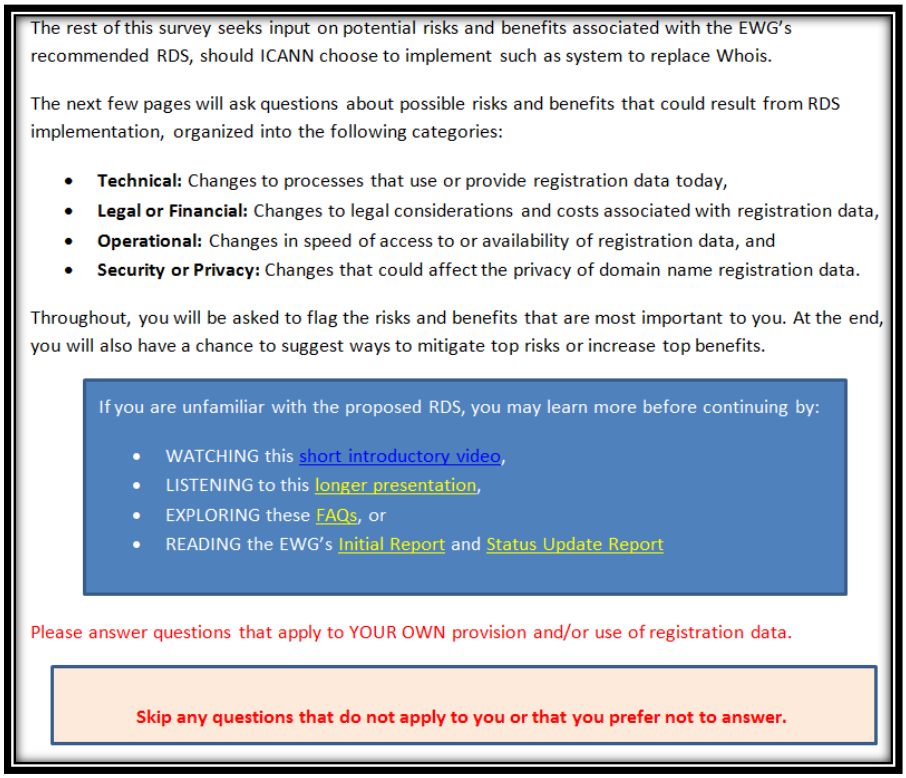
استطلاع مخاطر RDS - ملخص النتائج

في 14 مارس، قامت مجموعة عمل الخبراء في خدمات الدليل gTLD أو (EWG) بدعوة كافة الأطراف التي توفر أو تستخدم بيانات تسجيل أسماء نطاقات gTLD للمشاركة في استطلاع مخاطر RDS، ويشمل ذلك المسجلين وأمناء السجلات والسجلات بالإضافة إلى مجموعة واسعة من الأفراد وشركات الأعمال والمؤسسات الأخرى التي تستهلك بيانات WHOIS اليوم. وقد وفر هذا الاستطلاع للمجيبين عليه الفرصة لإخبار EWG حول المخاطر والمزايا التي قد تحتوي عليها **خدمة دليل التسجيل (RDS) من الجيل التالية** بالنسبة لهم.

هذه الوثيقة تلخص مخاطر ومزايا RDS والتي تم تحديدها من خلال هذا الاستطلاع. استخدمت مجموعة EWG إجابات الدراسة لتحديد وتقليل المخاطر الغير ضرورية والغير متوقعة عند إعداد التقرير النهائي الخاص بها (نشر في 6 يونيو 2014). أوصى EWG كذلك بأن يتم استخدام هذه الإجابات كمدخلات عند إجراء تقدير جميع المخاطر المستقبلية التي قد يتعرض لها RDS المقترح.

تصميم الاستطلاع

المقدمة الموضحة بالأسفل تفتح الطريق من خلال تقديم خلفية لهؤلاء الغير ملمين بخدمة RDS ومن خلال تقسيم المخاطر والمزايا إلى 4 مجموعات:



The rest of this survey seeks input on potential risks and benefits associated with the EWG's recommended RDS, should ICANN choose to implement such as system to replace Whois.

The next few pages will ask questions about possible risks and benefits that could result from RDS implementation, organized into the following categories:

- **Technical:** Changes to processes that use or provide registration data today,
- **Legal or Financial:** Changes to legal considerations and costs associated with registration data,
- **Operational:** Changes in speed of access to or availability of registration data, and
- **Security or Privacy:** Changes that could affect the privacy of domain name registration data.

Throughout, you will be asked to flag the risks and benefits that are most important to you. At the end, you will also have a chance to suggest ways to mitigate top risks or increase top benefits.

If you are unfamiliar with the proposed RDS, you may learn more before continuing by:

- WATCHING this short introductory video,
- LISTENING to this longer presentation,
- EXPLORING these FAQs, or
- READING the EWG's Initial Report and Status Update Report

Please answer questions that apply to YOUR OWN provision and/or use of registration data.

Skip any questions that do not apply to you or that you prefer not to answer.

لكل مجموعة، تم إظهار مثال للمخاطر والمزايا المحتملة للمجيبين وطُلب منهم ما يلي:

- اختر كل المخاطر الفنية التي من المحتمل أن تتأثر أنت بها.
- اختر اثنين (2) من المخاطر التي قد يكون لها التأثير الأكبر عليك.
- اختر اثنين (2) من المخاطر التي غالبا قد تحدث.
- اختر أياً من مخاطر RDS المقدمة حديثاً والتي ليست سابقا من مخاطر Whois المعروفة.

تم تشجيع المجيبين أيضا على إضافة مخاطر ومزايا محتملة أخرى. هذا الملخص لإجابات الاستطلاع يحدد المخاطر والمزايا الأكثر شيوعا إضافة إلى تلك الإضافات المكتوبة.

استطلاع مخاطر RDS - ملخص النتائج

نظرة عامة حول الإجابات

الاستطلاع الأولي لمخاطر RDS تم إجراؤه بالإنجليزية، حيث تم جمع 182 إجابة جزئية في 12 يونيو 2014. فقط أكثر من 100 من المجيبين أتموا الاستطلاع كاملاً.

كل الأجوبة باستثناء جواب واحد تم تقديمها قبل نشر التقرير النهائي لمجموعة EWG. وهكذا، تقدم تلك النتائج تقييماً مرجعياً لخدمة RDS كما هو مقترح في تقرير التحديث لمجموعة EWG بتاريخ (11 نونبر 2013) والذي تم تقديمه في ICANN48 في بوينس آيرس. لا يمكن النظر إلى هذه النتائج كتقييم مرجعي لمقترحات RDS النهائية والمفصلة في تقرير EWG ليونيو 2014. ومع ذلك، فإن هذه الإجابات ساعدت مجموعة EWG على فهم ما يعتقد المستخدمون والمقدمون لبيانات Whois أنه مهم ومؤثر احتمالاً وربما كذلك المخاطر والمزايا المرتبطة بأي جيل تال من RDS.

