Nutzen und Gefahren von Bugfix, Update, Patch und Co.

Kurányi wird entlassen?! Patch-Management im Privat- und Unternehmensumfeld

Wenn im Auto die Lampe für eine Fehlfunktion aufleuchtet, fährt man schnurstracks zur Werkstatt und zahlt bereitwillig Geld, damit die Bremsen funktionieren oder das ESP einsatzfähig bleibt. Wenn ein Programm auf dem PC die Information ausgibt, dass ein Update bereitsteht, so kann es durchaus sein, dass die Nachricht einfach weggeklickt oder ignoriert wird, da sie gerade stört. Und Geld würde man dafür erst recht nicht ausgeben wollen. Genau wie beim Auto sind nicht alle Updates sicherheitsrelevant, aber genau dies sollte man genau im Blick haben, um nicht Opfer von Angriffen zu werden. Es gibt heutzutage noch keine Sicherheitskultur im Internet und Systeme können auch nicht zu 100% geschützt werden, allerdings sollten die uns zur Verfügung stehenden Mittel mit hoher Priorisierung genutzt werden.

Kein Sicherheitsbewusstsein für digitale Medien

Patch-Management beschreibt die permanente Organisation von Updates für Geräte und Applikationen. Dies ist absolut notwendig, um Einfallstore in die eigene IT so gering wie möglich zu halten. Prominente Beispiele aus der nahen Vergangenheit zeigen die Probleme und das mangelnde Sicherheitsbewusstsein recht eindeutig:
Die Entwickler eines verbreiteten Content-Management-Systems haben ein Sicherheitspatch angekündigt, das bei Veröffentlichung sofort eingespielt werden soll, da die Veröffentlichung auch die Beschaffenheit des Fehlers mit sich bringt. Dieses Vorgehen ist gut, üblich und nachvollziehbar, allerdings nur effizient, wenn die Verantwortlichen das Update auch tatsächlich einspielen. Aufgrund dieses Fehlers wurde eine prominente Werbung gegen Vorratsdatenspeicherung auf der Webseite des Bundesinnenministers geschaltet [1] sowie eine „virtuelle" Entlassung von Kevin Kurányi auf der Seite des FC Schalke 04 bekannt gegeben [2]. Eine Studie des Instituts für Internet-Sicherheit hat zusätzlich ergeben, dass viele weitere Webseiten noch Wochen nach Bekanntgabe des Patches nicht aktualisiert wurden [3].

Die Manipulation der betroffenen Seiten konnte jedoch nur stattfinden, da ein zusätzlicher Fehler der Webseitenbetreiber gemacht wurde: Die Wahl eines schwachen Passworts für einen wichtigen Dienst der Webseite, der dem Angreifer Vollzugriff auf das System gewährleistet. In einem Fall heißt es, dass das Passwort „gewinner" lautete. Der Vorfall verdeutlicht, dass noch kein Sicherheitsbewusstsein für die digitalen Dienste besteht.

Das Internet verknüpft die Welt – Freund und Feind

Die virtuelle Welt bildet ständig wachsend eine große Anzahl an Geschäftsprozessen der Unternehmen ab. Speziell das Internet trägt enorm dazu bei, neue Vertriebskanäle zu eröffnen oder die globale Zusammenarbeit mit Firmen unterschiedlicher Herkunft zu vereinfachen. Für die meisten Unternehmen bedeutet der Ausfall der IT den Totalausfall aller Prozesse. Aber auch im privaten Umfeld findet das Internet beträchtlichen Zuspruch. Anwendungen wie Online-Banking, Online-Auktionshäuser oder E-Mail-Versand sind kaum noch wegzudenken.

Aber es gibt auch eine Kehrseite. Das Internet stellt für Kriminelle einen Eingang in die Systeme der Internetnutzer dar. Man muss sich der Tatsache bewusst sein, dass es keine hundertprozentige Sicherheit gibt. Ein an das Internet angeschlossenes System, sei es ein einzelner PC oder ein ganzes Netzwerk, ist potenziell angreifbar. Deshalb reicht es nicht mehr aus, nur den Zugang zum Internet zu überwachen. Es müssen zusätzliche Maßnahmen zum Schutz vor Risiken und Gefahren ergriffen werden und es muss mit einer ausgeprägten Sicherheitskompetenz gehandelt werden.

