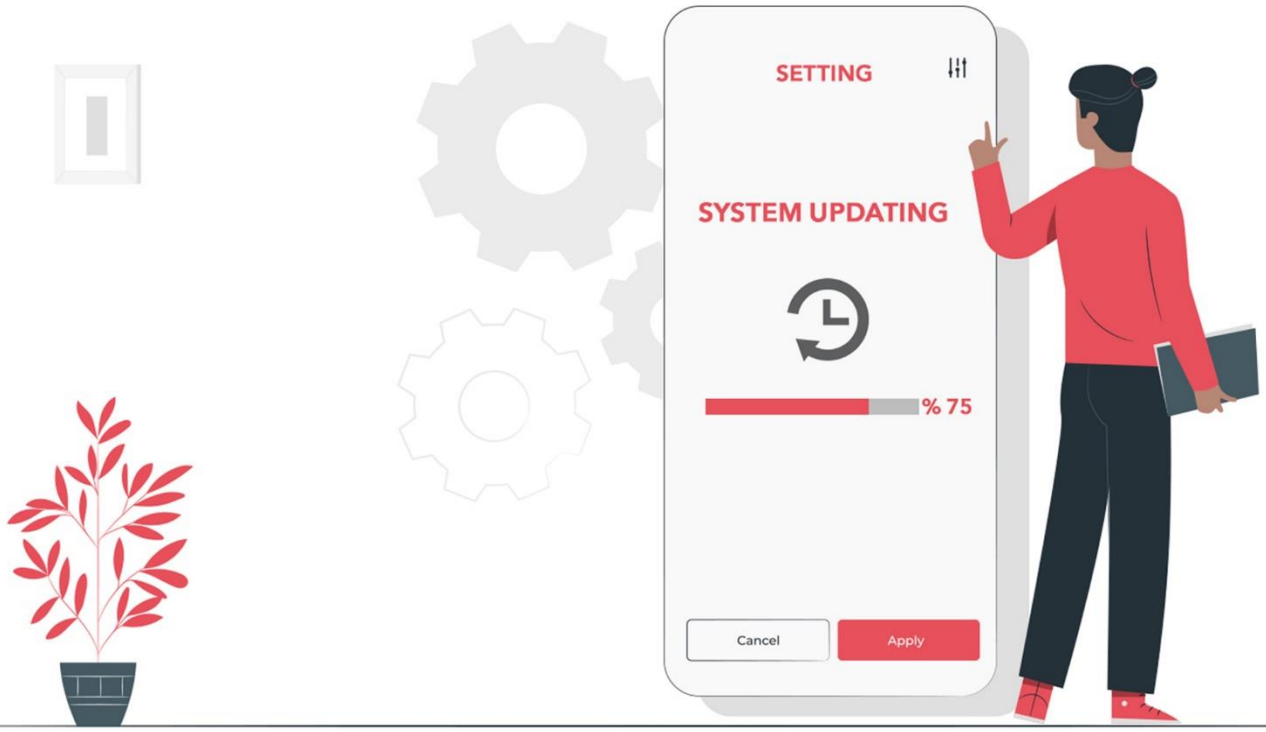

قد يكلفنا تجاهلها الكثير .. التحديثات الدورية تكسبنا الميزات وتجنبنا الاختراق

عشرات الثغرات الأمنية في أنظمة التشغيل والبرامج والتطبيقات.. كيف نتلافاها؟

للحصول على ميزات إضافية، ومعالجة الثغرات الأمنية التي قد تفتح المجال أمام عمليات التجسس وسرقة المعلومات والهجمات الخبيثة، التي تنتشر على نحو واسع ولا تفرق بين المستخدمين، ينصحنا خبراء الأمن الرقمي بتحديث نظام التشغيل والتطبيقات على أجهزتنا بشكل دوري، وعدم تجاهل إشعارات التحديث التي تصلنا أو تأجيلها، حتى لا ندفع الثمن غالياً جراء ذلك.

يعمل المطورون على إصدار تحديثات جديدة بانتظام لأنظمة التشغيل والبرامج والتطبيقات، من شأنها إغلاق نقاط الضعف الأمنية عند اكتشافها، وجعل الأجهزة الإلكترونية أكثر أماناً، في الوقت الذي يبحث قراصنة الإنترنت والمتسللون عن مزيد من الثغرات لاستغلالها في السيطرة على أجهزة المستخدمين وسرقة بياناتهم.

وتُرسل شركات البرمجيات تحديثات أمنية ضرورية بشكل مستمر، حرصاً منها على سد الثغرات التي قد تُكتشف في برامجها وأنظمتها، وقد يعمد البعض إلى إيقاف خاصية الحصول على التحديثات التلقائية، لكن ذلك قد يحول دون حصول الأجهزة على التصحيحات الأمنية ما يجعلها عرضة للهجوم.

