المبادرات المقترحة
لأمن واستقرار ومرونة DNS المحسنة

تقديم

هيئة الإنترنت للأسماء والأرقام المخصصة
(ICANN)

للتعليق العام

12 فبراير 2010

المبادرات المقترحة
لأمن واستقرار ومرونة DNS المحسنة

1. نظرة عامة

تعرض هذه الوثيقة السمات الرئيسية والمبررة وكذلك التكاليف المتوقعة لمبادرتين استراتيجيتين ذات صلة بأمن واستقرار ومرونة نظام أسماء النطاق (DNS) التي ترى ICANN ضروريا تها للوفاء بالتزاماتها بموجب نظامها الداخلي، وتأكيد الالتزامات لعام 2009 والخطة الاستراتيجية 2010-2013 لـ ICANN. وتقدم هذه الوثيقة أساساً لمناقشة أصحاب المصلحة المتعددين لهذه المبادرات المقترحة، ومسؤوليات ICANN في إنشاء قدرات مقترحة وكيف يمكن للمجتمع المضي قدماً في تنظيم الجهود الرامية إلى دعم هذه المبادرات. وقد تم اختيار مجموعة من الموظفين على أعلى مستوى والوقوف على الآثار المترتبة على الموارد، إلا أن تمويل البدائل اللازمة لهذه المبادرات لم يتم تحليلها إلى الآن.

ملاحظة: يتم اقتراح هذه المبادرات باعتبارها جهوداً لما تم تحديده في إطار الموازنة والخطة التشغيلية الخاصة بهيئة ICANN للعام المالي 2011 التي تم طرحها للمناقشة خلال اجتماع نيروبي.

2. الافتراضات

2.1 أصبح نظام اسم النطاق خدمة أساسية لها حق الأولوية في توفير الطاقة للإنترنت. ويتيح DNS تحليل الاسم لمستخدمي الإنترنت، وكذلك دعم البريد الإلكتروني والرسائل النصية والخدمة الصوتية القائمة على شبكة الإنترنت وغيرها من الخدمات والبروتوكولات الأساسية للإنترنت. وفي الوقت نفسه، توجد DNS داخل بيئة يتزايد فيها التهديدات والمخاطر. وتتعرض العمليات التقنية بالنظام إلى مجموعة من الهجمات مثل هجمات DDoS ضد خوادم الاسم المعتمدة لمستويات عليا وبما يشمل خوادم اسم الجذر؛ والهجمات الخطيرة التي تؤثر على سلامة قرار DNS كما وصفه الباحث الأمني دان كامينسكي؛ وغيرها من الطرق التي تشمل الهندسة الاجتماعية وتسمح بالهجمات الخبيثة لتسئ توجيه واستخدام خدمات DNS. وبالإضافة إلى ذلك يستغل المجرمين اعتماد المستخدمين على DNS واستخدام النظام بمختلف الطرق لإجراء مجموعة واسعة من الأنشطة الخبيثة.

2.2 يتعاون حالياً مجتمع المشغلين الذي يوفر خدمات DNS بنشاط مع البائعين والباحثين في مجال الأمن وإنفاذ القانون وفرق الاستجابة للرد على التهديدات الناشئة المنتشرة. وتوجد المبادرات داخل مجتمع DNS لتحسين تبادل المعلومات، بهدف تحديد النشاطات غير الشرعية وتعزيز التعاون المتعلق بـ DDoS وغيرها من الهجمات على نطاق النظام. وتتضمن هذه الجهود التعاونية عموما الجهود التي تبذلها DNS وأعضاء مجتمع الأمن التي تجتمع اختياريا لمعالجة الحالات الناشئة. وهناك العديد من الدعوات للعمل على معالجة وتخفيف مخاطر DNS النظمية التي تحققت في تلك السنة الماضية. [1] وتعرض الطبيعة الجادة والمترددة لهذه الدعوات الخاصة بالعمل الحاجة المتزايدة لتقييم المخاطر على نطاق المنظومة وكذلك التخطيط للطوارئ والوقوف على قدرات الاستجابة.

2.3 إن الجهود الحالية المبذولة لمعالجة مجموعة من التهديدات والمخاطر التي يتعرض لها DNS ليست مركزة بشكل منتظم. فعلى الصعيد التنفيذي، وضع متعهدي الأمن داخل DNS آليات قوية لفهم التهديدات واتخاذ إجراءات لتخفيف المخاطر الواقع عليهم وعلى عملائهم. ومع ذلك، فإن التعاون في هذا مجال لا يشمل بشكل عام مجموعة المشغلين DNS أقل قدرة وأقل تمويلا وغيرهم من أصحاب المصلحة الآخرين الذين لا يدركون التهديدات والمخاطر والذين يفتقرون إلى قدرات للرد بشكل مناسب عندما تتعلق هذه التهديدات بأمن والاستقرار والمرونة. وعلاوة على ذلك، أظهرت الجهود الحالية أن التركيز المستمر على الرصد والاستجابة والعلاج تحتاج إلى التصدي إلى التهديدات التي لا تتقبل بسهولة التصحيحات التقنية المترجمة. وعلى مستوى أعلى، تفتقر DNS إلى نقاط اتصال على نطاق المنظومة للمساءلة المتعلقة بالقدرات الأساسية في تقييم المخاطر والتخطيط لحالات الطوارئ

[1] انظر http://www.enisa.europa.eu/media/press-releases/improving-resilience-3-tips, و http://www.enisa.europa.eu/media/press-releases/guide-to-mitigate-vulnerabilities-threats-cyber-attacks, و http://www.it-scc.org/documents/itscc/IT-SCC_ITSRA_Release_08_21_09_clean_final2.pdf.

2.4 جوهريا، لا يمكن أن تعتمد هذه الأنواع من القدرات كليا على جهود المتطوعين الذين يعملون بدون الدعم التنظيمي المكرس ومناهج التشغيل المكررة وكذلك الالتزامات المتعلقة بالموارد طويلة الأجل. ويجب أن تصل الجهود الرامية إلى ضمان استقرار ومرونة DNS إلى مستويات الفعالية والمساءلة تمشيا مع النواحي الأخرى الحرجة للبنية التحتية للاتصالات التي تتطلب مستويات مماثلة من الاستثمار للموظفين المتفرغين للعمل الدائم والدعم.

