

COMPUTERWOCHE

www.computerwoche.de

MALWARE:

Wie gut ist Ihre IT geschützt?

Ein Chief Security Officer muss den Sicherheitsstatus seines gesamten Netzes kennen. Hier die wichtigsten Kriterien, die man für eine entsprechende Messung heranziehen sollte.

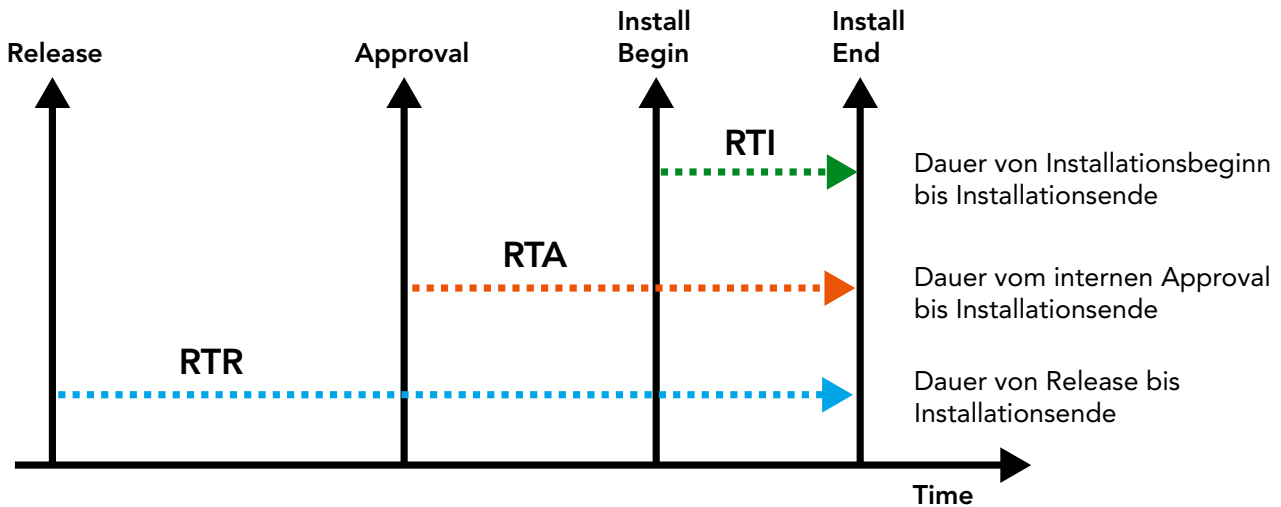
Von **Peter Graf***

Viren, Würmer und Trojaner sind noch immer die breitenwirksamsten Waffen der „Malware-Industrie“. Um sich gegen eine Infektion zu schützen, installieren Sicherheitsverantwortliche Virenschutz- und Patch-Systeme. Updates mit Virenpattern und Patches sind die letzte und gleichzeitig eine der wirksamsten Hürden im Abwehrwall. Ist jedes System im gesamten Netz mit aktuellen Virenpattern und den neuesten Patches versorgt, haben bekannte Schadpro-

gramme wenig Chancen. Neue Schadprogramme werden heute relativ schnell entdeckt und entsprechende Updates zeitnah bereitgestellt. Allerdings führen Rollouts nicht immer dazu, dass alle Rechner in einem Unternehmensnetz alle Updates erhalten. Verzögerungen und Fehler im Rollout-Prozess sind gang und gäbe. Deshalb ist es wichtig, den Sicherheitsstatus zu messen, um ihn für das gesamte Unternehmen beurteilen zu können.

Wie lange hat Malware eine Chance?

Ein möglicher Security-KPI ist das Rollout Time Release (RTR). Es zeigt, wie lange ein Unternehmen bis zur Installation eines Patches unzureichend geschützt ist.



Quelle: Graf/Ampeg

Je komplexer ein Netz ist, desto höher ist die Wahrscheinlichkeit, dass Updates im Verteilprozess manche Systeme zu spät oder gar nicht erreichen. Das mag an der Performance des Netzes liegen, an Rechnern oder Laptops, die zum Zeitpunkt des Rollouts nicht online sind, an technischen Störungen oder anderen Fehlern. Update-Störungen sind ein bekanntes Problem.

