Wann und wie oft sollte man Updates installieren?

Intention

Dieses Pattern befasst sich mit der generellen Update-Thematik für Software-Applikationen sowie Betriebssystemen auf dem eigenen Computer als auch auf dem Server. Fokussiert wird, wann, in welchen Zeitabständen und wieso Updates generell installiert werden sollen.

Problemstellung

Software oder Systeme aktuell zu halten ist wichtig. Systeme die **nicht** mit den aktuellsten Updates ausgestattet sind, bieten Angreifern mehr Angriffsfläche verglichen mit Systemen die durch stetige Updates auf dem neuesten Stand gehalten werden.

Szenario

Um das eigene System abzusichern und potenziellen Angreifern weniger Angriffsfläche zu bieten, muss es mit den aktuellsten Updates versorgt werden.

Lösung

Updates sollten in **regelmäßigen Abständen** installiert werden. Wichtig ist hierbei, dass der Ausdruck **regelmäßig** keine genaue Zeitangabe definiert. Wir empfehlen daher die Auto-Update Funktion zu nutzen, sofern eine Applikation diese anbietet. Abgesehen davon, sollten wichtige, sicherheitsrelevante Programme (z.B. Antiviren Software) täglich und die restlichen Programme wöchentlich oder monatlich auf Updates überprüft werden.

Bevor Updates jeglicher Art installiert werden, wird empfohlen sicherheitshalber ein Backup des Systems zu erstellen.

Updates können in ungünstigen Fällen zu Problemen oder Inkompatibilitäten führen. Vor allem größere Aktualisierungen oder Versionssprünge in Programmen können unter Umständen irreversibel sein. Gerade deshalb sollte für Updates genügend Zeit eingeplant werden um das System oder Programm nach einem Update auf Herz und Nieren zu prüfen. Mehr Informationen zum Thema Backups findet man im Pattern: „**Wann und wie sollte man Backups erstellen?**“.

- Es empfiehlt sich, **Systeme und Software von Anfang an aktuell zu halten**.

- Aktuell bedeutet, dass alle zum aktuellen Zeitpunkt bereitgestellten (vorrangig sicherheitsrelevanten) Updates für ein System oder eine Software installiert sind.
- Systeme, Software oder auch Websites die mit **sensiblen Daten** arbeiten, haben eine **höhere Priorität**.
- Es empfiehlt sich eine tägliche Prüfung auf Aktualisierungen für Systeme oder Computer die auf den Server der Website zugreifen, sowie für die Applikationen die auf dem Server laufen. Vor allem, wenn mit personenbezogenen oder sensiblen Daten (Kontodaten, Adressen, o.Ä.) gearbeitet wird.
- Üblicherweise kümmert sich der Webhoster um das Aktualisieren der Kern-Applikationen (z.B. Betriebssystem, mySQL, PHP, usw.).
- Einführung eines **Update-Tages** ist empfohlen. Beispielsweise **einmal im Monat** für das ganze System oder **einmal wöchentlich** für Systeme oder Applikationen, die mit **wichtigen bzw. personenbezogenen Daten** hantieren.
- Automatisierte Updates werden empfohlen, jedoch sollte man in regelmäßigen Abständen **(einmal Wöchentlich)** auch **manuell** danach suchen.
- Es gibt immer wieder Fälle in denen nach automatischen Updates die Update-Funktion nicht mehr ordnungsgemäß funktioniert und somit Updates nicht mehr automatisch aufgespielt werden.
- Informationsnetzwerk aufbauen, welches einen über Updates informiert. Viele Soft- und Hardware Anbieter stellen Mailinglisten oder Informationsseiten hierfür zur Verfügung.

Sollte ein System oder bestimmte Programme keinen Support in Form von Updates erhalten, wird angeraten sich nach Alternativen umzusehen, die aktuell gehalten werden.

Beispiele

Autoupdates
In bestimmten Zeitintervallen (z.B. stündlich, täglich oder wöchentlich) sucht das System selbstständig nach Aktualisierungen.

Patchday
An einem *Patchday* werden Updates zu einem fixen Zeitpunkt, der vorher festgelegt wird, aufgespielt. Die Updates werden vor dem Aufspielen auf das Hauptsystem üblicherweise auf einem separaten System getestet, um etwaige Probleme und Kompatibilitätsprobleme auszuschließen.

Software Update Strategie
Entwickeln einer eigenen Update-Strategie, die einen Zeitplan vorgibt in welchem nach Updates gesucht wird und diese aufgespielt werden. Zudem erlaubt dieser es auch, nachzuvollziehen wann und welche Updates für welche Systeme oder Software aufgespielt wurden.

WordPress Update
WordPress bietet zwei verschiedene Möglichkeiten der Aktualisierung. Die erste Möglichkeit ist die automatische Update-Funktion, Möglichkeit Nummer zwei ist das manuelle Update.

- Um die automatischen Update-Funktion von WordPress zu nutzen, wählt man im WordPress Admin-Panel in der Seitenleiste den Punkt „Aktualisierungen“. Sofern die WordPress-Installation mit den Standardeinstellungen installiert wurde, erreicht man diese Update-Funktion auch unter folgenden URL: www.beispielseite.at/wp-admin/update-core.php. Auf dieser Seite steht ob Aktualisierungen für WordPress, dessen Komponenten oder Plugins vorhanden sind. Sofern Aktualisierungen vorhanden sind, können diese automatisch durchgeführt werden.
- Um WordPress manuell zu aktualisieren, lohnt es sich folgende Anleitung anzusehen: https://help.one.com/hc/de/articles/115005585989-WordPress-manuell-aktualisieren.

Wichtige Mailinglisten

Im unten verlinkten Artikel wird die Update-Thematik etwas vertieft. Zusätzlich werden am Ende des Artikels wichtige Mailinglisten bereitgestellt: http://www.linux-magazin.de/ausgaben/2004/08/keine-wissensluecke/
Weitere Mailinglisten und Zusatzinformationen sind auch hier zu finden: http://www.netzmafia.de/skripten/sicherheit/sicher9.html

Referenzen

D. L. Parnas, “Software aging,” *Proceedings of 16th International Conference on Software Engineering*, Sorrento, 1994, pp. 279-287.
Bellissimo, Anthony, John Burgess, and Kevin Fu. “Secure Software Updates: Disappointments and New Challenges.” *HotSec*. 2006.
Understanding Patch and Update Management: Microsoft’s Software Update Strategy
Apple – Sicherheitsupdates
SCCM Softwareupdate Strategy
Why updating your Software is a Must Do
WordPress – Security Category Archive

Keywords

Updates, Sicherheit, Software, Backups