3. الأدوار والمسئوليات المنوطة بـ ICANN

3.1 يجب أن تعمل DNS في محيط آمن ومستقر ويمتاز بالمرونة. ولدى ICANN التزامات عديدة تتطلب بذل الجهود لتحقيق هذا الهدف. تنص المادة الأولى من اللائحة الداخلية الخاصة بـ ICANN على "أنه تتمثل مهمة ICANN في تنسيق أنظمة الإنترنت العالمية، على المستوى الكلي، للمعرفات الفريدة، وعلى وجه الخصوص لضمان التشغيل المستقر والآمن لنظم المعرفات الفريدة للإنترنت." تأكيد التزامات عام 2009 (http://icann.org/en/announcements/announcement-30sep09-en.htm) تؤكد على أن خوادم DNS بما أنها بمثابة المهمة الخطيرة ضمن بيئة الإنترنت، وبالتالي المخاطر المتصلة بالعملية التي يجب أن تُدار بشكل ملائم. التزمت ICANN "بالمحافظة على أمن واستقرار ومرونة DNS". وبالإضافة إلى ذلك فإن طلبات التأكيد الخاصة بـ ICANN لتحديد التهديدات الحالية والمستقبلية، وإجراء التخطيط المناسب للطوارئ.

3.2 تضمين هذه الالتزامات لـ ICANN واضح. ويحتاج التأكيد على هذه الالتزامات إلى بذل ICANN لجهود تعاونية من أجل تحديد وتخفيف المخاطر التي يتعرض لها الأمن والمرونة ونظام DNS في جميع أنحاء العالم، والذي يتضمن مجموعة واسعة من أصحاب المصلحة الذين يقومون بتشغيل واستخدام خدمات DNS.[2] نظرا لطبيعة DNS، فإن التشغيل الموثوق به والمرن لنظام الخادم الأساسي ولمجالات على أعلى مستوى يجب أن يكون المستوى الأول الذي يحظى بأولوية ICANN. كما أن نمو DNS من خلال الزيادة الطبيعية للاستخدام، وإدخال تكنولوجيا ومقترحات جديدة لإنشاء TLDs (بما في ذلك تلك التي تستخدم أسماء النطاقات الدولية) التي تتطلب المزيد من فهم ICANN والسعي للحد من مخاطر النظام. ومن الأهمية بمكان ملاحظة أن ICANN تسعى إلى تحسين أمن واستقرار ومرونة DNS منذ إنشائها. وتهدف ICANN *إلى تعزيز أمن واستقرار ومرونة الإنترنت* (http://www.icann.org/en/announcements/announcement-2-21may09-en.htm) ومعالجة مجموعة كبيرة من البرامج والأنشطة الحالية. تتناول المبادرات التي وردت في هذه الوثيقة المزيد من الجهود المبذولة التي يجب أن تضطلع بها ICANN للوفاء بهذه الالتزامات.

3.3 تتطلب ضرورات تحسين الفهم المنهجي والتخفيف من مخاطر DNS ومواجهة التزاماتها- من ICANN التعاون مع مجتمع DNS للشروع في العمل الذي يبنى على جميع الجهود السابقة المبذولة والتعاون الحالي. وتحقيقا لهذه الغاية، تقوم هذه الخطة الاستراتيجية الخاصة بـ ICANN للعام 2010-2013 بتحسين استقرار وأمن ومرونة DNS كأحد مجالات ICANN الأربعة للتركيز خلال هذه الفترة. وتتناول هذه الخطة الاستراتيجية على وجه التحديد شرط ICANN لوضع نهج لفريق الاستعداد لطوارئ نظام الحاسب بنظام اسم النطاق (DNS-CERT) فضلا عن التخطيط للطوارئ والممارسة لـ DNS. بينما تسعى ICANN إلى المضي قدما لضمان وضع نهج على نطاق المنظومة لتقييم المخاطر، والتخطيط وممارسة خطة الطوارئ لمكافحة التهديدات المحتملة، وتحقيق الانسجام التعاوني للقدرات للاستجابة إلى تحسين أمن واستقرار ومرونة نظام DNS الشامل. كما تعمل ICANN أيضا على التخطيط لبذل الجهود لتحسين نظام مقاييس واسعة حتى يتسنى لمجتمع DNS الحصول على فهم أوضح لأمن واستقرار ومرونة من DNS، واستباق التحديات والتصدي لها بفعالية.

[2] كما تهدف ICANN إلى توجيه دورها في إدارة المخاطر التي تحيق بأمن واستقرار ومرونة DNS، ولا تتناول القضايا المتصلة بالمنافسة بالأمن القومي بين الدول في مجال حرب الفضاء الإلكترونية أو التجسس أو التحكم في محتوى الاستضافة للإنترنت كما تم تناولها في خطة ICANN لتعزيز أمن واستقرار ومرنة الإنترنت. انظر http://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf.

3.4 تحتاج المنفعة المحتملة والنجاح العملي للمبادرات المبينة أدناه إلى دعم المجتمع المحلي والمشاركة. ومن ثمّ تكامل استعراض الجماعة وردود الفعل والتخطيط فيما يتعلق بتنفيذ هذه المبادرات خلال التخطيط العملي لـ ICANN وعمليات وضع الميزانية.

