TRUST IN GERMAN SICHERHEIT

G DATA TechPaper #0171

Patchmanagement Praxisleitfaden

G DATA Software AG | Januar 2018

Inhalt

1. Einführung

Die immer weiter steigende Komplexität und allgegenwärtige Bedrohung durch Schadsoftware stellt Netzwerkadministratoren ständig vor neue Herausforderungen. Die Anzahl der installierten Programme, die aktuell gehalten werden müssen, ist in der Vergangenheit ebenso gestiegen wie die Geschwindigkeit, in der neu bekannt gewordene Sicherheitslücken ausgenutzt werden. Für die Übernahme der laufenden Aktualisierung von Programmen werden Patchmanagement-Systeme genutzt, die automatisiert für eine schnelle Verteilung sicherheitsrelevanter Updates sorgen. Um in einem Unternehmen einen vollständigen Arbeitsablauf für das Patchmanagement zu entwickeln, der sowohl die volle Kontrolle über Netzwerkressourcen als auch alle installierten Programme beinhaltet, kann Software bei der Implementierung der Patchverteilung nicht isoliert von allem Anderen betrachtet werden. Dieses Dokument beschreibt einige Standards für die Patchverteilung sowie Hilfestellungen und Best Practices für die Realisierung sowohl in kleinen Netzwerken mit bis zu 50 Clientcomputern als auch für große Netzwerke.

1.1. Definition

Trotz der Tatsache, dass Softwarehersteller bemüht sind, fehlerfreie und sichere Programme zu veröffentlichen, sind während des gesamten Produktzyklus Aktualisierungen und Patches erforderlich. Typischerweise enthält ein Update neue Funktionen oder verbessert die Performance des Programms, wohingegen ein Patch Programmfehler behebt. Während Updates in einer Unternehmensumgebung in aller Regel nicht als kritisch zu bewerten sind, erfordern Patches schnelle Reaktionszeiten. Dies gilt insbesondere für sicherheitskritische Patches. Diese sollten so zeitnah wie möglich im Netzwerk verteilt werden, um die Ausnutzung von Sicherheitslücken durch Dritte zu erschweren.

Die Aufgabe eines Patchmanagements ist es, die Verteilung von Patches zu vereinfachen. Updates sind oft ebenfalls Bestandteil eines Vorgangs, in dem eine UPMS (Unified Update/Patch Management System) – Umgebung genutzt wird. Eine komplette UPMS-Umgebung bietet jedoch nicht nur die technischen Möglichkeiten der Verteilung von Patches im Netzwerk. Auch die Zeit, die das Ausrollen der Patches benötigt, sollte so kurz wie möglich gehalten werden, um vorhandene Ressourcen darauf verwenden zu können, Sicherheitslücken suchen, zu klassifizieren und Sicherheitsprobleme zu beheben. Je nach Größe des Netzwerkes kann dies entweder speziell hierfür abgestelltes Personal erfordern oder zumindest einen klar umschriebenen Arbeitsablauf, damit auf eventuelle Sicherheitsbedrohungen schnell reagiert werden kann.

Ein solcher Arbeitsablauf ist für jedes Unternehmen erforderlich, in dem die Sicherheit und Integrität des Netzwerkes effizient geregelt werden muss. Dies gilt für kleine und Kleinstnetzwerke im gleichen Maße wie für große Unternehmensnetze. Ein zentralisiertes Patchmanagement stellt ein bestimmtes Sicherheitslevel sicher und erleichtert die einfache und schnelle Verteilung von Patches.

1.2. Bedeutung

Patches beheben zumeist Sicherheitslücken, die es Angreifern ermöglichen, Zugriff auf ein System zu erlangen, auf dem eine bestimmte Software installiert ist. Um angemessen auf diese Bedrohungen zu reagieren, ist eine schnelle Verteilung von Patches unabdingbar. Die Tatsache, dass ein Patch veröffentlicht wurde, animiert Personen jedoch auch dazu, zu versuchen, eventuelle Sicherheitslücken gezielt auszunutzen. Dabei machen sich Angreifer die Tatsache zunutze, dass mit jedem Patch auch eine Beschreibung herausgegeben wird. Diese Beschreibung und die gezielte Analyse einer Patchdatei (Reverse Engineering) ermöglichen es einem Angreifer, sehr gezielte Angriffe auf ein Programm zu unternehmen. Dies erhöht zusätzlich den Druck auf Netzwerkadministratoren, schnell auf neue Bedrohungsszenarien zu reagieren. Durch Koordinierung und Standardisierung erhöht ein Patchmanagement-System die Geschwindigkeit und Effizienz, mit der neue Patches verteilt werden können.

Die Nichtanwendung von Patches führt zu Schwachstellen, die ausgenutzt werden können. Angreifer, die eine Sicherheitslücke in einem Programm nutzen, können (je nach Schwere der Sicherheitslücke) Zugang zu einem PC erhalten, Dateien darauf speichern, Programmcode ausführen, andere Rechner im Netzwerk übernehmen oder Schlimmeres. Malware-Infektionen, die durch Drive-by-Downloads verursacht werden oder Hackerangriffe sind schon für den Heimanwender äußerst unangenehm – Firmennetzwerke sind hier jedoch besonders verwundbar. Die Risiken sind ungleich höher; die bloße Tatsache, dass ein Angreifer Zugang zum Netzwerk erhalten hat, bedeutet eine Kompromittierung der Integrität der Daten und kann auch zum Verlust von Daten oder irreparablen Systemschäden führen, falls mehrere Systeme betroffen sind. Weitere Bedrohungen sind Ausfallzeiten kritischer Systeme, Diebstahl geistigen Eigentums, Schädigung des Unternehmensrufes und hohe Kosten im Falle eines Rechtsstreits beim Verlust von Kundendaten.

Standardisierte Vorgehensweisen für Patches erleichtern die Verhinderung von erfolgreichen Angriffen auf Programme mit Sicherheitslücken. Unabhängig davon ist ein effektives Patchmanagement nicht die einzige Maßnahme, die für einen effektiven Schutz des Netzwerkes erforderlich ist. Selbst wenn Programme vollständig gepatcht sind, können Angreifer noch immer Sicherheitslücken ausnutzen, die den Softwareherstellern noch nicht bekannt sind. Die Firmeninfrastruktur sollte immer sowohl auf der Client- als auch auf der Netzwerkebene durch Sicherheitssoftware geschützt werden, die signaturbasierte Malwarescans und proaktive Technologien nutzt.

1.3. Compliance

Es existieren kaum einheitliche Regelungen für den Arbeitsablauf eines Patchmanagements. Für viele Unternehmen ist das Patchmanagement nur ein Aspekt im Gesamtzusammenhang der IT-Sicherheit. Diese wiederum ist gut dokumentiert und wird auch bereits von zahlreichen Großunternehmen umgesetzt. Besonders zu erwähnen ist hier ISO/IEC 27002:2013[1]. Diese Richtlinie regelt die Verwaltung von Informationen zur Sicherung der IT und legt Standards für die

[1] https://www.iso.org/standard/54533.html

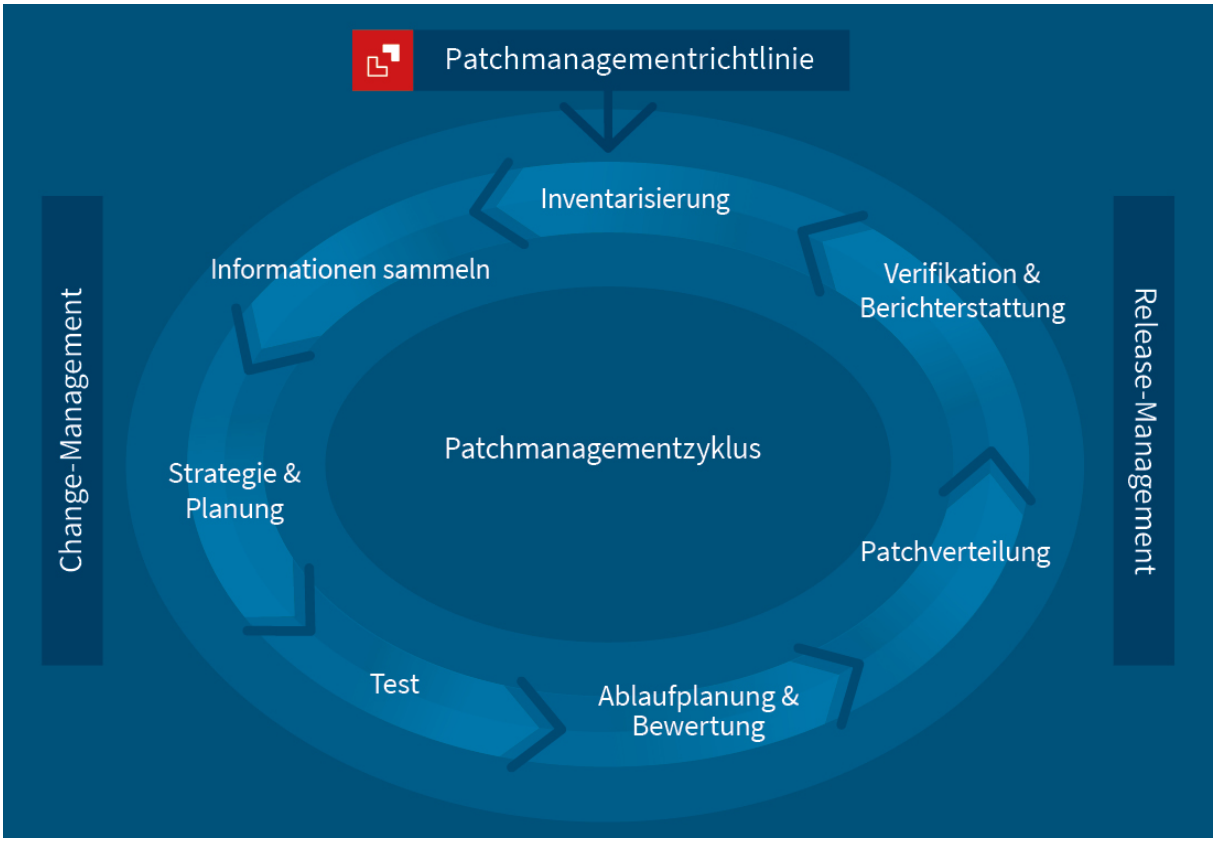
umfassende Verwaltung der IT-Sicherheit fest. Diese wurde bereits von vielen staatlichen Normierungsorganen übernommen. In ähnlicher Form bietet die „Standard of Good Practice“ des Information Security Forums zahlreiche praxisorientierte Ansätze für die IT-Sicherheit[2]. Auch ISO-Standard 15408-1:2009, auch bekannt als „Evaluation Criteria for Information Technology Security“ (Evaluationskriterien für die Sicherheit in der Informationstechnologie) stellt einen Rahmen für die Spezifikation, Implementation und das Testen der Sicherheitsanforderungen zur Verfügung[3].

In der Praxis haben Regierungsbehörden in verschiedenen Ländern eigene Standards und Empfehlungen für das Patchmanagement herausgegeben. In den Vereinigten Staaten können Unternehmen auf den „Guide to Enterprise Patch Management Technologies (SP800-40 Rev. 3)“ des National Institute of Standards and Technologies (NIST) zurückgreifen[4]. Regierungen in Europa haben ähnliche Anstrengungen unternommen: das United Kingdom National Cyber Security Centre stellt das Dokument „Manage Vulnerabilities – A Good Practice Guide“ zur Verfügung, der sich ebenfalls auf die kritischen nationalen Infrastrukturen konzentriert[5]. In Deutschland gibt das Bundesministerium für Sicherheit in der Informationstechnologie (BSI) Empfehlungen für Kleinunternehmen[6] heraus, ebenso wie für Großunternehmen[7].

2. Patchmanagement

Patchmanagement ist für jeden Computer entscheidend, unabhängig davon, ob es sich um einen Heimcomputer oder einen Firmen-PC handelt. Die Verfügbarkeit neuer Patches sollte gezielt überwacht und vorhandene Patches schnellstmöglich installiert werden. Die Art der Patchverwaltung ist eine Frage des Maßstabes, in dem sie zur Anwendung gebracht werden muss. Für Heimanwender kann das Microsoft-Update vollautomatisch Patches für Windows und andere Microsoft-Programme einspielen. Viele Hersteller sind zu automatischen und transparenten Updatemechanismen gewechselt, wie z. B. Adobe Reader oder Google Chrome. Trotzdem kann der Aufwand, den Überblick über alle installierten Programme zu behalten und für jedes einzelne über alle Sicherheitslücken und verfügbaren Patches informiert zu sein, für Nutzer von Einzel-PCs bereits hochgradig anstrengend und verwirrend sein. Dies gilt erst recht für Netzwerkadministratoren mit einer Anzahl zu betreuender Computer zwischen fünf und mehreren Tausend. An dieser Stelle kann ein standardisierter und regelmäßiger Patchmanagementzyklus vieles erleichtern, indem der Zeitaufwand für die Inventarisierung der installierten Software und deren Sicherheitslücken signifikant reduziert und Patches automatisiert installiert werden können. Ein effektiver Plan für das Patchmanagement schafft Klarheit über Zuständigkeiten, macht Änderungen nachvollziehbar, bietet eine Rollback-Möglichkeit, sorgt für das sorgfältige Testen und informiert alle Beteiligten über vorgenommene Änderungen.

