ACMP by Aagon

# WARUM SCHWACHSTELLEN- UND PATCHMANAGEMENT ZUSAMMENGEHÖREN


Stand 2020

www.aagon.de

# Copyright


Soest, März 2020.

# Warum Schwachstellen- und Patchmanagement zusammengehören

Schwachstellenanalyse bzw. Schwachstellenmanagement (Vulnerability Analysis/Management) und Patchmanagement sind essentielle Bestandteile einer jeden IT-Sicherheitsarchitektur. Sie erlauben es, Sicherheitslücken proaktiv zu schließen, sobald diese bekannt werden und Maßnahmenvorschläge zur Vermeidung vorliegen.

Miteinander integriert und eingebettet in einen ganzheitlichen Ansatz für Client Management können sie ihre Wirkung und Effizienz deutlich verbessern. Das ist besonders für den Mittelstand von enormer Wichtigkeit.

In diesem Whitepaper erfahren Sie, ....

- was Schwachstellen- und Patchmanagement sind
- welche Vorteile sie im Zusammenspiel mit anderen Komponenten des Client Managements haben
- und warum sie insbesondere im Mittelstand zusammen gedacht und umgesetzt werden sollten.

Zudem werden wir den Ablauf einer typischen Session im integrierten Schwachstellen- und Patchmanagement durchspielen und über die wesentlichen Grundlagen und Standards aufklären.

# Was ist Schwachstellenmanagement?

Mit Schwachstellenmanagement im engeren Sinne bezeichnet man den Abgleich der gesamten IT-Infrastruktur – Hardware und Software von Clients, Server, Netzwerkkomponenten usw. – mit Datenbanken über bereits bekannte Schwachstellen und die Planung von Maßnahmen, um diese zu beheben.

Zentrales Mittel sind dabei die in Form von zwei Industriestandards (CVE und CVSS) bereitgestellten Datenbanken für bekannte Schwachstellen und ihre Kritikalität, die kontinuierlich von Herstellern und anerkannten Experten aktualisiert werden.

Da sich sowohl die IT-Infrastruktur stetig verändert, der Kenntnisstand über Schwachstellen kontinuierlich wächst und immer wieder neue Angriffsmuster entwickelt werden, muss das Schwachstellenmanagement kontinuierlich als ständiger und in der Regel auch weitgehend automatisierter Prozess durchgeführt werden.

## HINTERGRUND

Der Common Vulnerabilities and Exposures (CVE) Industriestandard sorgt für eine einheitliche Namenskonvention für Schwachstellen. Damit wird der Austausch von Informationen zwischen den Datenbanken der verschiedenen Hersteller vereinfacht.

Das Common Vulnerability Scoring System (CVSS) ist ein Industriestandard zur Bewertung des Schweregrads von Schwachstellen, der von zahlreichen Herstellern unterstützt wird. Im CVSS werden Schwachstellen nach verschiedenen Kriterien bewertet und miteinander verglichen. Ziel ist die Möglichkeit zur Priorisierung bei der Behebung.

# Professionelles Patchmanagement mit ACMP

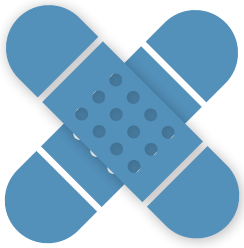
Mit unserer Client-Management-Suite ACMP automatisieren Sie Ihr Patchmanagement, soweit dies sinnvoll ist: Anstehende Aktualisierungen stehen Ihnen gesammelt über die Package Cloud zur Verfügung und können zu einem vorgegebenen Zeitpunkt automatisch installiert werden. Die Steuerung des Rollouts erfolgt zentral über ACMP.