معلومات ديمغرافية حول المجيبين

- التمثيل العالمي، يشمل أمريكا الشمالية (68%) وأوروبا (35%) وآسيا (20%) وأمريكا اللاتينية (14%) وإفريقيا (12%) وأوقيانوسيا (10%)[1]
- مقسمة بالتساوي بين الذين يستخدمون وبين الذين يقدمون بيانات التسجيل:
  - 84% يستخدمون بيانات تسجيل مطلوبة من Whois
  - 63% يقدمون البيانات، و 24% يجمعون ويخزنون أو يُرحلون بيانات Whois
  - هؤلاء الذين يستخدمون البيانات يشملون المسجلين (45-57%)، والأفراد من مستخدمي الإنترنت (50%)، ومستخدمي الإنترنت للأعمال (50%)، والطاقم التقني للإنترنت (40%)، وباحثي الإنترنت (41%)، ومستثمري OpSec بنسبة (36%)، وأصحاب الملكية الفكرية (27%)، والمستثمرين الآخرين (14%)، ووكالات إنفاذ القانون (5%) وحوالي 20 آخرين.
  - الذين يقدمون البيانات يشملون الأشخاص الطبيعيين (65%)، والأشخاص الاعتباريين (59%)، وأمناء السجلات (14%)، والسجلات (9%)، ومقدمي خدمة Proxy بنسبة (5%)، والجهات الخارجية (5%).

المخاطر التقنية لخدمة RDS

- **التأثيرات التقنية السلبية** الممكنة المذكورة غالباً (104 إجابة):
  1. ربما لم يعد لدي وصول عام بهوية مجهولة لجميع بيانات التسجيل (69).
  2. إن الاعتماد للوصول إلى البيانات المبوبة قد يكون أمراً مرهقاً (65).
  3. ممارساتي للوصول لبيانات التسجيل قد تكون في حاجة للتغيير (62).
- المخاطر المحددة على أنها الأكثر تأثيرا/الأكثر احتمالاً: 1و 2 الموضحان في الأعلى
- في ما يلي المخاطر المدرجة بشكل صريح، ومخاطر تقنية إضافية محددة:
  - خدمة RDS الجديدة يمكن أن تؤثر على الأطراف التي توفر Whois التاريخية والعكسية (8)
  - الوصول الآلي قد لا يكون متاحة بعد الآن (6)
  - عدم القدرة على الحصول على معلومات عن المجرمين، أو عن الشركاء التجاريين، أو عن مقدمي الطلبات (3.
  - الوقت المستغرق للحصول على البيانات أو التسجيل يمكن أن يزيد (2)
  - حقوق الخصوصية يمكن أن تُنتهك (2)
  - مصدر وحيد للفشل/ مخاطر SAC061 التقنية (2)
  - كمية ضخمة من المعلومات لإنفاذ القانون والمتطفلين - مجموعتان من المحتمل أن تسيئا الاستخدام
  - البيانات القابلة للبحث للجمهور سوف تختفي
  - [تسجيلات الدخول] التي يمكن أن أستخدمها قد تحتاج أن تتغير مبدئيا وبشكل مستمر بسبب الدوران
  - التحويل/الانتقا.
  - قضية متعلقة بالشؤون القضائية تم تقديمها
  - ما من تدقيق عام لبيانات التسجيل عند أمناء السجلات المعروفين بالتسامح في ما يخص البيانات المزيفة
  - تغييرات بيانات التسجيل قد تتطلب شهادات SSL

[1] ملاحظة: إجابات متعددة مسموحة؛ تعدى الإجمالي 100%

- يخالف نموذج DNS المفوض
- أفقد ظهور التسجيل بخصوص من يصل إلى بياناتي الشخصية في بعض الظروف
- أفقد القدرة على التحكم بشكل مباشر أو على تقييد الوصول لمعلوماتي
- تكاليف التطوير، وضمان الجودة، والمراجعة والتحديث، دون دخل لتعويضها

ملاحظة عامة: قام المجيبون بتحديد كل هذه الأمور كمخاطر تقنية، ولكن الكثير منها حقيقة يتم تغطيتها كأنواع أخرى من المخاطر التي تم احتسابها في مكان آخر في هذا الاستطلاع.

المزايا التقنية لخدمة RDS

- **التأثيرات الفنية الايجابية** الممكنة المذكورة غالباً (89 إجابة):
  1. بيانات التسجيل التي أصل إليها قد تكون أكثر دقة (58).
  2. الوصول إلى بيانات التسجيل قد يكون أكثر وحدة واتساقاً (56).
  3. قد أحصل على وصول إلى البيانات المبوبة التي حقا أحتاجها (41).
- المزايا المحددة على أنها الأكثر تأثيرا/الأكثر احتمالاً: 1و 2 الموضحان في الأعلى
- في ما يلي المزايا المدرجة بشكل صريح، ومزايا تقنية إضافية محددة:
  - تحسين دقة البيانات (من خلال إدارة وفاعلية الاتصال) (8)
  - قد يتم الوصول لبياناتي من طرف أولئك الذين لهم الحق القانوني لذلك، عوض أن يتم نشرها للعموم لرؤيتها
  - يمكن أن أحدد بسهولة أكثر مكرري الجرائم ومرتكبي السطو الإلكتروني بشكل متسلسل قبل أن أرفع دعوى قضائية أو أقدم شكوى UDRP، مما يوفر لعملائي المال والموارد
  - سأكون دائما بحاجة لتوفير مخرج Whois 43 وهذه ليست مسألة صعبة
  - بيانات التسجيل الموصول إليها ستكون ربما الأفضل من حيث قابلية التطبيق، والمنفعة، والجدية
  - تنقل النطاق بين المسجلين سيكون أسهل (بيانات Whois ستظل نفسها، لن تكون هناك حاجة بعد الآن لتحليل مخرجات Whois)
  - تأثير سلبي ناتج عن تخفيض استخراج البيانات واسع النطاق - مثال: بريد مزعج أقل

مخاطر قانونية ومالية لخدمة RDS

- **التأثيرات القانونية والمالية السلبية** الممكنة المذكورة غالباً (102 إجابة):
  1. كمية بيانات التسجيل المتاحة مجاناً للجميع قد تنخفض (68).
  2. تكلفتي الكلية للحصول على بيانات التسجيل قد ترتفع (66).
  3. تسجيل الدخول إلى RDS أو الإشعارات قد تتطلب تسوية بين تحقيقات نشطة (51).
- الخطر المحدد على أنه الأكثر تأثيرا/الأكثر احتمالاً: 1 الموضح في الأعلى
- في ما يلي المخاطر المدرجة بشكل صريح، ومخاطر قانونية ومالية إضافية محددة:
  - قد يجعل هذا تتبع المتطفلين والمعتدين على العلامات التجارية أكثر صعوبة (3).
  - الوقت المستغرق للوصول إلى البيانات قد يتأخر (3)
  - بدون وصول الجمهور إلى كافة البيانات، قد أقوم بابتكارات ذات قيمة مضافة أقل.
  - الكثير جداً من TLDs الجديدة تؤدي إلى زيادة التكاليف والكثير من التسجيلات بسوء نية.
  - نقص الشفافية لدى مالكي مواقع الإنترنت (تحديدا المواقع التجارية ذات المعاملات النقدية أو مدخلات البيانات الشخصية) قد يكون خطراً على المستهلكين.
  - قد يكون من الصعب تأكيد المعلومات بخصوص المجالات الأخرى التي يملكها المسجل عند تأكيد الأهلية في المجالات المقيدة.
  - الفشل لن يكون ممركزاً. هدف واحد "للهجمات" القانونية، ومن خلال DOS، وعلى التحكم، وغير ذلك من الهجمات.
  - قد يتطلب الأمر مني أن أوفر معلومات غير موجودة (على سبيل المثال عناوين بريدية حقيقية، أجل هناك أشخاص بدون مسكن ثابت ولديهم أسماء نطاقات مسجلة)

استطلاع مخاطر RDS - ملخص النتائج

- إن إنشاء احتكار لبيانات Whois سيؤدي إلى كبت الإبداع وسيمركز في مكان واحد الكثير من القوة على "دليل الهاتف" على الإنترنت.
- في بعض المواقف، ما أبحث عنه ليس جزءاً من البيانات التي أود مشاركتها حتى ولو تعلق الأمر بأشخاص يمكن الوثوق بهم.
- أود بأن تكون بيانات Whois الخاصة بي متاحة لكل الأطراف المهتمة كما هم الآن
- السجلات في الاتحاد الأوروبي EU وفي أماكن أخرى لها قوانين حماية البيانات لن تتمكن من تصدير البيانات إلى RDS مما سينقص فائدتها بشكل كبير.
- عبء التكاليف والجانب السلبي القانوني المحتمل جعلا المسجلين وأمناء السجلات والسجلات ذوي فائدة دنيا للأطراف المتأثرة، وفائدة قصوى للآخرين.