4. المخاطر التي تتعرض لها عملية DNS

4.1 بما أننا نبدأ عام 2010، يبقى النظام الإيكولوجي للإنترنت نابضاً بالحياة. وعلى نحو متزايد، فإن نشاط الإنترنت يعكس النطاق الكامل لدوافع الإنسان وسلوكه. وبصفة جزئية، يعكس هذا النشاط الطبيعة المنفتحة للإنترنت التي جعلت منه ابتكاراً ناجحاً وفعالاً وأتاحت الفرصة للتواصل والابتكار والمتاجرة ضمن مجتمعات عالمية. كما أن النظام الإيكولوجي يشمله تهديد أيضا لمستويات متزايدة من النشاط الخبيث الذي تجريه مجموعة متنوعة من الجهات الفاعلة، مع وجود مؤشرات قوية على تورط المنظمات الإجرامية بشكل متزايد. علما بأن مشهد التهديد يشمل التزوير والابتزاز وغيره من الأنشطة غير المشروعة عبر الإنترنت، الأمر الذي يقوض ثقة المستعملين في الخدمات المستندة إلى الإنترنت، والحرمان من خدمة (DDoS) وغير ذلك من الأنشطة التخريبية التي تزعزع استقرار البنية التحتية للإنترنت. بوجه خاص، فإن قدرة الجهات الفاعلة الخبيثة على شن هجمات على سير العمل في DNS نفسها وسهولة وتردد استخدام هذه الجهات تستعين بتحليل الاسم وخدمات التسجيل لتمكين مجموعة من الأنشطة الإجرامية الخبيثة التي تعرض مخاطر متزايدة لعمل الإنترنت، والدعوة إلى التشكيك في سلامة وموثوقية شبكة الإنترنت باعتبارها منصة عالمية للاتصالات.

4.2 توجد ثلاث فئات رئيسية لمخاطر الأمن والاستقرار والمرونة: الأنشطة الضارة (الهجوم ضد DNS أو الهجوم الذي يستغل تحليل الاسم أو أنظمة التسجيل)، والمخاطر التقنية في تحقيق الاستقرار لـ DNS، والمخاطر التنظيمية المتصلة بـ DNS.

4.2.1 مخاطر النشاط الخبيثة

4.2.1.1 تتمثل المخاطر الرئيسية التي تُعنى بها ICANN في توافر DNS لتحليل الاسم وإتاحة طائفة واسعة من المعاملات عبر الإنترنت. ومن ثمّ يتمثل الخطر الكبير في شكل هجمات DDoS ضد أولئك الذين يديرون خدمات DNS على مختلف المستويات للأنظمة. ويتوقف تأثير هجمات DoS على أنواع الخدمات المستهدفة وكذلك حجم الهجوم المعقد. وعلى مدى العقد الماضي، تم الهجوم على عمليات خوادم الجذر وكذلك المجالات ذات المستوى الأعلى (TLDs) بشكل مباشر. ويتكشف لنا أربع حالات: 1) في 21 أكتوبر 2002، وقعت أول حالة هجوم مسجلة ضد ثلاثة عشر خادم جذر DNS (http://d.root-servers.org/october21.txt)؛ 2) في فبراير 2006، وقعت هجمات ضد خوادم الاسم التي تعمل من قبل مقدم خدمة اسم TLD الرئيسي (http://www.icann.org/en/committees/security/dns-ddos-advisory-31mar06.pdf)؛ 3) في فبراير 2007، وقع هجوم ضد ستة من ثلاثة عشر خادم جذر DNS (http://www.icann.org/en/announcements/factsheet-dns-attack-08mar07.pdf)؛ 4) في الآونة الأخيرة، في ديسمبر 2009، وقعت هجمات DoS ضد مقدمي خدمات DNS ووردت في الأخبار مرة أخرى عندما أثر الهجوم ضد خدمة NeuStar's UltraDNS على العديد من مواقع التجارة الإلكترونية (http://www.cnn.com/2009/TECH/12/24/cnet.ddos.attack/index.html). ويوضح تاريخ الهجوم الزيادة المستمرة في الموارد المتاحة لتلك الهجمات، فضلا عن التطور التقني للجناة.

4.2.1.2 وتستمر الجهود كبيرة المبذولة من أجل التقليل من هذه المخاطر من حيث توفير المخصصات لعرض النطاق الترددي للتعامل مع DDoS وإنشاء ونشر التكنولوجيات والمنهجيات مثل النشر المتعدد، حيث يتم توجيه البيانات إلى أفضل أو أقرب الوجهات. ولندلل بمثال على نشر حلول anycast فإن نظام خادم جذر DNS قد نمى من وجود ثلاثة عشر موقعا (للنظم) إلى وجود أكثر من مائتي موقع (انظر التفاصيل في http://www.root-servers.org). توجد مستويات متزايدة من التخطيط والتعاون فيما بين مشغلي DNS، مع إنشاء منظمات مثل تحليل عملية DNS ومركز الأبحاث (DNS-OARC) (http://www.dns-oarc.org), مجموعة أمن إنترنت التسجيل (RISG) (http://registrysafety.org/website/) والجهود المبذولة لفهم المخاطر المرتبطة بـ DNS مثل أمن DNS العالمي لمناقشة مسألة الأمن والاستقرار والمرونة

4.2.1.3 جدير بالذكر أن طبيعة تشغيل DNS إلى جانب إدارة التوزيع على نطاق واسع لخوادم الاسم وحلوله، من شأنها تعريض المستخدمين إلى عدد من المخاطر الإضافية. كما أن بروتوكول DNS (بدون استخدام ملحقات الأمن) عرضة للهجمات التي توظف التوجيه الخاطئ للاستفسار. وعلى وجه التحديد، فإن الهجوم يأتي بمعلومات كاذبة في رده على استفسار DNS أو المعلومات التي تختلف عما يقصده اسم النطاق من (إعادة التوجيه، أو تعديل الرد). وتخدع مثل هذه الهجمات مستخدمي DNS بمجموعة واسعة من الطرق: توجيه المستخدمين إلى مواقع الويب من خلال المحتوى الاحتيالي أو الشفرة الخبيثة، مما يجعل رسائل البريد الإلكتروني تبدو وكأنها تأتي من مصادر غير موثوقة، وما إلى ذلك. وأن التقنيات اللازمة لتنفيذ هجمات من شأنها أن تسمح بفساد نظام تخزين DNS، وبالتالي التوجيه الخاطئ لحركة الإنترنت الحالية التي تمثل فرصة للنشاط الخبيث الذي قد يشكل مخاطر على سلامة DNS ككل.

