وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

مبادئ الأمن السيبراني التوجيهية
لشبكات Wi-Fi اللاسلكية العامة

الإصدار: 1.0

المؤلف: قسم سياسة ومعايير الأمن السيبراني

تصنيف الوثيقة: عام

تاريخ النشر: أبريل 2018

تاريخ الوثيقة:

التاريخ	وصف الاصدار	الاصدار
أبريل 2018	نشر النسخة الاولى	1.0

المحتويات:

1. 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 والبنية التحتية 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 البنية التحتية 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.

2. مقدمة:

تنتشر شبكات الإنترنت اللاسلكية (Wi-Fi) بصورة واسعة في المطارات والمنتزهات والمطاعم والمقاهي والمكتبات والفنادق. وقد أصبحت نقاط الاتصال اللاسلكي هذه (hotspots) منتشرة وشائعة بكثافة لدرجة أن الناس عادة ما يجدون أنفسهم وقد اتصلوا بها دون تفكير في الأمر. وبالرغم من أنه تسجيلك للدخول لكي تراجع حساباتك على وسائل التواصل الاجتماعي أو لكي تتصفح بعض المقالات الإخبارية، أو لأداء أي الأنشطة اليومية التي تتطلب تسجيل الدخول، مثل قراءة رسائل البريد الإلكتروني أو مراجعة حسابك المصرفي، قد يبدو أمراً بسيطاً خالياً من أي مشاكل أو مضار، إلا أنه قد تكتنفه مخاطر جمة عند استخدام الشبكات اللاسلكية العامة.

3. الجمهور

أي شخص أو جهة تمتلك أو توفر أو تستخدم شبكة لاسلكية متاحة للجمهور في دولة قطر.
أي منظمة تمتلك شبكة لاسلكية للضيوف وتوفر خدمات الإنترنت لمورديها وموظفيها المؤقتين وما إلى ذلك.

4. فهم المخاطر

إن مزايا هذه النقاط من قبيل سهولة الاتصال وتوافرها للجميع دون كلمات مرور والتي تجعلها مرغوبة للمستهلكين، هي نفسها التي تجعلها مرغوبة لدى القراصنة. إن هناك عدد كبير من المخاطر التي تصاحب هذه الشبكات اللاسلكية العامة. وفي حين أن أصحاب الأعمال يظنون أنهم يقدمون خدمات قيمة لعملائهم، إلا أن هذه الشبكات غالباً ما تكون مزودة بنظام أمنيّ منخفض المستوى أو لا تمتلك أي نظام حماية على الإطلاق.
وكلما ضعفت درجة أمن نقطة الاتصال بالشبكة اللاسلكية العامة، كلما كان الأمر سهلاً للقراصنة للاتصال والتصنت على المستخدمين، وتوزيع البرمجيات الضارة أو سرقة المعلومات الحساسة. لقد أصبحت تقنيات مثل التصيد والتلصص والاقتحام والهجوم الالكتروني (snooping, sniffing, phishing and MitM) أساليب معروفة تماماً في هذه السيناريوهات.

وقد ينتج عن تلك الهجمات احتيال على العملاء، مثل سرقة بيانات بطاقات الاعتماد. وقد تؤدي أيضاً إلى تسريب معلومات العملاء الشخصية، وصورهم ومحادثاتهم إلى القراصنة الإلكترونيين والذين قد يقوموا بإعادة بيعها أو استخدامها لأغراضهم الغير مشروعة.

5. المبادئ التوجيهية

1.5 مالك الشبكة/مزود الخدمة:

يجب التأكد من التركيب الآمن لأي أجهزة أو شبكات لاسلكية تستخدم لتشغيل الخدمة والدخول إلى الإنترنت أوتخزين أو إرسال أي معلومات عن العملاء بطريقة آمنة وبما يتفق مع مع سياسة تأمين المعلومات الوطنية (NIA) لدولة قطر. وستساعد هذه الأحكام على الحد من:

1. التهديدات السيبرانية من الإنترنت للعملاء
2. التهديدات السيبرانية التي قد تنشأ بصورة مقصودة أو غير مقصودة من العملاء لأطراف أخرى عبر الإنترنت.
3. التهديدات السيبرانية التي قد تنشأ بصورة مقصودة أو غير مقصودة من العملاء لعملاء آخرين على الشبكة اللاسلكية العامة الوطنية.