Die Entwicklung von Schwachstellen und Angriffen

100-prozentige Sicherheit gibt es wie im realen Leben auch im Internet nicht. Aktuelle Betriebssysteme, Protokolle oder weitere IT-Konzepte werden in Zukunft nicht mehr ausreichend sein, um Sicherheit zu gewährleisten. Neue proaktive Konzepte, wie Sicherheitsplattformen mit Trusted Computing, werden in diesem Kontext einen Quantensprung bringen. Nichtsdestotrotz kann bereits heute eine hohe Sicherheit erreicht werden, wenn alle Sicherheitsvorgaben beachtet sowie IT-Systeme und Sicherheitsanwendungen auf dem aktuellen Stand gehalten werden.

Der aktuelle Trend, Computer zu infizieren, besteht darin, schadhaften Code auf Internetseiten zu platzieren. Dieser Code wiederum nutzt bekannte Schwachstellen oder Sicherheitslücken bei der Software des Webseitenbesuchers aus und infiziert den Rechner.
Das englische IT-Sicherheitsunternehmen Sophos hat im Jahr 2008 durchschnittlich alle 4,5 Sekunden eine neu infizierte Webseite entdeckt [4]. Dies unterstreicht erneut die Wichtigkeit, sich vor möglichen Gefahren bestens zu schützen und die verwendete Software up-to-date zu halten.

Leider ist man auch mit dem aktuellsten Softwaresystem nicht komplett geschützt. Es sind immer häufiger automatisierte und großflächige Angriffe im Internet zu beobachten, bei denen die Sicherheitslücke noch nicht bekannt ist.

Diese so genannten Zero-Day-Attacken sind besonders gefährlich, da die Softwarehersteller noch keine passenden Gegenmaßnahmen für diesen Angriff bereitstellen können. Sind die entsprechenden Sicherheitsupdates jedoch erstellt und für die Nutzer verfügbar, so liegt es in der Verantwortung der Administratoren – oder im Privatumfeld der Nutzer selbst –, die Sicherheitslücken schnell zu stopfen.

Patch-Management und seine Notwendigkeit

Für Unternehmen gestaltet sich die Notwendigkeit eines Patch-Managements besonders kritisch. Neben der Abwehr von Wirtschaftsspionage müssen zusätzlich noch gesetzliche Vorschriften zur Datensicherheit, Verfügbarkeit und zum Datenschutz eingehalten werden. Diese unter dem Begriff IT-Compliance zusammengefassten Regularien zur Erhöhung der IT-Sicherheit können bei Nichteinhaltung hohe Strafen nach sich ziehen. Nicht zuletzt darf der finanzielle Schaden nicht unterschätzt werden, der entsteht, wenn die IT-Infrastruktur eines Unternehmens in Folge eines Angriffes beeinträchtigt wird oder gar zusammenbricht. Beim Computerwurm SQL-Slam-mer beispielsweise wird der weltweite Produktivitätsausfall in den ersten fünf Tagen auf etwa 1 Milliarde Dollar geschätzt [5].

Der wohl wichtigste Treiber für Patch-Management im Privatumfeld ist der Schutz vor dem Diebstahl persönlicher Daten. Auf den Festplatten vieler Nutzer finden sich neben privaten Briefen oder Fotos auch elektronische Steuererklärungen oder Informationen zu Konten oder Kreditkarten. Diese Daten können zum so genannten Identitätsdiebstahl missbraucht werden, bei dem Kriminelle die personenbezogenen Daten für Kreditkartenbetrug oder Ähnliches ausnutzen.

