Information des DIN-Verbraucherrates

DIGITALE SICHERHEIT – UPDATES

Vernetzte Geräte müssen über einen **Update-Mechanismus** für die Installation von Software-Updates verfügen, um vorhandene Sicherheitslücken zu schließen. Die im folgenden genannten Anforderungen gelten so grundsätzlich für Firmware, Software und Apps. Der Hersteller muss über die voraussichtliche Lebenszeit des Geräts unverzüglich Updates bereitstellen, wenn Sicherheitsmängel (= kritische Schwachstellen) vorliegen. Die Häufigkeit von Updates ist kein Qualitätskriterium eines Gerätes. Fehlende Updates sind unproblematisch, wenn keine Mängel vorliegen. Sehr viele Sicherheitsupdates können problematisch sein und auf ein unausgereiftes Produkt hinweisen.

- Der Updateprozess ist für den Verbraucher verständlich zu **dokumentieren** und soll **nutzerfreundlich**, **einstellbar** und **zweckmäßig** sein. Durch den Updateprozess darf die Nutzbarkeit des Gerätes nicht langfristig eingeschränkt sein, z.B. sollten Updateprozesse im Hintergrund laufen.

- Der Umgang mit Updates (Versionsnummer, Datumsstempel, Änderungen, Gewährleistungsansprüche, Funktionen, Gründe, Support) muss seitens der Hersteller transparent sein.

    - Bei der Erstinbetriebnahme müssen dem Nutzer **Hinweise** und **Einstellmöglichkeiten** angeboten werden.

        - Das Gerät muss dem Nutzer die Funktion bieten zwischen **Sicherheitsupdates** und **funktionalen Updates** zu unterscheiden und diese getrennt durchzuführen: Sicherheitsupdates (notwendige Updates) dienen der Fehlerbehebung (hinsichtlich Privacy, Safety und Security). Funktionale bzw. Funktionsänderungsupdates dienen dem Hinzufügen, Ändern oder Entfernen von Funktionen.

        - Der Start des Updateprozesses erfolgt **automatisch** oder **mit Rückfrage**. Die **Voreinstellung** sollte bei Sicherheitsupdates auf automatische Updates gesetzt sein, um auch nicht IT-erfahrenen Nutzern ein hohes Sicherheitsniveau zu bieten. Für fachlich versierte Nutzer muss das Updatemanagement auch selbstständig durchführbar sein, d.h. der Nutzer sollte die Möglichkeit haben, die Voreinstellung des Updatemechanismus auf manuelle Prüfung umzukonfigurieren.

- Nutzer sollten über die Wichtigkeit der Installation bereitgestellter Sicherheitsupdates informiert werden.

- Haushaltsgeräte und Unterhaltungsgeräte werden häufig als embedded systems programmiert und damit werden Updates en bloc statt modular durchgeführt. Aus

Gründen der Gebrauchstauglichkeit (Zeitaufwand, Datensparsamkeit etc.) sollten Updates immer **modular** durchgeführt werden.

- Geräte müssen **bei Inbetriebnahme und im laufenden Betrieb prüfen**, ob Sicherheitsupdates zur Verfügung stehen, sofern ein dafür geeigneter Netzwerkzugang besteht. Diese Information ist dem Nutzer zur Verfügung zu stellen. Dem Nutzer wird das Vorliegen von Updates angezeigt bzw. mitgeteilt.

- Geräte, die nicht ständig im Netz sind, müssen **aktualisiert** werden, sobald sie wieder mit dem Internet verbunden werden.

- Das Gerät muss sicherstellen, dass die **Authentizität** und **Integrität** von Updates vor deren Installation verifiziert wird. Das Merkmal des Geräts für die Überprüfung der Authentizität und Integrität eines Updates darf bei dessen Offenlegung nicht die **Integrität** von anderen Geräten gefährden, z.B. durch Verwendung eines vom Anbieter vergebenen Standardpasswortes oder -schlüssels.

    - Es wird empfohlen, die Authentizität und Integrität von Software-Updates, z.B. durch asymmetrische Signaturverfahren oder durch symmetrische Integritätssicherungsverfahren, bei denen Schlüssel verwendet werden, die individuell für jedes einzelne Gerät sind, sicherzustellen.

- Hersteller müssen für netzwerkfähige Geräte an einer dem Nutzer und dem gewerblichen Verkäufer bekannt gegebenen Stelle bereits **vor der Kaufentscheidung** darstellen, **bis wann** das Gerät noch mit Sicherheitsupdates versorgt wird. Das kann z.B. auf der Verpackung, auf der Homepage des Herstellers und in der Dokumentation erfolgen. Gewerbliche Verkäufer sollten diesen Hinweis deutlich sichtbar beim Produkt platzieren (analog zum MHD bei Lebensmitteln, z.B. Verpackung, Produktbeschreibung im Online-Shop). Werden zum Verkaufszeitpunkt eines Geräts schon keine Updates mehr bereitgestellt, muss darauf deutlich hingewiesen werden. Die Versorgung mit Sicherheitsupdates muss der voraussichtlichen **Lebensdauer** des Gerätes entsprechen.

- Nach dem Einspielen von Updates sollte das Gerät auf einen Zustand vor Einspielen des Updates oder eine Standardeinstellung **rücksetzbar** sein.

März 2019

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages

www.din.de/go/verbraucherrat