4.2.1.4 تقدم خدمات تسجيل أسماء النطاقات خط آخر من هجوم المجرمين. يعمل المهاجمون على استغلال نقاط الضعف التقنية (نقاط صعف المواقع على شبكة الإنترنت) والتشغيلية الخاصة بالتسجيل أو باسم النطاق للسيطرة بغير وجه حق على حساب سجل اسم النطاق (لمزيد من التفاصيل، انظر SAC040 (http://www.icann.org/en/committees/security/sac040.pdf). وبمجرد السيطرة على حساب التسجيل المسروق، يقدم المهاجم إنذارا بتهيئة DNS لكافة المجالات للحساب المسروق للإشارة إلى خادم الاسم الذي يسيطر عليه المهاجم، مع منح القائم بالهجوم السيطرة على تحليل الاسم من أجل شبكة النطاق للمجال والبريد الإلكتروني وتطبيقات الإنترنت الأخرى. ويستخدم اسم المجال هذا أو هجمات سرقة الحساب لطمس المواقع على شبكة الإنترنت، أو تعطيل البريد الإلكتروني أو غيرها من الخدمات الأخرى التي يقدمها المسجل، أو سرقة المعلومات الحساسة أو الشخصية.

4.2.1.5 وحيث أن DNS تهدف إلى خدمة مستخدمي الإنترنت، فإنه وللأسف يستغلها المجرمون لتسهيل طائفة واسعة من السلوك الإجرامي وإساءة المعاملة. وهذه النتيجة غير المقصودة هي أفضل مثال على الطريقة التي يتم فيها استغلال DNS لتسهيل نشاط ضار يشار إليه على أنه الخداع. ويتولى المخادعون تسجيل أسماء النطاقات على وجه التحديد لدعم الهجمات التي انطلقت من شبكات أجهزة الكمبيوتر التي تتضمن شبهاتأو التي تسمى "بوت نت". فغالبا ما يستخدم المهاجم بعض أسماء هذه النطاقات الخبيثة لتشغيل DNS الإجرامية لمجموعة من حلول DNS التي يتم برمجتها على وجه التحديد ونشرها من أجل حل استفسارات DNS التي تصدرها ضحايا السرقة. وتستخدم أسماء النطاقات الأخرى الخبيثة لاستضافة المواقع على شبكة الإنترنت. كما أن الردود على استفسار DNS الخاص بالضحية للاستعلام عن اسم نطاق شرعي لإحدى المؤسسات المالية أو التجارة الإلكترونية أو الخيرية أو الوكالات الحكومية أو الكيانات المماثلة توجه مباشرة هؤلاء المستخدمين غير المقصودين إلى مواقع الخداع أو الانتحال الشخصية. وتتفاعل الضحية ببراءة مع هذا الموقع الخداعة كما تفعل عادة مع المواقع الشرعية للمؤسسات المالية أو التجارة الإلكترونية أو الجمعيات الخيرية أو وكالات حكومية. وتصمم هذه المواقع الخبيثة بهدف سرقة الهويات والحسابات المصرفية وبطاقات الائتمان والمعلومات، وبيع منتجات وهمية أو غير مشروعة للضحية، للاحتيال على جمعية خيرية، وأكثر من ذلك.[3]

4.2.1.6 وعلى نحو متزايد، تلعب DNS دورا بارزا في إتاحة"بوت نت" للإيجار، ومهاجمة الشبكات التي تقدم الخدمة في اقتصاد مزدهر. كما تتألف"بوت نت"من مئات الآلاف أو حتى الملايين من أجهزة الكمبيوتر الخطرة (البوت) التي يتم التحكم فيها عن بعد لتنفيذ العديد من أنواع الهجمات الخبيثة (على سبيل المثال، DDoS) أو دعم الأنشطة

[3] وزارة الأمن الداخلي الأمريكية، ومجلس التنسيق الحكومي لتكنولوجيا المعلومات 2009. تقييم مخاطر الخط الأساسي لقطاع تكنولوجيا المعلومات. واشنطن العاصمة: مكتب الطباعة الحكومي، ص 32-33.

4.2.2 المخاطر التقنية

4.2.2.1 يمكن أن يتأثر تشغيل أو سلامة DNS سلبا إذا تسبب الاستخدام الواسع لممارسات التشغيل موضع الشك في حدوث انقطاع للخدمة، أو أدى التغيير التقني إلى الضعف غير المتوقع في أن المجرمين يستغلون تسهيل الأنشطة الخبيثة. ويتم حاليا مناقشة أمثلة هذا النوع الأخير من المشكلة وطريقة رد الفعل والتي وقعت في عام 2008. وقد اكتشف الخبير الأمني دانيال كامينسكي ثغرة خطيرة في بروتوكول DNS، وأوضح في وقت لاحق أن الممارسة التي تدعى تعديل الرد DNS يمكن استغلالها من قبل المهاجمين لسرقة المواقع على شبكة الإنترنت من الشركات الكبرى باستخدام خدمات استضافة المواقع بالكامل بعيدا عن الوصول الإداري لتلك المنظمات. وقد نشرت اللجنة الاستشارية لأمن واستقرار ICANN في وقت لاحق تحذيرا للتهديد المحتمل DNS لتعديل الرد المقدم إلى المجتمع (http://www.icann.org/en/committees/security/ sac032.pdf). ومن ثمّ قد وضعت النظم المخصصة وتحددت بحيث أن مشغلي ومستخدمي DNS يمكنهم اختبار نظمها لشدة التأثر واتخاذ تدابير وقائية أو علاجية. وبدأ مجتمع ICANN إجراء العديد من المبادرات التي قد تسهم في الكشف الأكثر تنسيقا والرد الأكثر تنظيما للتهديدات التي تتعلق بـ DNS ذات الصلة بهذه الأنواع. وهذا يشمل عمل ICANN مع الشركاء لإجراء ندوات سنوية لاستقدام خبراء معا لدراسة طبيعة التهديد، وبصورة جماعية تقييم المخاطر وتقديم توصيات بشأن كيفية التصدي للخطر. وقد أجريت الندوة الأولى في فبراير 2009 بالتزامن مع مركز *أمن* جورجيا للتكنولوجيا المعلومات (GTISC).

