الكتاب الرابع

الأمـن السيبراني

وحماية شبكات المعلومات

من الفيروسات

محتويات الفهرس

المقدمة

عادة ما توظف مجموعة متنوعة من الاستراتيجيات. تشمل الفحص المستند على الكشف عن نماذج معروفة من البرمجيات الخبيثة في كود قابل للتنفيذ ومع ذلك يمكن للمستخدم أن يكون مصابا ببرمجيات خبيثة جديدة التي لا يوجد لها حتى الآن توقيع. لمواجهة هذا الذي يسمى تهديدات اليوم صفر، يمكن استخدام الاستدلال. وهو أحد أنوع النهج الإرشادي الذي يستند إلى التوقيعات العامة للتعرف على الفيروسات الجديدة. مختلف أشكال الفيروسات الموجودة يتم اكتشافها بالبحث عن أكواد البرمجيات الخبيثة المعروفة في الملفات. بعض برامج الحماية من الفيروسات ويمكنها أيضا التنبؤ بما سوف يحدث تفعل إذا فتح الملف بمحاكاتها في صندوق رمل وتحليل ما تقوم به لمعرفة ما إذا كانت تنفذ أية إجراءات ضارة. إذا نفذت هذا، يمكن أن يعني هذا أن الملف ضار.