المزايا المالية والقانونية لخدمة RDS

- **التأثيرات القانونية والمالية الإيجابية** الممكنة المذكورة غالباً (68 إجابة):
  1. إن تحسين جودة بيانات التسجيل قد يعمل على نقص عدم الكفاءات المكلفة (42).
  2. إن الإنفاذ التعاقدي للالتزامات المتعلقة بالبيانات قد يكون أكثر قوة (35).
  3. قد يكون من الأسهل بالنسبة لي الحصول على وصول قانوني لبيانات التسجيل المبوبة (35).
- المزايا المحددة على أنها الأكثر تأثيرا/الأكثر احتمالاً: 1و 2 الموضحان في الأعلى
- في ما يلي المزايا المدرجة بشكل صريح، ومزايا قانونية ومالية إضافية محددة:
  - إن خطر حصولي على كميات كبيرة من البيانات الشخصية (بما في ذلك بيانات تجارية تشمل الأفراد) سوف يقل بشكل كبير.
  - سهولة القيام بعمل اتصالات بين ملاك النطاقات وسهولة اكتشاف الشبكات
  - يمكنني أن أرسل تأنيبا إلى مزود ICANN/RDS بسبب انعدام الشفافية، وأن أصيح أقل مساءلة.

المخاطر التشغيلية لخدمة RDS

- **التأثيرات التشغيلية السلبية** الممكنة المذكورة غالباً (87 إجابة):
  1. بسبب فشل RDS، فقد يتعرض وصولي لبيانات التسجيل للعرقلة (68).
  2. بسبب الاعتماد البطيء، فقد يتعرض وصولي للبيانات المبوبة للتأخير (66).
  3. بسبب عوائق خدمة RDS، فقد يتعرض وصولي لبيانات التسجيل للتأخير (65).
  4. بيانات التسجيل العائدة من خدمة RDS قد لا تكون متزامنة مع التحديثات الأخيرة (56).
- المخاطر المحددة على أنها الأكثر تأثيرا/الأكثر احتمالاً: 2 و 3 الموضحان في الأعلى
- في ما يلي المخاطر المدرجة بشكل صريح، ومخاطر تشغيلية إضافية محددة:
  - ترحيل وكشف الإجابة من خدمات الخصوصية Privacy والوكيل Proxy المعتمدة قد تتطلب وقتاً أطول (7)
  - سوف يتعرض عملنا للخطر بناءًا على قرارات السياسة لخدمة RDS.
  - الوصول المبوب للعامة لا يسمح بشفافية المستهلكين للذين يدفعون لهم مقابل الخدمات أو عند إدخال معلومات شخصية
  - خرق البيانات
  - قد يكون هناك عسر/تأخير متزايد في التعامل مع الرسائل غير المرغوب فيها/ الهجمات/القضايا الخاصة بالشبكة والقادمة من مصادر خارجية.
  - البيانات المبوبة لمستوى الاعتماد قد لا تلبي المتطلبات الفعلية.
  - القوانين التعسفية سوف تمنع احتياجات الوصول الصالحة.
  - أريد أن تملك كل الأطراف الوصول إلى بياناتي باستخدام التقنيات الموجودة حالياً.
  - المواقع المحتالة التي تشتغل عبر برامج شبكات المنتسبين ستكون محصنة بسهولة من إنفاذ القانون، ومن مقدمي الخدمات، ومن المستهلكين الذين تم خداعهم.
  - يجب تنفيذ والحفاظ على عملية ونظام جديدين عندما يكون الوضع الراهن غير مخالف.
  - ضياع وقت إضافي ودخل وفرص لزيادة الاتصال الأولي عن طريق مجلس IP عديم الخبرة والذي سوف يسيء الاستخدام أو سيستفيد من النظام الجديد بشكل غير لائق.

استطلاع مخاطر RDS - ملخص النتائج

المزايا التشغيلية لخدمة RDS

- **التأثيرات التشغيلية الإيجابية** الممكنة المذكورة غالباً (61 إجابة):
  1. ترحيل وكشف الإجابات من الوكلاء Proxies المعتمدين قد تتطلب وقتاً أقصر (40).
  2. قد يكون لدي وصول جد سريع لبيانات التسجيل بشكل أكثر كفاءة (40).
  3. الوصول الموثق خلال الوقت الحقيقي للبيانات المبوبة قد يكون أسرع من الوقت الحالي (39).
  4. وقت استجابة RDS قد يكون أفضل من Whois من حيث الوحدة وقابلية التوقع (35).
- المزايا المحددة على أنها الأكثر تأثيرا/الأكثر احتمالاً: 2 و 4 الموضحان في الأعلى.
- في ما يلي المزايا المدرجة بشكل صريح، ومزايا تشغيلية إضافية محددة:
  - خدمة RDS المجمعة قد تدعم بشكل أفضل الميزات مثل WhoWas وWhois العكسي (7)

