CERT.sa
المركز الوطني الارشادي لامن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

المركز الوطني الإرشادي لأمن المعلومات CERT-SA

لمحـــة:

المركز الوطني الإرشادي لأمن المعلومات بهيئة الاتصالات وتقنية المعلومات، هو مركز غير ربحي يهدف إلى رفع مستوى الوعي والمعرفة بأخطار أمن المعلومات، ويعمل بالتعاون مع أعضائه وشركائه على تنسيق جهود الوقاية والتصدي للأخطار والحوادث المتعلقة بالأمن الإلكتروني في المملكة العربية السعودية.

رؤيتنا:

أن نكون المرجعية الموثوق بها لأمن المعلومات في المملكة العربية السعودية.

مهمتنا:

- رفع مستوى الوعي بأمن المعلومات في المملكة العربية السعودية.
- تنسيق الجهود على المستوى الوطني لتفادي الاختراقات الأمنية، والعمل على احتواء أضرارها حال وقوعها.
- رفع مستوى الثقة في التعاملات الإلكترونية.
- التعاون والتنسيق مع المؤسسات والأطراف المؤثرة في تقديم خدمات الاتصالات وتقنية المعلومات في المملكة العربية السعودية في سبيل وقاية البنى التحتية والخدمات الإلكترونية من أخطار وتهديدات أمن المعلومات.
- تقديم المشورة والنصح للأفراد والمؤسسات فيما يتعلق بأمن المعلومات.

لمزيد من المعلومات الرجاء زيارة موقع المركز
www.cert.gov.sa

أمن الشبكات اللاسلكية

CERT.sa
المركز الوطني الارشادي لامن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

مجمع الملك عبدالعزيز للاتصالات
هاتف ٢٦٣٩٢٣١ ١ ٩٦٦+
فاكس ٤٥٤٦٩٨٤ ١ ٩٦٦+
ص.ب ٧٥٦٠٦ الرياض ١١٥٨٨
المملكة العربية السعودية
www.cert.gov.sa
info@cert.gov.sa

CERT.sa
المركز الوطني الارشادي لامن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

ZCO.477.00.33

أمن الشبكات اللاسلكية

تعتبر الشبكات اللاسلكية المحلية تقنية واسعة الانتشار، نظراً لما تقدمه من دعم لجميع المميزات التي توفرها الشبكات السلكية التقليدية. وأصبح اليوم للشبكات اللاسلكية قواعدها ومعاييرها التقنية التي ساهمت في استقرار هذه التقنية، وبالتالي الاعتماد عليها بالإنتاج في مختلف بيئات الأعمال، وخصوصاً مع سهولة استخدامها والأسعار المنخفضة لنقاط الوصول (Access Point)، بالإضافة لدعم الشبكات اللاسلكية في معالجات الأجهزة المحمولة واتساع انتشار هذه التقنية ويكاد لا يخلو منزل أو منشأة من نقاط الوصول للشبكات اللاسلكية.

وبقدر الانتشار لهذه التقنية بقدر ما تزيد أهمية العناية بتطبيق الإجراءات الأمنية لحماية الشبكات اللاسلكية، وإهمال هذا الجانب قد يعرض بيانات المستخدم والأنظمة المتصلة بالشبكة اللاسلكية لمخاطر كبيرة من المخترقين والمتسللين إلى داخلها.

وهناك عدد من الإجراءات التي يجب تطبيقها لحماية الشبكات اللاسلكية نلخصها فيما يلي:

١. الحماية باسم مستخدم وكلمة سر

يمكن حماية نقطة الوصول باسم مستخدم وكلمة سر يتم إدخالها كلما أراد المستخدم تغيير إعدادات نقطة الوصول، وينبغي التنبه إلى أن نقطة الوصول الجديدة (أو التي تم استعادة الإعدادات الافتراضية عليها) تكون محمية بكلمة سر متعارف عليها من قبل الشركة المصنعة، لذا يجب على المستخدم المبادرة بتغيير كلمة السر تفادياً لدخول أحد المتسللين إلى الشبكة والتحكم بها من خلال تغيير إعدادت نقطة الوصول، وبشكل عام ينبغي أن يختار المستخدم كلمة سر مناسبة تتكون مما لا يقل عن سبع خانات على أن تكون خليطاً بين الحروف والأرقام.

٢. تشفير الشبكات اللاسلكية

إن إحدى أهم طرق الحماية تتركز في تشفير الشبكات اللاسلكية، وهناك أكثر من نظام أو ما يسمى (بروتوكول التشفير) وهي ذات قوة حماية مختلفة، وفيما يلي توضيح لأنواع البروتوكولات المستخدمة ومميزاتها:

بروتوكول (WEP):

وهو من أقدم البروتوكولات المستخدمة في تشفير الشبكات اللاسلكية، إلا أنه يعاني من نقطة ضعف كبيرة، فباستطاعة أي مخترق محترف أن يكسر هذا البروتوكول خلال فترة قصيرة، وينصح باستخدام بروتوكول (WEP) مع مفتاح طوله ٢٦ خانة؛ لأنه يوفر حماية أفضل من المفتاح الأقصر ١٠ خانات، ويتم إنشاء المفتاح في نقطة الوصول ومن ثم يمكن نسخه لأي جهاز يتم توصيله بالشبكة اللاسلكية، ويسمى هذا النوع من المفاتيح مفتاح التشفير المشترك (PSK).

