LSI-Info T#08

PATCHMANAGEMENT

Version 1.0 vom: 04.08.2021

Management Summary

Ziel des Update- und Patchmanagements ist es, IT-Systeme auf einem aktuellen und sicheren Stand zu halten.

Updates und Patches (“to patch“ = „flicken“) sind Softwarepakete, welche bestehende IT-Systeme bzw. darauf installierte Treiber oder Anwendungen um Funktionen erweitern (Update) bzw. Fehler beheben oder Sicherheitslücken schließen (Patch).
Schlecht gewartete IT-Systeme sind für eine Vielzahl der durch Schadsoftware verursachten Schäden verantwortlich. Ein gut funktionierendes Patchmanagement trägt wesentlich zur Erhöhung der IT-Sicherheit bei.

Update- und Patchmanagement gliedert sich in folgende Bereiche:

- Beobachtung, ob Updates, Patches und Sicherheitslücken für die betriebenen Systeme vorliegen.
- Umgehende Beschaffung der Updates und Patches
- Bewertung der Kritikalität der damit geschlossenen Lücken (Patches) bzw. der zusätzlich gewonnenen Funktionalitäten (Updates).
- Planung der Installation auf Testsystemen (Updates, Patches) oder direktes Einspielen (Patches).
- Einspielen/Ausrollen der Updates oder Patches.
- Erfolgskontrolle und Dokumentation.

1. BEGRIFFE

1.1 Updatemanagement

Ein Updatemanagement sorgt dafür, dass die IT-Systeme neue Funktionen bereitstellen. Bei Fachanwendungen geschieht dies oft auf Grund geänderter rechtlicher Anforderungen.

- Beispiel für rechtliche Anforderungen an eine Anwendung: Das Fachverfahren AutiSta im Standesamt wird regelmäßig am 30.04. und 30.10. eines Jahres aktualisiert. In der Vergangenheit wurden mit solchen Updates Neuregelungen umgesetzt, damit z. B. eine gleichgeschlechtliche Lebenspartnerschaft oder eine Eheschließung mit einer diversen Person mit AutiSta gesetzeskonform beurkundet werden kann.

- Beispiel für funktionale Verbesserungen:
  Mit den halbjährlichen Feature Updates von Windows 10 wurde der Virenschutz (Defender) verbessert und ein neuer Browser eingeführt.

1.2 Patchmanagement

Mit einem Patchmanagement werden Fehler behoben und Sicherheitslücken in IT-Systemen geschlossen.

- Ein prominentes Beispiel stellen die Sicherheitspatches der Firma Microsoft dar, die an jedem zweiten Dienstag im Monat (dem sogenannten Microsoft-Patchday) veröffentlicht werden.

Bei zeitkritischen Sicherheitslücken werden Sicherheitspatches auch außer der Reihe anlassbezogen veröffentlicht.

1.3 Weitere Begriffe

Die Hersteller benennen Updates und Patches oft unterschiedlich.

Ein Service Pack von Microsoft ist üblicherweise eine Sammlung von Patches. Hiermit können aber auch neue Funktionen bereitgestellt werden.

Ein Hotfix ist eine „mit heißer Nadel gestrickte“ Fehlerkorrektur. Teilweise werden mit einem Hotfix auch Probleme behoben („gefixt“), die erst durch einen nicht ordnungsgemäß funktionierenden Patch entstanden sind. Ein Hotfix wird häufig nicht automatisch eingespielt und ggf. nur auf Nachfrage zur Verfügung gestellt. Der Einsatz eines Hotfixes sollte unter Berücksichtigung der Herstellerangaben sorgfältig abgewogen werden.

Mit einem Workaround soll ein Problem umgangen werden. Durch die Anwendung eines Workarounds kann die Ausnutzung einer Schwachstelle unterbunden oder zumindest deren Auswirkung abgemildert werden. Hersteller veröffentlichen Workarounds vor allem dann, wenn die entsprechende Sicherheitslücke bereits aktiv ausgenutzt wird und die Bereitstellung eines Patches zu lange dauern würde oder nicht möglich ist.
Ein Workaround und dessen Auswirkungen sollte sorgfältig geprüft werden. Er kann ggf. einen (eingeschränkten) Weiterbetrieb eines Systems ermöglichen, das ansonsten bis zum Vorliegen eines Patches aus Sicherheitsgründen außer Betrieb genommen werden müsste. Ein Workaround kann allerdings auch Seiteneffekte (Nebenwirkungen) aufweisen.