مخاطر الأمان والخصوصية لخدمة RDS

- **تأثيرات الأمان والخصوصية السلبية** الممكنة المذكورة غالباً (70 إجابة):
  1. بيانات التسجيل الخاصة بي قد تكون غير محصنة أكثر ضد الهجوم الخارجي (40).
  2. قد يقوم مشغل RDS بإساءة استعمال بياناتي (40).
  3. قد أضطر من أجل تسجيل نطاق gTLD أن أوفر هوية يمكن التحقق منها (24).
- المخاطر المحددة على أنها الأكثر تأثيرا/الأكثر احتمالاً: 1 و 2 الموضحان في الأعلى
- في ما يلي المخاطر المدرجة بشكل صريح، ومخاطر الأمان والخصوصية الإضافية المحددة:
  - "الأفراد من مستخدمي الإنترنت" غالباً ما يكونون أصحاب حقوق ويجب أن يمتلكوا القدرة للوصول إلى التسجيلات ذات الصلة للتحقيق في الانتهاكات التي تتم عبر الإنترنت (5)
  - الانشغال بأن الأفراد المستخدمين الذين يجب أن يمتلكوا الوصول قد يتم إقصائهم
  - توفير رقم هاتفي أو بريد إلكتروني صالحين أمران أساسيان لأصحاب الحقوق من أجل التحقيق في الانتهاكات.
  - استفسارات بيانات التسجيل لدي قد تتعرض لسوء الاستعمال من قبل مشغل RDS
  - قد يجب علي التوصل إلى تسوية بين الحقوق التي أملكها بصفتي شخصاً اعتبارياً وشخصاً طبيعياً وذلك باختيار أحدهما أو الآخر -- عندما يدعم تسجيل واستعمال اسم النطاق الخاص بي الاثنين. بناء عليه، سيُطلب مني التنازل عن حقوقي تحت فئة واحدة من الحقوق، على الرغم من أنني قانوناً أملك الحق في الاستفادة من كليهما.
  - خطر الخصوصية الشخصية المتمثل في كون بياناتي ستكون متاحة أكثر كمدير لاسم النطاق
  - خسارة التسجيلات بسبب المتطلبات الإضافية؛ الأعمال التجارية الناشئة قد لا يكون لديها معرفات الأعمال وهكذا... لكن لا تزال تحتاج إلى نطاق.
  - المهاجمون الخارجيون سيجدون الآن فرصة كبيرة للاستهداف.
  - هويتي الشخصية قد ترتبط قسراً بنطاق يمتلكه ويتحكم به كيان مؤسسي، وليس أنا شخصياً.
  - سيستغل الأفراد والمؤسسات الخبثاء القدرة على إخفاء معلوماتهم داخل البيانات المبوبة، مما يجعل من الصعب جداً على موظفي الأمن والامتثال أن يقوموا بالتحقيق عنهم بنجاح.
  - لا يمكنني تسجيل نطاق بهوية مجهول
  - كشف أسبابي للوصول إلى البيانات. إنها شرعية، لكنها أمور تخصني ولا تخص ICANN.
  - قد تكون بيانات التسجيل أقل قابلية للوصول من طرف السلطات الأمنية والماركات التجارية والجهات الأخرى الفاعلة في الإنفاذ من القطاع الخاص.
  - ستصبح بيانات التسجيل الخاصة بي أكثر عرضة للأطراف الأخرى، بما في ذلك أولئك الذين يتعاملون مع وطائف الأمان الخاصة للشركات الخاصة والذين سيريدون وصولاً أكثر لبيانات خاصة وحساسة من خلال gTLDs المتعددة.
  - احتمال ذكر اسمي في دعوى قضائية كنتيجة لإتاحة اسمي مع الشركة
  - إن عرض وصول الأطراف الأخرى لإنفاذ القانون هو نوع من منحهم وصولاً إضافياً، وهو وسيلة للالتفاف على أوامر ومذكرات استدعاء المحاكم. هذا ليس نوع الفرص أو العمليات التي يجب على ICANN أن تتدخل بشأنها.
  - قرارات سياسة ببيانات التسجيل المستقبلية قد تُتخذ من طرف كيان واحد.

استطلاع مخاطر RDS - ملخص النتائج

- وصول الأطراف الأخرى قد ينتهك القانون المحلي، أو الاحتفاظ بالبيانات، أو أمان البيانات، كما يوفر تعرضاً قانونياً للعميل بدون علمي بالأمر.
- وصول الأطراف الأخرى أو تسوية البيانات المخزنة قد ينشئ أداة بالجملة للاستخدام السيء لبياناتي أو لبيانات عملائي.
- وجود نظام جديد قد يعني وجود توجيه هجوم جديد أيضاً.

مزايا الأمان والخصوصية لخدمة RDS

- **تأثيرات الأمان والخصوصية الإيجابية** الممكنة المذكورة غالباً (55 إجابة):
  1. قد تكون بيانات التسجيل الخاصة بي محمية أكثر ضد إساءة الاستخدام (37).
  2. قد تكون بيانات التسجيل الخاصة بي أكثر تأميناً بشكل موحد (31).
  3. قد أقوم بنشر معرفات اتصال قابلة لإعادة استخدامها بدلا من اسمي (29).
  4. نسبة أقل من بيانات التسجيل الخاصة بي قد تكون متاحة بشكل عام أو بهوية مجهولة (27).
- المزايا المحددة على أنها الأكثر تأثيرا/الأكثر احتمالاً: 2 و 3 الموضحان في الأعلى.
- في ما يلي المزايا المدرجة بشكل صريح، ومزايا الأمان والخصوصية الإضافية المحددة:
  - قوانين كل من المصادقة والتوثيق والترخيص سيتم تطبيقها باستمرار ويمكن تدقيقها بسهولة (7)
  - سأميل بشكل أكبر لتحديث معلومات الاتصال الخاصة بي لتكون دقيقة حيث أن المطارد لن يتمكن من الوصول لها
  - سيتطلب الأمر شهادة قانونية بدلاً من شهادة طبيعية
  - ولوج مفتوح للكيان القانوني بطريقة أفضل

مزيد من التعليقات

عرض المجيبون 30 تعليقاً عن **المخاطر التي لا يمكن تجنبها**، تفاصيل بشأن المخاطر المذكورة سابقاً:

1. سيقل الوصول إلى بيانات التسجيل المتاحة حالياً بحُرية.
2. المخاطر 5a، و 5b، و 9b (تغير في الممارسات، تقليل الوصول العام المتاح بحرية) متأصلة في RDS.
3. أي كيان يتحكم في نقطة وصول مركزية فريدة لاسترجاع بيانات التسجيل سيحوز دائماً على الكثير من السلطة على مصلحة عامة.
4. قضية الوصول الغير محدود للبيانات حتى عن طريق أولئك الذين يملكون أوراق اعتماد هي قضية يحتاج المجتمع لفهمها بشكل أفضل. كون أنه من غير المحتمل أن تقوم RDS بفحص الأبحاث الواسعة من طرف الجهات الحكومية والأطراف الأخرى يُعد خطراً كبيراً.
5. إذا فشلت البنية، فلن نمتلك وصولاً جاهزاً للمعلومات. أو سيستغرق الوصول للاعتماد وقتاً طويلاً.
6. القدرة على الحصول على المعلومات بأسلوب فعال ووقت مناسب (لدعم العملاء لمتابعة تحقيقات المواقع المحتالة)
7. القدرة على حماية المستهلكين من عمليات الشراء و/أو إدخال بيانات شخصية من خلال المواقع المحتالة (بسبب نقص شفافية ملكية الموقع)
8. تخزين وإمداد ممركز لخدمة Whois لجميع التسجيلات من أي نوع من قواعد البيانات (بدلاً من أمناء السجلات والسجلات) يزيد من التعرض لاختراقات البيانات.
9. نظام كهذا سيكون بمثابة جذب لهؤلاء الذين يودون اختراق قواعد البيانات مما قد يتسبب في تكرار تأخير أو انقطاع الخدمة.
10. أعتقد أنه يمكن جعل الأشخاص يقومون بتوفير معلومات صحيحة وقت التسجيل، لكن كيف سيتم الحفاظ عليها؟
11. الامتثال لقوانين ICANN ليس هو السبب الوحيد لتوفير الوصول لخدمة Whois. عملياً، فإن التسجيل سيتعين عايه دائماً توفير كل من المخارج 43 و 80 الخاصة بوصول Whois، مما سيتسبب في زيادة التكلفة والخطر.
12. تحطم RDS ركيزة أساسية للإنترنت - تفويض السلطة والتحكم. تقوم بذلك عن طريق إدخال مجموعة كاملة من القضايا المرتبطة بالشؤون القضائية بأسلوب قاصر تقنياً.
13. يتجاهل هذه المشكلات: 1) كيف أجد خادم Whois لمنطقة ما؟؛ 2) نطاقات "خاصة" مفتوحة لتسجيل "الجمهور"؛ 3) القاعدة المثبتة، والأدوات والممارسات الموجودة.
14. الآلية الجديدة تملي بأن بيانات كثيرة تكون مخفية. هذا سيؤدي إلى خطر متزايد للجمهور حيث أن نطاقات [المشاكل] لن تُفعل ولن تتصاعد. سيتم كذلك فقد الأدلة الصالحة لإنفاذ القانون.
15. النظام الحالي يتطلب توفير قدر كبير من البيانات. هذه البيانات عرضة لمخاطر القرصنة عند التسليم أو التخزين بواسطة ذوي التوجه الأخلاقي المريب وأيضاً ذوي النوايا الغير مشروعة.
16. البشر يتدخلون - الفشل مبني في النظام.
17. تمركز السيطرة على من يصل إلى بيانات تسجيل اسم النطاق، وطلب لنوع ما من الصلاحية للشخص أو للكيان الذي يصل إلى بيانات تسجيل اسم النطاق، هاتان المسألتان تخلقان خطراً لا يمكن تجنبه للاحتكار ولتقليل قدرة منفذي القانون والمحققين الأمنيين من تحديد السلوك المسيء على الإنترنت. هذه المخاطر تبدو مستحيلة التجنب [في أي نموذج].
18. التباطؤ الشامل لعملية تسجيل النطاق سيكون غير قابل للتجنب إذا كانت بيانات التسجيل حالياً في حاجة إلى التصديق.