[2] https://www.securityforum.org/tool/the-isf-standardrmation-security/
[3] https://www.commoncriteriaportal.org/cc
[4] https://www.nist.gov/publications/guide-enterprise-patch-management-technologies
[5] https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/SICS%20-Manage%20Vulnerabilities%20Final%20v1.0.pdf
[6] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02221.html
[7] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01014.html



***Figur 1**: Patchmanagementzyklus*

Ein Patchmanagementzyklus besteht aus mehreren unterschiedlichen Stufen. Diese werden in Kapitel 3 des vorliegenden Dokuments eingehend erläutert. Zu beachten ist, dass es sich hier um einen Kreislauf handelt und nicht um einen linearen Prozess, der durch ein bestimmtes Ereignis in Gang gesetzt wird. Patches sollten vorbeugend installiert werden. Jeder Schritt des Patchzyklus muss eindeutig definiert und einer Person zugewiesen sein. Abhängig von den Wünschen und Anforderungen können Unternehmen auch verschiedene Schritte zusammenfassen und derselben Person zuteilen oder auch weitere Schritte nach Bedarf einfügen. Eine Integration mit bereits vorhandenen Änderungsverwaltungen und Veröffentlichungs-Standards ist gewünscht. Einige Schritte lassen sich automatisieren, vor allem bei der tatsächlichen Verteilung der Patches/Updates, allerdings müssen andere entscheidende Aktionen in jedem Patchzyklus manuell angestoßen werden. Planung ist hier von entscheidender Wichtigkeit, um den Ablauf zu optimieren.

Die Wiederholungsrate für den Patchzyklus ist einerseits abhängig davon, wie viele Ressourcen zur Verfügung stehen, andererseits von der Häufigkeit, in der neue Patches für die im Netzwerk eingesetzte Software veröffentlicht werden. Eine Hauptquelle für Patches ist Microsoft, die ihr Windows-Betriebssystem monatlich mit den neuesten Updates und Sicherheitspatches versorgen. Dieser voraussehbare Patchzyklus läuft immer an einem bestimmten Datum: jedem zweiten Dienstag im Monat. Diese Regelmäßigkeit gibt Netzwerkadministratoren ein gewisses Maß and Planungssicherheit, um Patches monatlich auszurollen. Manche Hersteller haben ihre Patchzyklen an den von Microsoft ausgerichtet, andere haben eine geringere Updatefrequenz. Oracle, beispielsweise, veröffentlicht Sicherheitsupdates für die weit verbreitete Java-Laufzeitumgebung in Abständen von drei bis vier Monaten. Wieder andere Hersteller veröffentlichen immer dann

einen Patch, sobald ein kritisches Sicherheitsproblem auftritt. Für die Planung des Patchmanagements haben schnelle Antwortzeiten einen Nachteil: Es kann einige Zeit vergehen, bis ein als sicherheitskritisch eingestufter außerplanmäßiger Patch vollständig getestet und verteilt ist. Andererseits können feste Patchtage dazu führen, dass bekannte Sicherheitslücken mitunter lange Zeit ungepatcht bleiben.

2.1. Patchmanagement-Richtlinien

Vor der Planung von monatlich durchzuführenden Schritten und der Festlegung von Zuständigkeiten sind vorher Standards zu definieren. Eine Patchmanagement-Richtlinie kann hier bei der Entscheidungsfindung während des Patchzyklus eine Hilfe sein. Insbesondere ist zu klären, welche Strategie zur Anwendung kommt: Sollen verfügbare Patches grundsätzlich immer installiert werden oder wird eine Klassifizierung stattfinden, die vorhandene Patches nach der Schwere der Sicherheitslücke bewerten, welche durch den jeweiligen Patch behoben wird? Werden Patches vorbeugend installiert (um mögliche Sicherheitslücken zu stopfen) oder nach Bedarf (sobald ein Problem bekannt wird) oder eine Kombination aus beidem? Um Zeit zu sparen, die sonst mit Einzelentscheidungen für alle Patches verstreichen würde, sollten so viele allgemeine Regeln wie möglich festgelegt werden. Dabei ist zu beachten: Grundsätzlich immer jeden Patch zu installieren stellt keine Lösung dar; um Schwierigkeiten mit der System- und Netzwerkauslastung sowie Kompatibilitätsprobleme zu vermeiden, müssen an dieser Stelle bewusste Entscheidungen getroffen werden.

Das Patchmanagement hängt noch von weiteren Faktoren ab, wie Konventionen für Softwareinstallationen, Netzwerkrichtlinien, und Sicherheitseinstellungen von Anwendungen. Zwar muss in jedem Patchzyklus die installierte Software inventarisiert werden, was aber immens erleichtert werden kann, wenn bereits bei der Installation gewisse Konventionen beachtet wurden. Es sollte im Vorhinein festgelegt sein, welche Programme erlaubt sind und welcher Rechner welche Programme erhält. Das Arbeiten mit White- oder Blacklisten kann die Menge an zu inventarisierender Software reduzieren und damit den Patchprozess deutlich beschleunigen. Dasselbe gilt für Sicherheitseinstellungen, Benutzerkonten und Passwörter.

Durch das Festlegen von verbindlichen Konventionen im gesamten Netzwerk sind während des Patchzyklus weniger Ausnahmefälle zu behandeln. Es ist jedoch hilfreich, wenn auch für den Fall einer Ausnahmeregelung eindeutige Handlungsanweisungen vorliegen. Dabei sollte sich ein Netzwerkadministrator nicht von Rechnern irritieren lassen, die während des Patchzyklus nicht erreichbar sind. Gleiches gilt für Patches, welche sich während der Testphase oder nach dem Verteilen als inkompatibel mit anderen Anwendungen erweisen oder für Sicherheitslücken, die wider Erwarten nicht durch den Patch behoben wurden. Schnelle Neuverteilung, Neukonfigurieren von Programmen, Neuinventarisierung von Software sowie Eskalationskanäle sollten fester Bestandteil einer Patchmanagement–Richtlinie sein.

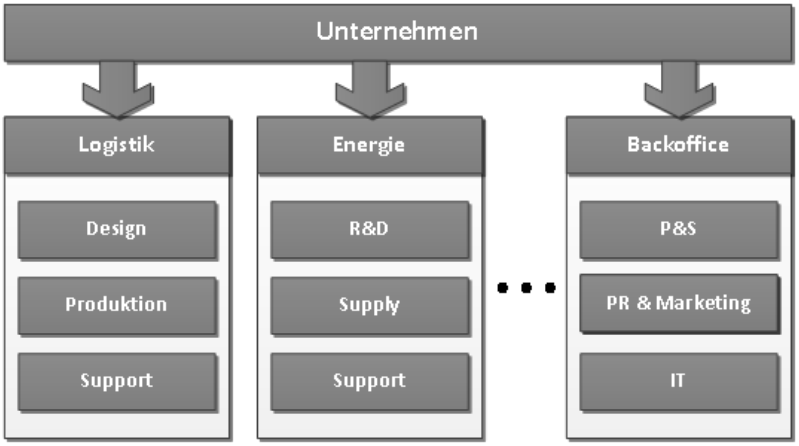
Ein weiterer Aspekt, der im Auge behalten werden muss, ist die Installation und Verteilung neuer Rechner im Unternehmensnetzwerk. Wenngleich es streng genommen nicht zum Patchzyklus gehört, muss sichergestellt sein, dass Installations-Images immer alle aktuell im Netzwerk eingesetzten Patches haben. Werden Systeme mit veraltetem Patchstand verteilt, bietet sich

Angreifern wieder eine neue Angriffsfläche, die unter Umständen erst während des nächsten Patchzyklus beseitigt wird.

2.2. Großunternehmen im Vergleich mit Klein- und mittelständischen Betrieben

In Unternehmen ist generell ein höheres Maß an Kontrolle erforderlich als im Heimanwenderbereich, wenn es darum geht, wie und wann Patches installiert werden. Werden für jedes installierte Programm die Mechanismen genutzt, die der jeweilige Hersteller vorsieht, ist das Ergebnis ein chaotischer Zustand, in dem einige Clients andere Versionen eines Programms nutzen als andere. Eine zentral verwaltete Updateverteilung bietet für jedes Unternehmensnetzwerk Vorteile, da die Bedienung vereinfacht und auf neue Sicherheitslücken schnell reagiert werden kann. Es gibt jedoch Unterschiede zwischen Firmennetzwerken. Patchmanagement in einem großen Unternehmensnetzwerk unterscheidet sich vom Patchmanagement in einem Kleinunternehmen.

In Großnetzwerken ist es wichtig, einen Überblick über die Netzwerkstruktur und dessen einzelnen Zonen und Client-Rollen zu haben. Je nach Größe des Netzwerkes kann es verschiedene Clientgruppen geben, von denen jede eine andere Funktion und Konfiguration hat. Während einige Gruppen direkt mit jedem Patch versorgt werden können, erfordern andere Gruppen eingehende Tests der jeweiligen Patches. Dies soll an folgendem Beispiel erläutert werden:

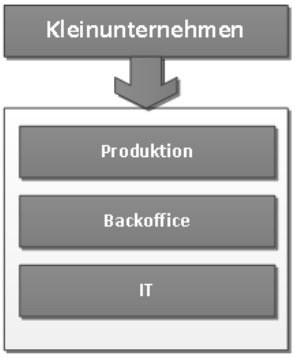


***Figur 2**: Großnetzwerkstruktur*

Ein Konzern mit mehreren Tochterunternehmen und verschiedenen Abteilungen kann in aller Regel nicht die gleichen Patchmanagement-Richtlinien überall anwenden. Die unterschiedlichen Programme, die in den jeweiligen Umgebungen in Gebrauch sind, sind jedoch nur ein Aspekt – die Auswirkungen von Patches auf Arbeitsumgebungen können ein Problem darstellen. Clients mit Standardprogrammen wie Microsoft Office und installiertem Browser, wie sie in Backoffice-Bereichen zur Anwendung kommen, können problemlos gepatcht werden; einige andere Gruppen benötigen aber möglicherweise eine stabile unveränderliche Umgebung. Dies betrifft in der Regel Rechner, die in der Qualitätssicherung oder Abteilungen mit ähnlicher Funktion stehen. Dort ist eine exakt definierte Umgebung erforderlich, in der Änderungen oft nicht ohne Weiteres möglich

sind. Diese Rechner bedürfen besonderer Sorgfalt bei der UPMS-Einbindung oder müssen manuell behandelt werden.

Personal- und Budgetmangel sind die häufigsten Herausforderungen in kleinen und mittelständischen Unternehmen, die die Schaffung einer detaillierten und dauerhaft laufenden Patchmanagement-Prozedur, in der aktuelle Patches annähernd in Echtzeit verteilt werden, verhindern. Gleichzeitig sind es aber gerade diese Unternehmen, die oft Ziel von Online-Kriminellen sind. Diese sind sich der Tatsache voll bewusst, dass dort ein reduziertes Sicherheitsbewusstsein herrscht und keine Mittel zur Verfügung stehen, die die Anschaffung von hochspezialisierter Sicherheitssoftware ermöglichen. Aus diesem Grunde unterscheidet sich das Patchmanagement in Netzwerken von Kleinunternehmen in einigen wichtigen Punkten von dem in Großnetzen. Um sicherzustellen, dass eine Patchmanagement-Richtlinie auch in einem Netzwerk durchgesetzt werden kann, in dem kein Personal und kein Budget dafür zur Verfügung steht, müssen einige der Prinzipien, die auch in großen Netzwerken angewandt werden, auf einen kleineren Maßstab gebracht werden.



***Figur 3**: Kleinbetriebnetzwerkstruktur*

Die Patch-Strategie und die Testprozeduren lassen sich stark vereinfachen, wenn die Anzahl verschiedener zu beachtender Konfigurationen kleiner ist. Kleinere Unternehmen haben wesentlich weniger Abteilungen und somit auch weniger Unterschiede in der Clientkonfiguration. Ebenso wie in einer größeren Netzwerkumgebung ist es jedoch erforderlich, etwas Zeit in eine genaue Aufstellung des Netzwerks sowie deren unterschiedliche Clienttypen zu investieren. Das untere Schema zeigt ein Beispielnetzwerk eines Unternehmens mit nur einem Unternehmenszweig. In kleinen und mittleren Betrieben kann das Netzwerk zumeist in nur zwei oder drei verschiedene Client-Rollen unterteilt werden. Die Anzahl unterschiedlicher Patches ist nun wesentlich kleiner – und obgleich kein einziger Schritt ausgelassen wurde, der auch in größeren Netzen empfohlen wird, ist ungleich weniger Zeitaufwand notwendig. Der Aufwand kann durch die Standardisierung von Clientkonfigurationen sogar noch weiter gesenkt werden. Diese Effizienzsteigerung ist vor allem entscheidend für Betriebe, die keinen eigenen Netzwerkadministrator haben. Kleinbetriebe können eine Patchmanagementsoftware einsetzen, die die meisten Schritte des Patchzyklus automatisiert. Eine solche Patchmanagementlösung kann es Betrieben ohne IT-Personal ermöglichen, bei installierten Programmen immer auf dem aktuellen Stand zu bleiben. Alternativ bleibt noch die Möglichkeit, die gesamte IT-Sicherheit auszulagern und im Rahmen eines Managed Service-Vertrages an einen Dienstleister zu übertragen.

