سياسة أمن البنية التحتية للحزمة العريضة

وزارة الاتصالات وتكنولوجيا المعلومات

يوليو 2014

Document Reference

قائمة المحتويات

تعريف المصطلحات والاختصارات

- **روبوت الكمبيوتر**: او "البوتنتس" مجموعة من أجهزة الكمبيوتر المعرضة للخطر والمتصلة بالإنترنت، والتي تدار عن بعد
- **بي جي بي**: البروتوكول الذي يدعم قرارات تحديد المسارات على الإنترنت، وهو محدد في آر اف سي-4271.
- **بي سي آي**: معهد استمرارية الأعمال.
- **الحزمة العريضة**: مدخل إلى الإنترنت يوفر قدراً اكبر من الحزمة العريضة بالمقارنة مع وسائل التقليدية للدخول بواسطة الاتصال.
- **البنية التحتية للمعلومات الحساسة**: مجموعة من أنظمة تقنية المعلومات والاتصالات، والخدمات وأصول البيانات، والتي تدعم البنية التحتية الوطنية لقطر.
- **سي سي تي ال دي (CcTLD)**: رمز البلد لنطاقات المستوى الأعلى، مثل qa.
- **دي ان اس (DNS)**: نظام اسم المجال هو نظام تسميات موزعة هرمياً لأجهزة الكمبيوتر أو الخدمات أو اي مصدر متصل بشبكة.
- **دي آر آي آي: (DRII)**: المعهد الدولي لمواجهة الكوارث.
- **هجوم دي دي أو اس (DDoS):** محاولة لجعل كمبيوتر أو مورد إنترنت غير متاح للمستعملين المراد لهم استخدامه أو لأداء وظيفة بعينها.
- **مزودو خدمة الاستضافة**: جهات تجارية تقدم خدمات استضافة مواقع إلكترونية لشركات أو مؤسسات أخرى أو أفراد.
- **آيزو**: المنظمة العالمية للمعايير.
- **إيكان (ICANN)**: منظمة عالمية غير ربحية مسؤولة عن تنسيق أنظمة إنترنت أساسية ذات خصائص متميزة، ومن أبرزها نظام اسم المجال (DNS).
- **مزود خدمة الإنترنت:** شخص مرخص لتقديم واحدة أو اكثر من خدمات الاتصالات إلى الجمهور أو مرخص لامتلاك أو إنشاء أو تشغيل شبكة اتصالات لتقديم خدمات اتصالات للجمهور. ويشمل ذلك مزودي المعلومات أو المحتوى باستخدام شبكة اتصالات.
- **ام آي سي تي (الوزارة):** وزارة الاتصالات وتقنية المعلومات.
- **البرمجيات الخبيثة**: محتويات خبيثة مثل نصوص مضرة أو قطع رموز يمكن أن تتسبب في الإضرار بالتشغيل العادي للإنترنت أو الأصول و/أو جهات الاستعمال التي تعتمد على الحزمة العريضة.
- **NIAP 2.0:** السياسة الوطنية لضمان المعلومات الإصدار 2.0 والصادرة من الوزارة.
- **اس بي سي (SBC)**: الضوابط الحدية للحلقات هي نبائط يتم نشرها بانتظام في شبكات بروتوكول ربط المحادثات الصوتية عبر الإنترنت (VoIP) للتحكم في الإشارات المنتشرة على الحدود بين شبكتين لتزويد الخدمة في بيئة تواصل مباشر.

1. *التفويض القانوني*

وفقاً للمادة 14 من القانون رقم 16 لعام 2014 والذي يحدد صلاحيات وزارة الاتصالات وتكنولوجيا المعلومات (يشار إليها فيما يلي باسم "الوزارة") فإن الوزارة تملك صلاحية الإشراف على قطاعي تكنولوجيا المعلومات والاتصالات وتنظيمهما وتطويرهما في دولة قطر على نحو يتوافق ومتطلبات أهداف التنمية الوطنية، وذلك بهدف خلق بيئة ملائمة للتنافس الشريف، ودعم تنمية هذين القطاعين وتنشيط الاستثمار فيهما، وتأمين وتعزيز فعالية البنية التحتية للمعلومات والتكنولوجيا، وتنفيذ برامج الحكومة الإلكترونية والإشراف عليها، وتعزيز الوعي المجتمعي بأهمية تكنولوجيا المعلومات والاتصالات في تحسين حياة الأفراد والمجتمعات وبناء مجتمع قائم على المعرفة واقتصاد رقمي.

وتحدد المادة 14 من القرار الأميري رقم 27 لعام 2014 دور وزارة الاتصالات وتكنولوجيا المعلومات بحماية أمن البنية التحتية للمعلومات الحيوية للدولة وذلك باقتراح وإصدار السياسات والمعايير والتأكد من الالتزام بها.