19. تقترح RDS أن يتم توسيع الوصول المبوب لوكالات إنفاذ القانون لكل/معظم الدول. لذلك فإن هدفها الرئيسي هو عرض المسجلين الفرديين للتحقيق من قبل الوكالات الأجنبية، والتي ليس لديهم أي واجب لطاعتها ولا سبب شرعي ليمتثلوا لها. وعليه فإن RDS تعتبر معيبة بطبيعتها
20. أية آلية للتسجيلات مجهولة الهوية سوف يساء استخدامها. على الأقل فإن دفع الأشخاص المؤذين للتسجيل تحت DBA أو صندوق بريد يوفر حاجزاً صغيراً أمام ولوج تسجيل النطاق لأغراض إجرامية.
21. الوصول المفتوح وإعاقة كثرة التكرار لبيانات التسجيل كلاهما يعارضان فوائد استغلال تسجيل النطاق، لذلك لا يمكن تجنب كون أي RDS جديدة مؤسسة من طرف ICANN "ستعالج" هذه "المشاكل" مع Whois الحالي.
22. من الواضح أن مؤلفي التقرير يركزون غالباً على حماية خصوصية عدد قليل نسبياً من مسجلي النطاقات من ذوي احتياجات الخصوصية الخاصة. على الرغم من ذلك، فإن الحالات المشروعة من هذه النوعية قليلة جداً ... التغييرات المقترحة ستعيق بشكل كبير عمل "الذين يحسنون الاستخدام"، وستؤدي إلى نظام بيئي للنطاقات سيكون أكثر عرضة لإساءة الاستخدام، وأكثر احتمالاً لأن يمتلئ ببيانات غير دقيقة وغير مفيدة.
23. الحصول على بيانات كبيرة هو بوضوح خطر أكبر لا يمكن تجنبه بالكامل.
24. أي تمركز للبيانات يطرح خطراً لا يمكن تجنبه لموضع فشل وحيد: المخترقون، ومجرمو الإنترنت، والكيانات المؤسسة بسوء نية مثل الحكومات المحتالة أو الحكومات التي تقمع الحقوق المدنية والإنسانية، يحتاجون للنظر في مكان واحد فقط للحصول على المعلومات الخاصة.
25. أي تقييد لوصول الجمهور إلى المعلومات حول هوية مالك النطاق يزيد من صعوبة البحث المكافح للبرمجيات الخبيثة و المكافح للبريد المزعج.
26. السجل الغير محتمل والحافل بالعمليات والامتثال الخاص بمؤسسة ICANN يجعل من غير المحتمل أن يعمل هذا الأمر
27. إن تسجيل البيانات الخاص بي سوف يتم نقله إلى بلد آخر لا أثق في سلطته القضائية.
28. يبدو أن نظام RDS الجديد سيحسن خصوصية بيانات التسجيل بشكل كبير مما سيحفز حرية التعبير والذي هو في رأيي أساس وميزة الإنترنت. اهتمامي الوحيد من حيث المخاطر التي لا يمكن تجنبها هو فيما يتعلق بالمشغلين والموظفين بالإضافة إلى الأشخاص والمنظمات الذين سوف يمتلكون أو قد يمتلكون الوصول غير المحدود و/أو غير المنظم لجميع تسجيلات البيانات.
29. إن الخدمة المركزية خطرة وغير ضرورية، وتورط ICANN في قضايا قانونية صعبة يمكن تجنبها. لننظر في بعض الحلول المحتملة الأخرى.
30. كيفما كانت نوعية أو بنية مسرح الكابوكي الذي قد يرتبط بموضع نشأة RDS أو ما قد تعرضه بشكل طفيف كفائدة لأي شخص غير اهتمامات LEA و TM، فسيتم النظر إلى RDS كمصدر بيانات ستسيء الحكومات استخدامه.

13 مجيباً قدموا إجابات مفصلة وأساساً منطقياً حول **المخاطر المقبولة**:

1. الخطر مقبول اعتماداً على العلاجات التقنية الموجودة اليوم (الحوسبة عالية الأداء، التوزيع المستند إلى تقنية cloud وتجاوز الفشل التقني لزيادة الإتاحة، إلخ. (5)
2. طالما أنها يتم تطويرها بطريقة تقنية مقبولة عامة ومصممة لضمان الإتاحة والأمان، فستخف المشاغل.
3. المواقع الغير تجارية (التي لا تمتلك وظائف تجارة إلكترونية أو متطلبات إدخال البيانات) تطرح قليلاً من المخاطر لدى المستهلكين وهؤلاء الذين يسعون جاهدين لحماية المستهلكين (الشركات، وكالات إنفاذ القانون وغيرها). سيكون نقص شفافية هذه المواقع مقبولاً.
4. القدرة على مواجهة قوانين الخصوصية المختلفة هي خطر مقبول يؤثر احتمالاً على الأعمال التجارية.
5. مخاطر الخروقات الأمنية لبيانات الوصول المبوبة تبقى مقبولة طالما أن الخطر لا زال أقل مما هو عليه حالياً في إطار قواعد البيانات العامة Whois.
6. الخطر الكبير للبيانات قد يكون مقبولاً من خلال حالة التصميم الدقيق والمراقبة التشغيلية. نقص الوصول إلى المعلومات المطلوبة لكل مستوى وصول مبوب يمكن تحسينه بواسطة التحليل الدقيق لمتطلبات أصحاب المصلحة.
7. سوف تستلم ICANN "رسوماً" أقل نتيجة لتنفيذ RDS. خدمة RDS المقترحة ستقلل الحجم الحالي للتسجيل في السوق، بسبب الطريقة المتعبة التي توجب على العميل أن يوفر كميات هائلة من البيانات قبل أن يكون قادراً على القيام بشراء أولي.