Patch-Management-Tools im Detail

Für Privatleute ist die Aufgabe von Patch-Management-Tools leicht beschrieben. Es muss sichergestellt werden, dass sämtliche eingesetzte Software auf dem neuesten Stand gehalten wird. Oft reicht es schon, wenn die automatischen Updates des Betriebssystem aktiviert sind. Auch andere Anwendungen melden sich heutzutage, wenn eine neue Version der Software zur Verfügung steht. Der Benutzer muss allerdings tatsächlich aktiv werden und den Aktualisierungen zustimmen.

Im Unternehmensumfeld gestaltet sich die Situation erneut schwerer. Die Komplexität der IT-Infrastruktur eines Unternehmens lässt ein einfaches Installieren der Updates oft nicht zu. Ein Unternehmen besitzt häufig eine Vielzahl unterschiedlicher Rechnersysteme wie Server, PCs oder Notebooks an unterschiedlichen Standorten oder Niederlassungen. Auch die Software ist oft heterogen. So verfügen Unternehmen über eine Menge an Applikationen mit unterschiedlichen Konfigurationen auf verschiedenen Betriebssystemen unterschiedlicher Versionen. Ein Patch-Management-Tool hilft daher nicht nur beim eigentlichen Einspielen der Sicherheitsupdates, sondern auch bei weiteren Aufgaben wie der Verwaltung von bereits installierten Patches oder bei Tests sowie der Konfliktanalyse.

Grundsätzlich lässt sich die Arbeitsweise eines typischen Patch-Management-Tools in mehrere Phasen unterteilen. In der Detect-Phase sucht das Tool nach neuen Sicherheitsupdates für sämtliche im Unternehmen eingesetzte Software und Betriebssysteme. Im zweiten Schritt, der so genannten Acquire-Phase, wird geprüft, ob die betroffene Sicherheitslücke nicht bereits durch die aktuellen Sicherheitsvorkehrungen behandelt ist. Wenn dies nicht der Fall ist, so wird das Patch für Tests zentral heruntergeladen. In der anschließenden Test-Phase wird das Sicherheitsupdate in einer realistischen Umgebung installiert und diverse Merkmale werden überprüft. Hauptaugenmerk wird auf die Tatsache gelegt, ob das Update mit der vorherrschenden Softwarelandschaft harmoniert. Es dürfen keinerlei Komplikationen oder Nebeneffekte entstehen und die Funktionsweise der restlichen Applikationen darf nicht berührt werden. Sind alle Tests bestanden, geht das Patch-Management-Tool in die Deploy-Phase. Hierbei wird zuerst die Erlaubnis zur Verteilung des entsprechenden Patches eingeholt. Ist die Verteilung genehmigt worden, findet die eigentliche Installation des Sicherheitsupdates statt. Abschließend wird die korrekte Installation des Patches sowie die Funktionstüchtigkeit des Systems überprüft. Den letzten Schritt bei der Einführung eines neues Patches stellt die Maintain-Phase dar. Hierbei wird ein Protokoll darüber geführt, wann bei welchen Systemen welche Updates eingespielt wurden. Dies ist ein wichtiger Punkt im Kontext der IT-Compliance, da ein Unternehmen Rechenschaft darüber ablegen muss, ob seine IT-Systeme jederzeit bestmöglich geschützt wurden. Außerdem wird das Patch im System vermerkt und oft zentral hinterlegt, um bei weiteren Instanzen der betroffenen Software schnell das Update ausführen zu können.

Vorteile, aber auch Nachteile beim Patch-Management

Neben dem offensichtlichen Gewinn an Sicherheit verursacht ein professionell eingesetztes Patch-Management weitere positive Effekte. Die Systemadministratoren werden wesentlich unterstützt, was für das Unternehmen Zeitersparnis und Kostenreduzierung darstellt. Außerdem kann durch die Prozessautomatisierung der personelle Aufwand verkleinert werden, ohne jedoch das Maß an Sicherheit zu mindern. Der Nutzen im Hinblick auf IT-Compliance ist ebenfalls nicht zu vernachlässigen. Die Einhaltung der gesetzlichen Vorgaben in Bezug auf Verfügbarkeit schützt das Unternehmen vor teils hohen Schäden, verursacht durch Produktivitätsausfall.