## Die Vorteile für Sie auf einen Blick:

- übersichtliches Dashboard inklusive Drilldown-Möglichkeit
- detaillierte Clientansicht
- integriertes Schwachstellenmanagement, keine Lösung „von außen“
- CVSS- und CVE-basierte Handlungsempfehlungen
- zukunftssicherer Ansatz
- flexible Reportmöglichkeiten
- direkte Reaktion, proaktives Handeln

**Mehr Informationen zum ACMP Schwachstellenmanagement finden Sie hier:**
**http://aagon.de/l/wpschwachstellen**

# Was ist Patchmanagement?



Software-Programme sind schon lange keine statischen Produkte mehr: Heutzutage erscheinen praktisch täglich neue Updates, Patches und Aktualisierungen, die Sicherheitslücken schließen und Funktionen verbessern. Das stellt die IT vor drängende Fragen: Wissen Sie genau, welche Patches für Ihre Systeme vorhanden sind, welche bereits aufgespielt wurden und welche noch fehlen?
Die genaue Kenntnis des Patch-Status ist Voraussetzung für die Vermeidung kritischer Sicherheitslücken, von Kompatibilitätsproblemen zwischen Programmversionen, fehlender Standardisierung und letztlich auch höherem Arbeitsaufwand für den Support.

## Machen Sie den Anwender nicht zum Admin!

Dieses Problem dürfen Sie nicht dem Anwender überlassen. Dazu müssten Sie nicht nur Ihren Nutzern lokale Admin-Rechte geben, Sie müssten auch darauf vertrauen, dass Ihre Nutzer alle Updates selbstständig bemerken und auch immer zeitnah installieren. Beides wird nicht funktionieren.

Die Lösung ist ein strukturiertes, weitgehend automatisiertes Patchmanagement.
Es umfasst die geplante Einspielung von Systemaktualisierungen zur Vermeidung von Sicherheitslücken und Behebung von Fehlern. Dazu wird die Verfügbarkeit von Patches automatisiert überwacht und verfügbare Patches werden auf ihre Kompatibilität mit anderen Software-Anwendungen hin getestet.

Als zweite zentrale Aufgabe ist die Verteilung von Patches auf Clients und Servern innerhalb des Netzwerks sinnvoll zu planen und die oft sicherheitsrelevante Systemaktualisierung zu koordinieren und zu standardisieren. Durch Standardisierung und Automatisierung werden Geschwindigkeit und Effizienz, mit der neue Patches verteilt werden, gesteigert.

## HINTERGRUND:

Man unterscheidet üblicherweise drei Arten von Patches:

- Bugfix: Fehlerbehebung zur Beseitigung von Systemfehlern (Abstürze) und funktionalen Fehlern
- Hotfix: verlangt sofortige Reaktion, da typischerweise Sicherheitslücken geschlossen werden oder Schäden an Daten und Infrastruktur abgewendet werden sollen
- Update: Regelmäßige, geplante Aktualisierungen, die neue Funktionen bereitstellen und oft mit Bugfixes zusammengefasst werden

# Professionelles Patchmanagement mit ACMP

Mit unserer Client-Management-Suite ACMP automatisieren Sie Ihr Patchmanagement, soweit dies sinnvoll ist: Anstehende Aktualisierungen stehen Ihnen gesammelt über die Package Cloud zur Verfügung und können zu einem vorgegebenen Zeitpunkt automatisch installiert werden. Die Steuerung des Rollouts erfolgt zentral über ACMP.

## Die Vorteile für Sie und Ihre IT-Abteilung liegen auf der Hand:

- Sie verhindern frühzeitig Sicherheitsrisiken aufgrund veralteter Software
- Sie erhalten einen einheitlichen Versionsstand auf allen Rechnern
- Sie bekommen weniger Kompatibilitätsprobleme dank standardisierter Softwarestände
- Sie reduzieren den Support-Aufwand und senken Ausfallzeiten

Auch Ihre Mitarbeiter profitieren von professionellem Patchmanagement: Einzelne Anwender brauchen sich nicht länger um anstehende Patches zu kümmern. Updates passieren automatisch im Hintergrund. Die Uhrzeit legen Sie fest: So können Ihre Mitarbeiter ungestört arbeiten.

**Mehr Informationen zum ACMP Patchmanagement finden Sie hier:**
**http://aagon.de/l/wppatch**

# Schwachstellen- und Patchmanagement – wie passt das alles zusammen?

Schwachstellen- und Patchmanagement sind beides Bestandteile des Client Managements. Das Client Management ist die zentrale Verwaltung und Steuerung von Client- und Server-Computern, Thin-Clients und Mobile Devices in einem Unternehmensnetzwerk mit dem Ziel, die Administration durch weitgehende Automatisierung so effizient wie möglich zu gestalten und zusätzlich für die einheitliche, verlässliche Umsetzung von Maßnahmen zu sorgen.