Als Hilfestellung können Kleinbetriebe eine Checkliste erstellen, die als Richtschnur für ein Patchmanagement dienen kann. Mit einem Patchmanagement-Zyklus als Grundlage bietet eine solche Checkliste die Möglichkeit, die wichtigsten Schritte schnell durchzuarbeiten. In kleinen und Kleinstbetrieben kann eine solche Checkliste sogar eine aufwändige Patchmanagement-Richtlinie ersetzen, allerdings sollten einige Eckpunkte, die für ein effektives Patchmanagement erforderlich sind, beachtet werden:

Inventarisierung

- ✓ Auflistung aller installierten Programme und Hersteller im gesamten Netzwerk
- ✓ Herausfinden des Updatezyklus der einzelnen Softwarehersteller
- ✓ Priorisierung der installierten Produkte nach Wichtigkeit

Informationen sammeln

- ✓ Prüfung auf neue Patches einmal pro Patchzyklus jedes Herstellers

Test

- ✓ Verfügbare neue Patches auf allen Systemen testen

Patchverteilung

- ✓ Patches verteilen, installieren und verifizieren

3. Vorgehensweisen im Patchmanagement

3.1. Stufe 1: Inventarisierung

Der erste Schritt jedes Patchmanagementzyklus ist die Aktualisierung des Inventars. Dies ist während jedes einzelnen Zyklus zu aktualisieren und durch Informationen wie Software-Versionsnummern installierter Programme zu ergänzen. Um das Inventar zu aktualisieren, muss zuerst sichergestellt werden, dass alle Maschinen im Netzwerk erfasst werden. In vielen Windows-basierten Unternehmensnetzwerken wird Active Directory genutzt. Der Domänencontroller (DC) kann problemlos eine Liste aller in der Domäne befindlichen Computer erstellen. Hierbei werden jedoch keine Maschinen berücksichtigt, die nicht Teil der Windows-Domäne sind. Hier können die Protokolldateien des netzwerklokalen DHCP-Servers (IP-Adress- oder Subnetz-Scan) hinzugezogen werden, alternativ auch die Liste der im lokalen DNS registrierten Computer. Eine Kombination dieser Methoden verspricht die besseren Resultate, da nicht jeder Computer durch jede der beschriebenen Methoden erfasst wird. Es kann erforderlich sein, zu mehreren Zeitpunkten Datenerhebungen durchzuführen, um eine komplette Liste zu erhalten. In kleineren Netzwerken sollte es nicht problematisch sein, alle Computer lückenlos zu erfassen. Ist auf den einzelnen Rechnern die Datei- und Druckerfreigabe aktiv, werden alle Computer in der „Netzwerkumgebung“ des Windows Explorers aufgelistet. Die Anwesenheit virtueller Maschinen (VMs) macht die Inventarisierung komplizierter. Dennoch sollten Sie in jedem Falle als integraler Bestandteil des Netzwerkes betrachtet und entsprechend behandelt und mit Patches versorgt werden, da eine VM im gleichen Maße ein potenzielles Ziel für Angreifer darstellt wie ein physikalischer PC.

Als Teil der Patchmanagement-Strategie sollte die Verteilung der Netzwerkcomputer und ihre Konfigurationen nach einer einheitlichen Konvention erfolgen, um die Erstellung eines vollständigen Inventars zu erleichtern. Nur solche Programme zu installieren, die für den Geschäftsbetrieb notwendig sind, minimiert die Angriffsfläche, die durch ausnutzbare Sicherheitsschwachstellen entsteht. Zudem wird der Zeitaufwand für das Patchmanagement dadurch geringer. Das Überwachen von Softwareinstallationen oder das komplette Blockieren unerwünschter Anwendungen führt zu einer messbaren Einsparung bei der Zeit, die für die Identifikation, das Beschaffen und die Verteilung von Patches notwendig ist. Eine White- oder Blackliste für Software ist ein effizienter Weg, die Installation neuer Programme auf ein Minimum zu beschränken. Zudem sollten Benutzer nicht die Möglichkeit haben, auf lokale Update- und Patcheinstellungen für installierte Programme Einfluss zu nehmen, um Diskrepanzen zwischen lokal installierten Updates/Patches und vom Server vorgegebenen Richtlinien zu verhindern. In diesem Zuge sollte auch das automatisierte Update von Programmen wie Adobe Flash Player, Adobe Reader sowie der Windows Update Service deaktiviert werden. Dabei muss sichergestellt sein, dass dabei alle Updateeinstellungen für jedes installierte Programm berücksichtigt werden und dass diese zentral verwaltbar sind.

Zu den Informationen, die im Zuge der Softwareinventarisierung beschafft werden sollten, gehört die Version des Betriebssystems sowie eine vollständige Liste aller installierten Programme und Patches. Dieses Mindestmaß an Informationen muss von jedem einzelnen Computer gesammelt werden, um eine Abfrage nach verfügbaren Patches zu ermöglichen. Zudem kann das Sammeln von Hardwareinformationen dem Netzwerkadministrator ermöglichen, das Auftreten von Komplikationen beim Anwenden von Patches, wie beispielsweise mangelnden Speicherplatz auf der Festplatte, unzureichende CPU-Leistung oder Arbeitsspeicher, bereits im Vorfeld zu verhindern. Ebenso wie bei installierter Software kann es den Patchprozess wesentlich vereinfachen, wenn alle PCs im Netzwerk ein identisches Hardwareprofil haben. Das erleichtert die Inventarisierung und erlaubt eine bessere Vorhersehbarkeit bei der Verifikation von Updates.

Um die Verteilung komplikationsfrei zu gestalten, sollten alle Dienste, die auf einem Clientcomputer laufen, dokumentiert werden; idealerweise wurden die Clientcomputer schon bei der Erstinstallation so konfiguriert, dass sie maximale Performance bei minimaler Angriffsfläche bieten. Je weniger Dienste auf einem Client laufen, desto weniger Dienste können als Angriffspunkt genutzt werden. Während der Inventarisierungsphase können Dienste identifiziert werden, die nicht unbedingt erforderlich sind und in diesem Zuge auch gestoppt und deaktiviert werden. Dabei muss sichergestellt sein, dass bestimmte Dienste keinen Einfluss auf den Patchprozess nehmen. In ähnlicher Weise muss auch gewährleistet sein, dass bei der Installation von Patches auf dem Clientcomputer die erforderlichen Berechtigungen vorhanden sind. Ohne Administratorberechtigungen kann der Patchprozess nicht erfolgreich zum Abschluss gebracht werden. Nicht zuletzt muss sichergestellt werden, dass alle Computer über einen stabilen Netzwerkzugriff mit ausreichender Bandbreite verfügen. Probleme mit der Konnektivität zum Netzwerk, die durch Überlastung oder lokale Probleme verursacht werden, können eine hohe Anzahl von Fehlern nach sich ziehen, die nachher aufwändig manuell nachbearbeitet werden müssen und die Patchverteilung so stark verzögern.

Mit Hilfe von einem Programm, welches ohne lokal installierte Agent-Komponente auskommt, können Server alle relevanten Daten ohne Umwege zentralisiert erfassen. Zum Beispiel: Zahlreiche Sicherheitslücken können von netzwerkbasierten Scannern gefunden werden. Einen solchen Scan nach Schwachstellen in die Inventarisierungsphase zu integrieren, hilft dabei gefundene Schwachstellen schnell zu finden und gezielt beheben zu können. Allerdings fehlen in manchen Fällen Informationen zur Verfügbarkeit passender Patches oder anwendbarer Workarounds. Ein weiterer Nachteil des Ansatzes ohne Agent-Komponente besteht darin, dass ausgeschaltete Maschinen oder solche, die nicht dauerhaft mit dem Netzwerk verbunden sind, nur unzureichend unterstützt werden können. Mit einer clientbasierten Lösung können diese Probleme vermieden werden. Die installierte Agent-Komponente verbindet sich zum Server, sobald der Rechner eingeschaltet wird. Eine Zeitplanung für die netzwerkweite Inventarisierung entfällt. Ein weiterer Vorteil ist, dass eine solche clientbasierte Lösung mit bereits installierten Sicherheitsanwendungen kombiniert werden kann. Die Informationen, die ohnehin im Zusammenhang mit der Sicherheitssoftware anfallen, können direkt weiterverwertet und in den Patchmanagementzyklus eingebracht werden.

Es können nicht alle Computer in den Patchmanagementzyklus eingebunden werden. Ziel sollte es zwar sein, alle PCs mit den neuesten Patches auszustatten, allerdings gibt es auch gute Gründe dafür, bestimmte Geräte von diesem Zyklus auszuschließen. Einige Abteilungen sind eventuell auf unveränderliche Umgebungen angewiesen (zu Test- und Vergleichszwecken oder zur Evaluierung) und benötigen vor der Verteilung von Patches weitere Tests. Ältere „Legacy“-Geräte benötigen in ähnlicher Weise eine spezielle Behandlung. Einige der Programme auf diesen Legacy-Geräten benötigen möglicherweise ältere Betriebssysteme, die nicht Bestandteil der sonstigen Ausstattung im Firmennetzwerk sind oder vom Hersteller nicht mehr mit Patches/Updates versorgt werden. Aktuelle Patches dort einzuspielen, kann wichtige Anwendungen negativ beeinflussen, sodass besondere Tests angebracht sind. Einige Legacy-Programme benötigen eventuell besondere Patches, um die Kompatibilität mit gepatchten Versionen anderer Programme zu wahren. Daher ist es sehr wichtig, diese Anforderungen in der Planung so früh wie möglich zu klären. Sollte sich während der Inventarisierung herausstellen, dass Legacy-Software genutzt wird, besteht eine höhere Chance, dass Kompatibilitätsstörungen auftreten.

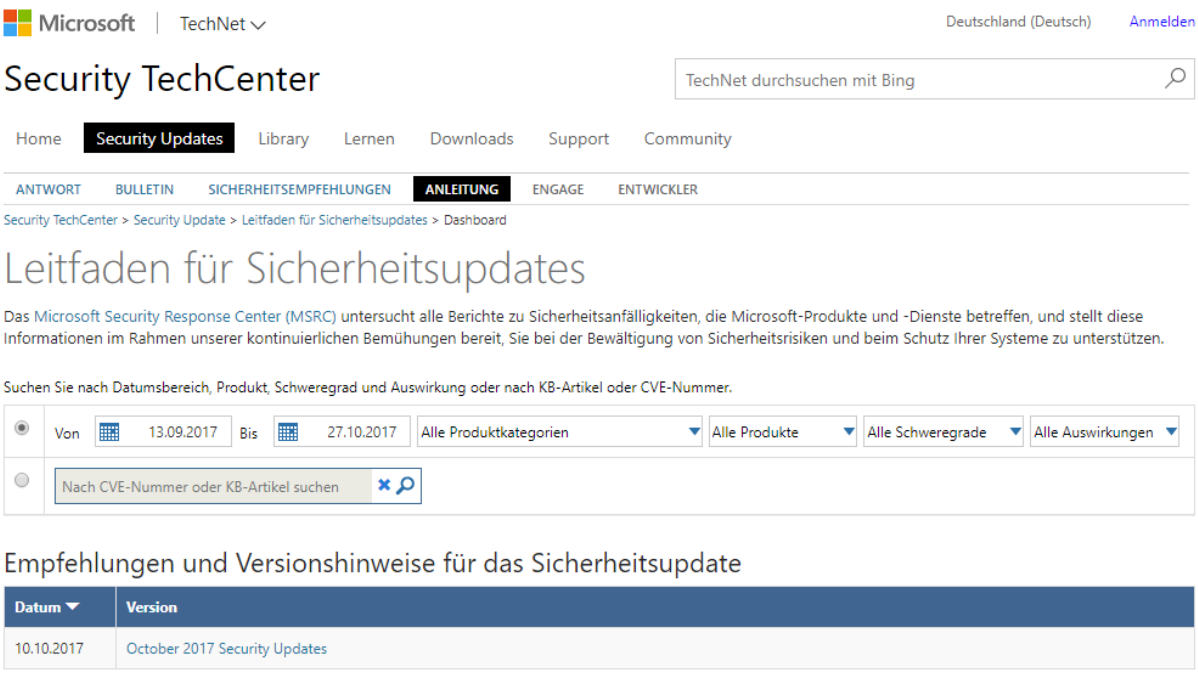
Computer, die nicht dauerhaft mit dem Netzwerk verbunden sind (z.B. VPN-Clients oder Laptops von Außendienstmitarbeitern), haben unter Umständen während der Inventarisierungs- und Verteilungsphase keine Verbindung zum Firmennetz. Hier ist darauf zu achten, dass keine Spitzen in der Rechner- und Netzwerklast dieser PCs auftreten. Eine separate Zeitplanung für Inventarisierung und Patchverteilung für diese Art PCs ist hier angeraten. Virtuelle Maschinen, die direkt in das Unternehmensnetzwerk eingebunden sind, sollten ebenso mit eingebunden werden, sofern sie sich nicht außerhalb des Produktivnetzes befinden oder durch Sicherheitslösungen oder besondere VLAN-Konfiguration isoliert sind.

Im Allgemeinen sollten PCs, die aus irgendeinem Grund (noch) nicht in den Patchmanagementzyklus eingebunden sind oder veraltete Programmversionen nutzen, besonders sorgfältig auf Schwachstellen und Infektionen mit Schadsoftware geprüft werden. Einen separaten Scan nach Schadsoftware anzusetzen oder betroffene Geräte bis zur Klärung ihres Status in ein eigenes (Sub-)Netz oder Firewall-Zone zu verlagern, hilft dabei Problemen vorzubeugen. Durch

zusätzliche Sicherheitsrichtlinien kann der Zugang zu Netzwerkressourcen weiter eingeschränkt werden.

3.2. Stufe 2: Informationen sammeln

Sobald ein vollständiges Inventar erstellt bzw. aktualisiert wurde, ist es entscheidend, über Update- und Patchzyklen sowie aktuelle Sicherheitslücken und andere Sicherheitsrisiken auf dem Laufenden zu sein und zu bleiben. Der Netzwerkadministrator sollte idealerweise die Softwareversion jedes im Netzwerk installierten Programms kennen und über bekannte Fehler und vorhandene Sicherheitsupdates informiert sein. Dies gilt gleichermaßen für Kleinunternehmen wie für Großbetriebe. Auch wenn ein Kleinunternehmen nicht das Budget zur Verfügung hat, einen Vollzeitadministrator anzustellen, ist das Sammeln von Informationen die Basis für eine angemessene und wirkungsvolle Patchmanagement-Richtlinie. Dabei spart es mitunter viel Zeit, Informationen aus Drittanbieterquellen wie entsprechenden Nachrichten-Webseiten zu beziehen oder auch von Patchmanagement-Programmen, die automatische Benachrichtigungen über neue Patches erstellen.