بروتوكول (WPA):

وهو بروتوكول أفضل من السابق، حيث يوفر مستوى أقوى من التشفير، وغالباً ما تدعم نقاط الوصول وبطاقات الاتصال في الأجهزة المتوفرة في الأسواق خلال الثلاث سنوات الماضية هذا البروتوكول، وتوفر أنظمة التشغيل الجديدة الدعم لاستخدام (WPA)، ويمكن استخدامه مع مفتاح تشفير يتم مشاركته (PSK) ومع خوارزمية التشفير (TKIP)، ففي ويندوز إكس بي يسمى ببروتوكول (WPA-PSK)، حيث يتوجب على المستخدم نسخ مفتاح التشفير للجهاز المراد توصيله للشبكة اللاسلكية، كما يمكن استخدامه على مستوى أكبر في المؤسسات باستخدام آلية التوثيق (802.1X/EAP) والتي يمكن من خلالها استخدام الشهادات الإلكترونية.

بروتوكول (WPA2):

وهو معزز للبروتوكول (WPA) ويتميز بأنه يستخدم خوارزمية (AES) للتشفير، كما أنه يستخدم الشبكات الثنائية (ad-hoc)، وهو متوفر بطريقة (PSK) أو باستخدام آلية التوثيق (802.1X/EAP) والتي يمكن من خلالها استخدام الشهادات الإلكترونية.

٣. تغيير معرف الشبكة اللاسلكية

يجب تغيير معرف الشبكة اللاسلكية (SSID) بحيث لا يدل على نوع نقطة الوصول أو مكان وجودها، فالمعرف الافتراضي في نقاط الوصول الجديدة يدل على نقطة الوصول والشركة المصنعة لها، مما يتيح للمتسللين فرصة مهاجمة نقطة الوصول والسيطرة عليها باستغلال الثغرات الخاصة بنوعها، أيضاً ينبغي تعطيل خيار الإعلان عن معرف نقطة الوصول (Broadcasting SSID).

٤. وضع نقطة الوصول في مكان مناسب

يفضل وضع نقطة الوصول في مكان مناسب بحيث تضمن تغطية المكان المراد تغطيته وتقليل نسبة تسرب الذبذبة خارج النطاق المطلوب، لأن وضعها في مكان قريب من أحد جوانب المنزل يقوي الإشارة في تلك الجهة من خارج المنزل وبالتالي يكون بمقدور من هو خارج المنزل الاتصال بالشبكة والعبث بها، وفي حالة وجود طابق تحت الأرض فينصح وضع نقطة الوصول فيه لأن ذلك يحد من خروج الإشارة خارج نطاق المنزل.

٥. تحديد قائمة مسبقة للأجهزة القادرة على الارتباط بنقطة الوصول

لتوفير حماية أعلى ينصح بتحديد قائمة مسبقة للأجهزة القادرة على الارتباط بنقطة الوصول، وذلك من خلال تسجيل عنوان كرت الشبكة (MAC) في نقطة الوصول، فلكل جهاز كمبيوتر يتحوي على دعم للشبكات اللاسلكية عنوان محدد يتم من خلاله الاتصال بنقطة الوصول، وللحصول على عنوان كرت الشبكة (MAC) في الجهاز المراد توصيله بالشبكة اللاسلكية يجب طباعة الأمر (ip config / all) في برنامج (Command Prompt) الموجود في قائمة الملحقات في نظام ويندوز، ويوجد العنوان في الجزء المخصص لكرت الشبكة اللاسلكي (Ethernet adapter Wireless Network Connection) أمام العبارة (Physical Address)، وهذا العنوان عبارة عن اثنتي عشرة خانة مفصولة بعلامة (-)، فعلى المستخدم نسخ العنوان ووضعه في قائمة العناوين المسموح لها بالاتصال بنقطة الوصول، وينبغى ملاحظة أن هذه الإعدادات يتم تطبيقها مرة واحدة فقط عند أول اتصال للجهاز بالشبكة اللاسلكية ولا داعي لتكرار ذلك في كل مرة. مع الأخذ بالاعتبار أنه يمكن عمل تزوير (Spoofing) لهذا العنوان من قبل المخترق، كما يصعب تطبيق هذا الأمر في حال كثرة المستخدمين.

٦. تحديث نظام تشغيل نقطة الاتصال

يجب تحديث نظام تشغيل نقطة الاتصال (Firmware) وبطاقات الاتصال في الأجهزة (drivers)، إلى أحدث النسخ المتوفرة.

٧. موثوقية الشبكات اللاسلكية

يجب التأكد من موثوقية الشبكات اللاسلكية التي يتم الاتصال بها، حيث يعمل بعض المخترقين على إنشاء شبكات وهمية على أجهزتهم لغرض خداع المستخدمين وسرقة معلوماتهم.