Aagon

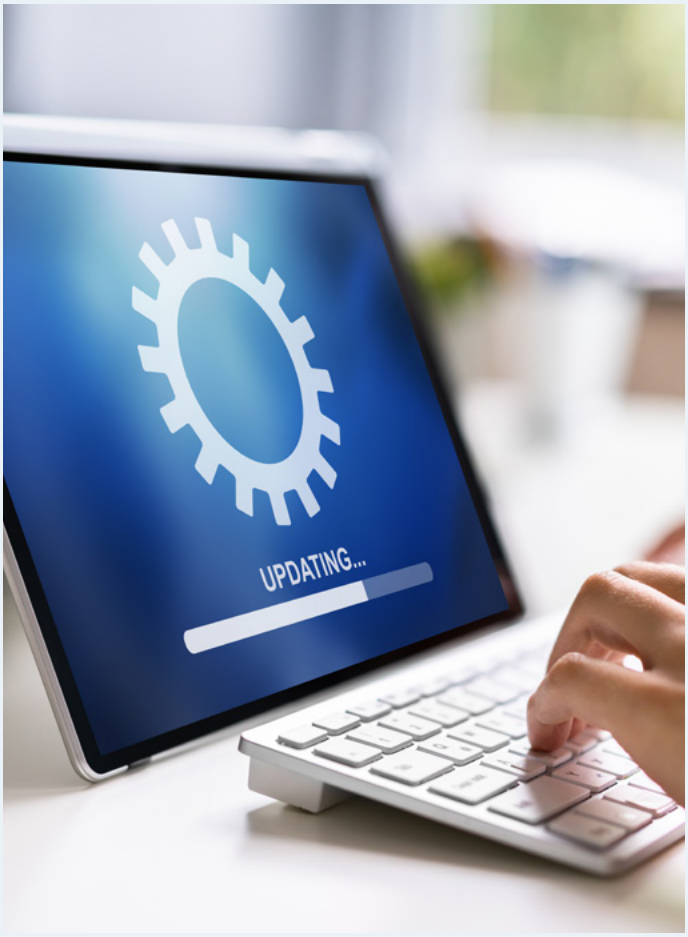
RATGEBER

5 Tipps für mehr IT-Sicherheit

Sichere Systeme benötigen ein effizientes Update-Management. Dabei setzen immer mehr Unternehmen auf leistungsstarke Alternativen zu WSUS.

Stand: Juli 2022

5 Tipps für ein effizientes Update-Management



Sicherheitslücken und Schwachstellen können im Falle eines Cyberangriffs schwere Konsequenzen nach sich ziehen. Die Ursachen dafür sind vielfältig, doch oft sorgen überholte Software und ein umständliches Update-Management dafür, dass Cyberkriminelle einen Weg in die IT-Systeme finden. Die folgenden Tipps helfen IT-Entscheidern dabei, potenzielle Einfallstore frühzeitig zu erkennen und zu schließen, noch bevor sie zum ernsten Sicherheitsrisiko für das Unternehmen werden.

Mehr Möglichkeiten und Aufwand durch Digitalisierung

Noch nie war das Thema IT-Sicherheit so komplex wie heute. Technologien entwickeln sich in hohem Tempo weiter – und damit auch das Potenzial für Cyberattacken aller Art. Für Unternehmen bedeutet das, jeden Tag verschiedenen Herausforderungen gerecht zu werden. Dazu zählen die Einhaltung der Datenschutz-Grundverordnung (DSGVO), des neuen IT-Sicherheitsgesetzes 2.0 sowie interne Richtlinien und Vorgaben. Aufgabe der IT-Abteilung ist es, Angriffe von außen und innen wirkungsvoll abzuwehren und vertrauliche Daten vor ungewollten Zugriffen zu schützen.

Dabei kontinuierlich das nötige Sicherheitsniveau zu gewährleisten ist schwierig, denn die Anforderungen ändern sich schnell. Das Thema Homeoffice zum Beispiel hat im Zuge der Pandemie innerhalb kürzester Zeit massiv an Bedeutung gewonnen, was wiederum völlig neue Anforderungen für IT-Sicherheitskonzepte mit sich brachte. Wer als Entscheider für die IT-Sicherheit eines Unternehmens zuständig ist, muss nicht nur unzählige Risikofaktoren durchblicken – auch im Hinblick auf passende Tech-Lösungen hat man heute die Qual der Wahl aus unzähligen Anbietern.

Software-Update-Management als Kernelement der IT-Sicherheit

Eine grundlegende Herausforderung besteht darin, die Betriebssysteme im Unternehmen auf dem aktuellen Stand zu halten und damit das Risiko für potenzielle Cyberattacken zu minimieren. Dabei kommt es aus vielen Gründen zu Komplikationen. Manche Updates beeinträchtigen die Funktion geschäftskritischer Anwendungen und müssen erst getestet werden, bevor sie unternehmensweit ausgerollt werden. Dazu fehlt es oftmals an effizienten Prozessen und Tools.