تم إعداد سياسة أمن البنية التحتية للحزمة العريضة وفقاً للقوانين السارية حالياً في دولة قطر. وفي حالة وجود تضارب بين هذه الوثيقة وقوانين دولة قطر يؤخذ بقوانين دولة قطر. وفي هذه الحالة يهمل ذلك النص المتضارب الوارد في وثيقة السياسة إلى الحد الذي يزيل التضارب وتظل باقي محتويات الوثيقة سارية المفعول. ويتعين بعد ذلك إجراء تعديلات لضمان التقيد بالقوانين السارية المفعول في دولة قطر.

2. مقدمة

إن دور البنية التحتية للحزمة العريضة في دعم الاقتصاد وفي مجال نقل المعلومات والتعليم والترفيه دور مشهود. وفي ظل الزيادة المطردة في الهجمات المتطورة على البنى التحتية للإنترنت على نطاق العالم، ومن أجل المحافظة على جودة هذه الخدمة الحيوية، أصبح لزاماً على الحكومة ومزودي الخدمات الاتفاق على الأسس التي تضمن بقاء البنية التحتية للإنترنت في دولة قطر سالمة وآمنة ومتماسكة.

إن أمن البنية التحتية للحزمة العريضة مجال يحظى بأهمية فائقة، وهو من الاتساع والضخامة بمكان، غير أن هذه الوثيقة تتناول فقط المسائل ذات الصلة المباشرة باحتياجاتنا الحالية.

إن الغرض من هذه السياسة الخاصة بأمن البنية التحتية للحزمة العريضة هو ضمان أن البنية التحتية للحزمة العريضة المتوفرة في قطر تفي بمتطلبات المجتمع ككل وأن مزودي الخدمات لديهم إرشادات واضحة بشأن ما هو متوقع منهم. ولهذا فهذه الوثيقة تهدف لتحقيق وإبراز الأهداف التالية:

1. رفع مستوى الثقة في خدمات الحزمة العريضة ومستوى استخدامها من قبل المجتمع بأسره، وذلك من خلال جهد فعال لضمان مستوى عالٍ من التوفر والتماسك.
2. مساعدة مزودي خدمة الإنترنت ومزودي خدمات الاستضافة (المزودين) على تقديم خدماتهم بطريقة آمنة.
3. رفع مستوى الأمن وضمان الخصوصية في البنية التحتية للإنترنت

والمبدأ الأساسي الذي يحكم هذه السياسة هي:

- تهيئة الأساس لبنية تحتية وخدمات إنترنت تتميز بالمرونة والتماسك السلامة والأمان

ملاحظة: وثيقة السياسة هذه تحل محل الإرشادات التي سبق نشرها (إرشادات أمن البنية التحتية للإنترنت) في مايو 2013

3. النطاق والتطبيق

تطبق هذه الوثيقة على:

- مزودي خدمة الإنترنت الذين يعملون في دولة قطر
- المنظمات التي تقوم بنشر البنيات التحتية للحزمة العريضة "مثل FTTH" والخدمات "مثل استضافة المواقع الإلكترونية"
- مزودي خدمات الاستضافة الذين يعملون في دولة قطر
- الأقسام التابعة للوزارة التي تقوم بدور تشغيلي متعلق بالبنية التحتية للإنترنت، مثل DNS (نظام اسم المجال) أو ccTLDs (رمز البلد لنطاقات المستوى الأعلى)

4. *أمن البنية التحتية لمزودي خدمة الإنترنت ومزودي خدمات الاتصالات الاخرى*

4.1. يجب على **مزودي خدمة الإنترنت ومزودي خدمات الاتصالات الاخرى** تنفيذ برامج إدارة استمرارية الأعمال حسب وثيقة **[NIAP 2.0]** القسم 9 أو أي ممارسة عالمية مشابهة مثل **ISO** 22301، أو **DRI** أو ممارسات **BCI.**

4.2. على **مزودي خدمة الإنترنت ومزودي خدمات الاتصالات الاخرى** التأكد من أن الخدمات الخاصة بشبكات البنية التحتية للإنترنت (التصميم والمكونات) والخدمات التكنولوجية المتعلقة بها تعتمد أفضل الممارسات المطبقة لدى الموردين فيما يتعلق بأمن المعلومات والتعامل مع الأزمات والتوفر العالي.

4.3. على **مزودي خدمة الإنترنت ومزودي خدمات الاتصالات الاخرى** تطبيق ضوابط (أمن المنتج) المذكورة في وثيقة **[NIAP 2.0]** القسم 5 والتي تنص على ضوابط مستقلة لتقييم التكنولوجيا والتحقق من استيفاء المسائل الأمنية للمكونات الرئيسية للبنية التحتية للحزمة العريضة مثل المفاتيح الرئيسية، والموجهات القاعدية، وأنظمة اسماء المجالات وبوابات الإنترنت.