Lücken im Patch-Rollout

Laut Umfrage geben viele Sicherheitsverantwortliche zu, dass in ihren Unternehmen manche Rechner gar nicht mit Pattern oder Patches versorgt werden können. Im Fehlerfall komme es außerdem vor, dass die Rollout-Systeme solche Lücken nicht zurückmelden. In letzter Konsequenz bedeutet das: Sicherheitsverantwortliche können nicht sagen, ob und wo in ihrem Netz Schwachpunkte entstehen.

Die Lücken können die Ursache für konkrete Malware-Infektionen sein, wie das Schadprogramm „Conficker“ gezeigt hat. Es sorgte seit Ende 2008 für Unruhe in den Sicherheitsabteilungen. Schon kurz nach dem Auftauchen des Programms im Oktober 2008 veröffentlichte Microsoft das sicherheitskritische Update MS08-067, mit dem Unternehmen die betreffende Lücke schließen konnten. Ein Vierteljahr später nistete sich der Wurm trotzdem auf den Rechnern der Bundeswehr ein. Nach Angaben der Conficker Working Group waren bis zum Dezember 2010 immer noch mehr als fünf Millionen Rechner mit einer der diversen Conficker-Varianten infiziert. Es scheint unwahrscheinlich, dass große Unternehmen und Organisationen den Microsoft-Patch nicht ausgerollt haben. Deshalb bleibt nur die Schlussfolgerung, dass durch Rollout-Fehler Lücken im Netz geblieben sind.

Typische Security-KPIs

Unternehmen, die den Sicherheitsstatus jedes einzelnen Rechners im Netz erfassen, sehen, wo Lücken sind und können diese sofort schließen. Alle anderen haben nur

die Möglichkeit zu reagieren, wenn die Schwachstellen durch eine Infektion evident geworden sind. Messbarkeit bedeutet Transparenz. Sie ist die Grundlage dafür, dass ein Unternehmen seinen Sicherheitsbetrieb verbessern kann. Deshalb ist die permanente und kontinuierliche Messung des eigenen Sicherheitsstatus so wichtig. Was aber definiert nun diesen „Sicherheitsstatus“ eines Rechners? Welche konkreten Messgrößen beziehungsweise Key-Performance-Indikatoren (KPIs) können dazu herangezogen werden?

Ein Restrisiko bleibt

Mit der Messung des Sicherheitsstatus geht ein Security-Level-Management einher – also eine Qualitätssicherung für die IT-Sicherheit. Damit lässt sich das Restrisiko für eine Infektion mit Viren, Würmern und Trojanern senken. Auch mit einer Messung der relevanten Indikatoren und einem professionellen Security-Level-Management kann man nicht zu hundertprozentiger beziehungsweise lückenloser IT-Sicherheit gelangen. Doch durch die geschaffene Transparenz erkennt der Sicherheitsverantwortliche genau, an welchen Stellen er weiterarbeiten muss.

Vordringliches Ziel eines jeden Sicherheitsverantwortlichen muss sein, alle Systeme im Netz möglichst aktuell zu halten. Zu welchem Grad dieses Ziel erreicht wird, lässt sich messen. Es ist möglich, nach jedem Rollout zu prüfen, ob alle beziehungsweise wie viele Rechner ein Virenpattern oder einen Patch auch tatsächlich erhalten haben. Ein gültiger Key-Performance-Indikator für die Update-Systeme wäre dementsprechend der „Erfüllungsgrad pro Rollout“, der für jedes System im Netz erfasst werden muss.

