Patchmanagement im KMU-Umfeld

Das Einspielen von Updates ist eine wirksame Massnahme, um Schwachstellen in der Sicherheit komplexer digitaler Systeme zu beheben. Mit einem guten Patchmanagement gelingt eine reibungslose Umsetzung auch im KMU.

Wichtigste Merkpunkte:

- Definieren Sie regelmässige Zeitfenster ausserhalb der Produktionszeiten für die Wartung Ihrer Systeme.
- Beziehen Sie Sicherheitsupdates ausschliesslich aus vertrauenswürdigen Quellen.
- Prüfen Sie Wirksamkeit und «Nebenwirkungen» von Sicherheitsupdates, bevor sie diese auf produktiven Systemen installieren.
- Legen Sie einen Plan für die Verteilung von Sicherheitsupdates auf Ihren Systemen fest.
- Halten Sie ein aktuelles Backup und ein Fallback-Szenario in der Hinterhand, falls beim Update etwas schieflaufen sollte.
- Dokumentieren Sie die an den Systemen vorgenommenen Wartungsarbeiten.

Sicherheitsupdates

Die Entwicklung von IT-Systemen schreitet immer schneller voran: Funktionalitäten von Applikationen nehmen stetig zu, und die Lebenszyklen von Hard- und Software werden tendenziell kürzer. Hersteller sind deshalb bestrebt, ihre neusten Errungenschaften mittels Aktualisierungen (Updates) schnell in Umlauf zu bringen.

Im KMU-Umfeld kann hierbei durchaus eine gewisse Zurückhaltung geübt werden, weil sich nicht jede Neuerung auch effizient auf den Betriebsprozess umlegen lässt. Eine strikte Ausnahme dazu bilden jedoch Sicherheitsupdates, welche möglichst umgehend eingespielt werden sollten.

Jedes komplexe System weist versteckte Fehler oder Schwachstellen auf. Vielfach bleiben diese lange unbemerkt und harmlos. Sind solche jedoch einmal entdeckt, werden sie zu ernstzunehmenden Verletzlichkeiten (im IT-Umfeld Vulnerabilities genannt), denn nun beginnt ein Wettlauf mit der Zeit.

Auf der einen Seite beginnen Hacker nach Wegen zu suchen, diese offengelegten Schwachstellen für ihre Zwecke auszunutzen und sogenannte Exploits zu entwickeln. Gelingt dies, können sich böswillige Akteure zum Beispiel unautorisierten Zugang zu Systemen und Daten verschaffen.

Auf der anderen Seite machen sich die Hersteller daran, mittels Sicherheitsupdates oder Patches diese Schwachstellen möglichst schnell zu beheben und damit allfälligen Exploits zuvor zu kommen oder bereits bestehende Exploits unschädlich zu machen.

Das Patchmanagement

Grundsätzlich sollten Sicherheitsupdates also möglichst schnell und flächendeckend eingespielt werden. Was auf einem privaten Einzelplatzsystem im Allgemeinen einfach zu bewerkstelligen ist, kann im KMU jedoch durchaus seine Tücken haben. Es braucht deshalb ein geordnetes Vorgehen in Form eines Patchmanagement-

Prozesses.

Für die Installation von Sicherheitsupdates sind jeweils folgende Schritte zu beachten:

- Identifikation der betroffenen Systeme und der hierfür geeigneten Sicherheitsupdates.
- Beschaffung der Sicherheitsupdates aus einer vertrauenswürdigen Quelle, insbesondere auch für Systeme ohne direkten Internet-Zugang.
- Vorgängiges Testen von Wirksamkeit und «Nebenwirkungen» von Sicherheitsupdates auf nicht kritischen Systemen.
- Systemabhängige Freigabe von Sicherheitsupdates und Terminierung der Installation ausserhalb der Produktionszeiten.
- Bei kritischen Systemen: Planung von temporären Ausweichlösungen und Fallback-Szenarien.
- Dokumentation der vorgenommenen Änderungen.

Da es sich hierbei um einen rollenden Prozess handelt, empfiehlt sich das Festlegen von periodischen, fixen Zeitfenstern für die Wartung der Systeme. So können Sicherheitsupdates über eine gewisse Zeit gesammelt, geprüft und vorbereitet werden, deren Installation jedoch bis zum nächsten Zeitfenster aufgeschoben werden.

Das Patchmanagement beschäftigt sich mit der Beschaffung, dem Testen und der Installation von Software-Updates. Die Hauptaufgabe ist das Schliessen von Sicherheitslücken in Betriebssystemen und Applikationen.

Weitergehende Informationen

Zur Identifikation der betroffenen Systeme und der hierfür geeigneten Sicherheitsupdates tragen zahlreiche Faktoren bei. Zum einen spielt die Hardware selbst eine Rolle. Hier sind es hauptsächlich die Firmware und die Treiber, die aktuell gehalten werden müssen. Es folgen das Betriebssystem sowie die installierten Applikationen, die auf verfügbare Updates geprüft werden müssen.

Für Systeme mit direktem Internet-Zugang existieren automatisierte Scanner-Lösungen, welche periodisch ein Hard- und Software-Inventar aufnehmen und online nach verfügbaren Updates suchen. Im KMU sollten diese Systeme höchstens unterstützend eingesetzt werden. Von einer unüberwachten Installation von Updates muss hingegen dringend abgeraten werden. Es sollte immer ein Techniker die Kontrolle über den Installationsprozess haben.

Die Beschaffung der Sicherheitsupdates kann ebenfalls ein heikles Unterfangen bedeuten, denn nicht immer handelt es sich bei den im Internet am einfachsten auffindbaren Updates um «Originalware». Das Risiko besteht in solchen Fällen darin, dass mit dem vermeintlichen Sicherheitsupdate der eigentliche Exploit aufs System gebracht wird. Wenn immer möglich, sollte man sich deshalb an die offiziellen Vertriebskanäle der Hersteller halten.

Bevor ein Update auf einem produktiven oder gar kritischen System eingespielt wird, sollte man sich dessen Kompatibilität mit dem betreffenden System und mit der Umgebung vergewissern. Optimalerweise geschieht dies durch das Testen von Wirksamkeit und «Nebenwirkungen» (d.h. potentiell unerwünschten Seiteneffekten) von Sicherheitsupdates in einer isolierten, nicht produktiven Umgebung. In KMU ist eine solche allerdings häufig nicht verfügbar.

Es ist dennoch ratsam, eine systemabhängige Freigabe von Sicherheitsupdates vorzunehmen, z. B. indem zunächst die weniger kritischen Systeme für die Behandlung vorgezogen werden. Erst nach einer gewissen Beobachtungszeit und einigen Tests kann man die restlichen Systeme folgen lassen.

Für die Installation von Updates sollten, insbesondere für kritische Systeme, genügend grosse Zeitfenster ausserhalb der Produktionszeiten reserviert werden. Ebenso sollte man sich mittels Backups (https://www.ebas.ch/datensicherung-im-kmu-umfeld/) und möglichen Ausweichlösungen auf ein Fallback-Szenario vorbereiten, sollte das Update nicht erfolgreich installiert werden können.

Die vorgenommenen Schritte des Update-Vorgangs sollten in einer Dokumentation nachvollziehbar festgehalten werden. Bei einer allfälligen späteren Fehlersuche könnten daraus entscheidende Hinweise auf deren Ursache gezogen werden.