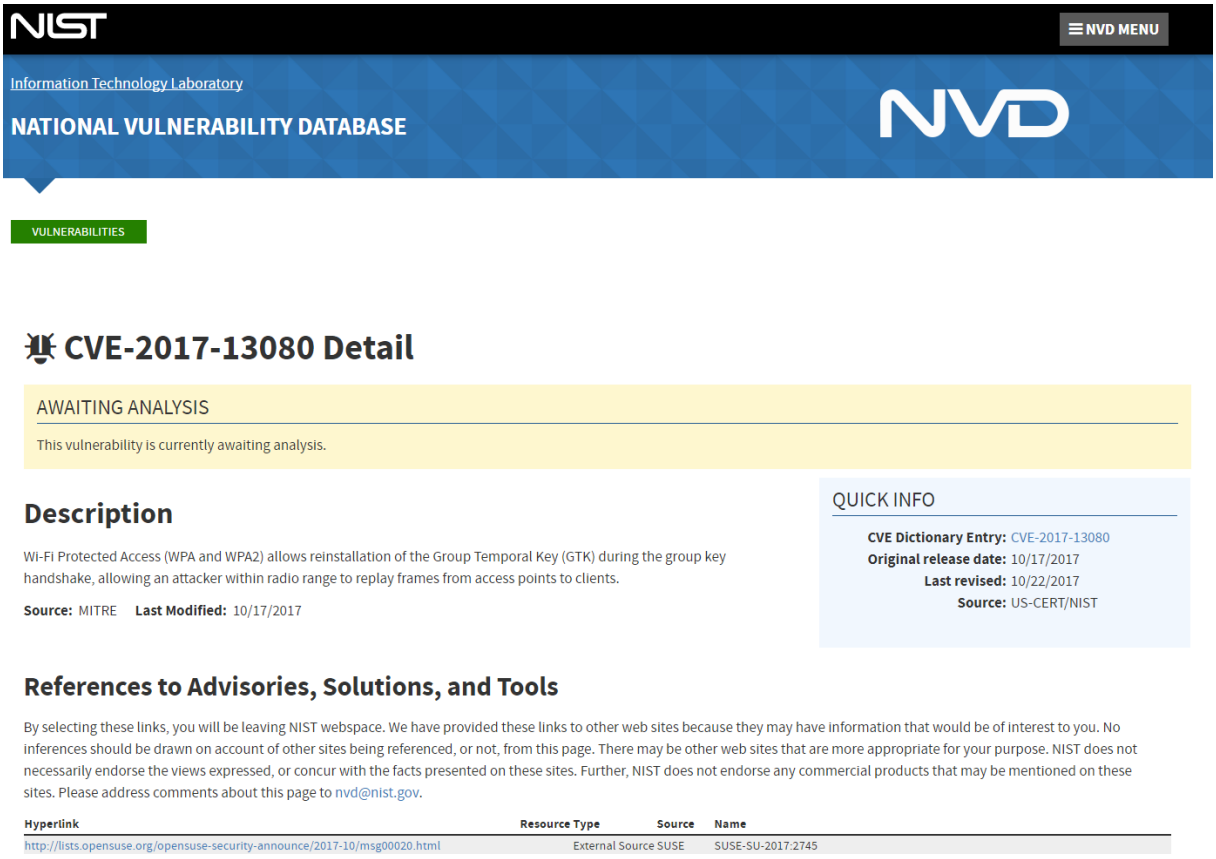
***Figur 4**: Informationen des Herstellers*[8]

Eine einfache Methode, sich über Updates zu informieren besteht darin, den Hersteller des jeweiligen Programms zu konsultieren. Die meisten Anbieter veröffentlichen Softwareupdates auf ihrer Internetseite, oft zusammen mit Informationen über die neuesten Ergänzungen und Sicherheitsupdates. Einige Webseiten bieten auch RSS-Feeds oder Mailbenachrichtigungsdienste an; dies ist ein effektiver und kostengünstiger Weg, sich auf dem aktuellen Stand zu halten. Zwar ist das Beziehen von Informationen ‚direkt von der Quelle' ein wirkungsvoller Weg, verlässliche Informationen zu erhalten, beinhaltet allerdings auch eine Menge vermeidbaren Aufwand. Viele kommerzielle Patchmanagement-Lösungen unterhalten eigene Datenbanken mit

[8] https://portal.msrc.microsoft.com/de-de/security-guidance

Versionsinformationen und ermöglichen es Administratoren so, schnell ihren eigenen Softwarebestand mit den aktuellsten Patches abzugleichen. Auch wenn das Vertrauen auf Drittanbieterquellen ein gewisses Risiko birgt, da die Daten nicht unmittelbar vom Hersteller stammen, ist die Nutzung dieser Drittquellen eine immense Erleichterung für den Informationssammelprozess. Diese Quellen enthalten vielfach hochwertige Informationen, zusammen mit Daten zur Klassifikation eines Patches sowie Verifikationsdaten und Informationen zu bekannten Kompatibilitätsproblemen mit verbreiteten Branchenanwendungen.

So wichtig Informationen zu den Patches selbst auch sein mögen, so wird trotzdem damit nicht das gesamte Spektrum an Informationen abgedeckt. In der Entwicklungsphase vor der Veröffentlichung eines Patches ist oft bereits bekannt, dass ein Patch veröffentlicht wird. Wenn einem Softwarehersteller eine Sicherheitslücke bekannt wird, so gibt dieser oftmals eine Sicherheitsinformation heraus. Darin enthalten sind Informationen über die Schwere des Problems wie auch ein Zeitansatz, wann eine Lösung bereitstehen wird. Auch Workarounds, die von Administratoren temporär angewendet werden können, bis ein Patch zur Verfügung steht, können Teil dieser Information sein.



***Figur 5**: Common Vulnerabilities and Exposures (CVE)-Datenbank*[9]

Hersteller können auch eine CVE-Nummernvergabestelle, die eine Datenbank mit verbreiteten Sicherheitslücken und Schwachstellen (Common Vulnerabilities and Exposures) verwalten, informieren. Viele Sicherheitslücken werden mit einer solchen CVE-Nummer belegt und ermöglichen es so Administratoren, auf dem aktuellsten Stand über Sicherheitslücken zu bleiben,

[9] https://nvd.nist.gov/vuln/detail/CVE-2017-13080

die beizeiten behoben werden müssen. Es wird eine zentrale CVE-Datenbank vom United States National Institute of Standards and Technologies (NIST) verwaltet[10]. Obgleich die CVE-Datenbank auf breiter Ebene als Informations-Pool genutzt wird, sind nicht alle Sicherheitslücken in ihr aufgeführt.

Trotz der Tatsache, dass nicht alle Sicherheitslücken in der CVE-Datenbank aufgeführt sind, fällt dennoch jeden Tag eine beträchtliche Datenmenge an. Alle neu auftretenden Sicherheitslücken nachverfolgen zu wollen wird sich jedoch als zu arbeitsintensiv herausstellen. Unabhängige Internetseiten so wie staatlich geförderte Computer Emergency Response Teams (CERTs) sind ebenfalls eine wertvolle Informationsquelle. Die US-Heimatschutzbehörde veröffentlicht beispielsweise Aktualisierungen zu neuen Sicherheitslücken sowie nützliche Hintergrundinformationen auf ihrer Internetseite[11]. Im europäischen Raum gibt es sowohl nationale Einrichtungen als auch das zentral verwaltete CERT-EU[12] und die European Network and Information Security Agency[13]. Die meisten Webseiten der hier aufgeführten Organisationen bieten Ratschläge zur Sicherheit sowie regelmäßig aktualisierte Nachrichten.

Herstellerinformationen und CVE-Datenbankeinträge stellen hochgradig technische Informationen bereit, die auf konkreten Fällen basieren. Zugänglicher sind an dieser Stelle Informationen der CERTs und eignen sich auch, um bei aktuellen Malware-Trends auf dem Laufenden zu bleiben. Diverse News-Webseiten stellen Artikel zu sicherheitsrelevanten Themen ins Netz und Antivirus-Hersteller veröffentlichen zu aktuellen Themen Whitepapers und Blogartikel.

3.3. Stufe 3: Strategie und Planung

Sobald Informationen über (demnächst) veröffentlichte Patches und Updates beschafft wurden, beginnt die Planungsphase. Die in dieser Phase gesammelten Erkenntnisse sollten, sofern noch nicht geschehen, in den Patchmanagement-Plan einfließen. So steht im Idealfall bereits fest, welche Art von Patches überhaupt und welche zuerst installiert werden. Je nachdem, wie kritisch eine Schwachstelle ist, kann es nötig werden, die Verteilung gegenüber dem normalen Zyklus entweder zu beschleunigen oder zunächst einen Workaround zur Anwendung zu bringen.

Die erste und wichtigste Erkenntnis ist, dass nicht jeder Patch und jedes Update installiert werden muss. Im Patchmanagement-Plan ist bereits festgelegt, welche Typen von Patches und Updates überhaupt zu installieren sind, um zu verhindern, dass langwierige und komplexe Entscheidungsprozesse zu viel Zeit in Anspruch nehmen. Stuft ein Softwareanbieter beispielsweise ein Update als notwendig ein, so kann die Entscheidung des Unternehmens oder des Netzwerkadministrators durchaus von dieser Einschätzung abweichen, da eine neu hinzugekommene Funktion nicht benötigt wird. Ebenso kann ein Softwarehersteller mit einem Update eine im Unternehmen benötigte Funktion entfernen. Bereits im Vorfeld zu entscheiden, ein bestimmtes Update auszulassen, kann Zeit bei Abwägungen, Verteilung und Verwaltung sparen, die effektiver für andere Updates und Patches genutzt werden kann. Unter gewissen Umständen können selbst Sicherheitsupdates ignoriert werden, wenn sie eine Sicherheitslücke betreffen, die

[10] https://nvd.nist.gov
[11] https://www.us-cert.gov
[12] https://cert.europa.eu
[13] https://www.enisa.europa.eu

im Unternehmensumfeld nicht ausgenutzt werden kann. Jedoch ist der Grundsatz „Vorsicht ist besser als Nachsicht“ an dieser Stelle ein guter Ausgangspunkt.

Unabhängig davon, aus welcher Quelle Informationen zu Patches oder Sicherheitslücken bezogen werden: Es wird fast ausnahmslos immer eine Einstufung des Schweregrads angegeben, die Administratoren bei der Entscheidung unterstützen soll, ob ein Patch installiert werden soll oder nicht (und wenn, wie schnell). Diese Einstufung wird entweder vom Hersteller vorgenommen oder durch den Herausgeber der Information. Diese Angaben helfen bei der Entscheidung, welche Patches zuerst zu installieren sind, sofern sie ein Produkt betreffen, welches in einem Firmennetzwerk eingesetzt wird.

Je ernsthafter eine Schwachstelle ist, umso schneller sollte sie durch die Verteilung eines Patches behoben werden. Die Einschätzung des Schweregrads basiert auf mehreren Faktoren: Kann eine Schwachstelle nur lokal ausgenutzt werden und nur wenn ein Angreifer direkten Zugang zu einem betroffenen PC hat, wird die Schwere niedriger bewertet als wäre ein Ausnutzen auch aus der Ferne (z.B. über das Internet) möglich. In einigen Szenarien kann ein Angreifer lediglich die betroffene Software zum Absturz bringen. In anderen wiederum erlaubt eine Schwachstelle Lese- oder Schreibzugriff auf das Dateisystem oder die Ausführung eines beliebigen Programms; auf diesem Wege könnten Daten gestohlen oder angeschlossene Geräte kompromittiert werden. Derlei Schwachstellen müssen so schnell wie möglich geschlossen werden. Ein weiterer Faktor ist die Verbreitung der Kenntnis von einer Schwachstelle. Wurde die Schwachstelle vom Hersteller selbst gefunden, ist die Chance vergleichsweise gering, dass sie aktiv von Angreifern ausgenutzt wird, da sie parallel sowohl vom Hersteller als auch potenziellen Angreifern hätte entdeckt werden müssen. Wurde eine Schwachstelle jedoch öffentlich gemacht (z.B. durch einen IT-Spezialisten) oder hat der Hersteller Daten zu der Schwachstelle von einem auf diese Informationen spezialisierten Händler erworben, so hat eine wesentlich größere Gruppe Zugang zu den technischen Details und hatte Gelegenheit, funktionierende Exploits zu erstellen und zur Anwendung zu bringen. In so einem Falle ist der Hersteller gehalten, in so kurzer Zeit wie möglich einen Patch zur Verfügung zu stellen; Administratoren sollten sich hierauf einstellen. Erschwerend kommt noch dazu, dass der Zeitpunkt der Veröffentlichung eines Patches gleichzeitig eine Phase stark gehäufter Angriffe einläutet. Durch gezielte Analyse (Reverse Engineering) von Patchdateien wird versucht, Rückschlüsse auf Details der Schwachstelle zu ziehen. Diese werden dann genutzt, um bis dahin ungepatchte Systeme anzugreifen.

Zusätzlich zum Schweregrad der Patches müssen die verschiedenen Funktionen der einzelnen Clients, die in der Patchmanagement-Planung aufgelistet sind, berücksichtigt werden. Ein Client, der eine höhere Verwundbarkeit aufweist als andere (z.B. ein Büro-PC, der für externe Kommunikation genutzt wird), sollte öfter und in kürzeren Abständen mit Updates und Patches versorgt werden als Rechner, die keine Berührung mit unter Umständen vertraulichen Informationen haben oder Rechner, die gar nicht mit der Außenwelt in Verbindung stehen. Es gilt für jeden Patch sorgfältig abzuwägen, ob er im gesamten Netzwerk installiert werden sollte oder nur auf PCs, die eine bestimmte Funktion erfüllen oder überhaupt nicht. In Netzwerken von Kleinunternehmen ist dies noch eher überschaubar, da die Anzahl der verschiedenen Funktionen, die einzelne Firmen-PCs erfüllen, begrenzt ist. Dennoch sollten einzelne Rechnerfunktionen klar

abgegrenzt werden. Die gleiche Patchkonfiguration unterschiedslos an alle Rechner zu verteilen, ist allgemein nicht empfohlen.