5.1.1 الحوكمة:

1. يجب تحديد مالك لهذه الخدمة. يجب أن يكون مالك الخدمة مسؤولاً عن تشغيل وتأمين الخدمة بمستوى مقبول.
2. يجب على مالك الخدمة أن يحدد الاستخدام المقبول لها فضلاً عن الإجراءات الأمنية لتلك الخدمة.
3. يجب أن يتم توثيق وتأمين المستندات الفنية بشأن تلك الخدمة مثل مستندات تصميم الشبكة ووظائفها، تفاصيل عناوين بروتوكول الإنترنت، إلخ، وتقديمها للآخرين فقط عند الحاجة للعلم.
4. الاحتفاظ بقائمة بكل الأجهزة المكونة للشبكة لتقديم هذه الخدمة وتوثيقها.
5. الحفاظ على وإدارة تقارير إحصاءات انشطة مستخدمي الشبكة.
6. اتفاقية أمن المعلومات: يجب صياغة اتفاقية أمن معلومات المستخدم.
7. خصوصية أمن المعلومات: تحديد سياسة الخصوصية لمستخدمي الشبكة.

5.1.2 التحكم في الدخول

1. يجب على كل الخدمة اللاسلكية، سواء كانت مجانية أو غير ذلك، تعريف وتوثيق هوية المستخدم وإصدار تصريح له قبل السماح له بالدخول إلى الإنترنت.
2. يجب أن تكون الخدمة قادرة على تعريف وتوثيق المستخدمين والتحقق منها بطريقة مقبولة. مثلاً: التوثيق ثنائي العنصر باستخدام جهاز نقال.
3. تقديم وعرض سياسة استخدام مقبول للمستخدمين بمجرد دخولهم للبوابة. ويجب أن يطلع المستخدم ويقبل شروط الاستخدام قبل السماح له بالدخول إلى أي موقع إلكتروني.

5.1.3 جمع و مشاركة البيانات

1. يجب أن تتضمن سياسة الاستخدام المقبول الإشعارات القانونية، وشروط سياسة السرية، والموافقة على استخدام أي معلومات شخصية معرفة قد تطلب أو تجمع من المستخدم أثناء عملية التسجيل للدخول إلى أو لاستخدام خدمة الإنترنت.

2. يجب استخدام وتقاسم أي بيانات تجمع من المستخدمين فقط وفقاً للقوانين والأنظمة المعمول بها بالدولة مثل قانون الخصوصية.
3. يجب عدم تقاسم المعلومات الشخصية المعرفة مع أي طرف ثالث إلا وفقاً لما يسمح به أو يتطلبه قانون حماية خصوصية المعلومات (المادة 18).