أشارت دراسة أجرتها جامعة "ميريلاند" الأميركية إلى أن عدد الهجمات السيبرانية التي ينفذها قراصنة الإنترنت في اليوم الواحد تُقدّر بنحو 2422 هجمة يومياً، أي بمعدل هجوم واحد كل 39 ثانية.[1]

وليس بالضرورة أن يحتوي التحديث على ميزة جديدة تماماً، فقد يكون هدفه معالجة ميزة موجودة مسبقاً، مثل تحديث برنامج الحماية ليتمكن من التعرف على الفيروسات والتهديدات الجديدة.

التحديثات :هي عملية إجراء تعديل أو استبدال أو إضافة على مميزات الأنظمة والبرامج بعد صدورها من قبل المطوّر، وذلك لتوفير مزايا جديدة فيها أو غلق ثغرات أو حل مشاكل، وأهم ما في هذه التحديثات هي التحديثات الأمنية.[2]

○ أنواع التحديثات:

1. **تحديثات عامة:** وتكون بهدف الحصول على ميزات وخصائص جديدة، كتحسين أداء المعالج ما يسهم في رفع كفاءته، وتحسين الذاكرة ما يعمل على تأمين سرعة أكبر للجهاز.
2. **تحديثات أمنية:** بهدف سد الثغرات المكتشفة، وعادة ما يتم إرسالها بشكل شهري.
3. **تحديثات الطوارئ:** عندما يتواجد ثغرة أمنية حساسة جداً يتوجب إغلاقها بأسرع فترة ممكنة، وعدم انتظار التحديث الأمني.[3]

الثغرات الأمنية: هي نقطة ضعف يمكن للمخترق من خلال استغلالها الوصول إلى أمور غير مصرح له القيام بها.[4]

○ أهمية التحديثات

أ. بالنسبة للمستخدمين:

إلى جانب مساهمة التحديثات في حماية خصوصية المستخدمين، عن طريق سد الثغرات الأمنية ودرء الهجمات الخبيثة، تعمل الإصدارات الجديدة على تحسين أداء الجهاز والميزات التي يوفرها، وتؤمن توافقاً أفضل بين الأجهزة والتطبيقات التي يرغب المستخدمون في تحميلها.

---

[1] "صائدو الثغرات.. قراصنة مصريون يجعلون الإنترنت أكثر أمانا"، الجزيرة نت، 11 كانون الثاني/يناير 2020. (آخر زيارة 10 شباط/فبراير 2020). http://bit.ly/2OH5X5k.

[2] "دليل خطوات عملية في الحماية الرقمية"، منظمة سوريون من أجل الحقيقة والعدالة. 5 كانون الأول/ديسمبر 2018. (آخر زيارة للرابط 10 شباط/فبراير 2020). https://stj-sy.org/ar/1045/.

[3] "أهمية تحديث نظام التشغيل"، Do3ni. 27 كانون الأول/ ديسمبر 2019. (آخر زيارة للرابط: 10 شباط/فبراير 2020). https://do3ni.com/system-update/.

[4] "مقدمة إلى أمن المعلومات عن الثغرات"، ماكتيوبس، 21 آب/أغسطس 2019. (آخر زيارة للرابط: 10 شباط/فبراير 2020). http://bit.ly/2UzOsaK.

ب. بالنسبة للشركات:

تسعى الشركات إلى إطلاق ميزات جديدة بشكل دائم، في محاولة منها لإرضاء المستهلكين والإبقاء عليهم وجذب المزيد منهم، ولأجل ذلك يعمل المطورون على مواكبة المستجدات التكنولوجية في سبيل ضمان تسويق جيد لتطبيقاتهم، إذ إن إصدار التحديثات بشكل منتظم يساعد في بناء ولاء مستمر لدى المُستخدم، نتيجة ما تضمنه تلك التحديثات من إصلاح للعيوب وإضافة للمميزات التي تطلبها مقترحات المستخدمين ومتغيرات السوق، فالتحديثات توفر وسيلة للتواصل بين المطورين وقاعدة المستخدمين الخاصة بهم وذلك عن طريق ملاحظات الإصدار.[5]

أصلح برنامج المراسلة "واتس آب *WhatsAPP*" ثغرة أمنية تسمح للمهاجمين بالوصول إلى ملفات محفوظة على أجهزة حواسيب المستخدمين عن بعد، وقال الباحث الأمني "غال وايزمان - *Gal Weizman*"، إن المخترقين تمكنوا من الوصول إلى أجهزة المستخدمين عن طريق إرسال ملف خبيث على "واتس آب" عندما ينقر عليه الضحية يشن المخترقون هجوم حقن الشيفرة المصدرية عبر موقع وسيط *"Cross-site scripting"* ويتمكنون بالتالي من الوصول إلى بيانات خاصة بالمستخدمين.[6]

○ 74 ثغرة أمنية في "ويندوز Windows"