In dieser Phase muss auch geklärt werden, ob die zur Installation ausgewählten Patches Abhängigkeiten haben. Einige Programme stellen einfache Updater zur Verfügung, die jede Version auf den aktuellen Stand bringen. Andere wiederum nutzen inkrementelle Updates, die eine Rückverfolgung über mehrere Versionen erfordern, um alle erforderlichen Patches zu finden und in der korrekten Reihenfolge zu installieren. Auch kann ein Patch die bereits erfolgte Installation eines bestimmten Treibers, einer Laufzeitumgebung oder eines anderen Programms voraussetzen. Die Patchbeschreibung enthält in aller Regel Informationen über derlei Abhängigkeiten, zusammen mit den Links zu den erforderlichen Patches oder den Patches selbst. Abhängigkeiten können an Komplexität gewinnen, wenn es darum geht, Systeme auf den letzten Stand zu bringen, die seit einer geraumen Zeit nicht gepatcht wurden. Windows-Updates und Service Packs sind oft von anderen Patches abhängig und erfordern größte Sorgfalt bei der korrekten Anwendung. Gerade während der Planungs- und Strategiephase muss verstärkt darauf geachtet werden, ob bestimmte Patches weitere Installationen erfordern.

Die Planungsphase sollte auch dafür benutzt werden, Entscheidungen über die Verteilung zu treffen. Zu allererst muss die Entscheidung fallen, zu welchem Zeitpunkt Patches zu installieren sind. Für sicherheitsrelevante Patches ist die erste Reaktion der meisten Administratoren „Je schneller, desto besser“. Eine schnelle Installation behebt in der Tat schnell eine Sicherheitslücke, doch sollten einige Überlegungen auch hier in Betracht gezogen werden. Um Kompatibilitätsproblemen vorzubeugen, müssen Patches getestet werden. Dies kann mehrere Tage in Anspruch nehmen. Die Verteilung selbst braucht ebenfalls eine gewisse Zeit. Nur in wenigen Fällen sollte ein PC zu einem Neustart gezwungen werden. Wird ein Neustart nicht erzwungen, kann es wiederum eine Zeit dauern, bis ein Patch tatsächlich in Kraft tritt. Je nach Größe des Netzwerkes ist auch eine stufenweise Verteilung ratsam, was die Verteilung wiederum weiter verzögert. Für mobile Mitarbeiter und VPN-User kann die Verteilung noch länger dauern, da sie nicht immer mit dem Netzwerk verbunden sind. (Für Clients, die nur über eine eingeschränkte Bandbreite verfügen können, muss bei der Festlegung der Priorität eines Patches gegebenenfalls die zu übertragende Datenmenge in Betracht gezogen werden.)

Als Richtwert kann festgehalten werden: Kritische Patches sollten zwischen 48 Stunden und einer Woche nach ihrer Veröffentlichung verteilt sein. Die Verteilung nicht-kritischer Patches oder Updates, die neue Funktionen bereitstellen, kann verzögert erfolgen. Wie bereits erwähnt, hängt die Planung entscheidend vom Aufbau des Netzwerks, der verfolgten Strategie und der Schwere einer Sicherheitslücke ab. Selbst wenn es um Patchmanagement geht, muss ein Gleichgewicht zwischen Sicherheit, Usability und Verfügbarkeit gefunden werden. Sollte es zu große Einbußen im Geschäftsbetrieb geben, als dass sich die Außerbetriebsetzung eines Systems zum Patchen nicht rechtfertigen lässt, muss die Patchverteilung verschoben werden. In anderen Fällen ist es unkritisch, einen User zum Neustarten des Rechners zu zwingen. Dabei will beachtet sein, dass nicht die Verteilung eines Patches entscheidend ist, sondern wann er zur Anwendung kommt. Neustarts, stufenweise Verteilung und andere Verzögerungen ziehen eine Verschiebung von Patches nach sich, sodass ein temporärer Workaround genutzt werden muss, um eine

Sicherheitslücke kurzfristig zu beheben. Allerdings ist ein Workaround niemals eine Lösung, sondern immer nur ein vorübergehender Ansatz, bis der richtige Patch angewendet wurde.

Das Setzen einer Frist im Vorhinein, die alle Besonderheiten des Netzwerks berücksichtigt und nur die Schwere eines Sicherheitsproblems als Variable hat, kann die Entscheidungsfindung beschleunigen. Die Festlegung eines Soll-/Ist-Wertes für die Patchanwendung kann ebenfalls hilfreich sein. Dieser sollte nach den ersten paar Tagen einen bestimmten Wert erreicht haben und sich schrittweise erhöhen. Das Ziel, die 100-Prozent-Marke bei der Patchdurchdringung zu erreichen, ist jedoch in der Praxis nahezu unmöglich, da manche Systeme möglicherweise kaum genutzt werden oder sich in Wartung befinden.

3.4. Stufe 4: Test

Die Testphase ist der wichtigste Schritt, um Komplikationen während und nach der Verteilung eines Patches zu vermeiden. Das Tagesgeschäft kann stark beeinträchtigt werden, wenn die Verteilung eines Patches dazu führt, das ein Client (vorübergehend) unbedienbar wird. Leider setzt die Geschwindigkeit, mit der neue Patches installiert werden sollten, der Zeit, die zum Testen zur Verfügung steht, manchmal enge Grenzen. Bei der Planung, welche Patches zur Anwendung kommen sollen, sind Sicherheit, Usability und Verfügbarkeit nicht immer miteinander vereinbar. Der Netzwerkadministrator sollte zu der Erkenntnis gelangen, dass nicht alle Patches gleich behandelt werden müssen und sollten. Kleine, unkritische Patches werden keine Lastspitzen im Netzwerk verursachen und auch keine Abhängigkeiten besitzen wie größere und komplexere Patches. Daher ist für solche weniger Testaufwand erforderlich. Gleichzeitig können Patches mit niedriger Dringlichkeit länger getestet werden, da sie nicht schnellstmöglich verteilt werden müssen. Auf jeden Fall sollten Patches in einer Umgebung getestet werden, die der Produktivumgebung so weit wie möglich ähnelt. Wie auch an anderer Stelle im Patchmanagement-Prozess haben es Administratoren kleinerer Netzwerke leichter, da weniger Konfigurationen zu berücksichtigen sind und somit der gesamte Patchprozess schneller abgeschlossen werden kann.

Um Tests für die einzelnen Patches durchzuführen, muss eine Testumgebung bereitgestellt werden. Im Idealfall beinhaltet diese alle Clientkonfigurationen, die auch in der Produktivumgebung anzutreffen sind. Eventuelle Fehler können nur in einer Testumgebung vorausgesehen werden, in der der Patchprozess so nah wie möglich an den Gegebenheiten des Produktionsnetzes ist. Dazu müssen mehrere Rechner zur Verfügung stehen, von denen jeder eine bestimmte Client-Rolle im Netzwerk repräsentiert. Das Testen von Patches für Maschinen, die zentrale Rollen im Netzwerk einnehmen, ist besonders schwierig, da es schwer ist, eine Testumgebung bereitzustellen, die wirklich alle Konfigurationsaspekte berücksichtigt. Eine Möglichkeit ist, eine Testumgebung aufzustellen, in der Clients und Server virtualisiert sind. Das Lokalisieren von potenziellen Problemen auf Anwendungs- und Konfigurationsebene ist zwar hiermit möglich, allerdings lässt eine solche Testumgebung Faktoren wie Netzwerkbandbreite oder Festplattenspeicher außer Acht. Eine weitere Alternative ist das Bestimmen eines weniger kritischen Bereichs des Produktivnetzes, welcher für Testzwecke eingesetzt wird. Auf diese Weise kann in einer Umgebung getestet werden, die so nah an der Produktivumgebung ist wie möglich. Solange die testweise Verteilung von Updates an nicht-kritische Systeme erfolgt, kann diese Herangehensweise wertvolle Erkenntnisse für die Patchverteilung liefern. Abgesehen jedoch vom

offensichtlichen Potenzial für auftretende Komplikationen findet hier eine Vermischung von Test- und Verteilungsphase statt: Es kann sich dann sehr schnell als schwierig herausstellen, diejenigen Maschinen, auf denen Patches getestet werden und solche, auf denen dies nicht stattfindet, auseinander zu halten.

Sind Rechner gefunden, die für Testzwecke verwendet werden können, kann mit dem Ausrollen der zu testenden Patches begonnen werden. Zuvor muss geklärt sein, ob es laut Hersteller bekannte Probleme gibt, die im Kontext des Firmennetzes gezielt getestet werden müssen. Die erste Hürde ist die Art des Installers, den der jeweilige Hersteller verwendet. Ein oft eingesetzter Standard ist der Microsoft Windows Installer (MSI). Da die meisten, wenn nicht sogar alle Windows-PCs das erforderliche Framework bereits mitbringen, nutzen die meisten Hersteller diese Technologie für ihre Installationen. Der Windows Installer ermöglicht eine einfache Versionsverwaltung sowie unbeaufsichtigte Installationen – beides sind Techniken, die für eine Verteilung von Patches entscheidend sind. Dennoch ist der Windows Installer kein „Selbstläufer“. Tests sind erforderlich, um eine Installation ohne unerwartete Fehlermeldungen des MSI-Prozesses sicherzustellen. Fehlende Installationsmedien oder zwischengespeicherte Dateien zählen zu den Fehlern, die am häufigsten auftreten und zu einer Unterbrechung einer Installation mit dem Windows Installer führen und die Verteilung eines Patches auf mehrere Netzwerk-PCs nachhaltig stören können. Auch können Hersteller eigene Installer verwenden. Solche Installer in einer Testumgebung auszuführen, gibt Administratoren die Gelegenheit, deren Verhalten zu beobachten und gegebenenfalls Anpassungen für die Verteilung auf breiter Ebene vorzunehmen.

Um die Usability zu bewerten, ist eine Prüfung wichtig, ob ein Patch einen Systemneustart erfordert. Befinden sich Dateien, die durch einen Patch ausgetauscht werden, noch im Zugriff, können diese nur getauscht werden, wenn das System neu gestartet wird. Es kann daher notwendig sein, zu prüfen, ob eine zu patchende Datei von einem Hintergrunddienst genutzt wird, sodass dieser gegebenenfalls vor der Installation des Patches vorübergehend angehalten werden kann. Für komplexere Patches, wie etwa Windows-Sicherheitspatches, ist unabhängig davon, ob man dies vermeiden möchte, fast in jedem Fall ein Neustart erforderlich. Sollte ein Neustart unvermeidlich sein, muss die Verteilung in der folgenden Phase (Planung und Bewertung) sorgfältig geplant werden, damit die Verteilung mit dem Geschäftsbetrieb und eventuellen Wartungsfenstern abgestimmt werden kann.

Nach Beendigung der Installation (einschließlich eines oder mehrerer Neustarts, falls notwendig) sollte jeder Rechner genauso funktionieren wie vor der Installation, abgesehen von den durch den Patch vorgenommenen Änderungen. Der Systemstart sollte funktionieren und nicht wesentlich länger dauern. Der Benutzer sollte keinerlei Dialogfenster, Benachrichtigungen, Nachrichten über Bereinigungsprozesse oder andere Nachwirkungen der Patchinstallation zu sehen bekommen.

Es sollte jedoch nicht nur die Installation getestet werden; zukünftige Kompatibilitätsprobleme oder vorher nicht getestete Szenarien erfordern unter Umständen die Deinstallation eines Patches. Daher muss es möglich sein, ein Programm auf einen Stand vor der Patchinstallation zurückzusetzen. Für Programme, die mit einem standardisierten MSI-Installer arbeiten, ist dies in der Regel einfach. Bei Programmen, die nicht über eine Versionsverwaltung verfügen oder einen nichtstandardisierten Installer benutzen, ist eventuell das Anlegen einer Sicherung vor der Installation eines Patches erforderlich, um ein Rückgängigmachen zu ermöglichen. Einige Patches

sind so verzweigt, dass für eine Deinstallation des Patches eine Neuinstallation eines wesentlichen Teils des Betriebssystems notwendig wird. Aus diesem Grund sollte die Dokumentation eines Patches sorgfältig studiert werden, um die Möglichkeit einer Inkompatibilität oder anderen Komplikationen bereits im Vorfeld berücksichtigen zu können. Falls es Unsicherheiten gibt, die innerhalb der Testphase nicht abschließend geklärt werden können, muss der betroffene Patch entweder in den kommenden Patchzyklus verschoben werden, um weitere Tests durchzuführen, oder die Verteilung muss schrittweise erfolgen, wobei genau auf eventuelle Auswirkungen auf die ersten Rechnergruppen geachtet werden muss, die den Patch erhalten.

Das Testen von Patches dient nicht nur der Erprobung der Verteilung, sondern auch der Einschätzung der Auswirkungen eines Patches auf den Endanwender. Nach der Installation eines Patches können bestimmte Programme eine veränderte Bedienung haben, da neue Funktionen eingeflossen sind oder im Zuge der temporären Behebung einer kritischen Sicherheitslücke bestimmte Teile des Betriebssystems oder eines Programms verändert wurden. Die Testumgebung sollte daher die Arbeitsumgebung der Anwender möglichst detailliert wiedergeben, um einen schnellen Vorher-/Nachher-Vergleich anstellen zu können. Je nachdem, wie viel Zeit für das Testen zur Verfügung steht, sollten auch verschiedene Arbeitsabläufe von Nutzern nachgestellt werden. Die Patchverteilung muss nicht zwangsweise komplett transparent ablaufen, im Falle von Änderungen sollten diese jedoch ausführlich dokumentiert und noch vor der Patchverteilung den betroffenen Anwendern kommuniziert werden.

Sobald die Verteilung der Patches ebenso wie die gepatchten Programme ohne weitere Probleme funktioniert, können beim Testen auch externe Faktoren mit einbezogen werden. Ein gepatchtes Programm wird unter Umständen nicht korrekt von einer im Unternehmen eingesetzten Anwendungskontrolle erkannt. Dies kann vor allem dann der Fall sein, wenn ausführbare Dateien verändert oder ausgetauscht wurden. White- und Blacklisten von Anwendungen müssen gegebenenfalls angepasst oder entsprechende Regeln anders strukturiert werden: so ist es möglich, Programme nach dem Produktnamen, dem Hersteller oder der Versionsnummer zu filtern. In ähnlicher Weise können (Gruppen-)Richtlinien in Windows einige Funktionen eines gepatchten Programms beeinträchtigen. Falls hier Probleme auftauchen, ist diesen mit Konfigurationsänderungen oder Modifikationen der problematischen Richtlinie entgegen zu wirken.

