INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Patchmanagement – Muss das sein?

Jeden Tag werden neue Lücken in Software entdeckt. Nicht nur Microsoft ist davon betroffen, sondern auch viele anderen Produkte. Eine aufwändige Arbeit für den Administrator. Da stellt sich oft die Frage, muss das sein?

Falls Sie Anregungen oder Ideen aus Ihrem eigenen IT-Alltag haben, nehmen wir diese gerne auf. Wir freuen uns auf ein Feedback von Ihnen.

Dies ist eine kostenlose Dienstleistung der GO OUT Production GmbH (www.goSecurity.ch/INFONEWS).

Inhaltsverzeichnis

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Allmonatlich erscheint von Microsoft die Aufforderung, die neuesten Patches einzuspielen. Jedoch ist nicht nur Microsoft davon betroffen. Praktisch für jede Software erscheinen in unregelmässigen Abständen Flickwerke, die es gilt, zu installieren. Einfach installieren ist dabei oft nicht möglich. Ziemlich viele Administratoren haben schon die Erfahrung gemacht, dass ein Patch anschliessend Probleme bereitet. Eine Testumgebung können sich aber nur wenige Firmen leisten und da ist jeder Patch eine Herausforderung. Daher warten viele einfach mal ab, was andere berichten. Wenn es keine Probleme gibt, dann wird der Patch (vielleicht) auch installiert.

Statistiken zeigen auf der anderen Seite, dass neue Schwachstellen im-mer 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 verfüg-bar, 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 an. Vielen ist sicher noch der SQL Slammer Zwischenfall der Schweizerischen Post in Erinnerung oder der Virenausbruch des Migros Genossenschaftbundes.

SQL Slammer hat alleine 75'000 Server in wenigen Stunden befallen und 55 Millionen IP-Adressen pro Sekunde gescannt. Da bleibt nur wenig Zeit bei Ausbruch oder Bekannt werden der Attacke zu reagieren.

1 Welche Schäden können entstehen?

Sollte ein schlecht gepatchtes System angegriffen werden, sind die Folgen nicht abschätzbar:

Downtime
Sind die Systeme nicht mehr erreichbar, steht oft der gesamte Betrieb still. Dies kann zu Produktionsausfällen, nicht eingehaltenen Terminen usw. 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 Back-up/Desaster-Recovery-Plan ist ein strukturiertes Vorgehen sehr schwierig. Dementsprechend dauert es relativ lange, bis die Systeme wieder 100%-ig zur Verfügung stehen.

Daten-Integrität
Wurde eine Lücke erfolgreich ausgenutzt, 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 dabei verhindert werden, dass mit manipulierten Dateien weiter gearbeitet wird.

Kosten
Nicht vergessen werden darf, dass alle Arbeiten nicht nur viel Zeit beanspruchen, sondern auch Geld kosten. Sei dies durch Überstunden der Administratoren, dem Arbeitsausfall der Mitarbeiter oder verpassten Aufträgen oder Auslieferungen.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

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 sehr selten von erfolgreichen Attacken zu lesen ist. Lieber hält man dies als „kleines" Geheimnis für sich, als dass es die 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.

Gestohlene Daten
Viel schwerer als das Stören der Systeme sind gestohlene Daten. Gelangen vertrauliche Daten in die falschen Hände ist der Schaden oft enorm.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2 Welche Risikostufen gibt es?

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: Kritisch (Emergency), Hoch (High), Mittel (Medium) und Niedrig (Low).

Bewertung	Definition
Kritisch	Über diese Sicherheitslücke könnte sich ein Internetwurm oder eine andere Schadsoftware ohne Aktion des Benutzers ausbreiten.
Hoch	Eine solche Sicherheitslücke könnte die Vertraulichkeit, Integrität oder Verfügbarkeit von Benutzerdaten oder die Integrität oder Verfügbarkeit von Ressourcen gefährden.
Mittel	Eine Sicherheitslücke, die durch unterschiedliche Faktoren (zum Beispiel eine Standardkonfiguration, Überwachung oder die schwierige Ausnutzung) beträchtlich entschärft wird.
Niedrig	Eine Sicherheitslücke, die nur extrem schwer auszunutzen ist oder deren Auswirkungen minimal sind.

