the topics for potential contract amendments