Die Nachteile hinsichtlich Patches seien ebenfalls erläutert. Durch die Veröffentlichung von Softwareupdates wird die entsprechende Sicherheitslücke nicht nur geschlossen, sondern auch publik gemacht. Kriminelle können das Patch analysieren und so das möglicherweise noch unbekannte Sicherheitsleck ausfindig machen und angreifen. Diese Vorgehensweise wurde in den bereits beschriebenen Fällen Schalke und Schäuble eingesetzt. Ein weiteres negatives Szenario stellt das potenzielle Einschleusen von Malware durch Sicherheitsupdates dar. An verschiedenen Stellen können Angreifer in den automatisierten Aktualisierungsprozess eingreifen und das Patch modifizieren bzw. schadhaften Code anhängen. Abhilfe für dieses Problem stellen verschlüsselte oder mit Signaturen versehene Updates dar.

Für Unternehmen mit einer komplexen IT-Infrastruktur bestehen zusätzliche Probleme. So existieren oft unzureichende Informationen über die Auswirkungen eines Patches auf die übrigen eingesetzten Softwareprodukte. Unverträglichkeiten zwischen verschiedenen Applikationen können schnell das Ausmaß des eigentlich zu verhindernden Produktivitätsausfall annehmen. Die Auswirkungen dieses Problems können durch eine intensive Nutzung der bereits beschriebenen Test-Phase reduziert werden. Personelle Ressourcen können eingesetzt werden, um die vorhandenen Sicherheitsupdates und ihren Kontext zu prüfen, die Wichtigkeit und Priorität zu ermitteln sowie die Risiken abzuschätzen.

Bei einem teilautomatisierten Patch-Management werden nur unbedingt notwendige Updates ohne Risiko eingespielt.

Abschließend sei das Problem der Skalierbarkeit angesprochen. Je nach Anzahl und Volumen der Patches kann die Bandbreite eines Unternehmens Schwierigkeiten bereiten. Die Lösung hierbei kann sein, großvolumige Patches zentral zu laden und auf verschiedenen Depot-Servern im Netzwerk bereitzustellen. Die verschiedenen Instanzen der Software werden nun mit den im Netzwerk vorhandenen Updates bedient und nicht mehr einzeln über das Internet.

Verantwortung und IT-Sicherheitskultur

Dort, wo professionelles Patch-Management oversized oder nicht einsetzbar ist, muss das IT-Sicherheitsbewusstsein besonders geschärft sein. Im Privatumfeld bedeutet dies beispielsweise, dass die automatisch bereitgestellten Aktualisierungen für das Betriebssystem auch wahrgenommen werden müssen. Oft muss der Benutzer lediglich einen einzelnen Mausklick auf ein gelb blickendes Symbol tätigen, um seine Software auf den neuesten Stand zu bringen.

Aber auch den eigentlich technisch versierten Administratoren von Webseiten muss ihre Verantwortung bewusst sein, die sie tragen. Nicht nur den Firmen hinter der Webseite kommt die Integrität ihrer Daten zugute, sondern auch den Besuchern: Die Internetpräsenz ist frei von schädlichem Code. Dass einigen Webmastern diese Verantwortung oft nicht bewusst ist, haben unter anderem die beschriebenen Vorfälle der ungepatchten Webseiten gezeigt. Aber auch die enorme Wichtigkeit der eingesetzten Passwörter darf nicht vergessen werden. Ein schwach gewähltes Passwort ist gleichermaßen fahrlässig wie ein Passwort, das auf einem Notizzettel am Monitor klebt.

Argumente für eine Erhöhung des IT-Sicherheitsbewusstsein gibt es zur Genüge, denn die entstehenden Probleme sind alles andere als virtuell. Für ein Unternehmen kann Wirtschaftsspionage einen enormen Verlust, wenn nicht den Ruin bedeuten. Neben dem Faktor Geld spielt auch das Ansehen des Unternehmens oft eine große Rolle. Wie kann einer Firma vertraut werden, bei denen die teils sensiblen Kundendaten schlecht geschützt sind? Die hohen Strafen bei Nichteinhaltung der IT-Compliance wurden bereits erwähnt.