3 Wie werden Patches unterschieden?

Nicht jede Sicherheitsgefährdung muss gleich behandelt werden. Daher geben die Hersteller jeweils an, um was es sich beim Patch handelt. Es werden die folgenden Begriffe unterschieden:

- **Sicherheitspatch**
  Eine allgemein veröffentlichte Korrektur für eine bestimmte Sicherheitslücke in einem bestimmten Produkt. Für einen Sicherheitspatch wird oft ein Schweregrad angegeben.
- **Kritisches Update**
  Eine allgemein veröffentlichte Korrektur für einen bestimmten kritischen, nicht-sicherheitsrelevanten Softwarefehler.
- **Update**
  Eine allgemein veröffentlichte Korrektur für einen bestimmten nicht-kritischen, nichtsicherheitsrelevanten Softwarefehler.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

- **Hotfix**
  Ein einzelnes Paket aus einer oder mehreren Dateien, um ein Problem in einem Produkt zu beheben. Die Begriffe QFE (Quick Fix Engineering update), Patch und Update wurden in der Vergangenheit als Synonyme für Hotfixes verwendet.

- **Update Rollup**
  Eine Sammlung von Sicherheitspatches, kritischen Updates, Updates und Hotfixes, die kumulativ oder für eine einzelne Produktkomponente, beispielsweise für den Microsoft Internet Information Server oder den Microsoft Internet Explorer, angeboten werden. Dadurch wird die Bereitstellung mehrerer Softwareupdates vereinfacht.

- **Service Pack**
  Eine kumulative Sammlung von Hotfixes, Sicherheitspatches, kritischen Updates und Updates die seit der Veröffentlichung des Produktes veröffentlicht wurden, einschliesslich vieler Problemlösungen, die nicht durch andere Softwareupdates verfügbar gemacht wurden. Service Packs können auch eine begrenzte Anzahl von Kundenwünschen enthalten, etwa Änderungen an der Oberfläche oder Funktionen.

4 Wie geht man vor?

Damit das untenstehende Vorgehen ohne grosse Verzögerung durchgeführt werden kann, ist ein sauberes, aktuelles Softwareverzeichnis notwendig. Mit diesem kann man auf einen Blick erkennen, welche Software auf welchen Geräten im eigenen Betrieb im Einsatz ist.

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

4.1 Festlegen

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.

Die Prioritätsstufe ist besonders wichtig, weil sie festlegt, wie schnell ein Softwareupdate den Änderungsprozess durchläuft. Bei der Festlegung der Prioritätsstufe für ein Softwareupdate können sich die folgenden Überlegungen als hilfreich erweisen:

- Welche Geschäftsressourcen sind kritisch? Werden diese Ressourcen bei der Installation des Softwareupdates einer potenziellen Sicherheitsverletzung oder Systeminstabilität ausgesetzt?

- Wird das Softwareupdate an einem System vorgenommen, auf dem ein geschäftskritischer Dienst ausgeführt wird, der in der Vergangenheit zum Ziel von Angreifern wurde? Dies kann ein guter Grund sein, die Priorität einer Änderungsanforderung zu erhöhen.

- Wurden bereits Gegenmassnahmen getroffen, durch die die Angriffspunkte, die aus einer bestimmten Sicherheitslücke resultieren verringert wurden? Damit kann die Priorität der Änderungsanforderung gesetzt werden, obwohl es immer noch angebracht sein kann, das Softwareupdate bereitzustellen, um die Sicherheitslücke zu beheben.

Welche Bedrohung ergibt sich aus der Sicherheitslcke für die Produktionsumgebung? Viele Security Bulletins und damit verbundene Softwareupdates betreffen möglicherweise nur ein paar Computer in der eigenen Umgebung. Falls die aus einer Sicherheitslücke resultierende Bedrohung gering ist, kann dies die Priorität der Anforderung verringern.