2. UMSETZUNG

2.1 Zuständigkeit

Das Update- und Patchmanagement sollte grundsätzlich der IT obliegen. Die Tätigkeiten erfordern ein tiefes Wissen der Abhängigkeiten von IT-Systemen und das Verständnis über die Auswirkungen eines konkreten Patches.

Für das Update- und Patchmanagement sollte innerhalb der IT die Zuständigkeit - einschließlich einer dazugehörigen Vertretungsregelung - festgelegt und entsprechende Stellenanteile zugeordnet sein.
Die Modalitäten der Aktualisierung unterscheiden sich bei unterschiedlichen Architekturen und Systemen. Daher ist es sachgerecht, dass diese Tätigkeit von Spezialisten mit Systemerfahrung durchgeführt werden (z. B. Windows-Experten für Aktualisierungen von Windows-Systemen, Linux-Experten für Aktualisierungen von Linux-basierten Systemen sowie Aktualisierungen von Microsoft Exchange, Datenbanken oder Netzwerktechnik durch die jeweiligen Experten).
Hier kann eine kommunale Zusammenarbeit viele Synergien bieten.

2.2 Informationsbedarf

Die zuständigen Personen, deren Vertreter sowie externe Dienstleister sollten sich kontinuierlich über das Vorliegen von Patches informieren. Dazu dienen Newsletter-Abonnements der Hersteller, Warnmeldungen von Sicherheitsinstitutionen wie dem LSI und ergänzende Informationen in der Fachpresse oder in Fachforen. Für diese sicherheitsrelevante Informationsbeschaffung bzw. Auswertung sollte ausreichend Zeit zur Verfügung stehen.

Neben der IT sollte sich der Informationssicherheitsbeauftragte (ISB) regelmäßig über Sicherheitslücken informieren und sich mit der IT abstimmen.

2.3 Planung und organisatorische Umsetzung

Update- und Patchmanagement erfordern zunächst entsprechende Analysen und Planungen, aus denen ein Konzept mit Prozessen und Zuständigkeiten erstellt werden soll.

2.3.1 WARTUNGSZYKLEN UND NUTZUNGSDAUER:

Die Zeitpunkte für End-of-Service bzw. End-of-Life sollten bereits bei der Beschaffung von Hard- und Software berücksichtigt werden. Für Wartungszyklen bieten sich Wiedervorlagen an. Bei der Terminsetzung sollten ausreichende Pufferzeiten eingeplant werden.

Vor allem bei IT-gesteuerten technischen Anlagen kann die Realisierung eines Updates erfahrungsgemäß lange dauern. Hier könnte sich aus Tests der IT und der Fachabteilung ergeben, dass auch verbundene Systeme upgedatet werden müssen und so die IT-Infrastruktur ausgebaut werden muss, Updatelizenzen beschafft oder Programmieraufträge an den Hersteller vergeben werden müssen. Aus Gründen des finanziellen Rahmens oder haushaltsrechtlicher Vorschriften könnte die Realisierung solcher Maßnahmen Jahre dauern.