24 طريقةً من أجل **تقليل أو نقل المخاطر** تم اقتراحها من طرف المجيبين:

1. الخطوات المتخذة لتحسين الدقة
2. مخاطر فشل/إعاقة خدمة RDS يجب أن تكون قابلة للتحكم من خلال المراقبة القوية لمشغل RDS.
3. إن قدرات Whois/WhoWas العكسية يمكن أن يتم بناؤها في RDS
4. التقليل من البيانات المتاحة بحرية يمكن أن يتم تطويره من خلال التحليل الدقيق لعناصر البيانات العامة حالياً، ومنع وصول الجمهور لتلك البيانات حيث الحاجة لمثل هذا المنع يمكن أن يتم إنشاؤها بموضوعية.
5. تصميم عملية اعتماد سهلة تؤدي إلى اعتماد مستمر.
6. تحديد استخدام اسم يجب أن يتم تبريره. يجب أن يكون الرد مبنياً على الشكوى. إذا كان الطلب صالحاً، فقد يتم إعطاء إجابة.
7. هل استقبل المسجل ملحوظة بأن المعلومات تم طلبها؟ وإذا تم ذلك، فهل حدد الطرف الذي قام بالطلب؟
8. يمكن تجنب أشد مخاطر RDS بمجرد تنفيذ جوانب المدقق في النموذج الحالي. إذا كان من المرغوب فيه جعل جميع بيانات التسجيل مطابقة لهيئة محددة، فيمكن إتمام ذلك من خلال سياسة ICANN عوض خدمة RDS الجديدة.
9. قد يتم تقليل المخاطر من خلال وسيلة للتمييز بين المواقع التجارية وغير التجارية لتوفير مزيد من الشفافية على المواقع التجارية.

10. على الأقل فإن بعض المخاطر قد يتم تقليلها عن طريق نهج اتحادي لكل سجل يخزن بياناته الخاصة.
11. إعادة التفكير في المخطط بأكمله وتجميع بيانات اتصال أقل. تطبيق مبادئ التناسب، والخصوصية عبر التصميم والخصوصية افتراضياً.
12. طلب حدود وقتية معقولة للإجابات على الاتصال والتي يمكن بعدها أن تكون النطاقات معلقة في انتظار الإجابة.
13. تخزين بيانات أقل.
14. وصول Whois يمكن ويجب أن يبقى مجهولاً ومفتوحاً لجميع مستخدمي الإنترنت.
15. أوقات إجراء التصديق على بيانات التسجيل تحتاج لأن تقل بقدر الإمكان من أجل أن يقوم مدراء النطاقات بتشغيل نطاقاتهم بشكل فعال وبكفاءة وبأقل وقت انتظار ممكن ناتج عن إجراءات التصديق.
16. السماح باختيار المستهلك عند اختيار مزود تصديق سيكون أمرا حكيماً، حيث سيتم تشجيع المزودين على تخفيض التكاليف وأوقات العمليات حتى يكونوا أحسن تنافسية.
17. مركزة التصديق على مجموعة صغيرة أو فرض التصديق من خلال مزود محدد سيقلل الحافز لتسريع العمليات وجعلها ذات كفاءة من حيث الكلفة.
18. السماح بتسجيل النطاقات للجميع (ليس فقط الأشخاص الذين يعتبرون بحاجة للحماية بواسطة بعض المنظمات) بهوية مجهولة تماماً، وبدون توفير أي بيانات تسجيل. إذا لم تكن هناك تقريباً أية بيانات تسجيل، إذن فلا إشكال في وصول الجمهور للمحتوى كاملاً.
19. إزالة جهالة الهوية في التسجيل.
20. يمكن تخفيف بعض المخاطر ببساطة عن طريق مقاربة مرحلية لتنفيذ RDS، مثلاً عن طريق جعل أي متطلبات معلومات إضافية اختيارياً لفترة مع جعل البيانات متاحة على البنية التحتية الموجودة الخدمة Whois. سيعني هذا بأن نظام RDS يستطيع التطور كما يمكن العمل بسهولة على الأعطاب/القضايا بدون التأثير على النظام الموجود، ثم بعد أن يتم إنشاؤها وتوفير الوقت الكافي للعمل على قضايا التكامل، فيمكن لأمناء السجلات/السجلات أن يقوموا بالانتقال. أود أن أقترح فترة مناسبة للبيانات الإضافية لتكون اختيارية، وللخدمات لتتداخل لتكون تقريباً خلال 3 سنوات، وسيسمح هذا بالكثير من الوقت لتغيير الأنظمة ولتوفير تعليم مناسب للعملاء.
21. إزالة جميع تسجيلات الوكيل "proxy"، وفرض دقة بيانات التسجيل، تتطلب أن تقوم السجلات بتقييد الوصول بالجملة، وتفوض وصول Whois المفتوح لكن بمعدل محدد لجميع بيانات التسجيل، وتمنع بيع بيانات التسجيل بالجملة من طرف السجلات وأمناء السجلات.
22. إزالة الحافز المالي لأمناء السجلات أو لغيرهم والذي يحفزهم على بيع خدمات تسجيل الخصوصية. إنه حالياً مصدر جيد للربح، تماماً كما كانت أرقام الهواتف الغير مدرجة بالنسبة لشركات الهواتف. ضمان أن أمناء السجلات لا يربحون *أي شيء* من عرض خدمات تسجيل خاصة أو من نوع الوكيل proxy. ضمان أن المسجلين الذين يمتلكون احتياجاً قانونياً للتسجيلات الخاصة أو من نوعية الوكيل proxy يدفعون رسوماً كافية ليبرهنوا على حاجتهم الصادقة للخدمة، حيث تذهب جميع العائدات من هذه الرسوم إلى الجمعيات الخيرية العامة (وهكذا يتم ضمان أن ICANN كذلك ليس لديها أي حافز لتشجيع التسجيلات الخاصة وتسجيلات الوكلاء proxy)
23. استشارة أفضل بشأن البيانات المطلوبة مقابل مستوى الوصول المبوب.
24. من أجل الحد من مخاطر إساءة استعمال الوصول إلى بيانات التسجيل الخاصة، فإن مثل هذا الوصول ينبغي أن يُصدق عليه بواسطة وثائق قانونية موقعة من قاض أو سلطة قانونية أخرى.
25. التغلب على تصورات سنودن/كافكا/أورويل بخصوص إساءة الاستعمال بالجملة لهذا الأمر من طرف مصالح مماحكة، عبر جعل الوصول إلى الطلبات وإلى النظام شفافاً تماماً بنسبة 100% لاطلاع الجمهور.
26. التغلب على مقاومة التغييرات بالجملة، اكتشف طريقة لزيادة المزايا وتقليل الجانب السلبي للمسجلين، وأمناء السجلات، والسجلات، مثل استخدام السجل لنظام تصديق ممركز.

