Next-Generation Patch-Management

Remediation, der Systemsanierer für ein sicheres Netzwerk

Nachrichten über Schadsoftware, Sicherheitslücken und neue Angriffsarten sind mittlerweile ein alltäglicher Bestandteil unserer digitalen Welt. Der Schutz des eigenen (Firmen-)Netzes ist vor diesem Hintergrund sowohl für Unternehmen als auch für Behörden eine Herausforderung, die aber durch Patch-Management-Systeme scheinbar gut handhabbar ist. Auch „Network Access Control"-Lösungen (NAC) bieten durch die sogenannte „Remediation" die Möglichkeit, Systeme automatisch in einen aktuellen Zustand zu bringen und zu halten. Macht also der Einsatz von Patch-Management-Lösungen den Einsatz von NAC beziehungsweise umgekehrt der Einsatz von NAC die Verwendung von Patch-Management-Lösungen unnötig? Oder ergänzen sich Patch-Management und Network Access Control?

In einer perfekten Welt gäbe es keine Schadsoftware, keine Viren, Würmer, trojanischen Pferde und der Gleichen. Nun wissen wir dass die Welt nicht perfekt ist und dass Schadsoftware eine erhebliche Bedrohung für Unternehmenswerte darstellt. Schadsoftware nutzt Schwachstellen in Applikationen und Betriebssystemen um in Rechnersysteme einzudringen beziehungsweise Schaden anzurichten. Sobald solche Schwachstellen in Programmen entdeckt werden, wird in der Regel in kurzer Zeit ein Patch veröffentlicht, der das Problem löst. Diese Patches müssen dann durch den Netzbetreiber möglichst schnell – im besten Fall automatisiert – an alle betroffenen Rechnersysteme verteilt werden. Nur so kann der Zeitraum für erfolgreiche Angriffe auf bekannte Schwachstellen (Window of Vulnerability) auf ein Minimum begrenzt werden. Genau an dieser Stelle kommen Patch-Management-Systeme zum Einsatz, die den Patch Prozess automatisieren. Die am Markt existierenden Patch-Management-Lösungen erfüllen allgemein die folgenden Funktionen:

- Zentrales Management
- Überwachung der Rechnersysteme
- Überwachung der Veröffentlichung von Patches
- Testen der Patches
- Automatisierte Patch Verteilung
- Automatisierte Patch Anwendung
- Erstellen von Berichten

Beim Einsatz eines Patch-Management-Systems wird der „Patch-Status" der angeschlossenen Rechnersysteme im Netzwerk permanent durch das System dargestellt. Die Überprüfung der Systeme und das Einspielen der Patches können prinzipiell zu beliebigen Zeitpunkten geschehen. Für einen größeren Funktionsumfang, wie zum Beispiel Softwareverteilung und entfernte Konfiguration, existieren weitere Systeme, die auf dem gleichen Prinzip basieren. Teilweise werden diese Funktionen in ein Gesamtsystem gebündelt, was den Aufwand des Administrators für das Aktualisieren und Konfigurieren der Rechnersysteme im Netzwerk weiter verringert und die Sicherheit weiter erhöht.

Grenzen erreicht ein Patch-Management-System allerdings sobald Rechnersysteme geprüft und gepatched werden sollen, die nicht beziehungsweise nicht durchgehend unter der administrativen Kontrolle des Netzwerkadministrators liegen – zum Beispiel Rechnersysteme von Außendienstmitarbeitern, Gästen oder Fremddienstleistern. Dabei besitzen die Rechnersysteme der letztgenannten zwei Gruppen wohl das größte Gefahrenpotenzial, da Sie bisher nicht „einschätzbar" sind. Ein weiterer Schwachpunkt von Patch-Management-Systemen besteht bei der Anwendung von Patches. Diese werden nicht immer automatisch zu einem festgelegten Zeitpunkt eingespielt. Um den Nutzer nicht zu den falschen Zeitpunkten bei der Arbeit zu behindern, bieten manche Systeme auf Benutzerwunsch eine Verschiebung. Es ist somit nicht sichergestellt, dass die Patches so schnell wie möglich angewendet werden. Weiterhin müssen die zu patchenden Systeme bereits am Netzwerk angemeldet sein, um Patches und entsprechende Anweisungen zu erhalten. Daraus folgt, dass Rechnersysteme sich für einen gewissen Zeitraum mit einem unzureichenden Patch-Level im Produktivnetzwerk befinden. Um das Risiko eines Schadens zu minimieren wäre es allerdings nötig, unzureichende Systeme von vornherein aus dem Netzwerk auszuschließen beziehungsweise in speziellen Netzwerken zu isolieren. Ein gutes Beispiel hierfür ist ein Außendienstmitarbeiter, dessen Notebook möglicherweise tagelang nicht mehr am eigenen Netzwerk angemeldet war. Dadurch kann sein Rechner einen so alten Patch-Level besitzen, dass es nicht mehr vertretbar wäre, ihm Zugriff auf das Netzwerk zu gewähren.

