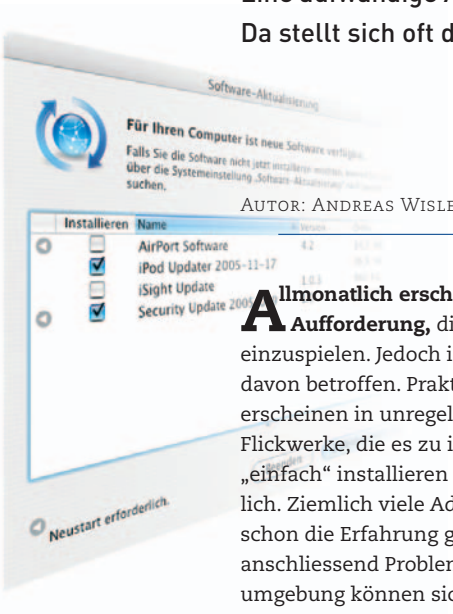
IT-Sicherheit

Patchen – muss das sein?

Jeden Tag werden neue Lücken in Software entdeckt und durch Patches behoben. Nicht nur Microsoft ist davon betroffen, sondern auch viele andere Produkte. Eine aufwändige Arbeit für den Administrator. Da stellt sich oft die Frage, muss das sein?



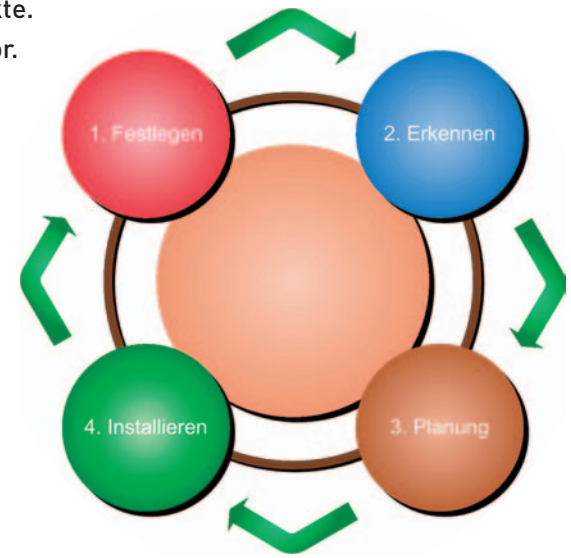
Autor: Andreas Wisler

Allmonatlich erscheint von Microsoft die Aufforderung, die neuesten Patches einzuspielen. Jedoch ist nicht nur Microsoft davon betroffen. Praktisch für jede Software erscheinen in unregelmässigen Abständen Flickwerke, die es zu installieren gilt. Doch „einfach" installieren ist dabei oft nicht möglich. Ziemlich viele Administratoren haben schon die Erfahrung gemacht, dass ein Patch anschliessend Probleme bereitet. Eine Testumgebung können sich aber nur wenige Firmen leisten und da ist jeder Patch eine Herausforderung. Daher warten viele einfach mal ab, was andere berichten. Wenn es keine Probleme gibt, dann wird der Patch (vielleicht) auch installiert.

Statistiken zeigen auf der anderen Seite, dass neue Schwachstellen immer schneller ausgenutzt werden. Inzwischen sind wir bei den vor einiger Zeit angekündigten Zero-Day-Attacken angelangt, das heisst, es sind schon am gleichen Tag Programme verfügbar, die diese Lücke ausnutzen.

Ganz auf einen Patch zu verzichten ist ein gefährliches Spiel mit dem Feuer. Beispiele von schlecht gewarteten Systemen trifft man immer wieder an. Vielen ist sicher noch der SQL Slammer Zwischenfall der Schweizerischen Post in Erinnerung oder der Virenausbruch des Migros Genossenschaftsbundes.

SQL Slammer hat alleine 75.000 Server in wenigen Stunden befallen und 55 Millionen IP-Adressen pro Sekunde gescannt. Da bleibt nur wenig Zeit, bei Ausbruch oder bekannt werden der Attacke zu reagieren.



Schaden, Folgen

Sollte ein schlecht gepatchtes System angegriffen werden, sind die Folgen nicht abschätzbar:

- **Downtime**
  Sind die Systeme nicht mehr erreichbar, steht oft der gesamte Betrieb still. Dies kann zu Produktionsausfällen, nicht eingehaltenen Terminen usw. führen.
- **Wiederherstellungszeit**
  Gleichzeitig mit der Downtime stellt sich auch die Frage, wie lange es dauert, bis die Systeme wieder bereit sind, Ihre Aufgaben zu erfüllen. Fehlt ein Backup/Desaster-Recovery-Plan, ist ein strukturiertes Vorgehen sehr schwierig. Dementsprechend dauert es relativ lange, bis die Systeme wieder zu 100 % zur Verfügung stehen.
- **Daten-Integrität**
  Ist eine Lücke erfolgreich ausgenutzt wurden, muss kontrolliert werden, ob die Daten nicht verändert oder anderweitig beschädigt wurden. Diese Kontrolle muss sich auf alle Daten beziehen, nicht nur auf die Daten der angegriffenen Systeme. Es muss verhindert werden, dass mit manipulierten Dateien weiter gearbeitet wird.
- **Kosten**
  Nicht vergessen werden darf, dass alle Arbeiten nicht nur viel Zeit beanspruchen,

sondern auch Geld kosten, sei dies durch Überstunden der Administratoren, den Arbeitsausfall der Mitarbeiter oder verpassten Aufträgen oder Auslieferungen.