Die Wartungszyklen von Microsoft Windows 10 sind von der Edition und der Version des verwendeten Feature-Packs abhängig.
Das LSI rät hier im Rahmen des sogenannten Semi-Annual Channel (SAC) zum Einsatz der Enterprise Edition - oder im Bildungsbereich zur funktionsgleichen, erheblich preiswerteren Education Edition - und der Verwendung eines im Herbst veröffentlichten Feature-Updates (wie 20H2). Diese Kombination wird 30 Monate mit Patches versorgt und ermöglicht sowohl den Anwendern als auch der IT ausreichend Zeit zur Nutzung bzw. zur Updateplanung.
Bei der Verwendung eines im Frühjahr veröffentlichten Feature-Updates (wie 21H1) oder einem Einsatz von Windows 10 Professional reduziert sich die Versorgung mit Patches auf lediglich 18 Monate. Der Preisvorteil einer solchen Lizenz relativiert sich neben dem Aufwand durch häufigere Updates durch deren geringere Sicherheitsfeatures. Erfahrungsgemäß können im Ordnungsbereich, speziell im Einwohnermeldewesen, aber auch in technischen Bereichen hohe Aufwände für Updates (Upgrades) anfallen.
Weiterführende Informationen speziell zu den sogenannten Bereitstellungsringen und allgemein zum Rollout von Windows sind hier zu finden:
https://docs.microsoft.com/de-de/windows/deployment/
Im Bayerischen Behördennetz werden umfangreiche Leitfäden für den Einsatz von Microsoft Windows 10 in der Bayerischen Staatsverwaltung zur Verfügung gestellt:
https://www.cio.bybn.de/intranet/cio/4/19819/index.htm

2.3.2 AKTUALISIERUNG EXTERN BETREUTER SYSTEME UND FACHVERFAHREN

Aktualisierungen von Fachverfahren und extern betreuten Systemen sollten vertraglich festgelegt sein. Die Anwendung der EVB-IT ist hilfreich, wenngleich zahlreiche Firmen ihre Dienstleistungen nicht auf dieser Grundlage anbieten:
https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle_EVB-IT/aktuelle_evb_it_node.html

Es ist wichtig, dass bei jeder externen Beteiligung vollumfänglich und eindeutig festgelegt ist, wer die Patches zur Verfügung stellt und wer sie installiert.

Die Problematik der Zuständigkeiten soll an zwei Architekturbeispielen verdeutlicht werden. Die aus Sicht des LSI erfahrungsgemäß klärungsbedürftigen Bereiche sind farblich hervorgehoben (je dunkler die Farbe, desto wichtiger ist die Prüfung der Zuständigkeit)

Architektur / Schicht	***Wer stellt hierfür Patches zur Verfügung?***
Fachverfahren einschließlich herstellereigener Standardsoftware	Fachverfahrens-Hersteller
Entwicklungsplattform des Fachverfahrens (z. B. Mendix, Uniface)	Fachverfahrens-Hersteller
Laufzeitumgebung z. B. Java oder .NET	Fachverfahrens-Hersteller oder Kommune? -> Bezug vom Hersteller der Laufzeitumgebung Bei Java bitte Lizenzproblematik beachten: Java kommt zwar mehrheitlich vom Fachverfahrenshersteller, aber z. B. nicht bei AutiSta (VfSt). .NET meist Kommune
Middleware (z. B. Apache Tomcat® oder JBoss)	Kommune –> Bezug vom Hersteller der Middleware oder Fachverfahrens-Hersteller?
Schnittstellen (z. B. Datenbankclient oder ODBC)	Kommune –> Bezug vom Hersteller der Schnittstelle oder Fachverfahrens-Hersteller?
Datenbank	Kommune –> Bezug vom Hersteller der Datenbank Selten vom Fachverfahrens-Hersteller (oft lizenzabhängig)
Server	Kommune? –> Bezug vom Hersteller des Betriebssystems

Webanwendungen	Webverfahrens-Hersteller
Add-ons zum CMS (Content Management System) und Drittanbieterscripte	Kommune –> Bezug vom Hersteller des Add-ons oder Webverfahrens-Hersteller?
CMS	Kommune –> Bezug vom Hersteller des CMS oder Webverfahrens-Hersteller?
Hostingpaket (Managed Server)	Provider
Webserver (Rootserver) mit verschiedenen Diensten / Paketen	Kommune

Im Rahmen der vorstehenden Festlegungen zur Bereitstellung der Patches
sollte zudem noch folgendes geklärt werden:
- Wer *installiert* die Patches?
- Wie erfolgt dies? (für Fernwartung sind entsprechende Regelungen zu beachten)
- Wann erfolgt dies? (Frist, Reaktionszeit, Downtime im Vertrag oder Service Level Agreement)

Diese Fragen sollten für jede Architekturschicht beantwortet, verbindlich vereinbart und im Rahmen des Patchmanagements berücksichtigt bzw. zumindest stichprobenartig kontrolliert werden.