Ein weiterer wichtiger Indikator für den Sicherheitsstatus eines Netzes ist die Dauer von Rollouts. Vor dem

Hintergrund einer permanent steigenden Anzahl von „Zero Day Exploits“ ist es nicht nur wichtig, dass die Updates ihr Ziel erreichen, sondern auch, wie schnell sie das tun. Diese Einschätzung bestätigen auch viele Security Officers. Sie sind der Meinung, dass schon Verzögerungen der Pattern- oder Patch-Rollouts um wenige Stunden zu „einer relevanten zusätzlichen Bedrohung“ führen. Virenpattern können sofort nach ihrer Veröffentlichung verteilt werden, was meist auch automatisiert geschieht. Patches dagegen werden von internen oder externen Computer Emergency Response Teams (Certs) auf ihre Systemverträglichkeit geprüft. Dieser Schritt kostet Zeit, so dass der Rollout danach umso schneller gehen muss.

Aktuelle Antivirensoftware nötig

Kein Messwert – aber für das Funktionieren des Sicherheitsbetriebs genauso wichtig – ist die Aktualität der Antivirensoftware und der dazugehörigen Scan-Engine. Ihre Aktualität sollten Sicherheitsverantwortliche immer im Auge behalten. Oft wird die „End-of-Life-Meldung“ des Herstellers der Schutzsoftware vom Security-Management missachtet. Teilweise auch, weil veraltete Hardware das Update auf die neue Software nicht erlaubt. Sind Software und Scan-Engine aber nicht aktuell, gibt die Messung der restlichen KPIs nicht viel Sinn.

Suche nach schwarzen Schafen

In der Praxis der Messung von IT-Sicherheit haben sich zwei gängige Methoden herauskristallisiert. In vielen Unternehmen ist es üblich, die Anzahl der „gefangenen“ Schadprogramme zu erfassen, um den Nutzen der Investition zu belegen. Dieser Wert und seine Entwicklung lassen aber keine Aussagen über den Sicherheitsstatus zu. Er eignet sich vielmehr zur Schwachstellensuche, wenn er für unterschiedliche Netzsegmente oder auch einzelne Rechner eingesehen werden kann. Weist ein Standort, Netzsegment oder Rechner signifikant mehr Schadprogramme auf als der Durchschnitt, so ist das ein Hinweis darauf, dass sich dort vielleicht ein Trojaner verbirgt, der andere Malware nachlädt.

Diese Art der Suche nach schwarzen Schafen ist allerdings nur sinnvoll, wenn die Überwachung permanent abläuft. Doch der Aufwand dafür ist ohne spezielle Tools hoch, und so analysieren Unternehmen die Unterschiede im Virenaufkommen in den seltensten Fällen differenziert. Viele Marktteilnehmer messen die Qualität des Sicherheitsnetzes daran, wie viele Viren es insgesamt



unschädlich macht. Hier muss klar gesagt werden: Die Anzahl der erkannten Malware oder eine Untersuchung, welche Kosten es verursacht, einen einzelnen Virus außer Gefecht zu setzen, sind keine validen Messwerte für IT-Sicherheit.

Stichproben nur bedingt geeignet

Als zweite Methode ist es in vielen Unternehmen gebräuchlich, den Erfolg von Rollouts zu prüfen. Von den befragten Sicherheitsverantwortlichen verlassen sich nur 34 Prozent allein auf ihre Update-Systeme und sind der Ansicht, dass die Sicherheit ihres Netzes auch ohne die explizite Kontrolle des Update-Erfolgs nicht grundsätzlich in Gefahr ist. Von der prüfenden Mehrheit begnügt sich allerdings etwa ein Drittel mit Stichproben. Werden diese Stichproben immer an denselben, als besonders kritisch eingestuften Systemen vorgenommen, kann dies zu deren Absicherung beitragen. Ein Indikator zur Beurteilung der übergreifenden Sicherheitslage lässt sich aus Stichproben aber nicht ableiten. Dies dürfte den Sicherheitsverantwortlichen auch bewusst sein, doch aus Mangel an Personal oder geeigneten Tools wird auf eine permanente Erfassung relevanter Indikatoren verzichtet. (ph/ue)

*Peter Graf ist Geschäftsführer der Ampeg GmbH in Bremen.

Sonderdruck aus COMPUTERWOCHE NR. 16/2011 für

AMPEG GmbH

Obernstraße 45-47
28195 Bremen

Telefon: 0421-525 870
Telefax: 0700-267 343 29
www.ampeg.de
www.security-lighthouse.de