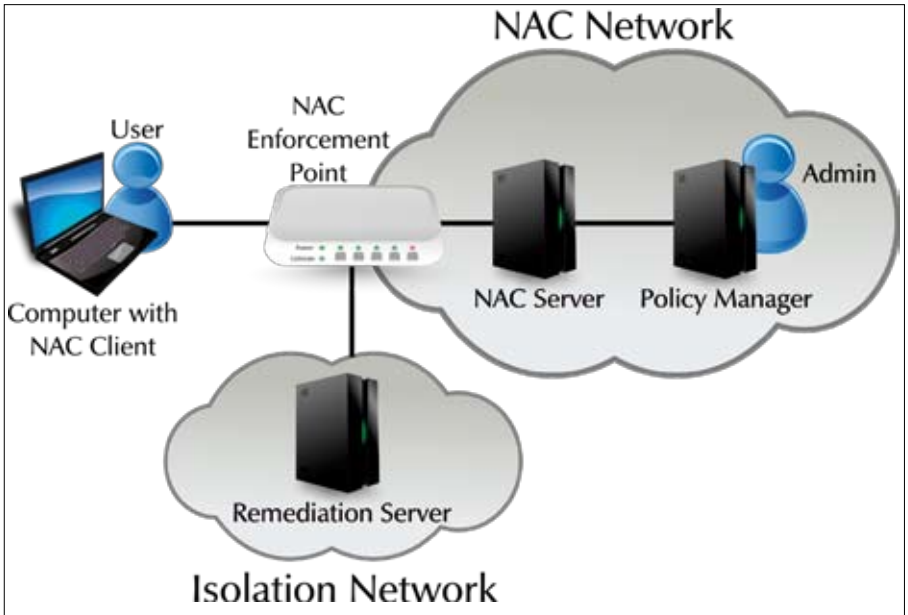
Network Access Control – Ein Türsteher für Netzwerke

Ein bereits vielfach eingesetzter und erfolgversprechender Ansatz für ein umfassendes Konfigurations- und Sicherheitsmanagement für Netzwerke ist Network Access Control (NAC) (Abbildung 1). Die Grundidee von NAC-Systemen ist es, den Netzwerkzugriff von Rechnersystemen von deren aktuellem Zustand abhängig zu machen. Bevor einem Gerät der Zugriff auf das Produktivnetzwerk gewährt wird, wird die Konfiguration auf die Einhaltung der geltenden Sicherheitsrichtlinien überprüft. Die Prüfung wird je nach NAC-Lösung entweder von den Komponenten selbst – die Unterstützung des Herstellers vorausgesetzt – oder von einem separaten Softwareclient durchgeführt. Denkbare Richtlinien sind zum Beispiel ein aktueller Patch-Level des Betriebssystems, eine aktivierte Personal-Firewall oder ein aktueller Virenscanner. Sollte ein Rechnersystem nicht richtlinienkonform sein, wird es als potentiell gefährlich eingestuft und der Netzzugriff verweigert beziehungsweise das System in einem speziellen Netzbereich isoliert. Von der Prüfung und Isolierung sind sowohl interne als auch externe Rechnersysteme – die beispielsweise einen Netzzugriff per VPN herstellen – betroffen. Damit einem isolierten System dennoch Zugriff auf das Netzwerk gewährt werden kann, erhält es im Isolationsnetzwerk die Möglichkeit sich in einen richtlinienkonformen Zustand zu bringen. Diesen Vorgang, der auch automatisiert durchgeführt werden kann, nennt man Remediation.

