



BHE-Empfehlungen zu Updates bei Videosicherheitsanlagen

Updates sind wichtig, um alle Systeme auf dem aktuellem Stand zu halten und um maximal mögliche Sicherheit zu gewährleisten. Es wird jedoch empfohlen, Updates nicht automatisch herunterzuladen und zu installieren, denn dies kann den Betriebsablauf stören:

- Bereits das Herunterladen von Updates kann Netzwerkbandbreite und Rechenleistung beanspruchen, die dann für die Video-Übertragung, -Analyse und -Anzeige fehlen.
- Es wäre ungünstig, wenn Systemkomponenten beispielsweise gerade während einer Alarmbearbeitung wegen eines Updates neu gestartet oder durch das Update inkompatibel werden.

Es ist zu unterscheiden zwischen Updates der

- Software, die auf Geräten (z.B. Videokameras, Recordern) fest installiert ist (so genannte „**Firmware**“),
- **Anwendungssoftware** auf PCs (z.B. Video-Management-Software, kurz „VMS“),
- **Betriebssysteme** (Operating System, kurz „OS“), z.B. Windows, LINUX, MacOS usw., sowie
- allen **weiteren Software-Komponenten**, die zur Ausstattung eines PCs gehören (z.B. Treiber).

Außerdem ist zu unterscheiden zwischen

- **Sicherheits-Updates**, mit denen neu erkannte Sicherheitslücken zeitnah geschlossen werden,
- **System-Updates**, die der Behebung von Fehlern, Verbesserung der Zuverlässigkeit und Robustheit, Performancesteigerung und Anpassung an neue OS-Versionen und Treiber dienen sowie
- **Funktions-Updates**, die neue oder verbesserte Funktionen bieten.

Letztere müssen nur dann installiert werden, wenn der Anwender diese Funktionen benötigt.



In der Praxis kann es vorkommen, dass sich durch ein Firmware-Update das Verhalten des betreffenden Gerätes ändert und die Kompatibilität zu anderen Systemkomponenten beeinträchtigt wird.

Deshalb empfiehlt es sich, vor einem Update alle Informationen des Herstellers (insbesondere zu den Änderungen) genau zu prüfen, um zu bewerten, ob das aktuelle Update überhaupt nötig und sinnvoll ist und was dabei ggf. zu beachten ist.

Jedes Update birgt auch das Risiko, dass etwas nicht mehr funktioniert, was vorher noch problemlos lief.



Deshalb wird empfohlen:

- Vor jedem Update alle Beteiligten informieren, die von Änderungen und Ausfällen betroffen sein könnten, z.B. die Leitstelle, die das betreffende Videosystem aufschaltet.
- Vor jedem Update beim Hersteller erkundigen und im Internet recherchieren, ob zu der neuen Version Einschränkungen oder Probleme bekannt sind. Es kam schon vor, dass Updates zu Fehlfunktionen oder Inkompatibilitäten geführt haben.
- Vor jedem Update alle vorhandenen Daten sichern und ggf. Wiederherstellungspunkte setzen, damit nach fehlgeschlagenen Updates wieder ein funktionstüchtiger Zustand hergestellt werden kann.
- Ein laufendes Update darf nicht unterbrochen werden, denn ein Abbruch kann zu einem inkonsistenten Zustand des Gerätes führen, so dass es möglicherweise nicht mehr erreichbar ist und nicht mehr verwendet werden kann. Deshalb muss sichergestellt werden, dass die Geräte während des Updates nicht ausgeschaltet werden, ihre Netzwerkverbindung zuverlässig ist und eine unterbrechungsfreie Stromversorgung gewährleistet ist. Akkubetriebene Geräte sollten während der Updates fest mit dem Stromnetz verbunden sein.
- Das Update erst einmal auf einzelnen PCs oder Videogeräten installieren und testen, ob damit die benötigte Funktion noch gegeben ist, bevor eine neue Version auf alle Systeme „ausgerollt“ wird.
- Nach jedem Update alle für den jeweiligen Anwendungsfall relevanten Funktionen umfassend testen, beispielsweise die Alarmbildübertragung zur Leitstelle.
- Updates sorgfältig dokumentieren (z.B. im Betriebsbuch), damit eventuell erst später festgestellte Auswirkungen den jeweiligen Versionen zugeordnet werden können.

Updates sollten erst nach Absprache mit allen eventuell Betroffenen gezielt zu vorher vereinbarten Terminen (Wartungszeiten außerhalb der Spitzenlast) und stets nacheinander auf den verschiedenen Geräten und PCs installiert werden, damit immer einige Geräte und Arbeitsplätze arbeitsfähig sind.