اقترح 13 مجيباً طرقاً حيث تكون **المخاطر مقايضات جيدة للمزايا**:

1. ترتبط المزايا المحتملة بكيفية تنفيذها (2)
2. أى مخاطر مرتبطة بالوصول المنخفض (حالياً مجاناً وبشكل عام) للبيانات قد تقل إذا ضمن المجتمع دقة أعلى للبيانات لأي بيانات تتطلب وصولاً مبوباً. الحد من الوصول بدون زيادة الدقة سوف يكون خللاً رئيسياً في أي نظام جديد مقترح (2).
3. في حين أن قاعدة البيانات المجمعة يمكن أن تزيد المخاطر الأمنية، فيمكن تحسين هذه المخاطر من خلال التصميم السليم والرقابة والخدمة المتوفرة بتواجد مطلق والتي تعرض النتائج بشكل مستمر يمكن أن يبرر هذه المخاطر.
4. وصول الأطراف الأخرى في مقابل بيانات أفضل (أي أكثر اكتمالاً وأكثر دقة) قد يكون واحدا من المقايضات الممكنة.
5. يقدم RDS المقترح عدداً من المزايا التي تفوق المخاطر. سهولة الوصول إلى بيانات المسجلين الدقيقة أمر بالغ الأهمية لإنفاذ حقوق الملكية الفكرية على الأنترنت. إن نظاماً لخدمة RDS يحسن وصول ودقة هذه البيانات سيكون مفيداً للغاية لأصحاب الملكية الفكرية ومستشاريهم من أجل معالجة التعدي على الملكية الفكرية IP وغيرها من إساءات الاستخدام ذات الصلة من طرف مسجلي اسم النطاق والمستخدمين الأخرين للإنترنت.
6. إذا كانت التكاليف والجداول الزمنية للتصديق يمكن السيطرة عليها والاحتفاظ بها في الحد الأدنى، فيمكن أن تكون فوائد النظام المقترح مقايضة عادلة للمزايا المقترحة للنظام. إذا لم يتم التحكم في التكاليف فإنها ستفوق المزايا بجدية.
7. إن تحسين جودة البيانات في قاعدة بيانات Whois مهم جداً، وجدير بالاهتمام. إن ربط المسجلين بطريقة متسقة بمجموعة نطاقاتهم الكاملة مهم جداً أيضا وجدير بالإهتمام، مما سيضمن أنه عندما يتم تحديد وتصحيح عدم دقة في نقطة بيانات الاتصال لمجال معين، فإنه سيتم تصحيحها في كل مكان تتواجد فيه.
8. ومن شأن تحسين الوصول البرمجي (بلا حدود معدل تعسفي أو غير المدروس أو ما إلى ذلك) أن يكون مفيداً بشكل كبير أيضا.
9. إن الوصول المنتظم/الموثوق/الصالح للاستخدام للبيانات الصحيحة هو مكسب واضح لأنه أصبح من الممكن تقليل المخاطر من خلال التصميم الدقيق والاستشارة.

استطلاع مخاطر RDS - ملخص النتائج

وقد قدم 25 مجيباً **المزيد من التعليقات** في نهاية الدراسة، على النحو التالي.

1. يفتقر الاقتراح إلى ميزات ملموسة لتحسين الدقة العملية للبيانات (قدرة المسجلين على الاتصال) لمستوى أعلى بكثير من خط الأساس لسنة RAA 2013 و (لنطاقات gTLD الجديدة) PICs. هذه تحتاج إلى التعبير عنها. وبالمثل، فإن قاعدة بيانات أكثر ثراء حيث توفر خدمات محسنة مثل البيانات التاريخية، يمكنها المساعدة في تبرير الحد من وصول الجمهور إلى هذا المورد.
2. أحد المزايا هو السماح لنا بتحديد المسجلين الذين يحاولون إخفاء هويتهم حتى يتمكنوا من الاستمرار في الأنشطة الخبيثة وتوزيع البرامج الضارة.
3. إن قدرة المستخدمين وأدوات الأطراف الأخرى على استخدام نظام Whois الحالي للوصول وحفظ معلومات Whois لأغراض تاريخية أمر بالغ الأهمية. أي نظام RDS مقترح يجب أن يضمن هذه القدرة. هذا يمكن أن يحدث إما مباشرة عن طريق RDS نفسه، أو بشكل غير مباشر من خلال الاستمرار في تمكين أدوات الأطراف الأخرى/العملاء من القيام بذلك.
4. إعطاء السيطرة الاحتكارية على هذا الصالح العام إلى كيان فردي يؤدي إلى خسارة للعالم مع فائدة صغيرة لا يمكن أن تتحقق عن طريق وسائل أخرى أقل مركزية.
5. لماذا يوجد عدد كبير من نطاقات gTLD الجديدة؟ هذا القرار كارثة بالنسبة لأصحاب العلامات التجارية لأنه يؤدي إلى زيادة تكاليف حماية الملكية الفكرية. وبالفعل، فنحن نواجه الآن الكثير من التسجيل بسوء نية على الرغم من أن فترات الازدهار بالنسبة لكثير من نطاقات gTLD الجديدة لم تبدأ حتى. كشركة صغيرة، قد لا تملك ميزانية للتسجيل للجميع لتفادي التسجيلات ذات النية السيئة. من ناحية أخرى، فإن تكاليف المتابعة القانونية مرتفعة.
6. حقيقة أن يكون هناك Whois مُتحقق منها هو في غاية الأهمية نظراً لإمكانية جهالة هوية الإنترنت. نحن نبحث عن المخالفين وأية بيانات غير دقيقة لم تعد مقبولة.
7. أؤيد تماماً الجهود المبذولة لجعل بيانات WHOIS أكثر دقة. سيكون تغييراً إيجابياً إذا لم تجعل قاعدة بيانات مغلقة مركزية الحصول على المعلومات أكثر صعوبة، ولم تبطىء عملية الحصول على المعلومات، ولم يكن لها تحديد لكمية المعلومات التي يمكن الحصول عليها، ولم تنشىء عمليات طويلة للشركات للحصول على الاعتماد للوصول إلى المعلومات أو لم تنشىء مشاكل الشفافية لمستخدمي شبكة الإنترنت. الكثير من اهتمامي يتعلق بكون مجتمع الأمن السيبراني قادراً على توفير حماية فعالة للمستهلكين من المواقع المحتالة التي قد تكسب ميزة من قاعدة بيانات مغلقة.
8. الجمهور المقترح فى مقابل بوابات الوصول لعناصر بيانات معينة هو فكرة جيدة. سيكون من المفيد أن نرى مزيداً من التفاصيل حول أغراض الكشف المقبولة، وتقييم مقدمي الطلبات هؤلاء، وكيف يبقى مستخدمو الوصول المبوب تحت المساءلة وما إلى ذلك، من أجل التعليق على ذلك.
9. بشكل عام، أي تحرك لمركزة البيانات يزيد كثيراً من مخاطر كل من الاختراق العلني والسري، والتفتيش الحكومى الغير مرئي والغير خاضع للمساءلة، ووسائط الفشل واسعة النطاق، والتدخل السياسي. رغم أن بعض أهداف RDS هي ذات قيمة، فإنها لا تفوق المخاطر التي يمكن التنبؤ بها تماماً. أعظم مخاطر RDS هي احتمال الاضطرار إلى دفع ثمن من أجل الوصول إلى معلومات WHOIS العامة، و/أو فقدان وصول الجمهور إلى معلومات إدارة الشبكة الأساسية بما في ذلك مهمة منع عنوان IP، والموقع الجغرافي، وإساءة استعمال صناديق البريد. يجب أن يزال من الجدول أي اقتراح لا يحمي وصول الجمهور الحر واستمرار توافر عناصر المعلومات هذه بأسرع وقت ممكن وبصورة نهائية.
10. ما زلت غير متأكد كيف يمكننا ضمان "دقة" بيانات التسجيل، بيانات اليوم الأول (على التسجيل) هو شيء معين، وأمر آخر هو "الاختبار الدوري" الذي أعتقد أنه الأهم. IMO، قد نضطر إلى الاستعانة بمصادر خارجية من خلال "وكالات" في كل مكان (بلد أو ربما مدينة) للقيام بالتدقيق ولكن هذا قد يؤدي إلى بعض الشكوك حول الدقة والمقايس مرة أخرى.
11. مجموعتا الأفراد التي سوف يرغب السجل المتوسط في منعها من الوصول بالجملة إلى بيانات Whois هم المتطفلون ووكالات إنفاذ القانون. توفير المعلومات بالجملة عن أي من هذه المجموعات من شأنه أن يسبب ضرراً بسمعة السجل لا يمكن إصلاحه. إن نظاماً مركزياً لخدمة RDS يتطلب أن يضع السجل سمعته في يد طرف آخر.
12. يجب أن يكون هناك قبول بكون جميع الأطراف لا يملكون نفس الحماية بموجب القوانين المحليةن وبكون الطلبات عبر الحدود للبيانات قد لا تتم متابعتها بسبب القضايا السياسية الخارجية. سيتم فقدان مورد حيوي في مكافحة الجرائم الإلكترونية المنظمة مع RDS.
13. باعتبارى مسجلاً فردياً، فإني أستخدم حالياً وظيفة خصوصية/وكالة proxy متاحة من أمين السجل الخاص بي لحماية هويتي الفردية من الوصول العارض الغير ضرورى من قبل الجمهور العام، الشيء الذي أجده مفيداً كإجراء وقائي ضد الإزعاج الشخصي مجهول المصدر. أود أن أرى مثل هذه الوظائف الخصوصية مفوضة لتكون متاحة بانتظام كلما تم استخدام أي أمين سجل، من أجل ضمان سوق تسجيل تامة التنافسية عبر جميع أمناء السجلات، وليس فقط مجموعة فرعية تطوعية من أمناء السجلات.
14. أكبر مخاطرة أشعر بالاهتمام إزاءها هي تكلفة التصديق على بيانات التسجيل الخاصة بي، والمصادقة بالنسبة لي للوصول إلى البيانات المبوبة. كما أشعر بالاهتمام إزاء أوقات المعالجة والتباطؤ العام الذي سوف تسببه هذه الإجراءات.
15. RDS فكرة عظيمة. هذا من شأنه المساعدة في حل العديد من المشاكل إذا ما تم تنفيذه بشكل صحيح. أنا أتطلع إلى وجود بعض الإسهامات. ومع ذلك، هذا الاستطلاع المحدد لم يتم إعداده بشكل جيد.
16. بصراحة، يبدو أن هذا النظام غير مدروس تماماً مثل خدمات "خصوصية WHOIS" المتاحة حالياً. مجرد استخدام هذه الأمور يضر بشفافية المؤسسة وبالتالي سمعتها على الإنترنت. شكرًا لكم على الاستماع.
17. لا أرى أية مزايا تذكر، بل هناك العديد من المخاطر بالإضافة إلى إساءة استخدام البيانات أو سرقتها. بشكل مثالي، سوف يتم إلغاء الحاجة إلى تزويد أمين السجل ببيانات التسجيل - إذا لم تكن هناك بيانات تسجيل، فلا يوجد أي خطر لإساءة استخدامها أو سرقتها.
18. إن ما يهمني هو القدرة على التعامل مع أنواع مختلفة من هجمات الشبكة/البريد المزعج/الاختراقات/غزو البيانات، وما إلى ذلك. وإنه في غاية الضرورة التوفر على اتصال صالح، وأن يقوم هذا الاتصال بالتعامل الفعلي مع مشاكل الشبكة التي يتم نقلها إليه. هذا يعني أن الاتصال يجب أن يتوفر على كل من السلطة والقدرة التقنية لضمان عدم كون نطاقهم مصدراً لسوء الإستخدام. النظام الحالي، خاصةً النطاقات المخفية خلف وكالات proxies لا يضمن بأن أمين السجل/الوكالة proxy سوف يتولى (أو يستطيع) معالجة المسائل في حينها.

