

good news! vom 13. August 2008

## **Warum Patch-Management häufig scheitert**

geschrieben von Edgars Kalejs

Die Vorkehrungen für die Behebung von Sicherheitsrisiken sind vielerorts nicht ausreichend. IT-Manager erweisen sich in einer Studie zwar meist risikobewusst. Gleichwohl mangelt es vielen Unternehmen an einem transparenten Patch- und Pattern-Management.

Die Gefahr durch so genannte Zero Day Exploits wird immer größer. Sicherheitslücken werden dabei innerhalb von weniger als einem Tag nach ihrem Bekanntwerden von Angreifern ausgenutzt. Die Mehrzahl der vom Sicherheitsdienstleister Ampeg Technologie und Computer Service GmbH im Rahmen einer Studie Befragten ist sich zwar dieser Gefahr durchaus bewusst. Doch der Wunsch nach aktueller Information und das Risikobewusstsein decken sich nicht mit der Wirklichkeit in vielen Betrieben. So bekommt in Meetings zur internen Sicherheitslage nur jeder Vierte tagesaktuelle Auswertungen zu Gesicht. In Betrieben mit mehr als 5.000 PC-Arbeitsplätzen ist dieser Anteil mit 29,4 Prozent etwas höher als im Durchschnitt aller Firmen. In Betrieben mit weniger als 1.000 elektronischen Arbeitsplätzen dagegen erhält nur jeder fünfte IT-Verantwortliche einen tagesaktuellen Überblick über die Sicherheitslage.

In etwas mehr als jedem vierten Unternehmen wird demnach in Sicherheits-Meetings mit Daten gearbeitet, die etwa eine Woche alt sind. Bei 17 Prozent sind die Angaben vier Wochen alt, bei noch einmal so vielen Firmen sogar noch älter. In den meisten Firmen wird bei Sitzungen zur Sicherheitslage das Viren- und Spam-Aufkommen mit dem des Vormonats verglichen. Jeweils mehr als 60 Prozent der Befragten gaben dies an. Ein Monatsvergleich der Zahlen an erfolgreich verteilten Patches und Viren-Signaturen findet indes nur in gut der Hälfte der Unternehmen statt.

Dass der Faktor Zeit beim Patch- und Pattern-Management eine große Rolle spielt, ist indes den meisten klar. Zwei Drittel gaben an, schon wenn sich die Auslieferung von Patches oder Virensignaturen um wenige Stunden verzögere, führe das zu einer großen zusätzlichen Bedrohung. Um die Verteilung von Patches und Patterns zu kontrollieren, hält die Hälfte der Befragten ein funktionierendes Management der Sicherheits-Updates für nötig. 51,1 Prozent sagten, das firmeneigene Sicherheitssystem sei ansonsten 'eigentlich nichts wert'. 68,1 Prozent hätten gerne die Möglichkeit, auf Abruf den Update-Status aller Rechnersysteme zu erfahren. Weitere 19,1 Prozent würde den Status immerhin gerne für besonders sicherheitskritische Systeme ermitteln können.

Wie lange es dauert, bis ein neuer Patch oder ein Pattern an alle Computer-Arbeitsplätze im Unternehmen verteilt ist, kann die Mehrzahl der IT-Manager nicht genau angeben. 44,7 Prozent sagten, sie könnten die Zeit abschätzen, 14,9 Prozent haben dazu überhaupt keine Erkenntnisse. 40,4 Prozent der Befragten gaben an, sie wüssten ziemlich genau, wie lange die Verteilung dauert. Konkrete zeitliche Vorgaben für die Verteilung von Patches und Virensignaturen gibt es indes in sechs von zehn Firmen. 12,8 Prozent der Befragten gaben an, ein neues Pattern sollte innerhalb einer Stunde nach Erscheinen auf jedem Rechner installiert sein. Weiteren 17 Prozent reicht es, wenn dies innerhalb von sechs Stunden geschieht. Jeder Fünfte meint, das dürfe bis zu zwölf Stunden dauern, mehr als ein Drittel findet einen Zeitraum von bis zu 24 Stunden ausreichend. 6,4 Prozent der Befragten sagten, die Pattern-

Verteilung dürfe sogar noch länger dauern.

Wie sehr sich bei den einzelnen Befragten Wunsch und Wirklichkeit decken, schlüsselt die Befragung nicht auf. Abweichungen werden gleichwohl deutlich. So sind neue Patterns in 7,5 Prozent der Unternehmen nach einer Stunde auf allen Rechnern verfügbar - fünf Prozentpunkte weniger als die Zahl derer, die sich eine Verfügbarkeit innerhalb einer Stunde wünschen.

Ähnlich sieht es bei der Frage nach Sicherheits-Patches aus. Jeder zehnte Befragte meint, ein neues Patch sollte binnen höchstens zwölf Stunden auf alle Rechner verteilt sein. Doch nur jedem Zwanzigsten gelingt das auch. Am stärksten decken sich Anspruch und Wirklichkeit bei der Angabe, es reiche aus, wenn ein neues Patch innerhalb von mehr als zehn Tagen auf den Systemen installiert sei. 14,9 Prozent sind dieser Ansicht, und bei 15 Prozent dauert die Verteilung tatsächlich so lange.

Geht es um die interne Freigabe eines Sicherheits-Patches, sind die Unterschiede zwischen Soll und Ist nicht groß. Jeder Fünfte meint, nach der internen Freigabe blieben bis zu zwölf Stunden, um ein Patch zu verteilen. Ebenso vielen gelingt es auch, diese Frist einzuhalten. Dass die Verteilung nach der internen Freigabe 24 Stunden dauern dürfe, meinen drei von zehn Befragten. So viele schaffen es auch, ein Patch innerhalb dieser Zeit zu verteilen. Dass Rechner gar nicht mit Patches oder Patterns versorgt werden, ist der Befragung zufolge keine Seltenheit. In mehr als jeder zweiten Firma kommt das vor, und die entsprechenden Rechner werden regelmäßig identifiziert. Rund sechs Prozent haben darüber keine gesicherten Erkenntnisse. Fast vier von zehn IT-Managern gaben dagegen an, sie könnten sicherstellen, dass so etwas nicht vorkomme. Fast die Hälfte der Befragten gab an, sie überprüften nach einer festgelegten Vorgehensweise, ob Patches und Patterns tatsächlich auf jedem Rechner ankommen. Ein weiteres Drittel überprüft das stichprobenartig, mehr als jeder Zehnte gar nicht.

Der Marktforscher Innofact AG hat die Befragung 'Kontrolle über IT-Sicherheit behalten' im Auftrag des IT-Sicherheitsdienstleisters Ampeg durchgeführt. 47 IT-Experten aus Firmen verschiedener Größe standen Rede und Antwort. Die meisten Befragten arbeiten als IT-Leiter oder Chief Security Officer.