3.5. Stufe 5: Ablaufplanung und Bewertung

In der Phase der Ablaufplanung und Bewertung kommen Informationen fast aller vorangegangenen Stufen des Patchmanagements zusammen: das Inventar des Netzwerks, Patchabhängigkeiten sowie das Installationsverhalten werden zu einem Verteilungsplan zusammengeführt.

Zu diesem Zeitpunkt weiß der Administrator, welche Patches ausgerollt werden müssen und kennt die Risikobewertung jedes einzelnen Patches. Die Bewertung der Schwere einer Sicherheitslücke ist jedoch nicht der allein entscheidende Faktor bei der Entscheidung, welcher Patch zu installieren ist. Einige Patches haben spezielle Systemanforderungen oder Kompatibilitätsprobleme, die vor der Installation eines Patches behandelt werden müssen. Zudem können in einigen Fällen nicht

alle Rechner gleichzeitig mit einem Patch versorgt werden. Einige Rechner sind eventuell in Benutzung, wohingegen wieder andere nur ein kleines und genau definiertes Zeitfenster für die Installation von Patches zur Verfügung haben. Es ist in jedem Fall empfehlenswert, Patches stufenweise zu verteilen und nicht an alle PCs gleichzeitig. So kann der Administrator noch auf unvorhergesehene Probleme reagieren, bevor ein Patch im gesamten Netzwerk installiert ist und im Notfall die Verteilung stoppen. Sind bei den Tests mögliche Schwierigkeiten mit einem bestimmten Patch aufgetaucht, so kann die Verteilung zunächst für eine kleine Gruppe von Clients erfolgen und eine weitere Verteilung erst freigegeben werden, wenn auf den ersten gepatchten PCs keinerlei Probleme auftreten.

Basierend auf dem Netzwerkbestand können PCs Gruppen zugeordnet werden, die zu unterschiedlichen Zeiten die Patches erhalten sollen. Auch wenn die angreifbarsten Rechner die kritischsten Patches als erste erhalten sollten, können die Umstände in der Praxis eine andere Vorgehensweise erfordern. Wichtig ist es, unnötige Verzögerungen bei der Verteilung von Patches zu verhindern. Die eigentliche Verteilung sollte zeitnah nach Abschluss der Planungsphase beginnen.

Einschränkungen in der Infrastruktur können eine Rolle bei der Patchverteilung spielen; die Verteilung von Patches über das Netzwerk kann die Infrastruktur stark belasten. Steht nur eine begrenzte Bandbreite zur Verfügung, muss eine Verteilung der Patches eventuell außerhalb der Geschäftszeiten eingeplant werden. Auf Rechnern, bei denen es wenig freien Festplattenspeicherplatz gibt, ist vorher eine Festplattenbereinigung angezeigt, um Speicherplatz freizugeben.

Wurde eine Zeitplanung ausgearbeitet, ist es an der Zeit, die Anwender über die geplante Verteilung von Updates zu informieren, insbesondere, wenn die Installation von Patches einen Neustart erfordert oder anderweitig einen kurzzeitigen Ausfall des Systems bedingt. Die Anwender frühzeitig zu informieren, führt auf deren Seite zu einem besseren Verständnis für diese Unannehmlichkeiten. Während der eigentlichen Verteilung kann der Administrator Benutzern sogar die Möglichkeit einräumen, Patchinstallationen oder Neustarts zu verschieben, falls der Rechner gerade in diesem Moment anderweitig benötigt wird.

Das Patchen von Servern im Produktivbetrieb erfordert besondere Sorgfalt. Die Einrichtung eines Wartungsfensters im Vorfeld ist ratsam, um ungeplante Ausfälle im Geschäftsbetrieb zu verhindern. Alle betroffenen Anwender müssen im Vorfeld informiert werden, dass der Server innerhalb des eingerichteten Wartungsfensters nicht zur Verfügung steht. Wenn möglich kann auch ein Ausweichserver eingerichtet werden, um den Ausfall benötigter Dienste und Funktionen abzufangen, falls beim Patchen des Servers Probleme auftauchen.

3.6. Stufe 6: Patchverteilung

Bei der Verteilung kommen alle vorigen Schritte zusammen. Sobald die Zeitplanung feststeht, beginnt die tatsächliche Verteilung der Patches an die PCs im Netzwerk. Die Verteilung besteht jedoch aus mehr Komponenten als dem bloßen Übertragen einer Installationsdatei an die Netzwerkrechner. Auf älteren Systemen ist es unter Umständen sinnvoll, zuerst einen vollständigen Virenscan durchzuführen, vor allem wenn die betreffende Maschine länger nicht

gepatcht wurde. Auf dem System befindliche Schadsoftware wird darauf vom Virenscanner beseitigt, damit die Patchinstallation reibungslos abläuft.

Nach der Verteilung und Verifikation hilft ein abschließender Bericht bei der Bewertung der Wirksamkeit der Patches sowie dem Aufdecken möglicher Schwierigkeiten. Vor der Verteilung von Installationsdateien an die Clients muss also feststehen, welche Aktionen protokolliert und welche gemeldet werden müssen. Theoretisch sollte jede Aktion, die das System beeinflusst, protokolliert werden, um eine spätere Analyse zu ermöglichen. Jede Änderung der Registry und im Dateisystem zu protokollieren ist eine Möglichkeit, dies zu erreichen, allerdings muss darauf geachtet werden, nicht zu viele Daten zu sammeln. Allzu große Datenmengen sind eher hinderlich bei einer schnellen Fehlersuche.

Bevor eine Patchdatei gestartet und installiert wird, ist eine Verifikation der Datei unerlässlich. Hersteller veröffentlichen oft Checksum-Dateien oder Hashes, mit deren Hilfe Administratoren ihre Downloads überprüfen können.

Es gibt Hersteller, die nur Delta-Patches veröffentlichen. Dort sind ausschließlich Änderungen der einzelnen Dateien gegenüber deren Vorgängerversion enthalten. Zwar spart dies Bandbreite und Speicherplatz, allerdings erfordert es auch einen eigenen Patch für jede einzelne Zielversion. Um Zeit beim Erstellen von Patches zu sparen, werden die meisten Produkte vom Hersteller mit vollständigen Patches versorgt, die komplette Versionen der zu aktualisierten Dateien enthalten. Dadurch wird das Patchen von Rechnern vereinfacht, die sonst mit Hilfe mehrerer Dateien gepatcht werden müssten. Die Patchdateien nehmen jedoch im Schnitt deutlich an Größe zu. Dies kann die verfügbare Bandbreite des Netzwerks deutlich belasten. Alle Patches werden einmalig von einem zentralen Patchmanagement-Server heruntergeladen und an alle PCs verteilt, die einen bestimmten Patch benötigen. Um zu verhindern, dass der Verteilvorgang der Patches andere netzwerkbasierte Prozesse stört, sollte die Gesamtnetzwerklast, die durch die Patchverteilung entsteht, begrenzt werden, indem die Verteilung so geplant wird, dass die Netzwerkauslastung nicht allzu groß ist. Zusätzlich kann die Verteilung gestuft erfolgen. Aus Performance- und Kompatibilitätsgründen sollten nicht alle Rechner zur gleichen Zeit gepatcht werden. Zur Lastverteilung können Patches entweder an räumlich im selben Bereich stehende Rechner verteilt werden, sodass nur eine begrenzte Zahl Netzwerkknoten eine Auslastung erfährt, oder an einzelne Clients innerhalb verschiedener Netzwerkbereiche. Selbst wenn die Testphase ohne Probleme beendet wurde, ist es ratsam, Client-PCs in Risikogruppen einzuteilen: so werden Patches zuerst an Standard-Desktop-PCs oder einzelne Server verteilt, bevor man zu komplexeren Systemen übergeht.

Patches müssen nicht unbedingt unmittelbar nach der Verteilung installiert werden. Unter gewissen Voraussetzungen kann es sinnvoll sein, die eigentliche Installation zu verzögern, beispielsweise wenn die Installation während der Geschäftszeiten erfolgen und so die Usability beeinträchtigen würde. In diesem Fall ist eine Startverzögerung der Installation bis zum Herunterfahren oder Neustarten des Systems oder beim Sperren des Bildschirms denkbar. Alternativ ist es auch möglich mit der eingesetzten Patchmanagementlösung die beiden Schritte zu kombinieren und die Verteilung erst dann zu starten, wenn ein Wartungsfenster besteht und die Patches dann auch installiert werden sollen. In ähnlicher Weise sollte der Netzwerkadministrator Neustarts bei der Verteilung und Installation mit einplanen, um die Anwender so wenig wie

möglich zu beeinträchtigen. Die Installation eines Patches und ein erforderlicher Neustart lassen sich auch erzwingen, wenn Sicherheitsüberlegungen hier die Usability überstimmen, jedoch sollte diese Praxis nicht die Norm sein und nur in Ausnahmefällen zur Anwendung kommen. Ein möglicher Mittelweg ist es, dem Anwender die Möglichkeit zu geben, eigenständig die Installation eines Patches zu verzögern, um beispielsweise eine Aufgabe fertig zu stellen, bevor das System neu gestartet wird. Um deutliche Abweichungen einzelner Maschinen vom Patchstand des übrigen Netzwerks zu unterbinden, sollte aber auch diese Möglichkeit eingeschränkt werden (beispielsweise max. einen Tag für die Patchinstallation oder eine Stunde für einen Neustart).

Die Patchverteilung aktiv zu beobachten ist wichtig: Sollte die Installation eines Patches fehlschlagen, kann dies Auswirkung auf die Installation folgender Patches haben, welche eine Abhängigkeit von dem Patch haben, dessen Installation fehlgeschlagen ist. Ein Mangel an verfügbarem Speicherplatz auf der Festplatte eines PCs ist nur ein häufiger Grund unter vielen für das Fehlschlagen von Updates. Die Installationsroutine eines Patches gibt zumeist einen Fehlercode zurück, wenn etwas bei der unbeaufsichtigten Installation schiefgeht. Im Falle eines Fehlers bei der Verteilung ist oft ein manuelles Eingreifen durch den Administrator erforderlich. Aus diesem Grund sollte eine Patchmanagement-Richtlinie auch definieren, wie mit unvorhergesehenen Problemen umzugehen ist und innerhalb welches Zeitraumes dies zu geschehen hat.

3.7. Stufe 7: Verifizierung und Berichterstattung

Obwohl eine datei-basierte Verifizierung bereits während der Verteilung stattfinden sollte, beginnt in dem Moment, in dem ein Patch auf alle betroffenen Rechner verteilt wurde, der Verifizierungs- und Reportingprozess. Die Bewertungsphase direkt nach der Verteilung besteht aus einer formellen Überprüfung, ob alle geplanten Verteilungen stattgefunden haben. Sind während der Verteilung Fehler aufgetreten, sind diese umgehend zu analysieren. Durch das Finden und Analysieren von Fehlern kann der Verteilungsprozess weiter optimiert werden. Einige Fehler haben möglicherweise ihre Ursache in der Hardware bestimmter Rechner, andere Probleme liegen eventuell in Domänenrichtlinien oder Netzwerkproblemen.

Abgesehen von der Analyse von Protokolldateien gibt es noch weitere Wege, das Installationsergebnis der Patches in Erfahrung zu bringen. Wenn die Phase der Inventarisierung ausgeführt worden ist, sollte eine vollständige Softwareinventarisierung bereits vorhanden sein. Durch eine Aktualisierung dieses Inventars und einen Vergleich mit dessen Vorgängerversion ist eine genaue Prüfung möglich, ob das jeweilige Programm tatsächlich auf die gewünschte Version aktualisiert wurde. Kleinere Patches, oder solche ohne richtigen Installer oder ein Versäumnis des Herstellers kann zu irreführender Versionsnummerierung oder dem Fehlen derselben führen. Die jeweiligen Prüfsummen aufzulisten kann hier hilfreich sein, erhöht allerdings die Menge zu sammelnder Daten. Dies wiederum kann zu Verwirrung führen. Sofern technische Dokumentationen in ausreichem Maß vorhanden sind, können diese einen schnellen und einfachen Weg aufzeigen, um die Behebung einer Sicherheitslücke zu verifizieren: Die gezielte testweise „Ausnutzung“ der fraglichen Schwachstelle. Ein Schwachstellenscanner kann gezielt prüfen, ob eine vermeintlich gepatchte Sicherheitslücke wirklich geschlossen wurde.

Es existieren unterschiedliche Wege, Abhilfe zu schaffen, sollte ein Patch nicht korrekt installiert worden sein. Waren mangelnder Speicherplatz auf der Festplatte oder ein Netzwerkproblem die Ursache, wird die Installation des Patches erfolgreich sein, sobald die Netzwerklast reduziert bzw. ausreichend freier Speicherplatz vorhanden ist. Es gibt jedoch auch Kompatibilitätsprobleme mit installierter Software oder auch andere Unwägbarkeiten, die eventuell eine manuelle Installation eines Patches erforderlich machen. Der praktischste Weg, dies zu bewerkstelligen, liegt darin, Fernzugriff auf die betreffende Maschine zu erhalten, um die manuelle Installation anzustoßen.

Für Anwender ist es einfacher, Performance-Engpässe im tatsächlichen täglichen Arbeitsablauf zu lokalisieren als in einer abgekapselten Testumgebung mit genau definierten Bedingungen. Insbesondere auf Clients, deren Software- oder Hardwareausstattung vom Rest der Netzwerkumgebung abweicht, ist das Risiko für Komplikationen größer. Indem der Administrator dem Anwender die Möglichkeit einräumt, Feedback zu Patches zu geben, hat er die Chance, Problemen auf die Spur zu kommen, die er selbst nicht oder nur schwer gefunden hätte. Zwar enthalten die Rückmeldungen der Anwender nicht immer Informationen, die direkte Rückschlüsse auf die Performance eines Patches zulassen, können aber dennoch wertvolle Hinweise in dieser Hinsicht geben.

