**La importancia de las actualizaciones**

Es posible que en algún momento te hayas preguntado: “¿Por qué mis dispositivos necesitan actualizaciones constantemente?” Para los consumidores, las actualizaciones proporcionan mejoras en el rendimiento y la estabilidad, ¡e incluso nuevas características! Pero desde el punto de vista de la seguridad, sirven para un propósito específico. Las actualizaciones permiten a las organizaciones abordar las vulnerabilidades de seguridad que pueden poner en riesgo a usuarios, dispositivos y redes.

En un video, aprendiste que las actualizaciones encajan en la estrategia de remediación de cada equipo de seguridad. Por lo general, se llevan a cabo después de una **evaluación de vulnerabilidad**, que es el proceso de revisión interna de los sistemas de seguridad de una organización. En esta lectura, aprenderás qué hacen las actualizaciones, cómo se entregan y por qué son importantes para la ciberseguridad.

**Cómo corregir brechas en la seguridad**

Una computadora desactualizada se parece mucho a una casa con las puertas sin llave. Los agentes de amenazas utilizan estas brechas en la seguridad de la misma manera: para obtener acceso no autorizado. Las actualizaciones de software son similares a cerrar las puertas con llave para mantenerlos fuera.

Un **parche de actualización** es una puesta al día del software y el sistema operativo que soluciona las vulnerabilidades de seguridad de un programa o producto. Por lo general, los parches contienen correcciones de errores contra vulnerabilidades y exposiciones de seguridad comunes.

**Nota:** Idealmente, los parches se encargan de reparar vulnerabilidades y exposiciones comunes antes de que los agentes de amenaza las descubran. Sin embargo, a veces se desarrollan como resultado de un **día cero**, que es un exploit que antes era desconocido.

**Estrategias comunes de actualización**

Cuando las actualizaciones de software están disponibles, los clientes y usuarios tienen dos opciones de instalación:

* Actualizaciones manuales
* Actualizaciones automáticas

Como aprenderás a continuación, cada estrategia tiene beneficios y desventajas.

**Actualizaciones manuales**

Una estrategia de implementación manual se basa en que los departamentos de TI o los usuarios obtengan actualizaciones de los desarrolladores. El *home office* o los entornos de pequeñas empresas pueden requerir que encuentres, descargues e instales las actualizaciones por tu cuenta. En entornos empresariales, el proceso por lo general se maneja con una herramienta de administración de configuración. Este tipo de herramienta ofrece una variedad de opciones para implementar actualizaciones, como para todos los clientes de tu red o un grupo selecto de usuarios.

**Ventaja:** Una ventaja de las estrategias de implementación de actualizaciones manuales es el control. Esto puede ser útil si los desarrolladores no testean bien las actualizaciones de software, lo cual puede llevar a problemas de inestabilidad.

**Desventaja:** Un inconveniente de las implementaciones de actualizaciones manuales es que uno puede ignorar u olvidarse por completo de alguna actualización crítica.

**Actualizaciones automáticas**

Una estrategia de implementación automática adopta el método opuesto. Con esta opción, el sistema o la aplicación pueden encontrar, descargar e instalar las actualizaciones.

**Consejo profesional:** La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) recomienda utilizar opciones automáticas siempre que estén disponibles.

Los usuarios y los grupos de TI deben habilitar determinados permisos antes de que las actualizaciones se puedan instalar o, enviar, cuando estén disponibles. Depende de los desarrolladores testear adecuadamente sus parches antes del lanzamiento.

**Ventaja:** Una ventaja de las actualizaciones automáticas es que el proceso de implementación se simplifica. También mantiene los sistemas y el software actualizados con los últimos parches críticos.

**Desventaja:** Un inconveniente de las actualizaciones automáticas es que pueden ocurrir problemas de inestabilidad si el proveedor no testeó minuciosamente los parches. Esto puede resultar en problemas de rendimiento y una mala experiencia del usuario.

**Software al final de su vida útil**

A veces, las actualizaciones no están disponibles para cierto tipo de software conocido como software al final de su vida útil (End-of-Life, o EOL). Todo software tiene un ciclo de vida. Comienza cuando se produce y termina cuando se lanza una versión más nueva. En ese momento, los desarrolladores deben asignar recursos a las versiones más nuevas, lo que lleva al software EOL. Si bien el software anterior sigue siendo útil, el fabricante ya no ofrece soporte.

**Nota:** Los parches y actualizaciones (updates) son muy diferentes de las ampliaciones (upgrades). Las *ampliaciones* son versiones completamente nuevas de hardware o software que se pueden comprar.

[CISA recomienda descontinuar el uso del software EOL](https://www.cisa.gov/tips/st04-006) porque representa un riesgo irreparable para los sistemas. Aun así, esta recomendación no siempre se sigue. Reemplazar la tecnología EOL puede ser costoso para empresas y particulares.

Los riesgos que presenta el software EOL siguen creciendo a medida que más dispositivos conectados ingresan al mercado. Por ejemplo, existen miles de millones de dispositivos de Internet de las cosas (IoT), como bombillas de luz inteligentes, conectados a redes domésticas y de trabajo. En algunos entornos empresariales, todo lo que un atacante necesita es un solo dispositivo sin parches para obtener acceso a la red y causar problemas.

**Conclusiones clave**

Actualizar el software y parchear las vulnerabilidades es una práctica importante en la que todos deben participar. Desafortunadamente, no siempre es así. Muchos de los ataques cibernéticos más grandes del mundo podrían haberse evitado si los sistemas se hubieran mantenido actualizados. Un ejemplo es el ataque WannaCry de 2017, que afectó a computadoras en más de 150 países y causó daños estimados en 4 mil millones de dólares. Desde entonces, los investigadores descubrieron que WannaCry podría haberse evitado si los sistemas infectados se hubieran actualizado con un parche de seguridad que se había puesto a disposición meses antes del ataque. Mantener el software actualizado requiere esfuerzo. Sin embargo, los beneficios que proporcionan hacen que valga la pena.