4.2.2.2 يمكن أن يتأثر نظام تشغيل DNS سلبا في حالة تنبيه التغييرات التقنية لـ DNS لسلوك النظام أو التسبب في الأحمال المرورية التي تتطلب تغيرات كبيرة في القدرة الحالية أو المخطط لها. للحد من إمكانية اعتماد الممارسات العملية التي يمكن أن تعرقل أمن واستقرار DNS على مستوى TLD، في عام 2009 قام مجلس ICANN بتنفذ خطوات لحظر استخدام إعادة التوجيه على أساس أن هذه الممارسة تشكل مخاطر على استقرار DNS على النحو الذي حددته اللجنة الاستشارية المعنية بالأمن والاستقرار (SAC041 http://www.icann.org/en/committees/security/sac041.pdf).[4] وفي عام 2010، سيتعين على مجتمع DNS مواصلة إجراء استعراض شامل للآثار المحتملة التي قد تنجم عن سلسلة من التغييرات المقترحة على المستوى الجذري لـ DNS: تنفيذ ملحقات أمن DNS (DNSSEC)، وتنفيذ IPv6 والحاجة إلى سجلات IPv6 لإضافتها إلى ملف المنطقة الجذرية، وتقديم المسار السريع لتمكين استخدام بطاقات أسماء النطاقات الدولية (IDN) على المستوى الأعلى DNS، وإدخال TLDs الجديد.

4.2.3 الإخفاقات التنظيمية

4.2.3.1 يشكل الإخفاق المحتمل للمنظمات التي تؤدي أدوارا رئيسية في عملية DNS مخاطر الفئة الكبيرة بشكل فعال. وفي صميم DNS، فإن قدرة ICANN، مشغلي خوادم الجذر، وسجلات ومسجلي TLD على تقديم الخدمات دون انقطاع أمرا ضروريا لأمن واستقرار DNS العام. وأن كل كيان من هذه الكيانات بمثابة مسؤولية فردية عن جدواها المالية الخاصة بها، واستمرارية الأعمال وإدارة المخاطر، ولكن على مستوى نظام الحكم يجب أن تكون لحالات الطوارئ عند توقف المنظمة على أداء وظيفتها، حسب الاقتضاء، وكيف ستتم استعادة الخدمات أو الاستمرار أو تشكيلها لضمان استمرار عمليات DNS الفاعلة ولحماية المسجلين.

[4] وزارة الأمن الداخلي الأمريكية، ومجلس التنسيق الحكومي لتكنولوجيا المعلومات 2009. تقييم مخاطر الخط الأساسي لقطاع تكنولوجيا المعلومات. واشنطن العاصمة: مكتب الطباعة الحكومي، ص 32-33.

4.2.4. قياس المخاطر والأمن والاستقرار والمرونة

4.2.4.1 لا يوجد في الوقت الحالي اتفاق كبير بشأن التدابير الصحيحة ومستويات الأداء المقبولة بالنسبة للنظام ككل المتصل بالمخاطر والأمن والاستقرار والمرونة. وقد قام المشغلون الفرديين والباحثين المستقلين بقياس الجوانب المختلفة لـ DNS، إلا أنه لم يأتي حتى الآن بجديد في تحديد وتنفيذ المعايير، ونظام المقاييس الواسعة أو مستويات الخدمة المقبولة. كما أنه يجب بذل الجهود لتحسين إدارة المخاطر المتعلقة بأمن واستقرار ومرونة DNS ويجب توجيهها بالقدرة المحسنة على قياس هذه الخصائص وتقييم جدوى البرامج والاستثمارات في الموارد.

4.2.4.2 يكون المحفز الأساسي لتحسين هذه الحالة بمثابة ضمان لتجهيز وقياس تركيب أجزاء DNS بشكل صحيح. وقد قدم فريق دراسة خادم الجذر 2009 (RSST) تقريرا عن تحجيم الجذر (http://www.icann.org/en/committees/dns-root/root-scaling-study-report-31aug09-en.pdf) يدعو إلى "إنشاء آليات فعالة للكشف عن المخاطر وتخفيفها لأنها أصبحت واضحة" وذلك فيما يتعلق بنظام خادم الجذر. كما أن إنشاء المقاييس والأدوات لا يشكل طرحا لبعض التحديات الهامة. وعلى وجه التحديد طالبت طبيعة توزيع DNS بنموذج تعاوني قياسي، يطالب بالمشاركة الفاعلة المتعددة للمشاركين والمنظمات. وأن موضوع نظم التحذير المبكر بالإنترنت يجري دراستها دراسة مختلفة، بما في ذلك الشبكة الأوروبية ووكالة أمن المعلومات (ENISA)، التي تجري أول ورشة عمل حول نظام التحذير المبكر بالإنترنت في مارس عام 2010 (http://www.enisa.europa.eu/events/ee/ EWNI2010). وقد عقدت ICANN، بالاشتراك مع جامعة كيوتو، الندوة العالمية الثانية لأمن واستقرار ومرونة DNS في فبراير من عام 2010، مع التركيز بصفة خاصة على القياس. وتهدف ICANN إلى التشجيع والمشاركة في الأنشطة التي من شأنها تحسين حالة تفهم كيفية قياس مخاطر DNS وصحة وأمن واستقرار ومرونة النظام كحافز أساسي لوضع تقييم المخاطر الفعالة، والتخطيط للطوارئ/والممارسات وقدرات الرد.

5. المبادرات الاستراتيجية

5.1 تتناول المبادرتين المعروضتين هنا تلبية الاحتياجات الهامة لوضع الإمكانات اللازمة لهيئة الإنترنت ICANN لتلبية الأمن والاستقرار والمرونة التي تم تحديدها في وقت سابق. كما تم الطرح في البداية، فإن هذه الوثيقة تهدف إلى توفير أساس لمناقشة أصحاب المصلحة المتعددين لهذه المبادرات المقترحة، ومسؤوليات ICANN في إنشاء قدرات مقترحة، وكيف يمكن للمجتمع المضي قدما في تنظيم الجهود الرامية إلى دعم هذه المبادرات. وقد تم تحديد الموظفين والآثار المترتبة على الموارد، إلا أن تمويل البدائل اللازمة لهذه المبادرات لم يجري تحليله. ولا تفترض هذه الوثيقة تمويل ICANN أو توفير موظفين لهذه المبادرات.