4.4. على **مزودي خدمة الإنترنت ومزودي خدمات الاتصالات الاخرى** تطبيق ضوابط (أمن التشفير) المذكورة في وثيقة **[NIAP 2.0]** القسم 10 "حيثما كان ذلك ممكناً من ناحية فنية" والإرشادات المطبقة عالمياً ولدى الموردين بشأن تشديد الضوابط الأمنية والممارسات العالمية للمكونات الرئيسية للبنية التحتية للحزمة العريضة مثل المفاتيح الرئيسية، والموجهات القاعدية، وأنظمة اسماء المجالات وبوابات الإنترنت.

4.5. على **مزودي خدمة الإنترنت** التأكد من تنوع البنية التحتية للتشبيك الرئيسي، باستخدام تقنيات من موردين مختلفين، لتجنب الانغلاق على مورد واحد كلما أمكن ذلك.

4.6. على **مزودي خدمة الإنترنت ومزودي خدمات الاتصالات الاخرى** تطبيق آليات مراقبة الأنظمة، وتغيير التحكم والتسجيل وفق أفضل الممارسات المذكورة في وثيقة **[NIAP 2.0]** القسمين 10 و11 على المكونات الرئيسية للبنية التحتية للحزمة العريضة.

4.7. على **مزودي خدمة الإنترنت ومزودي خدمات الاتصالات الاخرى** التأكد من أن المساندة والصيانة التي تتم من خارج دولة قطر تخضع للمراقبة والتسجيل، بما في ذلك الاتصالات المساندة.

4.8. على **مزودي خدمة الإنترنت ومزودي خدمات الاتصالات الاخرى** تطبيق تقنيات الكشف والمنع لضمان أن تغذيات الإنترنت للعملاء تتمتع "بأكبر قدر ممكن" من الحماية ضد الحركة الضارة مثل هجمات **دي دي او اس وأنشطة روبوت الكمبيوتر.**

4.9. على **مزودي خدمة الإنترنت** التأكد من أن أجهزة التشبيك التي يتم تركيبها للمستعملين في المنازل تمت مواءمتها/تقويتها وفق أحدث أفضل الممارسات الأمنية المتاحة في تاريخ تقديمها وأنها لا تحتوي على ثغرات يمكن أن تهدد خصوصية المستعملين.

4.10. يجوز للوزارة إعداد كتيب للإرشادات الفنية والتي يمكن طلبها عبر الموقع الإلكتروني http://www.qcert.org/contact-us

5. *أمن مسار الحزمة العريضة*

5.1. على **مزودي خدمة الإنترنت** استخدام الروابط المعتمدة لبروتوكول بوابات الحدود الخارجية كلما كان ذلك ممكناً فنياً عن طريق الاتصال المباشر بدون خادم. ينبغي على مزودي خدمات الإنترنت ايضاً تفضيل الاعتماد التحقق في الروابط الداخلية لبروتوكول بوابات الحدود الخارجية

5.2. على **مزودي خدمة الإنترنت** التأكد من قيامهم بعمل تواصل مباشر بين الأجهزة لضمان مرونة تغذية الإنترنت. يجب على **مزودي خدمة الإنترنت** التأكد من عدم وجود نقط إخفاق مفردة (منطقية او فعلية) من المزودين الرئيسيين، مثلاً، عن طريق التأكد من أن المسارات إلى المزودين الرئيسيين ونقاط الإنترنت متنوعة جغرافياً ومنطقياً.

6. *خدمات اسم المجال*

6.1. يجب على ملاك ومشغلي خوادم **الوزارة ومزودي خدمة الإنترنت** الخاصة بالمجالات العليا لمفتاح البلد والخوادم الخاضعة للرعاية/ والخوادم العامة غير الخاضعة للرعاية للمجالات العليا لمفتاح البلد :

أ. التأكد من عدم وجود نقطة إخفاق مفردة في خدمتهم

ب. قصر دخول الإدارة على ماكينة محلية آمنة، ولا يسمح بالدخول عن بعد

ج. تطبيق سياسات صارمة بشأن كلمة السر لكل الأجهزة الرئيسية حسب ضوابط AM 19-22: [**NIAP 2.0**]

د. انشاء سجلات تسجيل للدخول للنظام وادارة التغيير لستة أشهر على الأقل

هـ. استخدام خوادم ذات ضوابط أمنية مشددة تتم صيانة أمنها بصورة جادة وبانتظام حسب أفضل ممارسات المورد

و. التوقيع الرقمي على ملفات مناطقهم

ز. استخدام نظام مشفر للتحقق من أصل و سلامة بيانات نظام اسم المجال

ح. استخدام نظام تحقق مشترك للتشفير وسلامة بيانات النقل بين المناطق والتحديثات الديناميكية.