إذا ما تم السماح بالوكالات proxies، فمن اللازم إذن توضيح أن أي أشخاص يتم عرضهم بشكل علني في جداول عمليات بحث/استفسارات، فيجب أن يتحملوا مسؤولية سلوك النطاق الذي يقومون بحمايته، بما في ذلك القدرة التامة على إغلاق النطاق في حالة سوء استخدام كبير للشبكة.

19. الخطر الأكبر هو كيفية تسيير الوصول للمعلومات "المبوبة"، مثل هل سيضم ذلك رسوماً، وكيف سيكون مستوى صعوبة عملية الاعتماد للتمكن من الوصول. إذا كان هذا الأمر مكلفاً أو مرهقاً، فسوف يعرقل بشكل كبير العمليات التجارية الأساسية، والاتصال بأصحاب النطاقات، والأبحاث، وعدداً كبيراً من مجالات إدارة النطاق والبحوث.
20. أعتقد أن هذه العملية المقترحة هي حل للبحث عن مشكل وهي مدعمة بحجج مزيفة من أشخاص مدفوعين بآرائهم السياسية الجزمية.
21. لا أعتقد أنه قد تم النظر بعناية لمتطلبات الخصوصية للكيانات الطبيعية مقابل القانونية مقابل الشركات/المؤسسات التجارية. المسجلون الفرديون/الطبيعيون يجب أن تتوفر إمكانية الاتصال بهم بطريقة أو بأخرى من أجل السماح بإصلاح المشاكل التي تؤثر على الآخرين، ومع ذلك يجب دائماً أن يُسمح بحق عدم الكشف عن الهوية إلا في حالة وجود طلب قانوني ملائم. في المقابل، فإن الكيانات القانونية ذات القيود الضيقة فقط (مثل مراكز إيواء النساء، وبعض المنظمات السياسية المعرضة للخطر)، لا يجب إخفاء هويتها. إنه من غير الملائم على الإطلاق بالنسبة لهم العمل بطريقة سرية خاصة مع للشركات التجارية، ويجب أن تكون البيانات عامة/مجهولة الوصول. ثانياً، يجب أن تكون هناك عملية يمكن من خلالها تجريد سرية الهوية عن الهيئات التي أثبتت عدم جودة سريتها.
22. نحن نعاني الكثير من مرسلي البريد المزعج والبرمجيات الخبيثة والذين يستخدمون بيانات وهمية لإخفاء ملكية النطاقات. معلومات Whois يمكن ويجب أن تكون واضحة وجد معرفة. إن الحصول على خدمات الاستضافة من الكيانات الأخرى ليست بالصعوبة المفرطة، ولكن تحديد من هو المسؤول عن خوادم DNS لمجال معين بوضوح هو أمر مفيد من الناحية التشغيلية.
23. برأيي، أعتقد أن الخصوصية هي أهم بكثير من وصول الجمهور إلى بيانات التسجيل.
24. بما أنه لا توجد فوائد، يرجى التوقف عن القيام بما تفعلون. طالما أنه يعمل - لا تصلحوه. لا تنس أن عدداً من المسجلين يرغبون في أن تكون بيانات Whois الخاصة بهم قابلة للوصول كما هي عليه الآن، وكذلك أولئك الذين ليسوا أحراراً في استخدام POB أو حماية الخصوصية المقدمة من طرف أمناء السجلات.
25. RDS هي خدمة أكثر من اللازم في وقت واحد وفكرة سيئة. هذا يخلق عبئاً على أصحاب المنفعة الأقل، دون أن تكون هناك تكلفة حقيقية على الأكثر استفادة.

أخيراً، لقد ملأ حوالي 5 من 182من المجيبين معظم أو جميع الحقول الخالية بأجوبة لم تعالج مباشرة الأسئلة، ولكن بدلاً من ذلك ذكرت بأن RDS كانت فكرة سيئة أو ليست لها فوائد تذكر.