2.3.3 TESTABLAUF

Zunächst sollten die Vorgaben der Hersteller berücksichtigt werden (Systemvoraussetzungen, Hinweise und Readme-Dateien). Zu beachten sind die zahlreichen Abhängigkeiten von Fachverfahrensversionen zu den Versionsständen von Datenbanken und Schnittstellen. Das Umfeld sollte umfassend betrachtet werden. Beispielsweise könnte das Update einer Datenbank ein Update aller Datenbank-Clients voraussetzen, wofür ggf. wiederum vorher einzelne Fachverfahren aktualisiert werden müssen - hier ist ein schrittweises Vorgehen ratsam.

Grundsatz für die Aktualisierung von Servern und weiterer wichtiger Systeme:
Erst das Backup (incl. Validierung), dann die Aktualisierung.

Es sollten regelmäßige Wartungsfenster eingerichtet und kommuniziert werden. Auch außerplanmäßige Arbeiten sollten allen Betroffenen rechtzeitig bekannt gemacht werden. Dies sorgt für Klarheit auf Seiten der Anwender und der IT. Die Spanne der möglichen Einschränkungen reicht von der Nichtverfügbarkeit von Systemen eines bestimmten Fachbereichs über den vorübergehenden Ausfall eines zentralen Dienstes bis hin zu einer umfassenden organisationsweiten Downtime. In größeren Umgebungen können Ausweich- oder Clustersysteme die Verfügbarkeit gewährleisten.

Umgang mit Clients:
Bei kleinen Umgebungen sollte beispielsweise zunächst immer nur ein PC im Fachbereich aktualisiert werden. Nach erfolgreichem Test des Fachverfahrens kann dann die Aktualisierung der verbliebenen PCs fortgesetzt werden.
Bei größeren Umgebungen sollten Patchtest-Rechner oder -Gruppen festgelegt werden. Als Richtwert können 5 bis 10 % der Installationen zum Patchtest herangezogen werden.
Inkompatibilitäten von Aktualisierungen mit Fachverfahren können so von der Fachabteilung frühzeitig erkannt werden. Dies ermöglicht es der IT, situationsgerecht zu reagieren und ggf. den Hersteller und andere betroffene Kommunen im Behördenverbund zu informieren.

Die Personen an den Patchtest-Rechner sollten darüber informiert sein, dass hier zuerst gepatcht wird. Es empfiehlt sich hierfür Personen vorzusehen, die mit der Nutzung der IT und vor allem des Fachverfahrens vertraut sind. Diese Patch-Tester sollten rechtzeitig informiert werden, wann Patches ausgerollt werden. So kann die IT qualifizierte Rückmeldungen erhalten und Problemen mit inkompatiblen Aktualisierungen rechtzeitig begegnen.

War der Patchtest, aufgrund ausbleibender negativer Rückmeldungen, erfolgreich, werden nach einer festgelegten Zeitspanne auch die verbliebenen Systeme gepatcht. Wenn technisch möglich, sollte dies automatisch erfolgen und nachträglich überprüft werden. Abhängig von der Anzahl der zu aktualisierenden Systeme und der Leistungsfähigkeit der IT können Updates auch in mehreren Wellen durchgeführt werden. Durch die Nutzung von Wake-on-LAN können IT-Systeme auch außerhalb der üblichen Arbeitszeiten aktualisiert werden. Dies erhöht die Verfügbarkeit der Systeme und entlastet das Personal.

Bei kritischen Verfahren kann eine ausdrückliche Freigabe seitens der für den Patchtest verantwortlichen Personen (Fachverfahrensverantwortliche) sinnvoll sein.

