Aktualisierungen von Softwares sind notwendig, bergen aber auch gewisse Risiken.

PATCHEN – MUSS DAS SEIN?

SOFTWARE-SCHWACHSTELLEN KEINE CHANCE GEBEN

von Andreas Wisler

Jeden Tag kann von neuen Schwachstellen in Software gelesen werden. Nur wenige Stunden später sind Hacker bereits daran, diese Lücken anzugreifen. Wer bis dahin seine Software nicht aktualisiert hat, geht ein grosses Risiko ein. Dabei ist nicht nur Microsoft davon betroffen, sondern auch viele andere Produkte. Eine aufwändige Arbeit für den Administrator. Da stellt sich oft die Frage: Muss das sein?

Kaum den Computer gestartet, erscheinen unten rechts Meldungen von Software-Aktualisierungen. «Nicht schon wieder», werden sich sicherlich viele denken und dies auf später verschieben. Praktisch für jede Software erscheinen in unregelmässigen Abständen Aktualisierungen, die es gilt zu installieren. Einfach installieren ist aber nicht ohne ein gewisses Risiko. Viele Administratoren haben schon die Erfahrung gemacht, dass ein Patch anschliessend Probleme bereitete. Eine Testumgebung können sich aber nur wenige Firmen leisten und damit wird jeder Patch zu einer Herausforderung. Daher warten viele einfach mal ab, was andere berichten. Wenn es keine Probleme gibt, dann wird der Patch (hoffentlich) 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. Werden Systeme erfolgreich angegriffen, gelangen Daten in die falschen Hände. Auch wenn es Hacker in der Regel nur auf E-Mail-Adressen, Kreditkarteninformationen und Passwörter abgesehen haben, ist der Schaden gross. Im Internet sind Millionen von solchen Daten abrufbar.

SCHADEN, FOLGEN

Sollte ein schlecht gepatchtes System angegriffen werden, kann nicht nur ein Datenverlust die Folge sein:

> Downtime: Sind die Systeme nicht mehr erreichbar, steht oft der gesamte Betrieb still. Dies kann zu Produktionsausfällen oder nicht eingehaltenen Terminen 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 hundertprozentig zur Verfügung stehen.
> Daten-Integrität: Ist eine Lücke erfolgreich ausgenutzt worden, 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 Daten weitergearbeitet 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 verpasste Aufträge 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 ungern über erfolgreiche Angriffe berichtet wird. Lieber behält man dies als «kleines» Geheimnis für sich, als dass es 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. Zudem droht die DSGVO mit erheblichen Strafen, wenn ein Datenverlust aufgrund schlecht gesicherter Systeme erfolgte.
> Gestohlene Daten: Viel schwerer als das Stören der Systeme sind gestohlene Daten. Gelangen vertrauliche Daten in die falschen Hände, ist der Schaden oft enorm.


Schwachstellen in Systemen werden oftmals schnell von Hackern ausgenutzt.

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). Notfall-Patches sollten innerhalb von 24 Stunden installiert sein. Hohe Priorität bedeutet innerhalb weniger Tage, mittlere Priorität innerhalb von einer bis zwei Wochen sowie kleine Priorität innerhalb von einem bis zwei Monaten.

VORGEHEN

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

1. 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. Neue Schwachstellen und Updates/Patches 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. 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? Bei redundanten Systemen kann der Patch ohne Konflikte schnell installiert werden. Kontrollieren Sie auch, ob Patches zusammengefasst und in einem Schritt installiert werden können.
4. 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. Dennoch gibt es schnelle Wege, um sich über neue Patches zu informieren. 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 dafür auch eine eigene Seite vorgesehen, auf welcher über Sicherheitshinweise informiert wird. Im Internet sind ausserdem zahlreiche Newsletter vorhanden, die nur über Schwachstellen berichten (zum Beispiel CVE). 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.

Nebst den Newslettern gibt es auch spezialisierte Homepages, die alle Informationen sammeln und übersichtlich zusammentragen. Abonnieren Sie mindestens den Sicherheitsnewsletter der Hersteller der eingesetzten Software. So erhalten Sie alle Informationen schnell und zuverlässig und müssen nicht verschiedene Homepages aufsuchen.

LOGBUCH FÜHREN

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 führen. Somit haben Sie zu jedem Zeitpunkt die Übersicht.

ZUSAMMENFASSUNG

Das Aktualisieren der Systeme darf keine Arbeit nebenbei sein. Der Schaden, der ein fehlender Patch nach sich ziehen kann, kann sehr gross sein. Ein strukturiertes Vorgehen ist wichtig – die Informationen über neue Updates müssen vorhanden sein, damit der Patch zeitnah nach einem vorgelegten Schema getestet und installiert werden kann. Schützen Sie sich vor neuen Gefahren – ein Patch-Management hilft Ihnen, Ihre Systeme sicher zu betreiben. ●

ANDREAS WISLER

ist Inhaber und Senior Security Auditor bei der goSecurity GmbH.

www.gosecurity.ch