أمن الأجهزة الالكترونية المحمولة

الأجهزة الالكترونية بمختلف أشكالها قد تكون عرضةً للهجمات والاختراقات بطرق متعددة، ولا يقتصر هذا الأمر على أجهزة الحاسوب التقليدية فحسب ولكن يمتد ليشمل انواع أخرى من الاجهزة المحمولة كالهواتف النقالة وأجهزة المساعد الرقمي (PDA). تشتمل هذه النشرة على مجموعة من الاحتياطات التي يمكن اتخاذها لتقليل هذه المخاطر.

مسببات امتداد الخطر للاجهزة الالكترونية

في واقع الامر، لا يوجد مسببات لامتداد مخاطر انتهاك الخصوصية للاجهزة الالكترونية، ولكن الأمر هو أن الحواسيب العادية والتقليدية أصبحت تتقلص في الحجم وتزيد من تخصصها في تطبيقات معينة. فكافة الأجهزة الالكترونية المعنية هي عبارة عن أجهزة حواسيب بأشكال وصور مختلفة، فالهواتف النقالة وأجهزة المساعد الرقمي (PDA) و ألعاب الفيديو و أجهزة التوجيه والملاحة في السيارات والطائرات. القدرات الحاسوبية لهذه الأجهزة سببت وجود بعض المخاطر المختلفة والمرتبطة جميعاً بطبيعة الوظيفة والمهام الخاصة بهذه الاجهزة وهو الأمر الذي جعلها محل اهتمام لبعض ذوي اصحاب النوايا السيئة للقيام بمحاولات تعدي على خصوصية اصحاب هذه الاجهزة وكسر أنظمة الحماية عليها. فمثلاً قد يتمكن مهاجم معين من زرع فيروس ما في هاتف نقال، أو قد يقوم بسرقة الهاتف نفسه وحتى الوصول للملفات والبيانات المخزنة على الهاتف أو المساعد الرقمي (PDA). وقد يتعاظم الخطر إذا مان استخدام هذه الأجهزة يشمل أعمالاً خاصة بالمؤسسات والشركات والحكومات.

أنواع الأجهزة التي يشتمل عليها الخطر

كافة الأجهزة المحمولة عرضة للخطر، فطبيعتها المحوسبة تستلزم وجود نُظم تشغيل و برمجيات خاصة بتشغيل وإدارة موارد الجهاز المحمول وهذه البرمجيات والأنظمة قد تحتوي على بعض مواطن الخلل في البرمجة والتي بدورها قد تسبب وجود ثغرات مخفية تتيح بطرق معينة توجيه الجهاز المحمول لأداء وظائف لم تكن ضمن المخطط الطبيعي لعمل الجهاز. تزيد هذه المخاطر عند اتصال الجهاز المحمول بالانترنت أو بأي شبكة أخرى تكون عرضةً للانتهاكات، وهو ما يشمل الشبكات اللاسلكية أيضاً. قد يتمكن المهاجمون بطريقةٍ ما من تقمص هوية الجهاز المحمول أو استخراج معلومات وبيانات معينة منه عند وجود أي ثغرات في البرمجيات والأنظمة التي يحتويها الجهاز المحمول.

إجراءات الحماية الدارجة

- **الأمان المادي** – فصغر حجم الأجهزة المحمولة وسهولة التنقل معها قد يسبب أيضاً سرقتها أو فقدانها بنفس سهولة الاستخدام، ولذا ينبغي دائماً عدم ترك الجهاز في أماكن عامة أو في أماكن يسهل الوصول إليها.
- **تحديث البرامج والأنظمة** – فأغلب مصنعي الأجهزة المحمولة يصدرون نشرات توعية عن الثغرات المكتشفة في برمجة أجهزتها ويقومون أيضاً باصدار تحديثات خاصة بهذه الأجهزة، ولهذا فينصح دائماً بالعمل على التأكد من وجود تحديثات خاصة بالأجهزة المحمولة وتثبيتها خاصةً عندما تكون سبب هذه التحديثات وجود ثغرات أمنية.
- **الحماية بكلمات مرور قوية** – حيث تتوفر امكانية غلق (Lock) الجهاز والحماية بكلمة مرور (Password-Protect) في معظم الأجهزة المحمولة، ولهذا ينصح

أيضاً بتفعيل هذه الخيارات واختيار خالية من الأنماط المشهورة مثل (0000, 1234, 9876) وغيرها من الكلمات السهلة التخمين، إذا احتوى برنامج معين على القدرة على "تذكر" كلمات المرور فلا ينبغي تفعيله وانما الاعتماد على الذاكرة فقط لحفظ الأرقام السرية.

- **تعطيل وسائل الاتصال اللاسلكي** – تحتوي كافة الأجهزة المحمولة الحديثة على وسائل وتقنيات الاتصال اللاسلكي مثل الاتصال عبر الـ Bluetooth أو الـ WiFi وغيرها من تقنيات الاتصال الشبكي، وعلى الرغم من الفوائد الكبيرة لهذه التقنيات، يجب عدم ابقاؤها مفعلة والقيام بتعطيلها عندما لا يكون هناك حاجة لاستخدام الاتصال اللاسلكي.
- **تشفير الملفات** – وهو الخيار الغير مستخدم من غالبية مستخدمي الحواسيب بأنواعها بما في ذلك الأجهزة المحمولة. إذا كان الجهاز المحمول يحتوي على أي نوع من البيانات الشخصية أو المتعلقة بالعمل، فقد يكون من الطبيعي جداً البحث عن وجود خيارات خاصة بالتشفير في الجهاز المحمول، كثير من الأجهزة المحمولة الحديثة تحتوي على برامج خاصة بالتشفير، ولكن من الضروري أيضاً تذكر الكلمات السرية لأن فقدان هذه الكلمات السرية قد يعني فقدان البيانات وعدم القدرة على استرجاعها.

دائرة أمن المعلومات