2.3.4 ZEITSCHIENE

Ganz allgemein gilt, dass Patches mit hoher Kritikalität sehr zeitnah eingespielt werden sollten. Sicherheitslücken werden oft nach dem sogenannten CVSS-Wert eingestuft, dieser bietet für die Bewertung eine gute Orientierung.
Erklärung der CVSS-Skala (Common Vulnerability Scoring System):
Niedrig 0,1 - 3,9 / Mittel 4,0 - 6,9 / Hoch 7,0 - 8,9 / Kritisch 9,0 - 10,0
https://nvd.nist.gov/vuln-metrics/cvss
Kritische Patches sollten möglichst sofort, jedoch spätestens innerhalb von 3 Tagen, und Patches mit hohem Score innerhalb von 5 Tagen eingespielt werden. Reihenfolge: zuerst auf Patch-Testrechnern, danach auf allen weiteren.
Bei hochkritischen Lücken in remote angreifbaren Systemen, die bereits aktiv ausgenutzt werden, bleibt ggf. keine Zeit mehr zum Testen. In diesem Fall könnte die Lösung ein Backup und ein direktes Einspielen des Patches mit nachfolgendem Test sein.
Funktionsupdates sind in der Regel nicht zeitkritisch, können allerdings fristgebunden sein.

Falls ein automatisches Patchen nicht möglich sein sollte, raten wir zu einer Patch-Strategie mit folgendem priorisierten Vorgehen:
Priorität 1: Systeme, die direkt aus dem Internet erreichbar sind, wie Webserver, Proxy-Server, VPN-Gateways, Maileingangsserver bzw. Mail-Relay und SharePoint-Server.
Priorität 2: Systeme, die kritische Dienste bereitstellen wie Active-Directory-Domänencontroller, interne Mail-Server, DNS-Server, WSUS-Server, Backupsysteme und kritische technische Anlagen.
Priorität 3: Clients mit Internetzugang, bei denen zwingend mit Adminrechten gearbeitet werden muss.
Priorität 4: weitere Clients mit Internet- oder E-Mail-Zugang.
Priorität 5: alle vorstehend nicht genannten betroffenen Systeme.

2.3.5 TESTUMFANG

Je umfangreicher das Update ist, z. B. bei Hauptrelease-Wechsel, desto mehr Aufwand sollte IT-seitig in die Vorbereitung der Installation und in die Nachbearbeitung durch die Fachabteilung mit Funktionstest der Anwendung investiert werden. Erfahrungsgemäß wird der Aufwand an Personalressourcen durch die Fachabteilung oftmals unterschätzt.

Bei häufigeren Updates lohnt sich für die Fachabteilung ein Testkonzept, in dem Testobjekte und Testvorgänge beschrieben sind. Nach einer Prüfung, ob die Anmeldekennungen, Einstellungen und alle Daten vollständig übernommen wurden erfolgt der Check grundlegender Funktionen wie Erfassung oder Änderung. Im Anschluss könnte beispielsweise getestet werden, ob Ausdrucke und Berichte noch passen. Dazu kann ein Test-Datensatz erstellt werden, bei dem in allen Feldern die maximal zulässige Zeichenanzahl ausgenutzt wird. Neben Plausibilitätsprüfungen (Tests bewusster Falscheingaben, die vom Programm nicht akzeptiert werden dürfen, wie unzulässige Zahlen-, Datumswerte und Sonderzeichen) sind auch Suchvorgänge, Datenexporte und das Abrufen von Quartals- oder Jahresstatistiken empfehlenswerte Testfälle.

Bei größeren Kommunen und bedeutenden Verfahren können gesonderte Testumgebungen und ein Testmanagement mit automatisierten Tests hilfreich sein.
Die systemseitigen und lizenzrechtlichen Anforderungen einer Testumgebung sollten bereits bei der Beschaffung der Anwendung berücksichtigt werden.
Aus Datenschutzgründen dürfen in Testumgebungen nur Testdaten genutzt werden. Anonymisierte Echtdaten dürfen erst nach Freigabe durch den Datenschutzbeauftragten verwendet werden. Manche Fachverfahrenshersteller bieten spezielle Anonymisierungs-Skripte an.