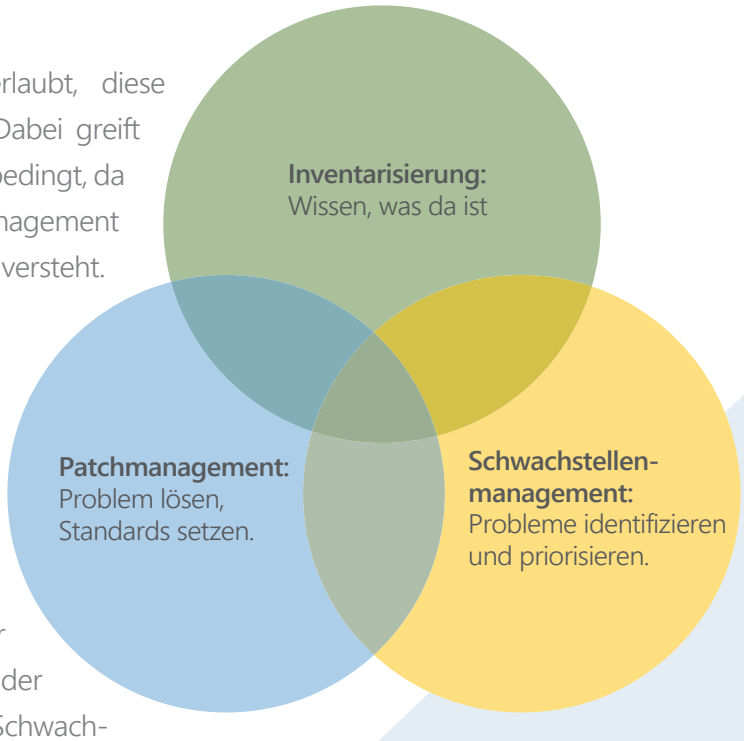
Im Kern ist Client Management also die automatisierte Durchführung von Maßnahmen auf den eingebundenen Clients und Servern. Dabei decken die Aufgaben im Client Management ein breites Spektrum ab: von der Inventarisierung von Hard- und Software über die Verwaltung von Lizenzen, Sach- und Anlagegütern sowie der Paketierung und Verteilung von Software und Betriebssystemen bis hin zum Helpdesk und Ticketing und schließlich Maßnahmen zur IT-Sicherheit wie Patchmanagement und Schwachstellenmanagement.

Zwischen diesen Aufgabengebieten gibt es unterschiedlich enge Beziehungen. Es gibt Module – wie beispielsweise die Inventarisierung –, die Grundlagen für die meisten anderen Aufgaben schaffen oder die – wie das Helpdesk und Ticketing – auf Daten aus allen anderen Aufgabenfeldern zurückgreifen. Andere Module wie das Lizenzmanagement haben nur wenige Berührungspunkte. Eine herausragende Rolle für die IT-Sicherheit spielen dabei die drei Module Inventarisierung, Schwachstellenmanagement und Patch-management. Zwischen ihnen ist das Zusammenspiel besonders wichtig.

Vereinfacht gesagt sorgt die Inventarisierung für vollständige Transparenz über die vorhandenen Systeme und die darauf befindliche Softwarelandschaft. Durch eine gute Inventarisierung weiß man letztlich, was tatsächlich in welchem Zustand vorhanden ist.

Das Schwachstellenmanagement erlaubt es, das, was da ist, mit umfassenden Datenbanken mit bekannten Schwachstellen zu vergleichen – sprich: Am Ende kennt man die vorhandenen Probleme im Detail.

Das Patchmanagement schließlich erlaubt, diese Probleme automatisiert zu beheben. Dabei greift der Begriff Patchmanagement hier nur bedingt, da man im engeren Sinne unter Patchmanagement nur das Einspielen bestimmter Updates versteht.




Wir werden später aber noch sehen, dass für die Behebung von Schwachstellen neben dem Patchen von Software auch andere Aktivitäten wie Konfigurationsänderungen und Ähnliches notwendig sind. In diesem Whitepaper wollen wir aber unter Patchmanagement die Gesamtheit der Maßnahmen zur Beseitigung von Schwachstellen verstehen.