5.2 جدير بالذكر أن المبادرة 2 فيما يتعلق بالحاجة إلى إنشاء DNS-CERT يرد تقديمها بمزيد من التفصيل في DNS-CERT والذي يرافق هذه الوثيقة.

5.1 المبادرة 1- تحليل مخاطر DNS على نطاق النظام والتخطيط للطوارئ والممارسة

5.1.1 تتعاون ICANN مع مجتمع DNS من أجل فهم المخاطر الرئيسية المتعلقة بـ DNS، بما في ذلك تحليل التهديدات والمخاطر الناشئة على النحو المطلوب في التأكيد على الالتزامات. وبمجرد تحليل هذه المخاطر، فإنه يجب تحديد مجتمع DNS لاستمرار أكبر مصدر للقلق من أمن واستقرار ومرونة DNS وضمان إتاحة جهود التخطيط للتخفيف من المخاطر التي تم تحديدها. وترى ICANN بأن لها دورا هاما في تمكين نظام التخطيط للطوارئ والتدريبات كجزء من مسؤولياتها في إطار التأكيد على الالتزامات. وسوف يكمل مثل هذا البرنامج الإستباقي قدرات الاستجابة التي يمكن أن يقدمها DNS-CERT بالإضافة إلى الاستفادة من هذه المنظمة كمركز طبيعي لدعم التخطيط للطوارئ وممارسة الرياضة.

5.1.2 الجانب الأول من هذه المبادرة من شأنه أن يشكل النهج المجتمعي لتحليل المخاطر التي تتضمن قبول إطار مخاطر DNS وتكرير المنهج لقياس المخاطر. وسوف يشمل هذا الجهد إقامة نهج لإجراء تقييمات لمخاطر DNS العادية ومقترحات التخفيف من الحدة. ومن شأنه أن يبني على العمل لعام 2010 فيما يتعلق بأمن واستقرار ومرونة DNS وكذلك الجهود التي يبذلها DNS-OARC وENISA وغيرها.

5.1.3 يوجد جانب آخر من جوانب هذه المبادرة يهدف إلى تعزيز التعاون على صعيد المجتمع المحلي للتخطيط في حالات الطوارئ واستخدام ذلك كأساس لتوجيه الجهود الرامية إلى إنشاء قدرات الاستجابة. وينبغي أن يبدأ أساس التخطيط للطوارئ من التوافق في الآراء حول إطار مخاطر DNS على نطاق المنظومة التي تحدد أهمية المخاطر لـ DNS والسيناريوهات الرئيسية. ومن ثمّ البناء على الجهود القائمة مثل التي تجرى من خلال الشراكات بين القطاعين العام والخاص والمعنية بحماية البنية التحتية الحساسة للولايات المتحدة مثل مجلس تنسيق قطاع تكنولوجيا المعلومات وENISA، فضلا عن تلك التي تجرى كجزء من المجتمع التنفيذي DNS مثل DNS-OARC وNL Net Labs. كما تتوخى هذه المبادرة المقترحة التنسيق الوثيق مع نشوء نظام الخادم الأساسي وآلية تبادل المعلومات مع المشغلين على نطاق مستوى التسجيل TLD. وأن تحليل المخاطر والاحتمالات الرئيسية يمكن استخدامها لتقييم مدى كفاية آليات الاستجابة الحالية، وذلك لتحديد العجز الذي يتطلب اتخاذ إجراءات، وعلى وضع خطط طوارئ لحالات الطوارئ المحددة. ومن ثمّ يجب دعم الجهود من جانب خبير على نطاق المجتمع المحلي/مجموعة العمل. وتتولى ICANN مسؤولية دعم الفريق ووضع خطة عمل لاستعراض المجتمع والتي من شأنها أن تشكل مدخلا لدورة ICANN السنوية للأمن والاستقرار والمرونة التشغيلية والتخطيط للميزانية.

5.1.4 بمجرد إجراء التخطيط للطوارئ، يلزم وجود برنامج ممارسة على نطاق المنظومة DNS بهدف ضمان تقييم القدرة على الاستجابة وتحديد العجز. [5] كما هو الحال مع DNS-CERT وجهود التخطيط للطوارئ، فإن وضع برنامج الممارسة ينبغي أن يبني على الأنشطة القائمة ويتضمن بذل الجهود مثل جهود TLD القائمة للطوارئ كعناصر فرعية لبرنامج أوسع نطاقا. وينبغي أن يتمثل الهدف في بدء برنامج للأنشطة التي تتوج في ممارسة نظام نصف سنوي DNS الذي يركز على الاستجابة لحالات الطوارئ الرئيسية. وبالإضافة إلى ذلك، ينبغي أن يتضمن برنامج للتكامل مع برامج أخرى مثل سلسلة الممارسة الصايبر متعددة الجنسيات وغيرها من الممارسات الدولية المتعددة من أصحاب المصلحة. وكما هو محدد في التأكيد على الالتزامات، تكون ICANN مسؤولية عن دعم المنهج على نطاق المجتمع لمثل هذا البرنامج، وتسهيل العناصر الفرعية للبرنامج حسب الاقتضاء، وتدبير ممارسة DNS على نطاق النظام مرتين سنويا.

