

دولة ليبيا
وزارة التعليم
مركز المناهج التعليمية والبحوث التربوية

تقنية المعلومات

للسنة الثالثة بمرحلة التعليم الثانوي
القسم العلمي

الدرس الثاني

المدرسة الليبية بفرنسا ـ تور

العام الدراسي:
1441 / 1442 هـ . 2020 / 2021 م.

2.1 وسائل تأمين البيانات المرسلة عبر الشبكات

هناك العديد من وسائل تأمين البيانات المرسلة عبر الشبكات، كالاستعانة بأنظمة التشفير واستخدام الجدران النارية، ووضع سياسات صارمة حول اختيار كلمات العبور وتحديثها المتكرر، من أمثلة وسائل حماية البيانات اعتماد مبدأ تشفير البيانات وكذلك اعتماد استخدام الجدران النارية لصد محاولات الاختراق بأنواعه.

1.2.1 تشفير المعلومات

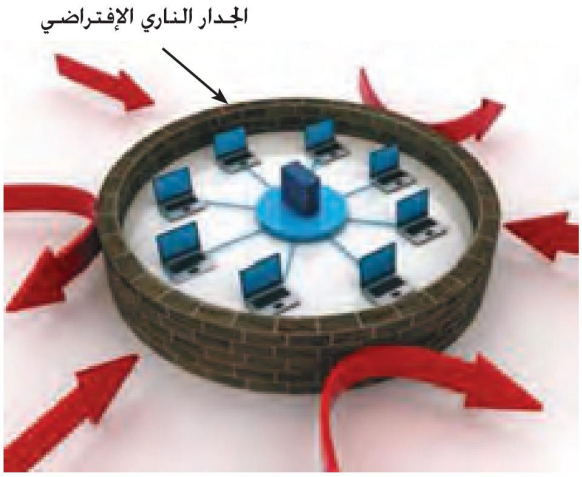
يتمثل تشفير المعلومات في تحوير البيانات الأصلية بطريقة معينة قبل إرسالها عبر شبكات المعلومات، ويقوم المتسلم بفك التشفير، وإعادة البيانات إلى صيغتها الأصلية اعتماداً على طريقة



جميع الحقوق محفوظة لـ مركز المناهج التعليمية والبحوث التربوية ـ ليبيا

التشفير نفسها، فعند اختراق شبكة الاتصالات والاطلاع على البيانات المرسلة ستكون مشفرة وغير مفهومة للمخترق؛ لأنه يجهل طريقة التشفير، ومن تم لا يمكنه استغلالها على أي نحو.

2.2.1 الجدار الناري



الجدار النارى هو جدار افتراضي وهو مصطلح يطلق على مجموعة من البرمجيات والأجهزة، التي تمثل الحد الفاصل، أو الوسيط بين شبكة معلومات وأخرى تتواصل معها، بمعنى أن انتقال المعلومات من شبكة معلوماتية لأخرى لا يتم مباشرة لإمكانية إحداث أى نوع من الضرر بالشبكة المستقبِلة؛ لأن المعلومات المرسلة قد تتضمن فيروسات ضارة وردت خلال معلومات أُرسلت من قبل شبكة معلوماتية أخرى، لذلك عند استقبال أي شحنة من المعلومات المرسلة يتم استقبالها وتمحيصها من قبل الجدار الناري، ويقوم بالتأكد من عدم وجود أي مخاطر أمنية تتخلل البيانات المستقبلة، كما يقوم الجدار الناري بالكشف عن المخاطر من خلال مجموعة من التعريفات، التي تحدد أسماء المواقع المشبوهة التي لا يسمح بالتواصل معها، أو منع التواصل مع مواقع وردت بها مصطلحات محددة كالمصطلحات الغرائزية أو الإرهابية أو العنصرية، أو تلك التي تزدري الأديان والمعتقدات وغيرها.

3.1 حماية البرمجيات

التطبيقات البرمجية في المؤسسات عادة ما يحدد لها أشخاص معينون لاستخدامها، ويقصد بأمن البرمجيات التطبيقية قدرتها على تحديد الأشخاص المخولين باستخدامها ومنع غيرهم، وهناك العديد من الطرق التي يمكن استخدامها في تأمين الاستخدام المشروع للتطبيقات البرمجية، ويتم تطبيق الحماية الأمنية للبرمجيات على مستويين:

1.3.1 مستوى تحديد شخصية المستخدم

في هذا المستوى يتم إما استخدام إدخال كلمات العبور أو الاستعانة بالصفات الشخصية، مثل بصمة الإصبع أو تمييز الصوت أو تمييز قزحية العين، وتعتبر بيانات الصفة الشخصية أكثر دقة في تمييز المستخدمين، لاستحالة تزويرها أو تقليدها مقارنة بكلمات العبور التي يمكن سرقتها أو توقعها.

جميع الحقوق محفوظة لـ مركز المناهج التعليمية والبحوث التربوية ـ ليبيا

1 . 3 . 2 مستوى تحديد صلاحيات الاستخدام

إثر تمكُن المستخدم من الدخول إلى شاشات التعامل مع التطبيق البرمجي فهو ليس بالضرورة مخولا باستغلال جميع الوظائف أو الخدمات التي يوفرها التطبيق البرمجى، فمثلا من خلال تطبيق برمجي بمؤسسة ما، غالباً ما تختلف صلاحيات المدراء وصلاحيات رؤوساء الأقسام وصلاحيات الموظفين بأنواعهم، لذلك فعلى مطوري التطبيقات البرمجية الاهتمام بتحديد صلاحيات الاستخدام ومنح كل مستخدم فرصة استثمار التطبيق البرمجي فقط، من خلال الصلاحيات التي منحت له من قبل إدارة المؤسسة.