Mit Remediation in eine sichere Welt

Die deutschen Entsprechungen für den Begriff "Remediation" im Sinne eines NAC-Systems sind Sanierung, Mängelbeseitigung und Nachbesserung. Die Absicht der Remediation ist es Konfigurationsänderungen, Aktualisierungen, Installationen und gegebenenfalls Löschungen von Software auf einem Rechnersystem vorzunehmen, um es in einen zu den aktuellen Netzwerkrichtlinien konformen Zustand zu bringen. Hierbei spielt es keine Rolle ob das Rechnersystem unter der administrativen Kontrolle des Netzwerkadministrators steht oder ob es sich um ein fremdes System handelt, denn beide werden – sofern kompatibel zur eingesetzten NAC-Lösung – gleichermaßen geprüft und gegebenenfalls nachgebessert bevor sie in ein Netzwerk eintreten dürfen. Die Arbeitsweise ist daher mit einem Patch-Management-System, Konfigurationsmanagement System oder einem System zur Softwareverteilung vergleichbar. Die Remediation umfasst sämtliche Aspekte, und vereint sie zu einer einzigen Komponente innerhalb einer NAC-Lösung. Die Remediation beginnt damit dass unzureichende Rechnersysteme in ein separates Netzwerk isoliert werden. Während der Prüfungsphase wurden dem NAC Client auf dem Rechnersystem bereits Remediationanweisungen übermittelt, die zum Herstellen eines richtlinienkonformen Zustands ausgeführt werden müssen. Die Anweisungen werden, gegebenenfalls nach einer Genehmigung durch den Benutzer, nacheinander ausgeführt. Dies kann soweit möglich automatisch geschehen. Aufgrund der hohen Komplexität mancher Richtlinien kann es ebenfalls nötig sein, dass der Benutzer entsprechende Anweisungen manuell ausführen muss. In diesem Fall werden dem Benutzer vollständige und möglichst ausführliche Hilfestellungen gegeben. Nachdem alle Remediationanweisungen ausgeführt wurden, initiiert der NAC Client ein Reassessment, also eine erneute Überprüfung des Systems. Dadurch wird verlässlich geprüft, ob die Remediationanweisungen erfolgreich ausgeführt wurden und das Gerät nun keine potentielle Gefahr mehr für das Netzwerk darstellt. Damit ist die Remediation beendet. Sollte das Reassessment erneut zu einer Isolation mit anschließender Remediation führen, wird der Vorgang wiederholt. Die Anzahl der möglichen Reassessments ist grundsätzlich nicht beschränkt. Hier muss individuell für jedes Netzwerk ein sinnvolles Verfahren gefunden werden, um die Produktivität der Endgeräte und ihrer Benutzer nicht negativ zu beeinträchtigen.

Der Einsatz von NAC-Lösungen mit einer Remediation kann also die Sicherheit eines Netzwerkes stark erhöhen. Allerdings wirft der Einsatz auch einige Fragen auf und birgt weitere Herausforderungen. Besonders viele Fragen wirft die Remediation bei der Anwendung auf fremden Rechnersystemen auf. Zunächst muss sich der Anwender fragen, ob er als Fremdbenutzer einem anderen Netzwerk überhaupt vertrauen kann. Aus der Antwort auf diese Frage kann dann abgeleitet werden inwieweit das Rechnersystem überprüft und entsprechend der geltenden Richtlinien verändert werden darf. Sollte das Netzwerk nicht vertrauenswürdig sein, kann auch den Änderungen durch das Netzwerk, beziehungsweise dessen Remediationanweisungen nicht vertraut werden. Weiterhin muss betrachtet werden inwieweit fremden Systemen eine



Ein bereits vielfach eingesetzter und erfolgversprechender Ansatz für ein umfassendes Konfigurations- und Sicherheitsmanagement für Netzwerke ist Network Access Control (NAC).

Vorgabe aufgezwungen werden kann, wie zum Beispiel die Nutzung eines speziellen Virenscanners. Nachdem beim Zugriff auf ein Netzwerk Änderungen am System vorgenommen wurden, wäre des Weiteren eine Rollback Funktion hilfreich um das System in seinen eigentlichen Ausgangszustand zurück zu versetzen. Bei so umfassenden Sicherheitskonzepten wie sie NAC-Lösungen bieten, muss man sich darüber hinaus die Frage nach einer Standardisierung stellen. Aktuelle NAC-Lösungen sind nicht vollständig zueinander kompatibel. Die Bemühungen der Trusted Computing Group (TCG) mit der Trusted Network Connect-Spezifikation (TNC) einen herstellerübergreifenden Industriestandard zu entwickeln sind noch nicht abgeschlossen. Positiv ist, dass die Mitglieder der TCG schon heute beginnen ihre NAC-Lösungen TNC-kompatibel zu gestalten, sodass in Zukunft eine vollständige herstellerübergreifende Interoperabilität zwischen unterschiedlichen Komponenten eines NAC-Systems möglich werden kann.