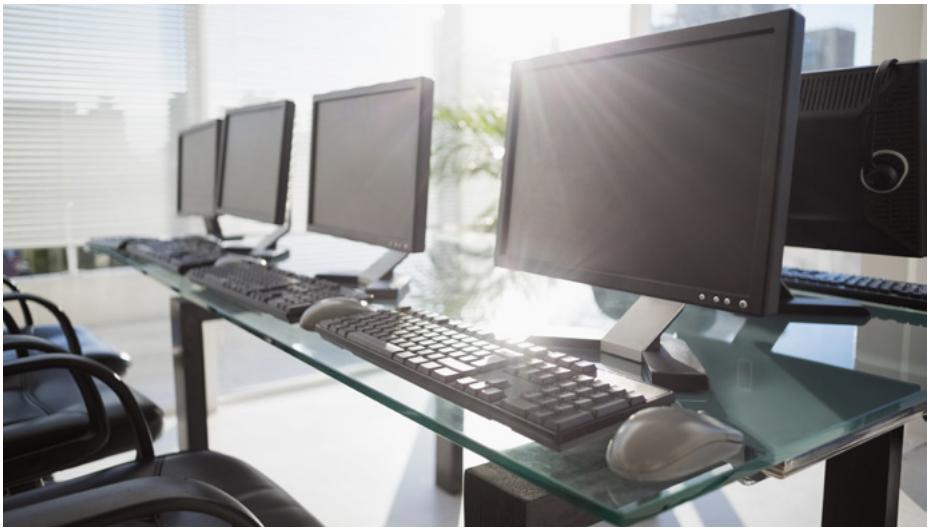
Die folgenden 5 Tipps helfen Administratoren dabei, ihr Update-Management effizient zu verwalten und die Unternehmens-IT zu optimieren.

1. Regelmäßiges Patch- und Update-Management

Praktisch jede Software weist Sicherheitslücken und Schwachstellen auf, die Hacker für Cyberattacken nutzen können. Besonders betroffen sind davon Betriebssysteme wie Windows, die in sehr vielen Unternehmen im Einsatz sind. Da im Laufe der Zeit immer wieder neue Sicherheitslücken auftauchen, sind regelmäßige Updates erforderlich. Für Unternehmen ist es unverzichtbar, diese so schnell und effizient wie möglich für das gesamte IT-Ökosystem auszurollen. Das ist jedoch leichter gesagt als getan.

Zum Thema Patch- und Update-Management gibt es verschiedene Software-Lösungen, mit denen sich Updates über komplexe IT-Infrastrukturen hinweg verteilen lassen. Neben einem Maximum an Sicherheit geht es auch darum, den stabilen Betrieb der Infrastruktur nach der Update-Installation zu gewährleisten.

Tipp // Die meisten Unternehmen nutzen für ihr Update-Management die Windows Server Update Services (WSUS) von Microsoft. Darüber hinaus gibt es inzwischen auch alternative Anbieter, die sich dem Thema Update-Management verschrieben haben und der Standardlösung des Software-Riesen innovative Features entgegensetzen. Viele davon sind in der Lage, den Anwendern eine bessere Usability zu bieten. CAWUM, das Complete Aagon Windows Update Management-Tool, bietet Administratoren etwa eine grafische Konsole, über die sich alle Informationen zu Updates und Status der Computer abrufen lassen. Dabei greift CAWUM auf die Microsoft-Datenbank zurück, um ohne Verzögerung genau die Patches anzubieten, die benötigt werden.



Für eine hohe IT-Sicherheit ist es wichtig, regelmäßig auf allen ans Firmennetzwerk angeschlossenen Geräten Sicherheitsupdates durchzuführen.

2. Altgeräte mit Sicherheits-Updates versehen

Besonders im IT-Bereich dauert es nicht lange, bis Geräte technisch überholt sind. Im Abstand von wenigen Jahren die gesamte Infrastruktur zu erneuern, ergibt jedoch wenig Sinn. Die Erneuerung erfolgt in der Regel schrittweise, was dazu führt, dass Geräte verschiedener Generationen im Einsatz sind. Vor allem Altgeräte werden nicht mehr regelmäßig mit Sicherheitsupdates bespielt. Entweder, weil sie in Vergessenheit geraten oder nur noch selten genutzt werden. Deshalb müssen IT-Fachleute aktiv dafür sorgen, dass diese Geräte kein Sicherheitsrisiko werden.

Tipp // Wenn Altgeräte als Teil des Firmennetzwerks im Einsatz bleiben, sollten IT-Experten sichergehen, dass diese alle relevanten Sicherheitsupdates erhalten. Kommt es dabei zu Komplikationen, ist es besser, das Gerät aus dem Netzwerk zu entfernen und durch ein neues zu ersetzen. Andernfalls könnte es zum Einfallstor für Cyberkriminelle werden. Per Update-Tool mit konfigurierbarem Patch-Plan lassen sich Sicherheitsupdates und Software bequem per Klick aufspielen.

