وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

# مبادئ الأمن السيبراني التوجيهية لتأمين أجهزة التوجيه اللاسلكية في المنازل والمكاتب الصغيرة

**الإصدار: 1.0**

**المؤلف: قسم إدارة مخاطر الأمن السيبراني**

**تصنيف الوثيقة: عام**

**تاريخ النشر: مارس 2018**

## تاريخ الوثيقة:

| التاريخ | وصف الاصدار | الاصدار |
|---|---|---|
| مارس 2018 | نشر النسخة الاولى | 1.0 |
| | | |

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

# ألمحتويات

## التفويض القانوني:

ينص القرار الأميري رقم (8) لسنة 2016 بشأن تحديد اختصاصات وزارة المواصلات والاتصالات (المشار إليها فيما بعد باسم "الوزارة"") على أن تختص وزارة المواصلات والاتصالات بسُلطة الإشراف على قطاعات تكنولوجيا المعلومات والاتصالات داخل دولة قطر وتنظيمها وتطويرها بطريقة متوافقة مع متطلبات أهداف التنمية الوطنية، بأهداف خلق بيئة مناسبة للمنافسة العادلة ودعم تطوير وتحفيز الاستثمار في تلك القطاعات؛ من أجل تأمين وزيادة كفاءة المعلومات والهياكل الأساسية التكنولوجية وتنفيذ برامج الحكومة الإلكترونية والإشراف عليها، بالإضافة إلى تحسين الوعي المجتمعي بأهمية تكنولوجيا المعلومات والاتصالات لتحسين حياة الفرد والمجتمع المحلي وبناء مجتمع قائم على المعرفة والاقتصاد الرقمي.

وتنص المادة (22) من القانون الأميري رقم (8) لسنة 2016 على دور الوزارة في حماية الهيكل الأساسي للمعلومات الوطنية الهامة عن طريق اقتراح وإصدار السياسات والمعايير وضمان الامتثال.

وقد أُعدت هذه المبادئ التوجيهية مع مراعاة القوانين المعمول بها حاليًا داخل دولة قطر. وفي حالة نشوء أي اختلاف بين هذه الوثيقة وقوانين دولة قطر، تعطى الأسبقية لقوانين دولة قطر. ويُحذف ذلك البند من الوثيقة الماثلة، على أن تظل بقية الوثيقة سارية المفعول بدون التأثير على باقي الأحكام. وعندئذ يجب أن تتم التعديلات الضرورية لضمان الامتثال للقوانين ذات الصلة المعمول بها داخل دولة قطر.

## مقدمة:

تحول الإنترنت على مدار العقد الماضي من كونه سلعة إلى ضرورة لكل منزل في قطر. وتشير الأرقام إلى أن معدل انتشار استخدام المنازل للإنترنت وصل إلى 99%. ومن أجل تحقيق إمكانية الاتصال المذكورة، تُزود منازلنا بأجهزة التوجيه السلكية واللاسلكية.

تُقدم أجهزة التوجيه اللاسلكية المذكورة من مزودي خدمة الإنترنت، وعادةً ما تكون مهيأة مسبقًا وجاهزة للاستخدام. ويتجه المستخدمون النهائيون عادةً إلى بذل جهد قليل لتهيئة تلك الأجهزة أو أداء أي تهيئة إضافية من أجل تأمين أنفسهم بشكل أفضل. حيث قد يرجع ذلك ببساطة إلى عدم معرفتهم بكيفية القيام بذلك أو أن عملية التهيئة تبدو صعبة للغاية.

لسوء الحظ تترك عملية التهيئة الافتراضية لأغلب أجهزة التوجيه اللاسلكية المنزلية الشبكات المنزلية عرضة للهجمات وتقدم قدر قليل من الأمان لها.