Patch-Management vs. NAC – Wer bietet mehr?

Die Remediation leistet also ähnliches wie ein Patch-Management-System. Sie sorgt dafür, dass alle geprüften Komponenten den Sicherheitsrichtlinien des Netzwerks entsprechen. Allerdings ist die Remediation umfassender und flexibler als stand alone Patch-Management-Lösungen. Neben Patches können auch beliebige andere Änderungen an Endgeräten durchgeführt werden, wie das Konfigurieren und gegebenenfalls Löschen von bereits vorhandener Software. Außerdem funktioniert sie für alle Rechnersysteme die sich mit dem Netzwerk verbinden wollen, auch für fremde NAC-kompatible Systeme. Eingangs wurde die Frage gestellt, ob die Remediation ein Patch-Management obsolet macht, oder ob beide kombiniert werden können. Die Remediation besteht aus der Mitteilung der Remediation-Anweisungen und der Anwendung dieser Anweisungen. Die Anwendung der Anweisungen kann entweder durch die betroffenen Komponenten selbst über die eingebauten Update-Routinen durchgeführt werden oder durch eine übergeordnete Instanz; also auch einem Patch-Management-System.

Die Verwendung eines Patch-Management-Systems als ausführende Instanz bringt dabei einen entscheidenden Vorteil mit sich. Rechnersysteme können nach der erfolgreichen Prüfung und Anmeldung am Netzwerk fortlaufend auf einem aktuellen Stand gehalten werden. Dadurch wird die Wahrscheinlichkeit einer Isolierung bei erneuter Messung auf ein Minimum reduziert. Zusätzlich entfällt eine Implementierung der fortlaufenden Aktualisierung seitens der NAC-Lösung.

Damit aber die Kombination beider Ansätze erfolgreich ist, muss in Zukunft noch ein Problem gelöst werden. Es fehlen Standards zur herstellerübergreifenden Anbindung unterschiedlicher Patch-Management-Systeme.

Aus der Forschung: tNAC – Trusted Network Access Control

Der Prozess der Remediation ist Bestandteil aktueller Forschung. Am Institut für Internet-Sicherheit der FH Gelsenkirchen wird derzeit in Kooperation mit der FH Hannover im Rahmen des tNAC-Projekts (http://www.tnac-project.org) eine vertrauenswürdige NAC-Lösung entwickelt. Ziel des tNAC-Projekts ist die Realisierung einer sicheren und vertrauenswürdigen NAC-Lösung basierend auf der Turaya Sicherheitsplattform und der Trusted Network Connect-Spezifikation. Eine besondere Herausforderung an die Remediation im tNAC-Projekt stellt die Sicherheitsplattform dar. Diese schützt Applikationen durch eine strikte Prozessisolierung um Manipulationen zu verhindern. Durch diese Trennung sind gesicherte Applikationen vor dem Zugriff anderer Applikationen geschützt, das heißt, dass also auch kein Patch-Client, welcher die Applikation gegebenenfalls aktualisieren soll, Zugriff erhält. Von daher müssen die unzureichenden Applikationen die Ausführung der Remediationanweisungen selbstständig vornehmen. Eine weitere Herausforderung der im tNAC-Projekt nachgegangen wird, ist die genaue Spezifizierung des Remediation Prozesses. Dieser wird in der TNC-Spezifikation nur grob skizziert und bedarf, insbesondere in Bezug auf die besonderen Gegebenheiten einer Sicherheitsplattform, einer detaillierteren Definition.

Fazit

Patch-Management-Systeme helfen dem Netzwerkadministrator dabei die Rechnersysteme unter seiner Aufsicht ständig aktuell zu halten und damit das Netzwerk zu schützen. Durch die Verwendung einer NAC-Lösung kann die Sicherheit und Integrität des Netzwerkes weiter erhöht werden. Innerhalb einer NAC-Lösung sorgt die Remediation dafür, dass die Netzwerkrichtlinien von allen Systemen erfüllt werden. Aufgrund der sich überschneidenden Aufgabenstellungen kann zur Durchführung der Remediation auch auf ein Patch-Management-System zurückgegriffen werden. ■

Prof. Dr. Norbert Pohlmann
Informatikprofessor für Verteilte Systeme und Informationssicherheit, Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen

Maximilian Stein ist Mitarbeiter des Instituts für Internet-Sicherheit im Forschungsschwerpunkt Trusted Computing

Marian Jungbauer ist Mitarbeiter des Instituts für Internet-Sicherheit im Forschungsschwerpunkt Trusted Computing