2.3.6. TIPPS

Eine Standardisierung der Systeme und Anwendungen erhöht die Effizienz, indem es die Aktualisierungsaufwände in Grenzen hält.
Bei Virenscannern erleichtert eine Enterprise-Lösung neben dem Signaturmanagement auch das Updatemanagement und bietet darüber hinaus noch weitere Features.
Üben Sie die Prozesse, vor allem die Abläufe für dringende Zero-Day-Notfallpatches.

2.4 Technische Umsetzung

2.4.1 VORBEMERKUNG ZU SEHR KLEINEN UMGEBUNGEN

Wenn lediglich eine Handvoll Arbeitsplätze vorhanden sind, werden oftmals automatische Updatemöglichkeiten direkt vom Hersteller am Client genutzt. Diese werden von Betriebssystemen, Office-Produkten und sonstigen Anwendungen zur Verfügung gestellt.
Die regelmäßigen oder anlassbezogenen Updates bzw. Patches, vor allem an Servern oder Netzwerkkomponenten, erfolgen häufig durch externe Unterstützung.
Hier sollte auf folgende Punkte Wert gelegt werden:

- Update-/Patch-Konzept,
- Administrationstätigkeiten durch qualifiziertes Personal,
- koordinierte Updates,
- ausreichend Bandbreite der Internetanbindung (ohne zentrale Update-/Patchverteilung muss in der Regel jeder Rechner selbst alle Updates, Patches und Treiber aus dem Internet laden),
- zentrale Inventarisierung (Stand der Systeme muss dokumentiert werden),
- detaillierte vertragliche Regelungen und
- Überwachung und Kontrolle der durchgeführten Arbeiten.

Das LSI empfiehlt zentrale Systeme zur Inventarisierung und zur Dokumentation der Patches und Updates.

2.4.2 IT-INVENTARISIERUNG

Eine ausreichende IT-Sicherheit kann nur mit Hilfe einer lückenlosen Inventarisierung aller IT-Systeme gewährleistet werden. Das haushaltsrechtlich gebotene Inventarverzeichnis ist für die IT bei weitem nicht ausreichend, da dort grundlegende IT-Informationen wie z. B. MAC-Adressen, weitere Hardwaredetails und Versionsstände fehlen. Für die IT-Inventarisierung bietet sich

als zentrale Komponente eine CMDB (Configuration Management Data Base) an. Diese kann automatisch über Agents mit Hard- und Softwareinformationen befüllt und aktuell gehalten werden. Darüber hinaus kann die CMDB auch Konfigurationsdaten und die logischen Verbünde der Systeme (Informationsverbünde) aufnehmen. Es empfiehlt sich die CMDB in Instanzen in unterschiedlichen Netzwerksegmenten zu platzieren (Externe Geräte – DMZ, Server – Server-Netz, Clients – Client-Netz). Entsprechende Lösungen finden sich auch im OpenSource-Bereich. Hilfreich sind Abgleiche des IT-Inventars mit Personaldaten (hier sollte der Datenschutzbeauftragte und der Personalrat beteiligt werden).