5.1.4 تعزيز الأمن

1. حينما تقوم بتصميم شبكتك، يجب عليك فصل شبكة أعمالك/مؤسستك عن الشبكة اللاسلكية المتاحة للعامة. ومن الأفضل أن يكون هذا الفصل مادياً، غير أنه يمكن قبول الفصل المنطقي إذا صوحب بضوابط امنية قوية ومتينة.
2. يجب استخدام ترتيبات كافية لأمن الشبكات مثل، التقسيم إلى قطاعات، التهيئة الملائمة للحلول الموحدة لإدارة التهديدات (مثلاً، الجدران النارية وغيرها)، بما يتفق مع أفضل الممارسات العالمية (مثل سياسة تأمين المعلومات الوطنية، NIST 800-41, NIST 800-53, ISO 27001 وغيرها)
3. استخدام معرفات مجموعة الخدمات SSIDs مختلفة عند تحديد أسماء الشبكات اللاسلكية. تجنب استخدام أسماء متشابهة مثل (ABC-Corp أو ABC- Public أو ABC-Guest)
4. استخدم بروتوكولات أمنية منيعة للشبكة اللاسلكية مثل WPA2 و EAP-TLS. لا تستخدم بروتوكولات WEP و WAP.
5. قم بتعطيل كلمات المرور المعدة من قبل المصنع على محولات وأجهزة توجيه الشبكة ونقاط الوصول للشبكة. استخدم كلمات مرور جديدة منيعة بما يتفق مع أفضل الممارسات. على سبيل المثال 12 رمز على الأقل وتحتوي واحداً على الأقل من الأحرف الصغيرة (a-z)، ومن الأحرف الكبيرة (A-Z) ورقم (0-9) وعلامة ضبط او رمز خاص.
6. قم بتهيئة نقاط الوصول/وأجهزة التوجيه وفقاً لأفضل الممارسات العالمية/أفضل ممارسات المورد. قم بتفعيل التشفير (إن كان متوفراً)، فغالباً تكون ميزة التشفير معطلة بحسب اعدادات المصنع.
7. احذف/عطل جميع الحسابات الافتراضية من المعدات والأجهزة المستخدمة، مثلاً، الحساب الأساسي، حساب المشرف، إلخ.
8. قم بتغيير كلمة المرور بانتظام ودورياً.
9. حافظ على سجلات دخول المستخدمين. ويجب أن تحتوي سجلات المستخدمين على معلومات من شأنها أن تكشف هوية المستخدم، مثل اسم المستخدم (إذا كان ينطبق)، رقم الهاتف الجوال، (يستخدم للتوثيق) واسم بروتوكول الإنترنت المعطى والتاريخ والوقت.
10. قم بتفعيل آلية السجلات الأمنية على كل الأجهزة. يرجى الرجوع إلى: "Guidelines for Incident Management – Prerequisite Measures" للدعم والإرشادات.

11. احتفظ بالسجلات الأمنية لمدة 120 يوماً على الأقل,
12. يجب اتخاذ ترتيبات كافية لضمان اكتشاف نقاط الدخول المشكوك فيها وتقنيات التلصص والتجسس على الشبكات اللاسلكية العامة والتصدي لها ومنعها. يوصي بشدة إستخدام أنظمة الشبكات IDS/IPS عندما تكون الشبكات اللاسلكية متاحة للعامة، أوموجودة جنباً إلى جنب مع الشبكات المؤسسية.
13. استخدم آليات التبادل الدينامية والشبكات الافتراضية الخاصة لإرسال المعلومات الشخصية المعرفة أو معلومات الدفع، لتقديم آلية كافية للتشفير وحماية الدخول من بداية العملية إلى نهايتها.
14. قم بإصلاح وترميم وتحديث البنية التحتية لشبكتك بصورة منتظمة.

5.1.5 الأمن المادي

1. يجب اتخاذ تدابير كافية لتأمين نقاط الدخول بصورة مادية لمنع الوصول المادي غير المصرح به أو الأضرار المادية الاعتيادية.
2. يجب التأكد من تأمين الموجه اللاسلكي أو مزود خدمة الدخول (نقطةالاتصال) تجاه مستخدمي الشبكة اللاسلكية العامة/شبكة الضيوف. وينصح بألا يوجدا في مكان ظاهر، أو أن يتم تركيبهما في مكان لا يمكن الوصول إليه مثل الأماكن العالية (أعمدة) أو تحت السقف المستعار.
3. إذا كانت هناك منافذ لشبكة داخلية سلكية (شبكة إيثرنت) على الجدران، يرجى التأكد من أنها بعيدة عن وصول الزوار وأنها مؤمنة بصورة كافية. وإذا لم تكن مستخدمة فيمكن فصلها من الشبكة.