مع ظهور إنترنت الأشياء، أصبحت الكثير من المنازل الآن تحتوي على أجهزة منزلية متصلة بالإنترنت مثل الكاميرات وأجهزة التليفزيون والأتمتة المنزلية والثلاجات وأنظمة الترفيه. حيث تتصل تلك الأجهزة بالإنترنت من خلال أجهزة التوجيه اللاسلكية المنزلية المهيأة مسبقًا، ومن ثم يمكن أن تكون عرضة بسهولة لتهديدات الإنترنت. فالحصول على أجهزة توجيه لاسلكية منزلية غير مهيأة بشكل جيد يمنح المهاجم الفرصة للتحكم في الأجهزة المتصلة بالإنترنت في المنازل والقيام بأعمال خبيثة تهدف إما إلى إحداث اضطراب في أسلوب حياتنا أو الكشف عن خصوصياتنا.

تقدم هذه الوثيقة المبادئ التوجيهية حول كيفية تأمين أجهزة التوجيه اللاسلكية المنزلية بشكل أفضل وتقليل الثغرات المتعلقة بأجهزة التوجيه اللاسلكية المنزلية قدر الإمكان. ويسري نطاق هذه الوثيقة على جميع المنازل السكنية/ المسبار الشمسي (سوهو)/ بروتوكول سامبا التي تحتوي على أجهزة توجيه لاسلكية منزلية مقدمة من مزودي خدمة الإنترنت.

## الجمهور:

ملاك المنازل والمكاتب الصغيرة في دولة قطر والموظفين العاملين على تركيب أجهزة التوجيه اللاسلكية الجديدة في المنازل والمكاتب الصغيرة.

## فهم المخاطر:

توفر معظم أعمال التهيئة الافتراضية لأغلب أجهزة التوجيه اللاسلكية المنزلية القليل من الحماية. ويمكن الوصول إليها عبر الإنترنت، واكتشافها بسهولة، بالإضافة إلى ضعفها نتيجة سوء تهيئتها وعادةً ما تكون قيد التشغيل في جميع الأوقات. وتقدم مجموعة العناصر المذكورة للمهاجم ثغرات يمكن استغلالها على النحو الأمثل.

علاوة على ذلك، تستغل البرمجيات الخبيثة أعمال التهيئة الافتراضية للنشر والتكرار في جميع أنحاء الإنترنت، ومن ثم تتم تهيئة الأجهزة المصابة بتلك البرمجيات كجزء من برمجيات البوت نت وتستخدم لتسهيل النشاط السيبراني الخبيث الذي ينتهك الحدود.

## المبادئ التوجيهية:

فيما يلي قائمة غير حصرية بالخطوات التي يمكن أن يتخذها المستخدم لتحسين أمن أجهزة التوجيه اللاسلكية المنزلية للحد من احتمالية تعرض الشبكات الداخلية للخطر من أصحاب النوايا الخبيثة:

1. **تغيير معرف مجموعة الخدمات الافتراضي لشبكات الاتصال اللاسلكي (واي فاي):** معرف مجموعة الخدمات هو اسم الشبكة اللاسلكية الخاصة بجهازك، وهو الاسم الذي تراه عند محاولة الاتصال بشبكة لاسلكية على جهازك. وبشكل غير تقليدي، تحتوي أجهزة التوجيه اللاسلكية المنزلية على معرف مجموعة الخدمات الافتراضي خاص بالمصنع لتحديد تصنيع وطراز الجهاز في الواقع. ويمنح ذلك المهاجم المعلومات اللازمة لتحديد نقاط الضعف المتعلقة بجهاز التوجيه اللاسلكي المنزلي الخاص بك.
   أ- **وضع معرف مجموعة خدمات عام (المنزل، المكتب...إلخ)** لا يحدد مالك الجهاز. ويعد معرف مجموعة الخدمات الذي ينشر اسم منازل أو شركات بارزة أكثر جاذبية للمهاجمين من الأسماء العامة.
2. **تشفير الحركة اللاسلكية باستخدام نظام الوصول إلى الشبكات اللاسلكية – بمعيار التشفير المطور (WPA2-AES):** يعد نظام الوصول إلى الشبكات اللاسلكية – بمعيار التشفير المطور أكثر الخيارات أمانًا التي يمكن استخدامها للحماية من رؤية المهاجمين لحركتك على الإنترنت. وبشكل عام، يمكن تحديد الشبكات الآمنة بوضع رمز قفل بجوار اسم شبكة الواي فاي وطلب تسجيل كلمة المرور للاتصال بها.