2.4.3 UPDATESYSTEM

Ein Updatesystem prüft die Aktualität der Systeme anhand des Inventarisierungsstandes. Hierfür stellt es Abfragen, Filter, Berichte und Aktionen/Jobs zur Verfügung.
Über einen Dienst bzw. Agenten werden am Client die fehlenden Aktualisierungen über das Netzwerk angefordert und anschließend eingespielt. Virtuelle Systeme und Systeme außerhalb des Active Directory müssen ggf. von Hand in das Updatesystem aufgenommen werden.
Das Updatesystem sollte über ein sogenanntes Repository verfügen. Dieses ist eine zentrale datenbankgestützte Sammlung von Updates und Patches, die von den Softwareherstellern automatisch bezogen und gruppiert werden. Die zu aktualisierenden Rechner und Systeme beziehen ihre Updates und Patches dann ausschließlich vom Updatesystem und nicht mehr vom Hersteller aus dem Internet. Bei den auf diese Weise aktualisierten Systemen und Anwendungen sollte die Funktion zum automatischen Update deaktiviert werden.
Darüber hinaus gibt es die Möglichkeit, Updates über *Softwareverteilungssysteme* zu verteilen. Die eingesetzte Lösung hängt von den Erfordernissen und der Größe der Kommune ab. Die Spanne reicht vom reinen Updatesystem für Windows-Systeme (beispielsweise Microsoft-WSUS-Server) bis hin zu einem umfassenden Softwareverteilungssystem. Mit einem reinen Updatesystem wie WSUS von Microsoft können nicht alle Programme und Tools aktualisiert werden. Softwareverteilungssysteme bieten über die Aktualisierung hinaus die Möglichkeit der Deinstallation und der Neuinstallation von Anwendungen. Für einige Softwareverteilungssysteme sind zeitsparende und erfahrungsgemäß wirtschaftliche Abonnements vorprogrammierter Paketvorlagen (prefabricated software) erhältlich.
In allen Updatesystemen sollte die Kritikalität der Sicherheitslücken in entsprechenden Zeitplänen berücksichtigt werden.
Zentrale Updatelösungen sollten die Updates möglichst zertifikatsbasiert beziehen und auf die Clients ausrollen.
Für die Verwaltung und Aktualisierung von Mobilgeräten können spezielle Mobile Device Management Systeme (MDM) genutzt werden. Die Mobilgeräte sollen sich damit regelmäßig abgleichen. Größere Aktualisierungen wie Betriebssystemupdates sollen nur über WLAN erfolgen.
Hinweise:
Professionelle Lösungen, die einer Gemeinde auf den ersten Blick zu teuer erscheinen, könnten in kommunaler Zusammenarbeit wirtschaftlich und sicher zu betreiben sein.
Für das Aktualisieren von Windows 10 bzw. Server 2016 oder höher sollte eine geeignete WSUS-Version zum Einsatz kommen (ebenfalls Version 2016 oder höher).

2.4.4 PATCHEN VON HAND

Bei manuellen Downloads sollten authentische Bezugsquellen verwendet werden, ausschließlich von bekannten, sicheren Webseiten des Herstellers (https://...).
Wenn der Hersteller die Möglichkeit bietet, die Authentizität von Updates oder Patches mit sogenannten Hashwerten zu verifizieren, sollte dies dringend genutzt werden. Hierfür gibt es frei verfügbare Tools oder Kommandozeilenbefehle wie certutil.

2.4.5 IOT

Auch in Kommunen werden zunehmend IoT-Geräte (Internet of Things = Internet der Dinge) wie vernetzte Überwachungskameras, Beamer, Haustechnik, Zutritts-Systeme etc. eingesetzt. Aus dem Internet erreichbare IoT-Geräte werden häufig angegriffen. Sie sollten daher ebenfalls auf einem aktuellen und sicheren Firm- und Softwarestand gehalten werden.
Weiterführende Informationen können dem LSI-Info „T04_IoT“ entnommen werden.

2.5 Dokumentation

Das Update- und Patchmanagement sollte ausreichend dokumentiert werden. Die Managementsysteme bieten hierfür entsprechende datenbankgestützte Abfragen und Berichte.

§ 3. RECHTLICHE EINORDNUNG

Das Erfordernis eines Patchmanagements einschließlich Dokumentation ergibt sich u. a. aus Art. 5 Abs. 1 Buchstabe f, Art. 5 Abs. 2 DSGVO und Art. 32 Abs. 1 Buchstabe b der DSGVO.

Im *Bayerischen Behördennetz* dürfen gemäß BayITSiR-13 ausschließlich Betriebssysteme und Software-Komponenten eingesetzt werden, für die durch den Hersteller Sicherheitsupdates angeboten werden.

Daneben wird von allen zertifizierungsfähigen *Informationssicherheitsmanagementsystemen* ein Patchmanagement gefordert.
Exemplarisch im IT-Grundschutz des BSI „OPS.1.1.3 Patch- und Änderungsmanagement“:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2021.html

Bitte beachten Sie beim Betrieb kritischer Infrastrukturen die einschlägigen Vorgaben.

? KONTAKT

Weitere Informationen finden Sie unter:
https://lsi.bayern.de/kommunen/
Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:
Beratung-Kommunen@lsi.bayern.de.
Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911/215 49 - 523 für Sie erreichbar.