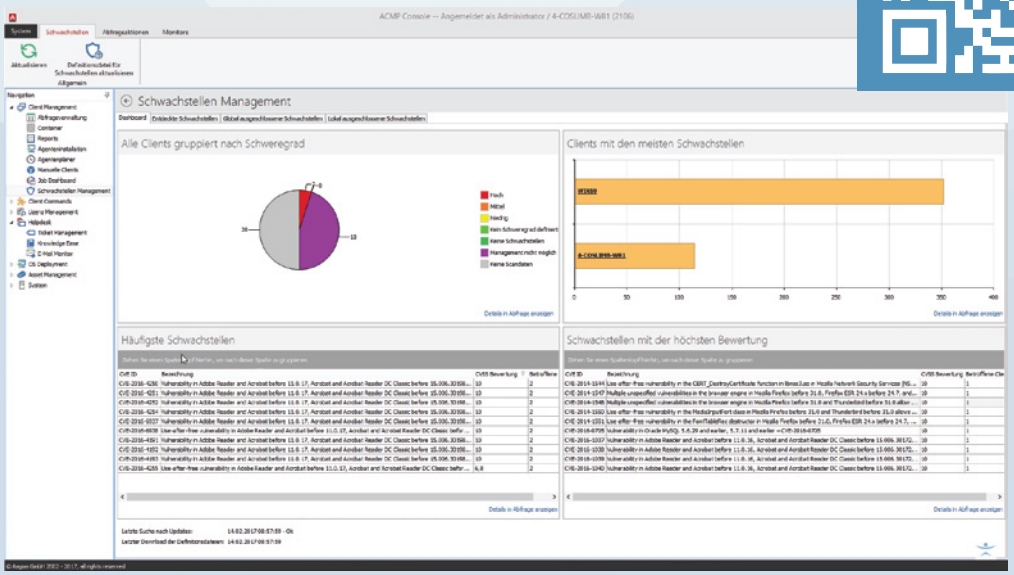
# Wie sieht das in der Praxis aus?

In einer Dashboard-Übersicht hat der Administrator jederzeit einen vollständigen Überblick über die Sicherheitslage aller gescannten Clients. Dabei werden die gefundenen Schwachstellen pro Client nach den international anerkannten und weitverbreiteten CVSS- und CVE-Kategorien dokumentiert, entsprechend priorisiert und zur einfacheren Übersicht zu einem Gesamtrisikowert verdichtet. So können die Schwachstellen schnell nach Dringlichkeit abgearbeitet werden.

Wichtig ist hier die volle Transparenz bis zum einzelnen Client hinab. Gute Lösungen bieten die Möglichkeit, einzelne Schwachstellen für bestimmte Clients oder auch global auszuschließen. Wird beispielsweise auf einem bestimmten Client zwingend eine alte Java-Version benötigt, kann dies entsprechend für die Schwachstellenanalyse vorgemerkt werden. So wird das Analyseergebnis nicht durch bekannte und akzeptierte Ausnahmen unübersichtlich und das Augenmerk wird direkt auf bislang unbekannte Schwachstellen gelenkt.

Ist das Schwachstellenmanagement vollständig in das Client Management integriert, kann die Integration nun ihre volle Stärke ausspielen: Direkt aus dem Schwachstellenmanagement heraus können einzelne oder auch Gruppen von Schwachstellen genauer analysiert und ihre Behebung geplant werden. Für jede Schwachstelle ist hinterlegt, welche Produkte – häufig sind es mehrere zugleich – betroffen sind und wie die Schwachstelle behoben werden kann. Im einfachsten Fall kann die Schwachstelle direkt durch den Push eines Patches auf die betroffenen Clients beseitigt werden.

DEMO-VIDEO
Schauen Sie sich an, wie das konkret in ACMP funktioniert:
https://youtu.be/qwSghN-1yf8



Bei komplexeren Situationen können auch mehrere Schwachstellen einem sogenannten Container zugeordnet werden. Damit kann die Beseitigung der Schwachstellen strukturiert vorbereitet und die automatisierte Umsetzung der Maßnahmen geplant werden. Dem Container werden dann die notwendigen Client Commands für die Beseitigung der Schwachstellen zugeordnet.