5.1.1 الخطوات المحددة والمقترحة

5.1.1.1 إنشاء مجموعة استشارية لخبير تقييم المخاطر والتخطيط للطوارئ DNS. ويجب أن تتألف من خبراء من عمليات DNS ومجتمعات الأمن السايبر. وأن ICANN من شأنها أن تدعم الفريق بمجموعة من الموظفين. وينبغي أن ينصب التركيز الأولي للفريق على إقامة إطار مقبول لدى المجتمع لمخاطر DNS التنظيمية وتحديد الأخطار الحالية الرئيسية بحلول الربع الثالث من عام 2010. وبالإضافة إلى ذلك، فإن المجموعة ستبني على العمل من DNS SSR 2010 حول المقاييس لإنشاء أطر مقبولة لدى المجتمع لقياس الصحة والأمن والاستقرار والمرونة لـ DNS بحلول أوائل 2011. وستكون المجموعة مسؤولة أيضا عن إنشاء خط أساسي للتخطيط للطوارئ بحلول الربع [2] من عام 2011. وستجري المجموعة تقريرا سنويا بمخاطر DNS والتخفيف منها مع التقرير الأول ليتم تسليمها في الربع [3] من عام 2011.

5.1.1.2 إنشاء آلية لتبادل معلومات الجذر DNS التي من شأنها أن تكون جهدا تعاونيا بالاشتراك مع مجتمع مشغل خادم الجذر وغيرهم من المعنيين بمجتمع خادم الجذر على أساس التوصيات لعام 2009 ودراسة قياس الجذر. وسوف تشكل مجموعة العمل بدعم من فريق ICANN لتحديد الاحتياجات الفنية ومراقبة الأداء. على أن تشمل القدرات الرئيسية اكتمال نمذجة نظام جذر DNS وتبادل المعلومات المحسنة بين المنظمات المشاركة في نظام الجذر، ونشر إمكانية أجهزة الاستشعار اللازمة، والدعم التحليلي لتقييم الصحة الحالية لنظام الجذر DNS وتقديم إنذار للمشكلات الناشئة. وسوف تبذل الجهود للعمل مع المجتمع على تنفيذ ونشر أجهزة استشعار وقياس تلك المقاييس التي من شأنها أن تسمح بنظرة عامة عن خادم الجذر ونظام TLD وطريقة العمل. وسيتطلب هذا الجهد بالتعاون مع مشغلي TLDs ومشغلي خادم الجذر وNTIA وICANN وغيرهم من المشاركين في تشغيل وإدارة البنية التحتية DNS الأساسية. ندرك أن هذا النظام سوف ينشأ بطريقة متآزرة مع تطوير DNS-CERT.

[5] وأن متطلب هذا البرنامج لـ DNS يتم تبينه على وجه التحديد في تقييم مخاطر قطاع تكنولوجيا المعلومات DHS.

5.1.1.3 التخطيط وممارسات الطوارئ للدعم المستمر لمشغلي خادم الجذر. وعقب الاتصالات الناجحة وممارسة الجدول الأولي الأعلى بحلول النصف الثاني من عام 2010، تخطط ICANN إلى العمل مع المشغلين لتشكيل نهج برنامجي للتخطيط للطوارئ والممارسات القائمة على السيناريوهات. تقوم ICANN بنشر إمكانيات الاتصالات، التي من شأنها أن تكمل وتعزز من الأنظمة الحالية التي تستخدمها في عملياتها الخاصة بجذر الخادم.

5.1.1.4 النضج المستمر لممارسات والتخطيط للطوارئ TLD. يعتمد مشغلو ICANN وسجل TLD لإجراء اختبارات لبيانات الضمان عام 2010 وحتى 2011 على تطور مواصفات البيانات لعملية النطاق الأعلى العام الجديد (gTLD). ويتم التخطيط لتدريبات إضافية مع التركيز على الاتصالات وعناصر الاستجابة اللازمة بين ICANN ومشغلي سجل TLD.

5.1.1.5 البدء في تطوير برنامج ممارسة DNS والتقييم. يشتمل مثل هذا البرنامج على حشد الجهود الحالية والذي يتطلب المشاركة من جانب طائفة واسعة من أصحاب المصلحة بما فيها تلك التي تشارك في عمليات DNS ومقدم خدمة DNS ومجتمعات المستخدمين ومجتمع أمن السايبر الأوسع. وهذا البرنامج من شأنه أن ينطوي أيضا على فهم والاستفادة من التفاعل مع أمن السايبر وما يرتبط بها من ممارسة أخرى وبرامج التقييم. وبحلول نهاية عام 2010، فإن هذا الجهد من شأنه تقييم طبيعة ومدى كفاية الجهود القائمة وتحديد الفجوات الرئيسية. وبحلول منتصف عام 2011، يتم وضع ورقة عمل برنامج ممارسة DNS المقترح لاستعراض المجتمع. بالإضافة إلى ذلك، ترعى ICANN نظام محدود من الممارسة في النصف الثاني من عام 2011 باعتباره نموذجا أوليا مع المشاركة الطوعية عبر مجموعة من أصحاب المصالح التي تهدف إلى إقامة تخطيط طويلة الأجل وعمليات تنفيذ. وسوف تبدأ الممارسة لتخطيط هذا النموذج في عام 2010. ومن ثمّ مشاركة فريق CANNI وغيره من أعضاء مجتمع DNS في العملية الثالثة للسايبر متعددة الأطراف وربما أيضا المشاركة في العمليات الدولية الأخرى.

5.1.2 عرض الموارد

5.1.2.1 عرض الحاجة إلى الخمس وظائف لفريق العمل الدائم:

- كبير المنسقين وتقييم المخاطر والتخطيط للطوارئ وبرنامج التدريب
- منسق التخطيط للطوارئ
- منسق برنامج التقييم
- مخطط العملية
- محلل النظم/خبير النمذجة ونظام تبادل معلومات الجذر

5.1.2.2 تشمل متطلبات الدعم تعريف المتطلبات لتبادل نظام خادم الجذر وتقديم الدعم لتحليل المخاطر وجهود تبادل معلومات خادم الجذر والبنية التحتية والتكاليف المرتبطة بها لتشمل التراخيص ودعم البرمجيات ومعدات دعم النمذجة وتبادل معلومات نظام جذر الخادم ونظم الاتصالات ونشر النموذج لنظام الاستشعار والسفر وتكاليف الاجتماعات لمجموعات العمل والموظفين والمرافق المادية ودعم تكنولوجيا المعلومات لموظفين إضافيين.

