Patching macht Webanwendungen sicher. Sicher?

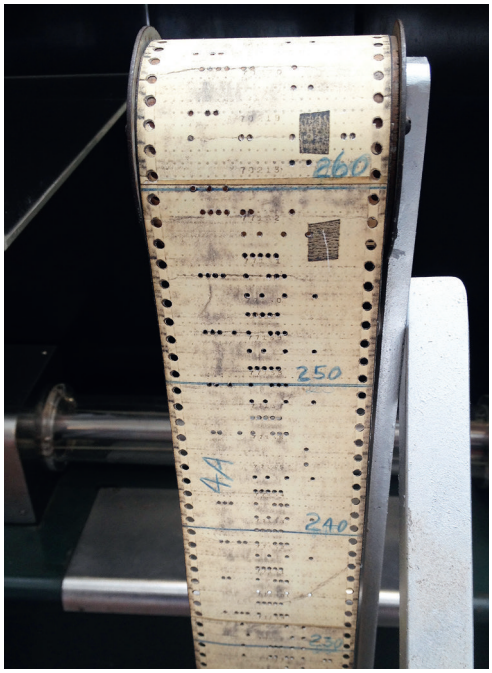
In den letzten Monaten traten Sicherheitslücken bei Internetanwendungen auf, die nicht nur IT-Spezialisten Bauchweh bereiteten. Zur Behebung dieser Lücken wird das Patching eingesetzt. Nur: Das «Flicken» einer Lücke ist nicht immer möglich. Manchmal verursacht der Patch selbst Probleme. So sind weitere Massnahmen nötig, um eine Anwendung sicher zu betreiben. Kaspar Geiser

Um Sicherheitslücken zu schliessen, gibt es verschiedene Möglichkeiten. Man unterscheidet zwischen Patches, Updates und Upgrades. Als Patches («Flicken») bezeichnet man kleine Software-Updates, die Probleme einer Anwendung beheben. Typischerweise stellen die Hersteller oder Programmierer diese Patches zur Verfügung. Patches werden zeitnah zu auftretenden Problemen erstellt. Deren Einspielung geschieht im laufenden Betrieb und vom Anwender unbemerkt.

Patches betreffen nur einen Teil einer gesamten Anwendung: Zum Beispiel nur das Frontend einer Webanwendung. Beinhaltet ein Patch auch neue Funktionen oder die Anpassung eines Layouts, spricht man von einem Update. Dieses bedingt meistens eine Unterbrechung der Webanwendung und unter Umständen auch Anpassungen an verschiedenen Stellen, beispielsweise die Erweiterung einer Tabelle in einer Datenbank. Durch ein Upgrade gewinnt die Webanwendung neue Funktionen. Zusätzlich sind Anpassungen an der Middleware, der Hardware oder ein Ausbau der Verfügbarkeit einer Anwendung nötig. In den Vordergrund rücken dabei die Fallback-Prozeduren: Es muss während oder nach einem Upgrade immer möglich sein, wieder zur vorhergehenden Version zurückzukehren. Im Gegensatz zu Patches und Updates bedingen Upgrades eine detaillierte Planung und eine Vorankündigung beim Anwender.

Kleine Veränderung – grosses Risiko

Patches erscheinen auf den ersten Blick als die schnellste und einfachste Möglichkeit zur Problembehebung in einer Webanwendung. Das bedeutet aber nicht, dass das Patching ohne Risiko ist. Auch ist es kein Allerweltsmittel zur Behebung von Sicherheitslücken. Patches können neue Probleme verursachen. Dies zeigte sich im Fall von «Poodle», der jüngst bekannt gewordenen Lücke im SSL-V3-Protokoll. Rasch waren Patches verfügbar, die die betroffenen Systeme wieder sicher machten. Doch kaum war ein Teilsystem «sicher», funktionierte das Gesamtsystem nicht mehr, weil beispielsweise andere Webanwendungen mit der gepatchten Anwendung via SSL 3.0 kommunizieren wollten. Der Patch verhinderte dies. Die Folge dieses spezifischen Problems: Billettautomaten, die keine Kreditkarten mehr validieren oder Eingangskontrollen, die keine Tickets mehr lesen können.



Lochkarten wurden noch wirklich «gepatched», also mit einem Flicken versehen, wie hier bei einem Mark I von 1944. Bild: Wikimedia Commons

Verteilung reduziert das Risiko

Um Risiken bei Internetanwendungen zu vermeiden, empfiehlt es sich, eine Anwendung auf verschiedene Systeme zu verteilen. Im Falle einer Lücke in einer Datenbank müssen nicht unbedingt das Gesamtsystem, sondern nur die betroffenen Datenbanksysteme gepatched werden. Sind diese zudem durch Firewalls vom Internet und den Webanwendungen getrennt, bedeutet eine Lücke nicht zwingend auch ein Risiko für die entsprechende Gesamtanwendung. Dies wiederum bringt den Vorteil, dass man Anwendungen nicht aufgrund einer Lücke stoppen und die IT-Abteilungen keine unmittelbaren Aktionen auslösen müssen.

Die Anwendung schützen

Für geschäftskritische Anwendungen und die Verarbeitung sensitiver Daten sind weitere Schutzmassnahmen nötig. Da die meisten Lücken in Anwendungen auftreten, müssen diese nicht direkt mit dem Internet verbunden werden. Mit einer WAF (Web Application Firewall) wird zwischen Anwender und Anwendung ein System gestellt: Dieses gibt nur sinnvolle und gültige Anfragen an eine Anwendung weiter. Eine WAF schützt die Anwendungen, indem sie die Anfragen, die zur Ausnützung einer Lücke führen, erst gar nicht an eine gefährdete Anwendung weitergibt. Auch ermöglichen diese Systeme eine filigrane Konfiguration: Diese lässt eine Ausnahme für eine nötige SSL-V3-Kommunikation für bestimmte Quellsysteme noch immer zu. Das Gesamtsystem für Angreifer aus dem Internet ist jedoch für diese unzugänglich.

Gute Vorbereitung ist das A und O

Eine Lücke kann jederzeit in jeder Anwendung oder in jedem Betriebssystem auftauchen. Als IT-Dienstleister ist es notwendig, sich einen genauen Überblick über die System- und Anwendungslandschaft zu verschaffen. Dies wiederum bedingt zentrale Systeme, die über automatisch aktualisierte Inventare verfügen. Über solche Inventare können innerhalb kürzester Zeit die von einer Lücke betroffenen Systeme eruiert werden. Danach kann man mit der Planung der Massnahmen starten. Das Fazit: Vorsicht vor vorschnellen Patches. Neben einem guten Überblick über die eigene Systemlandschaft ist es ausserdem wichtig, Anwendungen auf verschiedene Systeme aufzuteilen. Weitere Schutzmassnahmen wie eine Web Application Firewall schützen die eigenen Systeme ebenfalls.

Kaspar Geiser ist Geschäftsführer und Inhaber der Aspectra AG.