Auch hier zeigen sich die Vorteile des integrativen Ansatzes: Zu Beseitigung vieler Schwachstellen ist nicht nur das Einspielen von Patches und Updates notwendig. Oft sind zusätzliche Änderungen beispielsweise an den Registry-Einträgen oder der Firewall-Konfiguration notwendig.

Über das Einspielen von Patches – der Kernfunktion des Patchmanagements – hinaus, können mit den Möglichkeiten zur Desktop Automation in einem integrierten Ansatz auch alle anderen notwendigen Änderungen zur Beseitigung von Schwachstellen automatisiert werden.

## ACMP Client Commands und Desktop Automation:

Ohne große Programmierkenntnisse helfen Client Commands bei der Bewältigung aller administrativen Aufgaben auf Server- und Clientsystemen. Mehr als 170 eigene Client-Command-Befehle, die der Benutzer intuitiv, ganz einfach per Drag & Drop benutzt, bilden das Grundgerüst der Automatisierung. Die native Unterstützung von Skript- und Programmiersprachen wie PowerShell, Visual Basic und Delphi Skript erlaubt die problemlose Integration von bereits bestehenden Programmen direkt in ACMP. Die bidirektionale Variablenübergabe von ACMP Client Commands und den nativen Programmiersprachen ermöglicht sogar eine Mischung der verschiedenen Sprachen. Der vollständig integrierte Formular-Editor rundet das positives Gesamtbild ab.

# Synergien in einem integrierten Ansatz

Im Grundsatz gibt es zwei Denkschulen in der IT, wenn es um die Bewältigung einer zusammenhängenden Menge an Aufgaben geht:

• Best-of-Breed: Man wählt für die Erledigung jeder einzelnen Aufgabe das bestmögliche Spezialwerkzeug aus und versucht, diese Einzellösungen irgendwie zusammenzubringen.
• Integrierte Suite: Alle Aufgaben werden in einer übergreifenden Lösung erledigt, wobei für die einzelnen Aufgaben typischerweise einzelne Module bereitstehen, die jedoch auf eine gemeinsame Basis zurückgreifen.

Je nach Aufgabenstellung und Bereich in der IT wird man sich mal für die eine oder die andere Denkschule entscheiden. Im Folgenden wollen wir darstellen, warum wir davon überzeugt sind, dass im Client Management im Allgemeinen und im Zusammenspiel von Inventarisierung, Schwachstellen- und Patchmanagement für die proaktive IT-Sicherheit im Besonderen, der integrierte Ansatz der bessere ist.

Viele Schwachstellenmanagement-Lösungen im Best-of-Breed-Ansatz benötigen eine eigene Konfiguration und bringen eine ganze Reihe aufwändiger Voraussetzungen mit, an die sich eine IT anpassen muss, um die Lösung in ihrer gesamten Bandbreite einzusetzen.

> Die Qualität der Inventarisierung ist der wichtigste Faktor für den Erfolg von Schwachstellenmanagement und Patchmanagement.

Eigenständige Schwachstellenmanagement-Lösungen bringen wahlweise ihre eigenen Scanner mit oder importieren vorhandene Inventardaten über Schnittstellen – beides ist suboptimal. Im ersten Fall ist zu berücksichtigen, dass Scanning eine invasive und performance-einschränkende Tätigkeit ist, die alle vorhandenen Systeme tangiert. Demnach sind alle zusätzlichen Scan-Komponenten nicht nur ein weiteres Risiko für Sicherheit und Performance, sondern auch mit mitunter erheblichen Administrationsaufwänden behaftet und binden so unnötig dringend gebrauchte Ressourcen. Daher wird jede IT-Organisation die Zahl der Scan-Komponenten und Scan-Läufe minimieren wollen.

Im zweiten Fall gilt, dass jeder Import über Schnittstellen zwischen zwei Softwareprodukten unterschiedlicher Hersteller unwillkürlich mit dem Stille-Post-Syndrom zu kämpfen hat – man versteht sich zwar, aber irgendwas geht immer verloren und nach mehreren Stafetten ist die ursprüngliche Bedeutung nicht mehr nachvollziehbar. Dabei muss es nicht zwingend zu tatsächlichen Datenverlusten kommen. Es reicht, wenn die Semantik und Intention der Daten auf der Strecke bleiben, um den Erfolg der Lösung zu torpedieren.