Priorität	Empfohlener Zeitrahmen	Empfohlener maximaler Zeitrahmen
Kritisch	Innerhalb von 24 Stunden	Innerhalb von 2 Wochen
Hoch	Innerhalb von einem Monat	Innerhalb von 2 Monaten
Mittel	Stellen Sie ein neues Service Pack oder Update-Rollup mit einem Fix für diese Sicherheitslücke je nach Verfügbarkeit innerhalb von 4 Monaten bereit.	Stellen Sie das Softwareupdate innerhalb von 6 Monaten bereit.
Niedrig	Stellen Sie ein neues Service Pack oder Update-Rollup mit einem Fix für diese Sicherheitslücke je nach Verfügbarkeit innerhalb eines Jahres bereit.	Stellen Sie das Softwareupdate innerhalb eines Jahres bereit. Sie können auch entscheiden, auf das Update ganz zu verzichten.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

4.2 Erkennen

Neue Schwachstellen und Updates/Pachtes werden über verschiedene Wege veröffentlich. Organisieren Sie sich so, dass Sie an diese Meldungen gelangen. Sobald neue Patches verfügbar sind, sollten diese auch installiert werden. Mögliche Orte finden Sie unter Informationsquellen.

4.3 Planung

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? Kontrollieren Sie auch, ob Patches zusammengefasst und in einem Schritt installiert werden können.
Definieren Sie zu diesem Zeitpunkt auch, wer die Installation durchführt. Müssen allenfalls weitere Personen miteinbezogen oder informiert werden? Dies ist vor allem bei hochverfügbaren Systemen der Fall.
Und sollte wirklich einmal etwas nicht klappen, ist das Notfallkonzept von zentraler Bedeutung. Wo wurden die Daten gesichert? Wie kann ich das System wieder zum Laufen bringen? Habe ich Ausweichmöglichkeiten? Dies sind nur einige Fragen, die mit diesem Handbuch pro System beantwortet werden müssen.

4.4 Installieren

Im letzten Schritt gilt es, gemäss Planung die Patches zu installieren. Es empfiehlt sich vor der Durchführung eine Sicherung der wichtigsten Daten zu machen. Spielen Sie nun die Updates ein.

Überprüfen Sie am Schluss, ob alle Systeme noch wie gewünscht funktionieren. Dies gilt nicht nur für das Betriebssystem, sondern auch für die installierte Software und Dienste.
Oft ist kein Neubooten mehr notwendig. Wir empfehlen Ihnen aber trotzdem, dies nach jedem Patches durchzuführen. Sollten Fehler vorhanden sein, erkennen Sie diese beim Booten (z.B. in Eventlog-Einträgen).
Mit der Installation und der Kontrolle ist der Patchprozess noch nicht abgeschlossen. Führen Sie abschliessend das Logbuch des Systems nach (siehe auch Logbuch)

5 Welche Möglichkeiten habe ich sonst noch?

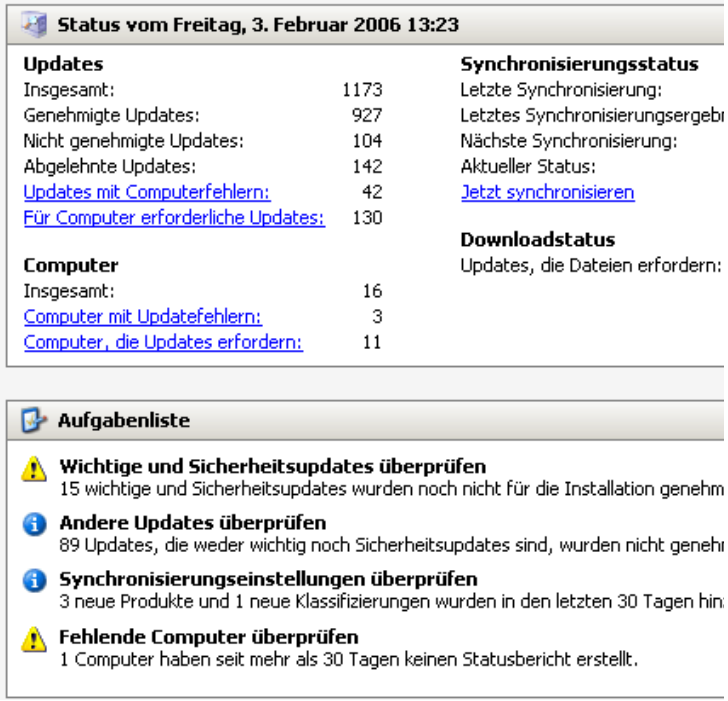
Jedem Patch „nachzurennen“ ist sehr zeitaufwendig. Auch wenn alle Informationen bereits vorhanden sind, ist eine zentrale Lösung von Vorteil. Seit einigen Monaten steht WSUS (Windows System Update Service) zur Verfügung. Mit dieser Lösung können alle Patches und Updates zentral verwaltet und freigegeben werden. Dies spart zusätzlich sehr viel Bandbreite, da nur noch ein Gerät die Patches herunterlädt. Als weitere Erleichterung ist das Aufsetzen eines neuen Systems ebenfalls sehr schnell erledigt, da alle Patches sofort zur Verfügung stehen.