Falls neue Sicherheitslücken erkannt werden, können Updates besonders dringend sein. Sie müssen dann ggf. auch einmal außer der Reihe installiert werden. Doch auch in diesem Fall sollten die vorgenannten Schritte beachtet werden. Zum Thema IT-Sicherheit sollte man sich z.B. bei www.heise.de/security und vor allem beim Bundesamt für Sicherheit in der Informatik (www.bsi.bund.de) regelmäßig informieren. Automatische Updates sollten deaktiviert bleiben. Stattdessen sollten fachgerecht geplante Updates im Rahmen der regelmäßigen Instandhaltung vom Systembetreuer oder Errichter durchgeführt werden. Updates sind Bestandteil der Produkt- und Systempflege der Hersteller, unterliegen dem Urheberrecht und können kostenpflichtig sein.

Fernzugriff (Remote Service)

In bestimmten Fällen bieten Facherrichter einen Fernzugriff, auch Remote Service genannt, an. Beim Fernzugriff wird eine Datenverbindung aufgebaut. Der Zugang zur Videoanlage muss durch den Betreiber autorisiert werden. Zur Durchführung des Fernzugriffs ist es erforderlich, dass ein Service-Mitarbeiter des Facherrichters Zugriff auf bestimmte Funktionen der Videosicherheitsanlage erhält. Eine vorherige Datensicherung ist dringend zu empfehlen (Mitwirkungspflichten des Betreibers; ggf. Auftragserteilung an den Facherrichter). Der Zugang sollte zeitlich begrenzt sein und ist, sofern nicht anders vertraglich vereinbart, nach dem Beenden des Fernzugriffs zu schließen. Passwörter sollten ggf. geändert werden.

Softwarepflege

Um die Betriebssicherheit der Software zu gewährleisten, empfiehlt es sich, einen Softwarepflegevertrag abzuschließen. Die dynamische Entwicklung der Technik macht es erforderlich, dass Software stets auf dem neuesten Stand gehalten und an geänderte Umgebungsbedingungen (z.B. Updates des Betriebssystems oder neue Firmware in den Videogeräten) angepasst wird.

Dabei ist zu berücksichtigen, dass eine Software während der Nutzung ständigen Verbesserungsbestrebungen unterworfen ist und daher u.U. in bestimmten Abständen ein Update erfolgen muss. Dies stellt keinen Mangel dar, sondern ist eine systemimmanente Eigenschaft von Software.

Langzeitunterstützung

Unter der Bezeichnung LTS (engl. long-term support) bieten einige Hersteller eine verlängerte Versorgung ihrer Produkte mit Updates an, insbesondere zur Aufrechterhaltung der Betriebssicherheit (Sicherheits-Updates). Damit können diese Produkte auch über die üblicherweise vorgesehene Lebensdauer hinaus sicher betrieben und genutzt werden. Produkte, zu denen LTS angeboten wird, bieten somit eine größere Investitionssicherheit.

Fachgerechte Ausführung

Der Fachrichter setzt für die Installation und Instandhaltung aller Systeme und Systembestandteile und somit auch der Software nur entsprechend qualifiziertes Personal ein. Die vorschriftsmäßige Installation aller Komponenten, insbesondere die Ausführung der Software-Updates, obliegt dem Fachrichter.

Der BHE empfiehlt vor jeglicher Änderung der Software, eine ordnungsgemäße Datensicherung zu erstellen, wofür der Betreiber verantwortlich ist (Hinweis: kann ggf. über den Instandhaltungsvertrag delegiert werden).

Funktionsprüfung

Nach Abschluss eines Updates ist eine Funktionsprüfung durch die Fachkraft des Fachrichters durchzuführen. Damit muss sichergestellt werden, dass alle betroffenen Systeme und/oder Systembestandteile den bestimmungsgemäßen Gebrauch erfüllen, insbesondere dass die Aufschaltung auf Leitstellen im Alarmfall zuverlässig funktioniert.

Der Umfang der Funktionsprüfung richtet sich nach den Herstellervorgaben.

Der Fachrichter muss unter Berücksichtigung normativer Vorgaben sowie der Herstellerangaben festlegen, ob und in welchem Umfang Prüfungen von Systemen und Systembestandteilen durchgeführt werden müssen. Ist ein Update fehlgeschlagen, ist der vorhergehende Stand unter Verwendung der Datensicherung wiederherzustellen. Danach muss erneut eine Prüfung erfolgen.