أطلقت شركة "مايكروسوفت Microsoft " تحديثات للبرامج من أجل سد 74 ثغرة أمنية في نظام التشغيل "ويندوز" والبرامج الأخرى، منها 13 ثغرة أمنية خطيرة، وقالت الشركة إن الخطر الأكبر يتمثل في ثغرة أمنية بمتصفح "إكسبلورر Explorer "، تم استغلالها من قبل قراصنة الإنترنت، وأوضحت أن المستخدم يقع في فخ هذه الثغرة الأمنية عند استدعاء مواقع ويب مزيفة في "إكسبلورر"، إذ تقوم هذه المواقع بإحداث خطأ في ذاكرة الحاسوب، وبالتالي تفتح الباب أمام القراصنة لاختراقه، أو تسريب البرمجيات الضارة والأكواد الخبيثة.[7]

○ صائدو الثغرات

تعرض العديد من الشركات الكبرى حول العالم، مثل "مايكروسوفت Microsoft" و"غوغل Google " و"آبل Apple" و"فيس بوك Facebook "، مكافآت باهظة لمن يكتشف ثغرات في أنظمتها الإلكترونية ويقوم بالإبلاغ عنها.

---

[5] "كم مرة يجب أن تقوم بتحديث تطبيق الجوال الخاص بك". نماء. 2017. (آخر زيارة للرابط: 10 شباط/فبراير 2020). http://bit.ly/2tNDaEQ.

[6] "تحذير! ثغرة أمنيّة في واتس آب WhatsApp تسمح للمهاجمين بالوصول إلى بياناتكم"، سلامتك. 5 شباط/فبراير 2020. (آخر زيارة للرابط: 10 شباط/فبراير 2020). http://bit.ly/3brWkRJ.

[7] "74 ثغرة أمنية في نظام التشغيل ويندوز.. فكيف تحمي جهازك؟"، الجزيرة نت. 18 تشرين الثاني/نوفمبر 2019. (آخر زيارة للرابط: 10 شباط/فبراير 2020). http://bit.ly/37ctwt8.

وتوظف بعض هذه الشركات باحثين ممن لديهم خبرة في اختراق المواقع لإجراء الاختبارات على أنظمتها، بينما تلجأ أخرى إلى منصات الاختراق الأخلاقي مثل "هاكر ون HackerOne"، التي تضم ما يزيد عن 450 ألف مخترق، وبحسب تقرير لها فإن عدد الثغرات والتهديدات الأمنية التي تم الإبلاغ عنها وحلها عبر المنصة وصل إلى ما يزيد عن 123 ألفاً، وقد دفعت مقابل ذلك مكافآت تجاوزت 62 مليون دولار، وتمكن ستة مخترقين من الحصول على مكافآت تجاوزت المليون دولار لكل منهم.[8]

أطلق اسم "القبعات البيضاء *white hat*" على المخترقين الأمنيين الأخلاقيين، الذين يقومون بعمليات اختراق قانونية ومصرح بها لكشف نقاط ضعف الأنظمة والتطبيقات وإبلاغ أصحابها لتداركها، قبل استغلالها من قبل المخترقين المجرمين المعروفين باسم "القبعات السوداء *Black hat*"، وخلف الكواليس يدور سباق محموم بين القبعات البيضاء والسوداء، حول من يكتشف أولاً الثغرات الأمنية ونقاط ضعف الأنظمة.[9]

○ نصائح يُفضل القيام بها قبل تنزيل التحديثات

1. **التحقق من وجود مساحة تخزين كافية:** حذف التطبيقات غير المستخدمة والملفات الزائدة من الجهاز لتحرير السعة التخزينية وجعل النظام خفيفاً وخالياً من المشاكل.
2. **الشحن الكامل للبطارية:** لتجنب فصل الجهاز بمنتصف التحديث ما قد يتسبب في أضرار كبيرة، إذ إن بعض التحديثات يكون حجمها كبيراً ويحتاج تنزيلها إلى وقت طويل.
3. **التأكد من الاتصال بشبكة Wi-Fi قوية:** إذ قد يتسبب الاتصال البطيء أو غير الموثوق به في عدم قيام التحديث بالشكل الصحيح.
4. **حفظ نسخة احتياطية** من الملفات.
5. **تحديث التطبيقات عقب إنهاء تثبيت تحديث النظام:** لأن الشركات المطورة للتطبيقات عادة ما تقوم بإطلاق تحديثات جديدة بعد صدور تحديثات رئيسية لنظام التشغيل، وذلك لجعلها متوافقة معها.[10]

---

[8] "صائدو الثغرات.. قراصنة مصريون يجعلون الإنترنت أكثر أمانا"، الجزيرة نت. 11 كانون الثاني/يناير 2020. (آخر زيارة للرابط: 10 شباط/فبراير 2020). http://bit.ly/2OH5X5k.

[9] المرجع السابق نفسه.

[10] "نصائح مهمة قبل تحديث أي نظام تشغيل مهما كان جهازك!"، ArabApps. 29 أيلول/سبتمبر 2016. (آخر زيارة للرابط: 10 شباط/فبراير 2020). http://bit.ly/3brWecA.