5.1.6 الإبلاغ عن الحوادث ومعالجتها:

1. قم بتسجيل أي حادث يتعلق بامن المعلومات.(مخالفة أو نشاط سيبراني إجرامي) داخلياً وكذلك بإبلاغ كيوسرت والجهات الأمنية في الدولة (وزارة الداخلية).
2. يمكن إبلاغ الحوادث لكيوسرت من خلال الموقع الإلكتروني أو بالاتصال بالخط الساخن 44933408 974+
3. بمجرد اختفاء او فقدان أي جهاز، يجب تغيير معرف مجموعة الخدمات (اسم الشبكة اللاسلكية) وكلمة المرور.

5.2 مستخدمو الشبكات اللاسلكية العامة:

5.2.1 عادات امنية سليمة:

1. لا تستخدم أجهزة قديمة أو إصدارات/نسخ قديمة قد تكون عرضة للاختراقات وليست محدثة بصورة كافية للاتصال بالشبكات اللاسلكية العامة.
2. لا تترك اتصالك بالشبكة اللاسلكية Wi-Fi أو البلوتوث في وضع التشغيل في الأوقات التي لا تستخدمها فيها.
3. لا تترك شبكتك اللاسلكية تتصل تلقائياً بالشبكات الأخرى.

4. تجنب استخدام شبكة لاسلكية عامة غير محمية بكلمة مرور.
5. لا تتقاسم اسم المستخدم خاصتك، أو كلمة مرورك أو أجهزتك النقالة لاستقبال الاعدادات الأمنية للدخول للشبكات اللاسلكية العامة مع أي شخص بما في ذلك أصدقائك.
6. لاتدخل إلى المواقع التي تطلب/تخزن معلوماتك الحساسة مثل المعلومات المالية أو الصحية عندما تكون متصلاً بشبكة لاسلكية عامة. وإذا كان ذلك ضرورياً:

أ. من الأفضل استخدام خدمات 3Gأو 4G أو 5G من مشغل خدمات الهاتف الجوال الذي تشترك معه، بدلاً من نقاط اتصال الشبكات اللاسلكية العامة.

ب. لا تدخل إلى أي حساب من خلال أي تطبيق من تطبيقات الهاتف الجوال. بدلاً من ذلك إذهب إلى الموقع الإلكتروني وتأكد من استخدامه لبوتوكول HTTPS قبل الدخول.

ت. اتصل عن طريق شبكة افتراضية خاصة.

ث. قم بتسجيل الخروج من الحسابات عند ما تنتهي من أعمالك فيها.

7. عندما تتصل أو تكون متصلاً بشبكة لاسلكية عامة:

أ. حاول معرفة ما إذا كانت الشبكة قانونية. تحقق من معرف مجموعة الخدمات قبل الاتصال، حيث يمكن للمستخدمين ذوي النوايا السيئة إنشاء نقطة مزود خدمة لاسلكية باستخدام أسماء شبكات يتعمدون أن تشبه أسماء المقاهي الشهيرة أو الفنادق المواقع التي توفر شبكات لاسلكية مجاناً.

ب. قم بتعطيل ميزة تبادل الملفات في جهاز الكمبيوتر خاصتك.

ت. قم باستخدام أجهزتك الخاصة مثل هاتفك النقال، جهازك اللوحي عند الدخول إلى مواقع تخزن أو تطلب إدخال أي معلومات حساسة. قد يكون من الأفضل الدخول لتلك المواقع الحساسة من خلال شبكة هاتفك النقال بدلاً من اتصال الشبكة اللاسلكية العامة.

ث. تجنب استخدام المحطات المشتركة/العامة للدخول إلى أي مواقع تتطلب إدخال أي معلومات حساسة.

ج. عند استخدام المحطات العامة/المشتركة تأكد من تسجيل الخروج من كل بوابة قمت بتسجيل الدخول لها. امسح تاريخ تصفحك واحذف الذاكرة الانتقالية قبل مغادرة المحطة.