الضوابط أعلاه هي محاولة لضمان مرونة وتماسك وأمن خدمات نظام اسم المجال في قطر، وهي متوافقة مع الأجندة الأمنية لمنظمة إيكان (**http://www.icann.org/en/groups/ssac/dns-security-update-1.htm**); والقراءات الفنية المساندة (**http://www.icann.org/en/groups/ssac/reading**).

6.2. مهام التشفير المتعلقة بالفقرة 6.1 (و) أو (ز) أو (ح) أعلاه يجب أن تستخدم نموذج أمن أجهزة لكل من التحكم بالمفاتيح ومعالجة الشفرات حسب **NIAP 2.0** the القسم 10.

6.3. على **مزودي خدمة الإنترنت** الذين يقدمون خدمات أسماء المجالات المتكررة:

أ. استخدام خوادم ذات ضوابط أمن مشددة تتم صيانتها بصورة جادة

ب. التأكد من أن الخدمات تقدم فقط للمستخدمين المصرح لهم (أي ليس تكراراً مطلقاً)

7. استضافة البرمجيات الخبيثة

7.1 على **مزودي خدمة الإنترنت ومزودي خدمات الاتصالات الاخرى** بذل جهودهم للتأكد من عدم استضافة وعدم تخزين وعدم توفر البرمجيات الخبيثة في قطر.

7.2 على **مزودي خدمة الإنترنت ومزودي خدمات الاتصالات الاخرى** التأكد من أن إرشاداتهم الخاصة بالاستضافة (أو ما شابهها) تتضمن النصوص التالية:

7.2.1 لا يسمح بأي محتوى يتضمن رمزاً خبيثاً قابلاً للتطبيق

7.2.2 لا يسمح بأي محتوى يوجه المستعملين إلى خوادم خبيثة معروفة

7.3 إذا نما لعلم الوزارة أن أحد **مزودي خدمات الاستضافة** يقوم باستضافة برمجيات خبيثة مخالفاً نص القسم 7 من هذه الوثيقة، يجوز للوزارة، بعد التحقيق في الأمر، أن تصدر للمزود إشعاراً كتابياً بالتفكيك. ويجب على **مزود خدمة الاستضافة** و/أو **مزود خدمة الإنترنت** أن يقوم، عند استلام إشعار التفكيك، بإزالة البرمجيات الخبيثة المعنية أو حظر الخادم (الخوادم) المتعلقة بها، أو إخراجها خارج الشبكة، في أسرع وقت ممكن ولكن بما لا يتجاوز أربع وعشرين (24) ساعة من وقت استلام الإشعار كحد أقصى.

8 التصدي للأنشطة الضارة

8.1 على **مزودي خدمات الاستضافة** التأكد من أن أجهزة المستخدمين النهائيين، الموجودة داخل دولة قطر، والتي تقوم بشن هجمات مستمرة ضد الأهداف التالية، يتم حظرها على الفور من الإنترنت:

8.1.1 البنية التحتية للإنترنت في قطر، بما في ذلك:

8.1.1.1 الهجوم على خوادم الاسم qa. (خوادم المستوى العليا لرمز البلد) وخوادم الأسماء الخاضعة للرعاية أو العامة غير الخاضعة للرعاية

8.1.1.2 الهجمات المتعلقة ببروتوكول تحديد المسارات (بي جي بي)

8.1.1.3 الهجمات على مسارات البنية التحتية/الرئيسية أو البنية التحتية لتقديم الخدمة، بما في ذلك الضوابط الحدية للحلقات لربط المحادثات الصوتية عبر الإنترنت **(VoIP)**

8.1.1.4 البوابات العالمية للإنترنت

8.1.2 منظمات البنية التحتية للمعلومات الحساسة كما هي معرفة في مسودة قانون حماية **البنية التحتية للمعلومات الحرجة**.

8.2 على **مزودي خدمة الإنترنت** التأكد من أنه يتم تنبيه أصحاب أجهزة المستخدمين النهائيين، الموجودة في دولة قطر، والمتصلة بالإنترنت وتنتج حركة خبيثة، (عن طريق الهاتف أو البريد الإلكتروني) بمشكلة البرمجيات الخبيثة. ويجب حظر الأجهزة التي تواصل إنتاج البرمجيات الخبيثة بعد اثنتين وسبعين (72) ساعة من إبلاغ أصحابها، مؤقتاً لحين قيام مستخدم الخدمة بتنظيف الأجهزة. ويجوز لمزودي خدمة الإنترنت إحالة الأجهزة المصابة الخاصة بالمستخدمين النهائيين إلى **http://call.qcert.org/** وهو مركز اتصال أنشأته الوزارة لمساعدة المستخدمين النهائيين على تنظيف أجهزتهم.