Aber auch im Privatumfeld gibt es eine Reihe guter Gründe für mehr IT-Sicherheitsbewusstsein. Jeder Anwender sollte darauf bedacht sein, seine digitale Privatsphäre bestmöglich zu schützen. Der ebenfalls bereits angesprochene Identitätsdiebstahl ist ein Phänomen, das zur Diffamierung oder zum Betrug ausgenutzt werden kann. Auch das allerseits bekannte Problem Spam kann in diesem Kontext aufgegriffen werden. Infizierte Computer können nach E-Mail-Adressen durchsucht werden, welche an Spammer verkauft und anschließend mit unerwünschten E-Mails „versorgt" werden.

Fazit und Ausblick

Professionelles Patch-Management ist ein guter Ansatz für Unternehmen, die Sicherheit ihrer IT-Infrastruktur zu erhöhen. Aber nicht nur die Sicherheit wird gesteigert, auch Aspekte wie Zeit-, Kosten- und personeller Aufwand werden optimiert. Das immer wichtiger werdende Feld der IT-Compliance, gesetzlicher Vorschriften in Bezug auf Datensicherheit, Verfügbarkeit und Datenschutz zur Erhöhung der IT-Sicherheit, wird ebenso behandelt.

Auch im Hinblick auf die Entwicklung der IT-Sicherheitslage bieten Patch-Management-Tools eine wertvolle Hilfe. Nicht nur die Anzahl der Attacken nimmt kontinuierlich zu, auch die Geschwindigkeit der Angreifer steigt (Stichwort Zero-Day-Attacken). Immer komplexer werdende Software bietet viel Angriffsfläche und gestaltet zudem das Beherrschen der Updates schwieriger. Es ist offensichtlich, dass die aktuellen Sicherheitssysteme und -konzepte bald nicht mehr ausreichen und neue Technologien gebraucht werden. Bis diese Techniken einsetzbar sind, muss mit dem gearbeitet werden, was vorhanden ist. Eine erhöhte Sicherheitskultur würde dies positiv beeinflussen.

Aber auch kleine Unternehmen oder Privatleute müssen sich diese Gefahren bewusst machen und Gegenmaßnahmen treffen. Die Verantwortung, die jeder einzelne Benutzer besitzt, hat Folgen in der virtuellen Welt, aber auch in der Realität. Das IT-Sicherheitsbewusstsein muss im gleichen Maße geschärft sein wie das Bewusstsein für „reale" Gefahren. Glaubt man den Statistiken erfolgreicher Angriffe trotz vorhandener, aber nicht genutzter Sicherheitsupdates, gibt es in dieser Hinsicht noch viel zu tun.

Für die Zukunft ist die Entwicklung wünschenswert, dass die IT-Anwender mit derselben Sensibilität auf Sicherheitswarnungen ihres Systems reagieren wie auf Warnlichter oder seltsame Geräusche am Auto. Dann wären wir auf einem guten Weg zu einer Sicherheitskultur für das Internet.

Quellen:
[1] http://www.heise.de/security/Website-von-Wolfgang-Schaeuble-ueber-Typo3-Luecke-gehackt-Update--/news/meldung/132315
[2] http://www.taz.de/1/leben/internet/artikel/1/hacker-feuern-kuranyi-schalke-nicht/
[3] http://www.internet-sicherheit.de/aktuelles/mitteilungen/nachricht/nachricht-detail/die-gefahr-von-sicherheits-updates-am-beispiel-von/
[4] http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf
[5] http://news.zdnet.co.uk/itmanagement/0,1000000308,2129738,00.htm

Autoren

Prof. Dr. **Norbert Pohlmann** ist Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de).

Dipl.-Inform. (FH) **Markus Linnemann** ist Geschäftsführer des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen.

B.Sc. **Sebastian Feld** ist wissenschaftlicher Mitarbeiter des Instituts für Internet-Sicherheit im Forschungsschwerpunkt Identity Management.