Die Qualität der Inventarisierung ist der wichtigste Erfolgsfaktor bei der proaktiven Sicherheit. Hier gilt das gute alte Sprichwort „Garbage in, Garbage out!" Werden die vorhandenen Systeme, Softwarestände und Konfigurationen nicht richtig und vollständig er- und gekannt, können weder Schwachstellenmanagement noch Patchmanagement richtig funktionieren.

Zusätzlich spricht für den integrierten Ansatz im Client Management, dass die Scan-Komponente mit jeder zusätzlichen Aufgabe im Client Management immer besser wird. Investitionen in die Scanner-Technologie zahlen sich über mehrere Use-Cases hinweg aus. Innovationen für einzelne Use-Cases befruchten somit auch andere. Ein Beispiel ist die Analyse virtualisierter Systemlandschaften: Die genaue Analyse von Instanzen gängiger Plattformen wie Hyper-V oder VMWare ist in der Erstellung aufwendig und Speziallösungen können geneigt sein, nur das Nötigste für ihren Anwendungsfall zu ermitteln. Integrierte Client-Management-Suiten bringen dagegen sehr viele Daten in einer Datenbank einheitlich und redundanzfrei zusammen. Das bedeutet mehr Synergien und Analysemöglichkeiten. So wird der Scanner einer integrierten Lösung immer ein besseres, weil breiteres Ergebnis liefern können. Die richtige Bewertung einer Schwachstelle wird womöglich durch Daten erleichtert, die ursprünglich für eine ganz andere Aufgabe erhoben wurden.

Als letzter, aber durchaus wichtiger Aspekt, ist die einfachere und schnellere Einführung des Schwachstellen- und Patchmanagements in einer integrierten Client-Management-Umgebung zu nennen. Viele für die Einführung notwendigen Informationen und Konfigurationen sind bereits vorhanden. Das gilt insbesondere für den Scan-Prozess zur Inventarisierung. Das technische Aufsetzen von Scan-Komponenten, die letztlich das gesamte Netzwerk scannen, ist typischerweise ein aufwendiger Prozess, der viele Prüfungen der Komponenten und die Einrichtung besonderer Rechte für die Scan-Prozesse beinhaltet. In großen IT-Organisationen oder Unternehmen mit besonders strikten Datenschutz- und Sicherheitsbestimmungen bringt dies mitunter einen erheblichen administrativen Genehmigungsaufwand mit sich. In einer integrierten Suite-Lösung muss dieser Vorgang nur einmal durchlaufen werden. Für die Insellösungen des Best-of-Breed-Ansatzes dagegen mehrfach, was in der Regel zu erheblich längeren Einführungszeiten für das Schwachstellenmanagement führt.

# Besondere Anforderungen des Mittelstands

IMittelständische Unternehmen stehen in ihren Anforderungen internationalen Konzernen oftmals nicht viel nach – tun sich jedoch aus Budgetgründen schwer, die dafür notwendigen Kapazitäten und Know-how-Tiefe aufzubieten. Gleichzeitig sind viele mittelständische Unternehmen besonders lohnenswerte Ziele für Wirtschaftsspionage und Cyberattacken, da sie oftmals anerkannte Technologieführer mit spezifischem, einzigartigem Know-how sind. So ist gerade der Mittelstand auf eine besonders effiziente Umsetzung von IT-Services angewiesen. Ohne eine weitgehende Automatisierung von Schwachstellenanalyse und Patch-management sind selbst kleinere IT-Landschaften nicht effizient zu sichern.

Ohne eine weitgehende Automatisierung von Schwachstellenanalyse und Patchmanagement sind selbst kleinere IT-Landschaften nicht effizient zu sichern.

Aus diesem Sachverhalt ergibt sich ein weiterer Grund für die Zusammenführung von Schwachstellen- und Patchmanagement in einem ganzheitlichen Ansatz für Client Management. Eine umfassende Lösung für Client Management wie ACMP bietet so gut wie alle für eine mittelständische IT notwendigen Tools in einer einheitlichen Umgebung. Die Mitarbeiter in den IT-Abteilungen unserer mittelständischen Kunden erledigen rund 90 Prozent des täglichen Arbeitsaufwandes ausschließlich mit und innerhalb von ACMP.