3. **وضع كلمة مرور معقدة لنظام حماية الوصول إلى الشبكات اللاسلكية – بمعيار التشفير المطور (WPA2-AES):** استخدم كلمة مرور معقدة عند وضع كلمة مرور لنظام حماية الوصول إلى الشبكات اللاسلكية – بمعيار التشفير المطور وتأكد من تغييره باستمرار.

اختر كلمة مرور بحيث:

أ- تحتوي على حروف وأرقام ورموز.

ب- استخدم أحرف كبيرة وصغيرة.

ج- تكون أطول من 8 أحرف.

4. **قم بتغيير اسم المستخدم وكلمة المرور الافتراضيتين لتسجيل الدخول بجهاز التوجيه اللاسلكي:** يضع المصنعون أسماء مستخدمين وكلمات مرور افتراضية للأجهزة لتمكين المستخدم من الاتصال بأجهزة التوجيه اللاسلكية. وعادةً ما تحتوي أسماء المستخدمين وكلمات المرور على امتيازات إدارية وتبقى عادةً دون تغيير بعد التثبيت الأولي. حيث يمنح عدم تغيير أسماء المستخدمين وكلمات المرور الافتراضية فرصة سهلة للمهاجم لاختراق شبكتك، ولذلك يجب تغييرها على الفور بعد التثبيت.
5. **أغلق جهاز التوجيه اللاسلكي الخاص بك في حالة عدم استخدامه:** في حين أن فتح وإغلاق أجهزة التوجيه اللاسلكية كل مرة عند الحاجة إلى استخدام الإنترنت قد يكون أمرًا غير عملي، ضع في الاعتبار إغلاق جهاز التوجيه اللاسلكي عند السفر أو في حالة عدم استخدامه لفترات طويلة.
6. **تعطيل دعم التركيب والتشغيل العالمي:** قم بتفعيل ذلك الخيار فقط في حالة الحاجة إلى دعم التركيب والتشغيل العالمي بشكل مخصص.
7. **تعطيل بروتوكول نقل الملفات:** قم بتفعيل ذلك الخيار فقط في حالة الحاجة إلى بروتوكول نقل الملفات بشكل مخصص.
8. **تفعيل جدار الحماية لجهاز التوجيه اللاسلكي:** تأكد من تفعيل خاصية جدار الحماية في جهاز التوجيه اللاسلكي الخاص بك وتهيئتها للسماح للمستخدمين المرخص لهم فقط بالوصول إلى الشبكة. وسيعمل تفعيل تلك الخاصية على تسهيل حجب المرور عن الأجهزة المنزلية خارج الشبكة المنزلية، بالإضافة إلى إيقاف الحركة غير المرغوب بها بالشبكات المنزلية.
9. **تفعيل التسجيل:** قم بتفعيل خاصية التسجيل على جهاز التوجيه اللاسلكي الخاص بك واستعرض تسجيلات الدخول بشكل دوري للتأكد من حدوث أي خلل. ويمكن أن تكون تسجيلات الدخول أيضًا مفيدة في المساعدة في التحقيق في حالة حدوث أي هجوم.

ضع في اعتبارك أن ما ذكر أعلاه قائمة فقط بالخطوات المقترحة التي يمكن اتخاذها لتأمين جهاز التوجيه اللاسلكي الخاص بك بقدر ما يمكن. لمزيد من المساعدة حول أي مشكلة فنية، يرجى الرجوع إلى مزود خدمة الإنترنت الخاص بك.

## الإبلاغ عن الحوادث:

يمكنك الإبلاغ عن أي نشاط مشبوه أو سلوك غير معتاد من خلال جهات الاتصال المنزلية إلى كيو سرت. حيث يقدم فريق كيو سرت خدمة التعامل مع الحوادث العامة لمستخدمي الإنترنت من خلال وسائل الاتصال التالية:

أرقام الخط الساخن: 44995444-974+/ 44995445-974+

الموقع الإلكتروني: http://call.qcert.org/

لمزيد من المعلومات حول خدمة التعامل مع الحوادث العامة وتحميل الأدوات مجانًا، يرجى زيارة بوابة كيو سرت الإلكترونية على الرابط التالي: http://call.qcert.org/