Dies könnte zum Beispiel wie untenstehend Abgebildet aussehen:

Weitere Hersteller haben Programme zur zentralen Verwaltung von Patches erstellt. Hier müssen jedoch oft spezielle Installationsdateien erstellt werden, die anschliessend verteilt werden können.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

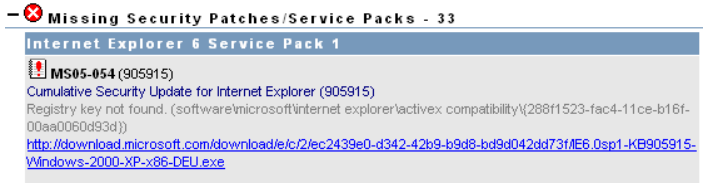
Telefon 052 320 91 20
Fax 052 320 91 21



6 Wie kann ich den Sicherheitsstand kontrollieren?

Auf dem Markt sind zahlreiche Programme vorhanden, die die Systeme nach Schwachstellen und fehlende Patches/Updates absuchen. Kostenlos ist zum Beispiel der Microsoft Baseline Security Analyzer, der jedoch nur Microsoftprodukte absucht. Sehr verbreitet ist der GFI Languard Network Security Scanner oder Nessus.

Alle Programme zeigen übersichtlich, wie es um den Patchstand steht.



Ausschnitt aus GFI Languard Network Securtity Scanner

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

7 Wo kann ich mich informieren?

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. Folgende Möglichkeiten bestehen:

Homepage des Herstellers
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 auch eine eigene Seite reserviert, wo über Sicherheitshinweise informiert wird (z.B. Microsoft unter: http://www.microsoft.com/switzerland/security/de/ oder MAC http://www.apple.com/support/downloads/).

Newsletter
im Internet sind zahlreiche Newsletter vorhanden, die nur über Schwachstellen berichten (z.B. Bugtraq). 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.

Spezialisierte Homepages
Nebst den Newslettern gibt es auch spezialisierte Homepages, die alle Informationen sammeln und übersichtlich zusammentragen. Eine Möglichkeit ist dabei http://www.securityfocus.com/

Abonnieren Sie mindestens den Sicherheitsnewsletter des Herstellers der eingesetzten Software. So erhalten Sie alle Informationen schnell und zuverlässig und müssen nicht regelmässig verschiedene Homepages aufsuchen.

8 Wie führe ich Kontrolle?

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.

Dies kann z.B. so aussehen:

Zeitpunkt	Server	Tätigkeit	Wer?
15.01.06 21:35	Web-Server	Patch xy eingespielt Pacht yz eingespielt Kontrolle der Dienste → alles i.O.	P. Meier

9 Zusammenfassung

Patchen darf keine Arbeit nebenbei sein. Der Schaden, der ein fehlender Patch nach sich ziehen kann, darf nicht unterschätzt werden. Ein strukturiertes Vorgehen ist dabei wichtig. Die Informationen über neue Updates müssen vorhanden sein, damit der Patch nach einem vorgelegten Schema installiert werden kann. Schützen Sie sich vor neuen Gefahren – ein Patchmanagement hilft Ihnen dabei weiter.