- **Image**
  Oft leidet unter einem erfolgreichen Angriff auch das Image einer Firma. Will ich tatsächlich hier bestellen? Kann mir diese Firma für die Zukunft garantieren, dass dies nicht mehr passiert? Dies sind sicherlich Gründe dafür, dass nur sehr selten von erfolgreichen Attacken zu lesen ist. Lieber hält man dies als „kleines" Geheimnis für sich, als dass es die Presse, Kunden oder Mitbewerber erfahren.
- **Rechtliche Situation**
  Schlecht gewartete Systeme bergen auch die Gefahr, dass diese für illegale Zwecke missbraucht werden. Der meiste Spam wird über genau diese schlecht geschützten Systeme verbreitet. Auch werden diese für Dateiablagen jeglicher Art ausgenutzt.
- **Gestohlene Daten**
  Viel schwerer als das Stören der Systeme wiegen gestohlene Daten. Gelangen vertrauliche Daten in die falschen Hände ist der Schaden oft enorm.

Risikostufen

Die verfügbaren Patches werden in verschiedene Stufen eingeteilt: Kritisch, Wichtig, Moderat und Gering. Kritische und wichtige Patches sind dabei mit besonderem Augenmerk zu beachten und baldmöglichst zu installieren.

Damit die Administratoren einfach erkennen können, wie wichtig der Patch ist, wird zusätzlich jedem Patch eine Priorität zugeordnet: Notfall (Emergency), Hoch (High), Mittel (Medium) und Klein (Low). Notfallpatches sollten innerhalb von 24 Stunden installiert werden. Hohe Priorität bedeutet innerhalb von Wochen, mittlere Priorität innerhalb Monate sowie kleine Priorität innerhalb eines Jahres.

Vorgehen

Um Patches zu installieren, sollte ein vierstufiges Verfahren angewendet werden:

1. Festlegen
Legen Sie als erstes fest, welche Systeme gefährdet sind. Sind diese Systeme von aussen erreichbar oder beschränkt sich die Angriffsfläche auf die interne Struktur? Je grösser die Gefährdung ist, umso wichtiger ist es, dass diese Systeme im Auge behalten werden.

2. Erkennen
Neue Schwachstellen und Updates/Pachtes werden über verschiedene Wege veröffentlicht. Organisieren Sie sich so, dass Sie an diese Meldungen gelangen. Sobald neue Patches verfügbar sind, sollten diese auch installiert werden.

3. Planung
Planen Sie in einem weiteren Schritt, wie und wann diese Patches installiert werden. Muss dabei ein Wartungsfenster vorgesehen werden, in welchem die Systeme nicht verfügbar sind? Oder beschränkt sich das Problem nur auf eine Applikation, die auch an einer Randstunde aktualisiert werden kann? Kontrollieren Sie auch, ob Patches zusammengefasst und in einem Schritt installiert werden können.

4. Installieren
Im letzten Schritt gilt es, gemäss Planung die Patches zu installieren. Überprüfen Sie anschliessend, ob alle Systeme noch wie gewünscht funktionieren. Dies gilt nicht nur für das Betriebssystem, sondern auch für die installierte Software.

Informationsquellen

Patches können nur dann installiert werden, wenn auch bekannt ist, dass solche vorhanden sind. Die Wege, um an solche Informationen zu kommen, sind vielfältig. Oft fehlt aber die Zeit, alle diese Informationen zu verarbeiten. Folgende Möglichkeiten bestehen:

- **Homepage des Herstellers:** jeder Hersteller erwähnt auf seiner Homepage, wenn neue Patches verfügbar sind. Meistens sind auch viele Detailinformationen vorhanden, welche Lücken dabei geschlossen werden. Einige Hersteller haben auch eine eigene Seite reserviert, wo über Sicherheitshinweise informiert wird (z.B. Microsoft unter: www.microsoft.com/switzerland/security/de).
- **Newsletter:** Im Internet sind zahlreiche Newsletter vorhanden, die nur über Schwachstellen berichten (z.B. Bugtraq). Die meisten Hinweise sind jedoch für die eigene Umgebung irrelevant und der Newsletter wird nur noch flüchtig quer gelesen. Daher lohnt es sich, den Newsletter des Herstellers der eingesetzten Software zu abonnieren.
- **Spezialisierte Homepages:** Nebst den Newslettern gibt es auch spezialisierte Homepages, die alle Informationen sammeln und übersichtlich zusammentragen. Eine Möglichkeit ist dabei www.securityfocus.com

Abonnieren Sie mindestens den Sicherheitsnewsletter des Herstellers der eingesetzten Software. So erhalten Sie alle Informationen schnell und zuverlässig und müssen nicht regelmässig verschiedene Homepages aufsuchen.

Logbuch

Damit Sie nicht die Übersicht verlieren, empfiehlt es sich, eine Liste mit der vorhandenen Software zu führen. Auf dieser Liste sind auch die aktuelle Version, die Homepage des Herstellers sowie installierte Patches peinlich genau zu notieren. Somit haben Sie zu jedem Zeitpunkt die Übersicht.

Zusammenfassung

Patchen darf keine Arbeit nebenbei sein. Der Schaden, der ein fehlender Patch nach sich ziehen kann, darf nicht unterschätzt werden. Ein strukturiertes Vorgehen ist dabei wichtig. Die Informationen über neue Updates müssen vorhanden sein, damit der Patch nach einem vorgelegten Schema installiert werden kann. Schützen Sie sich vor neuen Gefahren – ein Patchmanagement hilft Ihnen dabei weiter. ◆

Zum Autor

Andreas Wisler (Tel. 052 320 91 20) ist Geschäftsführer der GO OUT Production GmbH, welche sich mit IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. Er unterrichtet in der Klubschule Migros den Lehrgang „IT-Security Manager", darüber hinaus veröffentlicht er regelmässig einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.goSecurity.ch bestellt werden kann. Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.