Ob mit oder ohne Einbeziehung der Rückmeldungen von Anwendern, es sollte immer eine technische Möglichkeit geben, einen Patch wieder rückgängig zu machen. Zwar sollten eventuelle Probleme bereits in der Testphase gefunden und ausgeräumt sein, allerdings gibt es in der Praxis immer wieder Situationen, in denen nach dem Einspielen eines Patches entweder Beeinträchtigungen der Performance eintreten oder bestimmte Funktionen nicht mehr zur Verfügung stehen. In diesem Fall muss der Administrator eine Möglichkeit haben, einen Patch zentral wieder zurückzuziehen.

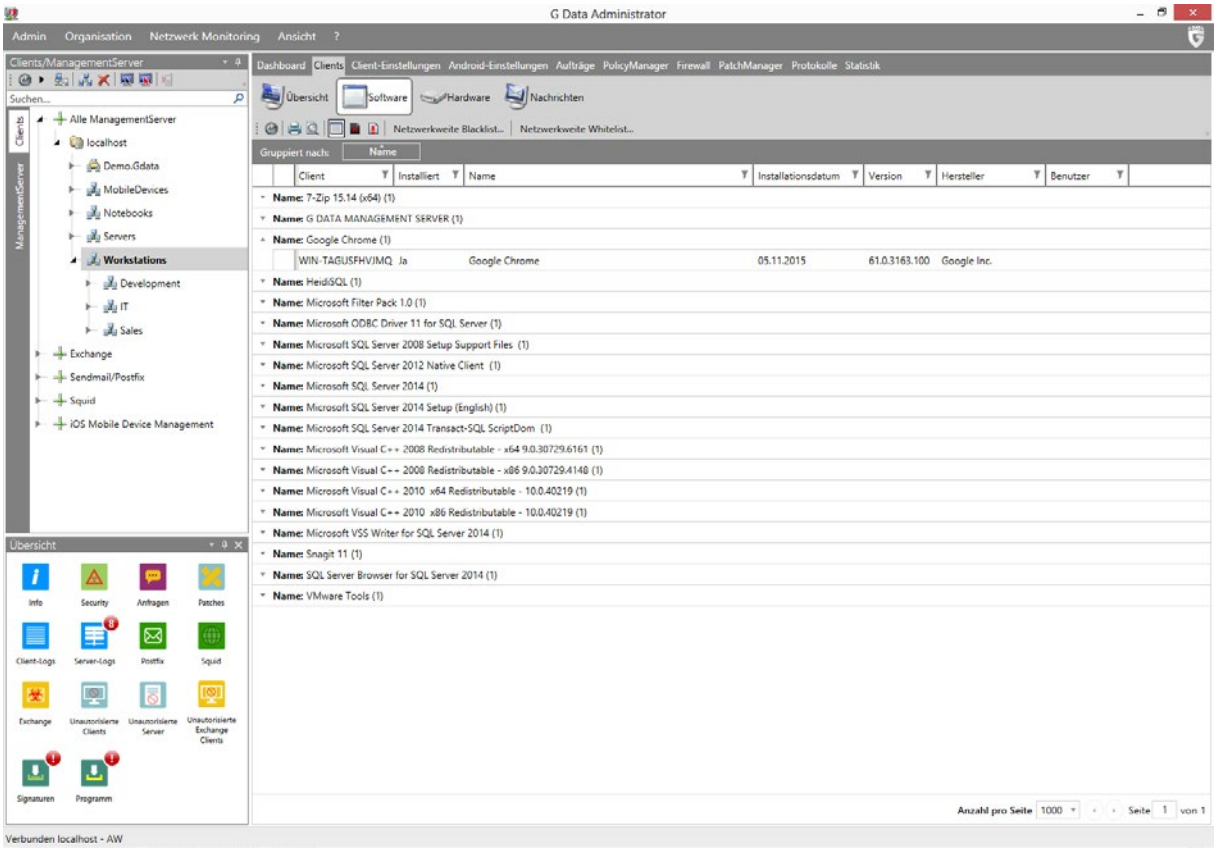
4. G DATA Patch Management

G DATA unterstützt alle Phasen des Patchmanagementzyklus. Manche Funktionalität, wie z. B. die Softwareinventarisierung, ist Teil aller G DATA Businesslösungen. Um das Testen und Verteilen von Patches zu optimieren, bietet G DATA ein optionales Patch Management Modul an, das mit allen Businesslösungen kombiniert werden kann. Es ist komplett mit dem G DATA Administrator integriert und hat die gleichen Systemvoraussetzungen wie der G DATA Management Server. Das G DATA Patch Management unterstützt die Verwendung des Microsoft SQL Server Express, aber für mittelgroße bis große Netzwerke wird der Einsatz einer Standalone-Installation des Microsoft SQL Servers empfohlen.

4.1. Stufe 1: Inventarisierung

Zuerst einmal ist es entscheidend, eine Inventarisierung aller Rechner, ihrer Hardware und darauf installierter Programme durchzuführen. Um die Patchverwaltung zu erleichtern, muss jederzeit bekannt sein, welche Programmversionen derzeit innerhalb des Firmennetzes in Gebrauch sind. G DATA enthält ein schlankes und leicht zu bedienendes Werkzeug für diese Aufgabe in allen Businesslösungen. Das „Clients“-Modul gibt dem Netzwerkadministrator eine vollständige Aufstellung aller installierten Programme für jeden einzelnen Clientcomputer im Netzwerk. In der

Standardübersicht sind Installationsdatum, Hersteller und derzeit installierte Version des jeweiligen Programms aufgelistet. Durch das Auflisten nach der Versionsnummer ist es möglich, schnell herauszufinden, ob die aktuellste Version eines Programms auf allen PCs installiert ist.



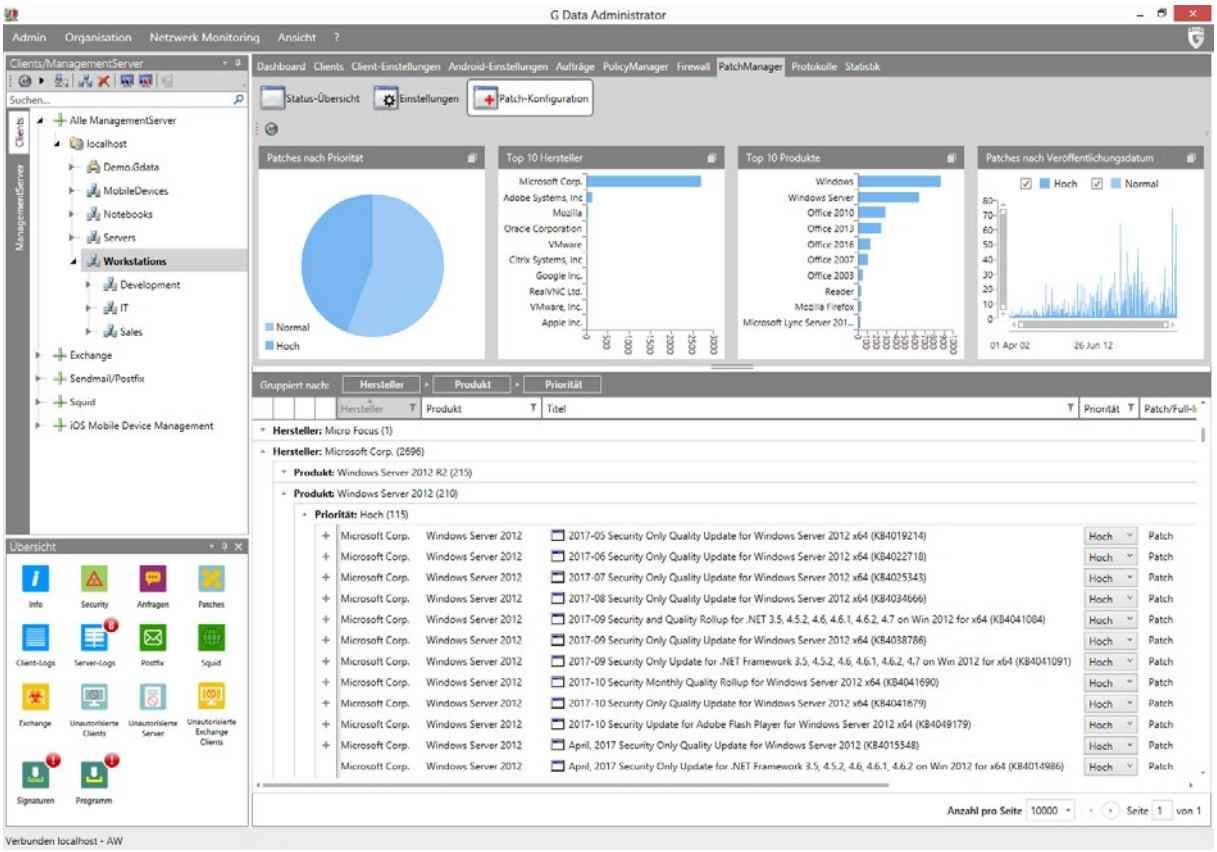
***Figur 6**: G DATA Administrator > Clients > Software*

An diesem Punkt ist es empfehlenswert, die installierten Programme auf Abweichungen von der Standardinstallation im Netzwerk zu prüfen. Als Administrator kann man nicht über jedes potenzielle Sicherheitsproblem bei jeder existierenden Software im Bilde sein. Die Inventarliste hilft dabei, nicht genehmigte Programme im Netzwerk zu finden. Danach kann der Administrator entscheiden, ein Programm auf die Liste der im Firmennetzwerk offiziell zugelassenen Programme zu setzen (Whitelist) oder diese zu entfernen und ihre Ausführung zu blockieren (Blacklist). Nutzer der G DATA Endpoint Protection Business können den darin enthaltenen PolicyManager für diese Aufgabe einsetzen und nötigenfalls netzwerkweite Richtlinien sowie Black- und Whitelisten festlegen, um die Softwareumgebung gezielt zu kontrollieren.

Es ist nicht nur wichtig, über installierte Programme auf dem Laufenden zu sein; die erfolgreiche Verteilung von Patches und Updates ist ebenso von physischen Voraussetzungen abhängig, wie der durch die Verteilung erzeugten Netzwerklast oder der Hardwarekonfiguration der Zielrechner. Letzteres kann mit der Hardwarebestandsauflistung abgefragt werden. Die Abfrage zahlreicher Daten wie Prozessorgeschwindigkeit und Arbeitsspeicher hilft bei der Einschätzung der Verteilungsgeschwindigkeit von Patches und deren Performance. Ebenfalls von Bedeutung kann die Kenntnis des verfügbaren Festplattenspeichers sein, um Fehler bei der Patchverteilung zu verhindern. Zusätzlich können Daten wie BIOS und Mainboard-Firmware erfasst werden, um diese mit aktuellen Versionen zu vergleichen.

4.2. Stufe 2: Informationen sammeln

Sobald die Inventarisierung abgeschlossen ist, ist es die Aufgabe des Administrators, sich über die Verfügbarkeit aktueller Updates und Patches zu informieren und diese Informationen mit seinem Inventar abzugleichen. G DATA Patch Management stellt eine Liste aller zur Verfügung stehenden Patches auf dem „Patch-Konfiguration“-Karteireiter bereit. Dieser Datenbestand wird automatisch aktualisiert sobald ein Hersteller einen neuen Patch veröffentlicht. Die Liste kann gruppiert und sortiert werden, um einen Überblick über wichtige Patches für Software, die für den Administrator relevant ist, zu erhalten. Über die Eigenschaften-Anzeige eines einzelnen Patches können weitere Informationen und oft auch vollständige Release-Notes abgerufen werden.



***Figur 7**: G DATA Administrator > PatchManager > Patch-Konfiguration*

4.3. Stufe 3: Strategie und Planung

Administratoren können einzelne oder mehrere Patches gleichzeitig auf Anwendbarkeit auf spezifischen Systemen prüfen. Dazu wird ein Softwareerkennungsauftrag für den/die betroffenen Client(s) angelegt. Alternativ kann das G DATA Patch Management über die Einstellungen auch so konfiguriert werden, dass alle neuen, hoch priorisierten Patches direkt auf Anwendbarkeit überprüft werden. Zuletzt können Sie über den „Aufträge“-Karteireiter auch einen automatischen Software-Erkennungsauftrag einplanen, der immer ausgeführt wird, sobald ein neuer Patch verfügbar ist.