3. Prozesse automatisieren

Wer Prozesse automatisiert, kann die dadurch freigewordenen Ressourcen an anderer Stelle nutzen. Automatisierung spielt daher in der digitalen Transformation jedes Unternehmens eine Schlüsselrolle. Besonders beim Thema Datenübertragung zahlt sich Automatisierung in vielfacher Hinsicht aus, da die Fehleranfälligkeit sinkt und es zu weniger Risikofaktoren bei höherer Effizienz und Sicherheit kommt.

Auch in Sachen Update-Management macht Automatisierung vieles einfacher. Mit entsprechenden Tools lässt sich im Vorfeld festhalten, welche Updates mit welcher Priorität installiert werden müssen. Schließlich möchte man keine Zeit verlieren und möglichst sofort die gesamte Infrastruktur auf den aktuellen Stand bringen, sobald kritische Sicherheitsupdates verfügbar sind. Mit dem CAWUM-Modul von Aagon lässt sich die Reihenfolge anstehender Updates dezidiert festhalten. Damit werden Updates mithilfe von Verteilerringen und dynamischen Containern flexibel über die Infrastruktur verteilt – und das auch in Außenstellen.

Tipp // Automatisierte Prozesse sorgen dafür, Abteilungen zu entlasten und die IT-Sicherheit zu erhöhen. So lassen sich mit dem passenden Tool frühzeitig Kriterien für den Roll-Out von Updates festlegen und aktuelle Standards etablieren.

4. Serverlizenzen und Lizenzgebühren einsparen

Viele Unternehmen verfügen über ungenutzte Software- und Serverlizenzen. Mit einer Anforderungsanalyse wird festgehalten, welche Lizenzen tatsächlich nötig sind und welche nicht. Die Vorteile für die IT-Abteilung sind offensichtlich: Mehr Überblick und weniger Wartungsaufwand.

Tools wie das ACMP Lizenzmanagement von Aagon helfen dabei, alle Aspekte der Lizenzverwaltung innerhalb eines Unternehmens zu optimieren. Dabei werden unterschiedlichste Lizenztypen berücksichtigt und detaillierte Abhängigkeiten abgebildet.

Tipp // Mit einem ausgefeilten Lizenzmanagement bleiben Nutzungs- und Zugriffsrechte jederzeit im Blick. Unerwünschte Software auf Firmenrechnern kann so frühzeitig identifiziert werden, noch bevor sie zum Problem wird. Dadurch werden Daten besser geschützt und die IT-Sicherheit erhöht.

5. Mitarbeiter für Sicherheitsthemen sensibilisieren

Bei aller Automatisierung bleibt der Faktor Mensch weiterhin äußerst wichtig. Auch dann, wenn es um IT-Sicherheit geht. Es kommt immer wieder vor, dass Mitarbeiter verschiedener Abteilungen selbstständig Software und Tools auf ihren Geräten installieren, die nicht Bestandteil der „offiziellen" IT-Infrastruktur eines Unternehmens sind. Dadurch entsteht die sogenannte Schatten-IT und damit ein signifikanter Risikofaktor.

Tipp // Schulungen und gezielte Trainings informieren Geschäftsführung und Mitarbeiter über die Gefahren, die von Schatten-IT, Ransomware und anderen digitalen Bedrohungen ausgehen. Zwar lässt sich Schatten-IT nur selten vollständig vermeiden, doch das Risiko sinkt deutlich, wenn die Mitarbeiter dafür sensibilisiert sind.

Fazit: IT-Sicherheit beginnt bei der Basis

Regelmäßige Updates sind ein grundlegender Faktor, wenn es um die IT-Sicherheit im Unternehmen geht. Dazu gehört auch ein effizientes Update-Management. Mit Tools wie CAWUM bietet Aagon eine leistungsstarke Alternative zu WSUS, mit der sich das Update-Management deutlich einfacher als bisher gestalten und abwickeln lässt.

Über Aagon

„Manage any device in a connected world!" – Aagon entwickelt seit 30 Jahren Client-Management- und -Automation-Lösungen und ist der Spezialist für die Verwaltung von Endgeräten und die Automatisierung von Standardaufgaben. Durch sorgfältige Entwicklungen, mehr als 20 Jahre Marktreife und die enge Zusammenarbeit mit unseren Kunden und Partnern sind unsere Produkte 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 von Aagon. 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 Anwendertreffen an Standorten in ganz Deutschland sind nur drei Beispiele, wie nah am Kunden ACMP wirklich entwickelt wird.

Aagon GmbH
Lange Wende 33
59494 Soest
Tel.: 02921 789 200
E-Mail: info@aagon.com
Web: www.aagon.com

READERS' CHOICE IP INSIDER AWARD 2021

techconsult PUR 2022 Professional User Rating ★ 4-FACH ★ CHAMPION ★

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.