5.1.2.3 يتوقع إجمالي التكاليف لدعم هذا الجهد من يوليو 2010 إلى يونيو عام 2011 بما يقرب من 1.25 مليون دولار أمريكي للموظفين و850,000 دولار أمريكي للحصول على الدعم. وأن الإجمالي المتوقع في السنة الأولى من حيث التكلفة السنوية لهذه المبادرة سوف يكون 2.1 مليون دولار أمريكي.

5.1.2.4 **الافتراضات:** تحليل المخاطر من شأنه أن يزيد من تهديد المعلومات والتحليل DNS-CERT. كما أن نظام تبادل معلومات جذر الخادم من شأنه التأثير على منفذ الويب 2.0 المتقدمة لـ DNS CERT لدعم تبادل المعلومات.

5.2 المبادرة 2 - DNS-CERT

5.2.1 بالإضافة إلى التقييم الإستباقي للخطر والتخطيط للطوارئ والممارسة، فإن مجتمع DNS يحتاج إلى قدرات في الرد فعالة وتشغيلية على نطاق النظام لمعالجة تحديات الأمن والاستقرار والمرونة. وقد تم التنسيق على نطاق واسع للهجوم على DNS والذي يمكن أن يؤدي إلى تداعيات اقتصادية وسياسية كبيرة، ومع ذلك لا توجد نقطة مركزية

5.2.2 تعمل DNS-CERT على تنسيق الجهود الحالية مع مجتمع DNS للحفاظ على الوعي بالأوضاع العامة للمجتمع بحيث يمكن الوصول إلى الخبرة الصحيحة في أي وقت. وأن أصحاب المصلحة الرئيسيين لمثل هذا الجهد من شأنهم أن يكونوا مشغلين DNS ومستخدمين وبائعين وباحثين في مجال الأمن ومستجيبين لما هو طارئ. وأن DNS-CERT من شأنها التأثير على عدد من الجهود الحالية التي تسعى إلى تحديد التهديدات وتبادل المعلومات وتسهيل الاستجابة عبر DNS. ويمكن أن تساعد أنشطة DNS-CERT في التعاون والمساعدة في تنسيق هذه الجهود وتوفير الخدمات في المناطق غير المشمولة حاليا أو مع الجهات المعنية التي لم تشارك في هذه الجهود. ويمكن إطلاق DNS-CERT مع دعم ICANN، إلا أن الهيكل التنظيمي المحدد ونموذج الموارد سيتم تحديده من خلال الحوار مع المجتمع. وفي هذا الصدد، فإن الإشراف على DNS-CERT من شأنه القيام به من جانب مجلس قائم على المساءلة أمام CERT، فضلا عن تقييم أنشطة DNS-CERT القائمة على أساس احتياجات أصحاب المصلحة التي تخدمها المنظمة. وسوف يشرف على العمليات التي يقوم بها DNS CERT فريق أساسي من الموظفين الإداريين والفنيين بمساعدة فريق كبير من الخبراء قادرين على تقديم دعم ملموس لـ DNS-CERT عند العمل في نطاق متباعد جغرافيا.

5.2.3 توفر DNS-CERT خدمات إستباقية (تحليل التهديدات وفاعلية DNS ورصد الأمن وحالة الوعي وتبادل المعلومات) وكذلك الخدمات التفاعلية (التي تكون 365 × 24 × 7 نقطة اتصال، وتنسيق التعامل مع الحادث، وضعف الدعم الإداري والخدمات الاستشارية الأمنية) لأعضائها. ومن ثمّ فإن هذا النهج هام لسببين: (1) المعلومات الخاصة بطبيعة التهديد الإستباقية يمكن أن تساعد مجتمع DNS للتخطيط لمواجهة التهديدات من خلال التدريب والممارسة، و(2) خدمات التعامل مع الحادث يمكن أن تساعد مع قيود الموارد الكبيرة، مثل المسجلين في المناطق الأقل نموا في العالم. كما تقدم معلومات التهديد والتحليل الإنشاء المتصور لتحديد مخاطر DNS النظامية وقدرات التحليل الموضحة في المبادرة 1. يحدث تعريف المتطلبات الوظيفية للقدرات الأساسية التي تقدمها DNS-CERT من خلال التحليل للمنظمات المجتمعية الذي ينطوي على تحليل أصحاب المصلحة والمتعاونين المحتملين لـ DNS-CERT.

5.2.2 عرض الموارد

5.2.2.1 بناءا على تقييم فرق CERT الداخلية ذات حجم مماثل وعلى قدر من المسؤولية، نعتقد أن DNS-CERT يمكنها أن تعمل منذ البداية بميزانية سنوية للموظفين لما يقرب من 15 شخصا بما يشمل المدير واثنين من كبار المديرين وفريق إدارة الحوادث مكون من عشرة أشخاص وإدارة شؤون الموظفين/والدعم القانوني. وأن التكلفة المتوقعة للموظفين تبلغ 2.6 مليون دولار أميركي. وتقدر تكاليف الدعم لسفر الموظفين والاتصالات وأدوات التحليل والمرافق المادية ودعم تكنولوجيا المعلومات تقدر بمبلغ 1.6 مليون دولار أميركي. وأن التكلفة الإجمالية المقدرة للسنة الأولى لهذه المبادرة تبلغ 4.2 مليون دولار أميركي. يرد مزيد من التفصيل في ملف DNS-CERT الذي يرافق هذه الوثيقة.

6. الخلاصة

تزداد تحديات الأمن والاستقرار والمرونة التي تواجه DNS. وتتمتع ICANN بمسؤوليات كبيرة في ظل نظامها الداخلي والتأكيد على الالتزامات للعمل مع مجتمع DNS لمواجهة تلك التحديات. وعلى وجه التحديد، يطلب إنشاء DNS على نطاق المنظومة والتخطيط للطوارئ وقدرات الاستجابة التعاونية. وتقدم هذه الوثيقة العامة أساسا للمناقشة بين أصحاب المصلحة المتعددين لهذه المبادرات المقترحة لتلبية هذه الاحتياجات.