Obwohl Administratoren das Patch Management über die Einstellungen so konfigurieren können, dass wichtige Patches automatisch installiert werden, sollten Patches immer vorher getestet

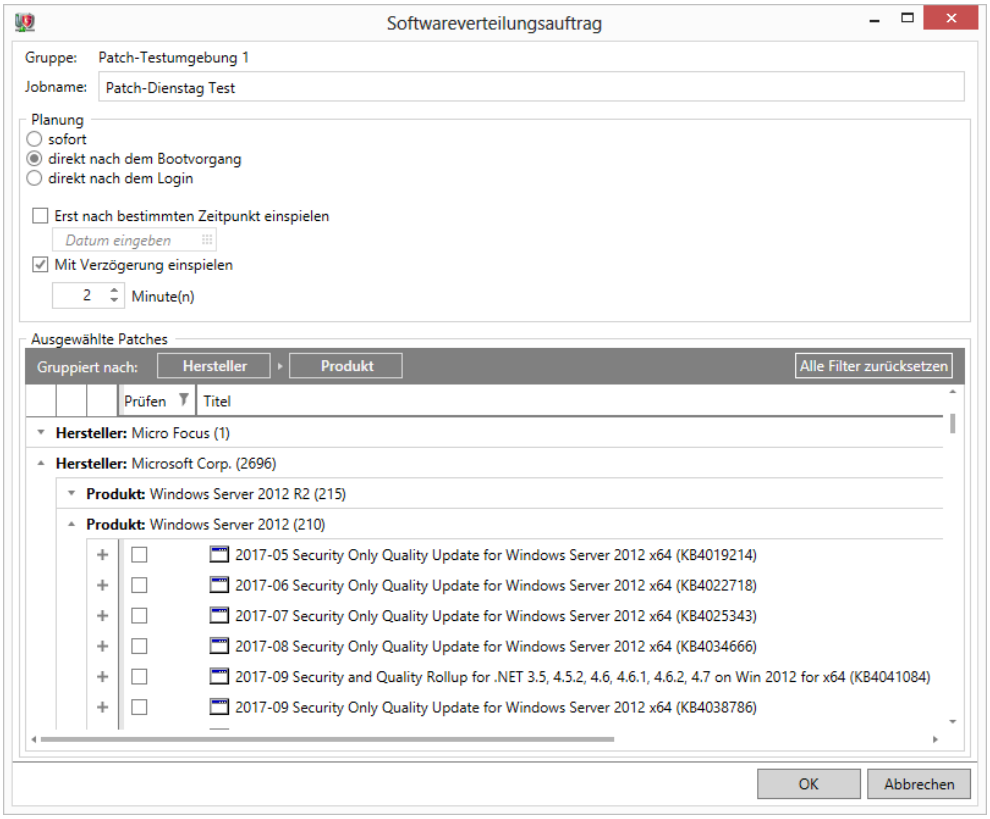
werden. Nach der Prüfung auf Anwendbarkeit wählen Sie die Clients oder Workstations aus, die einen Patch erhalten sollen und öffnen den Karteireiter „Status-Übersicht“ des Patch Managements. Sortieren Sie die einzelnen Einträge nach ihrem Status. Ziel dessen ist es, einen schnellen Überblick zu erlangen, welche Patches anwendbar sind, welche Patches bereits installiert und welche nicht anwendbar sind. Zur Auswahl für eine Installation stehen solche, die als anwendbar gekennzeichnet sind.

Um die Entscheidung, welche Patches verteilt werden sollen, zu erleichtern, stellt das G DATA Patch Management für jeden einzelnen Patch einen Satz an Informationen bereit. In der Ansicht „Patch-Konfiguration“ ist das Produkt aufgeführt, für das der Patch gilt sowie das Veröffentlichungsdatum, offizieller Name und gegebenenfalls die Priorität. Für jeden Patch steht normalerweise auch ein Link bereit, unter dem sich weitere offiziellen Release Notes befinden. Diese Informationen helfen dem Netzwerkadministrator bei der Bewertung der Schwere einer Sicherheitslücke sowie bei der Festlegung eines Zeitrahmens, in dem ein Patch zur Behebung zu installieren ist. Dabei sollten Patches mit einer höheren Priorität schneller installiert werden als solche, die als nicht-kritisch eingestuft sind. Zugleich muss nicht jedes im Netzwerk eingesetzte Programm sofort gepatcht werden – kritische Anwendungen sollten Patches eher erhalten als selten genutzte unkritische Anwendungen. An dieser Stelle wird die zuvor festgelegte Patchmanagementrichtlinie wieder wichtig, in der genau geregelt ist, welche Patches in welcher Reihenfolge zu installieren sind (siehe Abschnitt 2.1).

Entscheidend ist, dass nicht alle Patches immer installiert werden müssen. Sinn und Ziel eines Patchmanagements ist nicht, Entscheidungsprozesse zu vermeiden, sondern Administratoren genügend Material an die Hand zu geben, um eine auf fundierten Informationen basierende Entscheidung zu treffen und die anschließende Verteilung so effizient wie möglich zu gestalten. Das G DATA Patch Management stellt im Rahmen seiner Möglichkeiten diese Informationen zur Verfügung, allerdings liegt die finale Entscheidung für die Verteilung oder Zurückhaltung eines Patches immer beim Netzwerkadministrator.

4.4. Stufe 4: Test

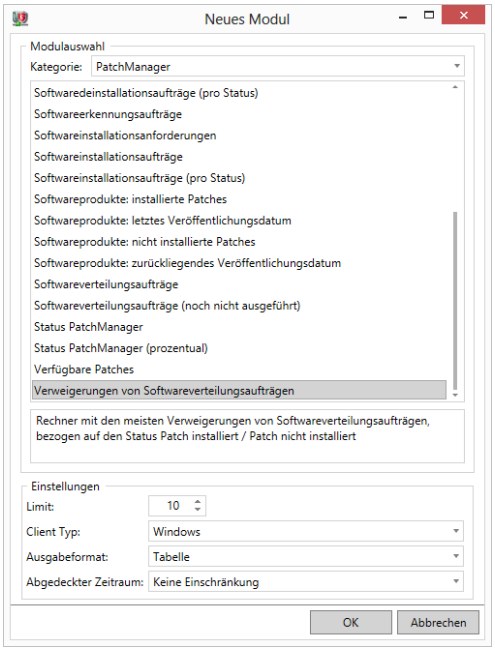
Ist die Entscheidung zur Installation eines Patches gefallen, beginnt die Testphase. Es ist empfehlenswert, die Tests auf Maschinen vorzunehmen, die die unterschiedlichen Konfigurationen, die im Netzwerk auftauchen, so gut wie möglich repräsentieren. So können mögliche Schwierigkeiten so gut wie möglich im Vorfeld abgefangen werden, ohne den Produktivbetrieb zu stören. Dabei stehen Netzwerkadministratoren nicht immer ausreichend Geräte zur Verfügung, um das Netzwerk im kleinen Maßstab nachbilden zu können. Virtualisierung ist ein empfohlenes Hilfsmittel hierfür. Sollte es keine anderen Alternativen geben, ist der Test auch in einem kleinen nicht kritischen Teil des Netzwerks denkbar. Wie auch die Entscheidung ausfällt: mit dem G DATA Administrator ist das Anlegen verschiedener Testgruppen möglich. Das G DATA Patch Management kann Patches an einen oder mehrere Clients in einer oder mehreren Gruppen verteilen, um so das Installationsverhalten eines Patches beobachten und bewerten zu können (siehe Abschnitt 3.4 für weitergehende Informationen zu Maschinen, die in eine Testumgebung aufgenommen werden sollten).



***Figur 8**: G DATA Administrator, Aufträge, Softwareverteilungsauftrag (Test)*

Um einen oder mehrere Patches in einer Testgruppe zu verteilen, wählen Sie zunächst die Gruppe in der Clientverwaltung aus. Öffnen Sie den Karteireiter „Aufträge“ und legen einen neuen Softwareverteilungsauftrag an. Wählen Sie die zu installierenden Patches sowie die Zeit, zu der diese verteilt werden sollen. Sie können die Auswahl der Patches vereinfachen, indem Sie sie zum Beispiel nach Hersteller oder Produktnamen sortieren. Wiederholen Sie diese Schritte für alle zu installierenden Patches für alle Gruppen, die die Patches erhalten sollen. Um eventuelle Probleme mit einem bestimmten Patch besser eingrenzen und zurückverfolgen zu können, empfiehlt es sich, jeweils nur einen einzelnen Patch pro System gleichzeitig zu installieren. Unter PatchManager > Status-Übersicht kann der jeweilige Status für die Patches überprüft werden.

Sowohl während der Test- als auch der Verifikationsphase nach der Verteilung im Netz bietet der ReportManager Statistiken über die Verteilung sowie über Rechner, die Fehlermeldungen verursachen. Interessant sind vor allem Berichte über die Patches, die am häufigsten nicht installiert wurden, sowie über Rechner mit unbearbeiteten Softwareverteilungsaufträgen (was beispielsweise auf Installationsprobleme beim Client hindeuten könnte) und über Rechner mit den häufigsten Patch-Anfragen oder –Ablehnungen.



***Figur 9**: G DATA Administrator > ReportManager > Neues Modul*

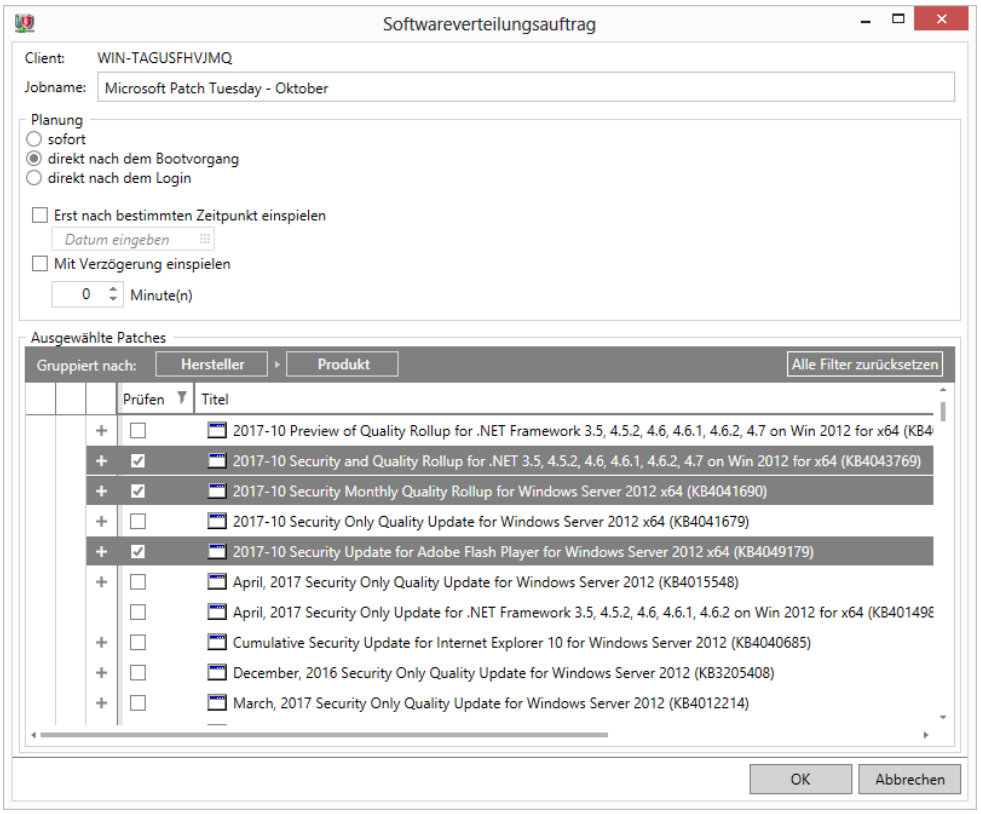
Zusätzlich zu den im Patch Management und ReportManager zur Verfügung stehenden Optionen kann der aktuelle Stand des Patch-Tests auch direkt unter „Aufträge“ abgefragt werden; öffnen Sie dazu den jeweiligen Auftrag und prüfen Sie die Details des jeweiligen Patches. Stellt sich heraus, dass ein Patch nicht erfolgreich verteilt wurde, aktualisieren Sie einmal das Softwareinventar und prüfen Sie die installierte Version. Schlägt die Verteilung des Patches fehl, prüfen Sie das System einmal lokal und versuchen, den fraglichen Patch lokal zu installieren. Generell gilt: Verursacht ein Patch beim Testen Probleme, sollte er nicht automatisiert auf breiter Front verteilt werden.

4.5. Stufe 5: Ablaufplanung und Bewertung

Nach Abschluss der Testphase ist es an der Zeit, die Verteilung zu terminieren. Sind alle zu verteilenden Patches ausreichend getestet, kann eine Zeitplanung erfolgen. Ziehen Sie die im Vorfeld festgelegte Patchrichtlinie zurate, um festzulegen, in welcher Reihenfolge welche Patches an welche Maschinen zuerst ausgeliefert werden sollen. Nutzen Sie auch die „Nachrichten“-Funktion (auf dem „Client“–Karteireiter) um Benutzer auf die bevorstehenden Updates hinzuweisen und eventuell erforderliche Neustarts anzukündigen.

4.6. Stufe 6: Patchverteilung

Steht die Zeitplanung fest, kann für fertig getestete Patches mit der Verteilung begonnen werden. Nutzen Sie den Karteireiter „Aufträge“, um einen Softwareverteilungsauftrag mit den entsprechenden Patches für die betroffenen Clients zu erstellen. Um die Arbeitsabläufe der Anwender nicht zu stören, ist eine Planung der Verteilung für eine bestimmte Zeit möglich, ebenso kann die Verteilung für den kommenden Systemstart oder die nächste Benutzeranmeldung geplant werden. Optional kann auch eine Verzögerung mit eingebaut werden, die die Verteilung während anderer ressourcenintensiver Arbeit verhindert.



***Figur 10**: G DATA Administrator > Aufträge > Softwareverteilungsauftrag (Verteilung)*

4.7. Stufe 7: Verifizierung und Berichterstattung

Um die Verteilung der Patches zu verifizieren und bewerten zu können, ist das Inventarisierungstool eine entscheidende Hilfe. Zusätzlich bietet das G DATA Patch Management Usern die Möglichkeit, eine direkte Rückmeldung zu geben. Ist die entsprechende Option aktiviert, kann ein Anwender auch das Zurückziehen eines Patches anfordern. Patches, die zwar anwendbar, aber nicht für die Verteilung geplant sind, können vom Anwender direkt angefordert werden, falls ein schnelles Patchen erforderlich ist. Die Verteilung und das Zurückziehen von Patches ist direkt im Patch Management integriert und ermöglicht es Netzwerkadministratoren, aus dem ReportManager heraus direkt die Planung der Verteilung oder das Zurückziehen eines Patches vorzunehmen. Führen wir uns folgendes Beispiel vor Augen: Ein Anwender kann Anwendung A nicht mehr verwenden und wartet auf die Verteilung eines Patches. Während der Patch getestet wird, stellt der Netzwerkadministrator fest, dass der Patch mit Anwendung B nicht kompatibel ist und entscheidet daraufhin, dass der Patch nicht verteilt wird. Der Anwender nutzt jedoch die inkompatible Anwendung B nicht und besteht auf die Installation des Patches. Der Anwender kann die Installation dieses Patches über das G DATA Patch Management gezielt anfordern. Wurde die Anfrage für den Patch freigegeben, erfolgt die Verteilung auf regulärem Weg.