Das schafft erhebliche Vorteile: Zum einen ist das notwendige Know-how einfacher aufzubauen und weiterzuentwickeln, weil sich die Administratoren nur mit einer Umgebung beschäftigen müssen. Das spart Trainingskosten und erlaubt auch kleineren Teams, Personalengpässe durch Urlaub, Krankheit oder sonstige Ausfälle einfacher zu überbrücken.

Zum anderen greifen alle einzelnen Aspekte des Client Managements – von der Inventarisierung, über Lizenzierung und Softwareverteilung bis hin zu Patch- und Schwachstellenmanagement – nahtlos ineinander. Das schafft Synergien und reduziert deutlich die Aufwände: aufwendige Schnittstellen zwischen verschiedenen Tools fallen weg und Doppelerfassungen von Daten werden vermieden. Diese Effizienzgewinne sind insbesondere in mittelständischen IT-Abteilungen von enormer Bedeutung.

Drittens ergeben sich durch die Synergien einer integrierten Lösung nicht zuletzt weitere Kostenvorteile auch bei der Lizenzierung und dem Betrieb der Lösung an sich.

## Vorteile des integrierten Ansatzes im Mittelstand

- Höhere Qualität als ein Sammelsurium an Insellösungen (Beispiel Scan)
- 90 Prozent des täglichen Arbeitsaufwandes in einer zentralen Umgebung
- Ein Tool für alle Automatisierungsaufgaben
- Minimierung von Aufwänden durch Synergien für die IT
- Einfacher Aufbau und Pflege von Know-how sowie Reduktion von Trainingsaufwänden
- Schnellere Einführung der einzelnen Module

# Fazit

In diesem Whitepaper haben wir aufgezeigt, warum Schwachstellen- und Patchmanagement gemeinsam in einem ganzheitlichen Ansatz für Client Management auf Basis einer integrierten Produktsuite wie beispielsweise ACMP umgesetzt werden sollten. Es gibt erhebliche Vorteile mit Blick auf die Qualität und den Wirkungsgrad der einzelnen Leistungsbereiche. Zahlreiche Synergien sorgen für eine höhere Effizienz in Einführung und Nutzung solch integrierter Lösungen gegenüber einem Best-of-Breed-Ansatz mit mühsam verbundenen Insellösungen.

Besonders mittelständische Unternehmen profitieren durch den integrierten Ansatz. Alle Leistungen in einem Produkt und aus einer Hand sorgt für hohe Effizienz, geringen Trainingsbedarf und einfache Pflege des Know-hows.

# Über die Aagon GmbH

„Client Management für Unternehmen jeder Größe“: Das ist unser Produkt ACMP, das die Aagon GmbH mit äußerster Sorgfalt seit 1996 entwickelt. Mit mehr als 20 Jahren Marktreife, ist es perfekt auf Ihre Anforderungen und Bedürfnisse zugeschnitten.

Individuelle Beratung und die beste Unterstützung von Kunden und Partnern bei der Installation und ersten Einrichtung gehören deshalb zum Standard der Aagon GmbH. Ein umfassendes Verständnis von Kundenbedürfnissen und der ständige Kontakt zu unseren Kunden und Partnern ermöglichen Softwareentwicklung auf Augenhöhe.

Webinare-on-Demand, zahlreiche Whitepaper und die beliebten Treffen zum Erfahrungsaustausch an Standorten in ganz Deutschland sind nur drei Beispiele, wie nahe am Kunden ACMP wirklich entwickelt wird.


EIN PRODUKT DER
Aagon GmbH
Lange Wende 33
D-59494 Soest
Fon: +49 (0)2921 - 789200
Fax: +49 (0)2921 - 789244
sales@aagon.com
www.aagon.de

Software
Bundesverband IT-Mittelstand
Made in Germany
100%
Service
Qualität
Zukunft

AAGON UNTERSTÜTZT DIE ARBEIT DES WWF DEUTSCHLAND
WWF