

IT VISION 2010

Referent:

Thomas Poredda

IT-Consulting

Updatemanagement – Ihre Informationen heute

Warum muss ich überhaupt mein System patchen?

- IT-Compliance und IT-Security

Erste Schritte

- Verstehen der Updateverwaltungsprozesse
- Kenntnis der verfügbaren Tools
- Auswählen der richtigen Tools für Ihre Bedürfnisse
- Wissen, wo ich die neusten Informationen finde

Planen und Bewerten

- Bestandsaufnahme / Ermitteln vorhandener Computerressourcen
- Bewerten der Sicherheitsbedrohung und der Sicherheitsrisiken
- Bewerten der vorhanden Infrastruktur zur Softwareverteilung



Updatemanagement – Ihre Informationen heute

Identifizieren

- Zuverlässiges Erkennen neuer Software-Updates
- Feststellen, ob Softwareupdates für die Produktionsumgebung relevant sind
- Beziehen der Quelldateien des Softwareupdates
- Überprüfen der Sicherheit und Installierbarkeit der Updates
- Bestimmen, ob das Software-Update als normale Änderung oder als Notfallmaßnahme gelten soll

Evaluieren und Prüfen

- Bestimmen geeigneter Maßnahmen
- Planen der Veröffentlichung des Softwareupdates
- Erstellen der Veröffentlichungsversion
- Durchführen eines Testes auf Akzeptanz der Version

Updatemanagement – Ihre Informationen heute

Bereitstellen

- Vorbereiten der Bereitstellung
- Bereitstellen des Softwareupdates auf den Zielcomputer
- Überprüfen nach der Implementierung



IT VISION
2010

Warum muss ich überhaupt mein System patchen?

IT-Compliance und IT-Security

- Generelle Anforderungen an die IT-Security
- Rechtliche Pflichten zur IT-Security
- Konkrete Maßnahmen zur IT-Security und IT-Compliance
- Sanktionen bei Verstoß gegen IT-Compliance Anforderungen
- Die Änderungen in 2009 und 2010 im Datenschutz
 - Datenschutzpranger
 - Datensicherheit
 - Sonstige Änderungen



Warum muss ich überhaupt mein System patchen?

IT-Compliance und IT-Security

- **Generelle Anforderungen an die IT-Security**
- Rechtliche Pflichten zur IT-Security
- Konkrete Maßnahmen zur IT-Security und IT-Compliance
- Sanktionen bei Verstoß gegen IT-Compliance Anforderungen
- Die Änderungen in 2009 und 2010 im Datenschutz
 - Datenschutzpranger
 - Datensicherheit
 - Sonstige Änderungen



Warum muss ich überhaupt mein System patchen?

IT-Compliance und IT-Security

- Generelle Anforderungen an die IT-Security
- **Rechtliche Pflichten zur IT-Security**
- Konkrete Maßnahmen zur IT-Security und IT-Compliance
- Sanktionen bei Verstoß gegen IT-Compliance Anforderungen
- Die Änderungen in 2009 und 2010 im Datenschutz
 - Datenschutzpranger
 - Datensicherheit
 - Sonstige Änderungen



Warum muss ich überhaupt mein System patchen?

IT-Compliance und IT-Security

- Generelle Anforderungen an die IT-Security
- Rechtliche Pflichten zur IT-Security
- **Konkrete Maßnahmen zur IT-Security und IT-Compliance**
- Sanktionen bei Verstoß gegen IT-Compliance Anforderungen
- Die Änderungen in 2009 und 2010 im Datenschutz
 - Datenschutzpranger
 - Datensicherheit
 - Sonstige Änderungen



Warum muss ich überhaupt mein System patchen?

IT-Compliance und IT-Security

- Generelle Anforderungen an die IT-Security
- Rechtliche Pflichten zur IT-Security
- Konkrete Maßnahmen zur IT-Security und IT-Compliance
- **Sanktionen bei Verstoß gegen IT-Compliance Anforderungen**
- Die Änderungen in 2009 und 2010 im Datenschutz
 - Datenschutzpranger
 - Datensicherheit
 - Sonstige Änderungen

IT VISION
2010

Warum muss ich überhaupt mein System patchen?

IT-Compliance und IT-Security

- Generelle Anforderungen an die IT-Security
- Rechtliche Pflichten zur IT-Security
- Konkrete Maßnahmen zur IT-Security und IT-Compliance
- Sanktionen bei Verstoß gegen IT-Compliance Anforderungen
- **Die Änderungen in 2009 und 2010 im Datenschutz**
 - **Datenschutzpranger**
 - Datensicherheit
 - Sonstige Änderungen



Warum muss ich überhaupt mein System patchen?

IT-Compliance und IT-Security

- Generelle Anforderungen an die IT-Security
- Rechtliche Pflichten zur IT-Security
- Konkrete Maßnahmen zur IT-Security und IT-Compliance
- Sanktionen bei Verstoß gegen IT-Compliance Anforderungen
- Die Änderungen in 2009 und 2010 im Datenschutz
 - Datenschutzpranger
 - **Datensicherheit**
 - Sonstige Änderungen



Warum muss ich überhaupt mein System patchen?

IT-Compliance und IT-Security

- Generelle Anforderungen an die IT-Security
- Rechtliche Pflichten zur IT-Security
- Konkrete Maßnahmen zur IT-Security und IT-Compliance
- Sanktionen bei Verstoß gegen IT-Compliance Anforderungen
- Die Änderungen in 2009 und 2010 im Datenschutz
 - Datenschutzpranger
 - Datensicherheit
 - **Sonstige Änderungen**



Erste Schritte

- Verstehen des Updateverwaltungsprozesse
- Kenntnis der verfügbaren Tools
- Auswählen der richtigen Tools für Ihre Bedürfnisse
- Wissen, wo ich die neusten Informationen finde



IT VISION
2010

Erste Schritte

- **Verstehen des Updateverwaltungsprozesse**
- Kenntnis der verfügbaren Tools
- Auswählen der richtigen Tools für Ihre Bedürfnisse
- Wissen, wo ich die neusten Informationen finde



IT VISION
2010

Erste Schritte

- Verstehen des Updateverwaltungsprozesse
- **Kenntnis der verfügbaren Tools**
- **Auswählen der richtigen Tools für Ihre Bedürfnisse**
- Wissen, wo ich die neusten Informationen finde



IT VISION
2010

Verfügbare Tools

Produkt	MBSA	Microsoft Update	WSUS	System Center Essentials 2007
Unterstützte Software und Inhalt	Bei der Sicherheitsupdateerkennung mit MU identisch. Konfigurationsprüfungen für Windows, IE, Exchange und SQL	Windows 2000+, Exchange 2000+, SQL Server 2000+, Office XP+ mit optimiertem Support	Identisch mit MU	Identisch mit WSUS 3.0 + Drittanbieter- und benutzerdefinierte Updates
Unterstützte Inhaltstypen	Service Packs und Sicherheitsupdates	Alle Softwareupdates, Treiberupdates, Service Packs (SPs) und Feature Packs (FPs)	Identisch mit MU, aber nur mit kritischen Treiberupdates	Alle Updates, SPs und FPs + Drittanbieter- und benutzerdefinierte Updates und .MSI- und .EXE-basierte Anwendungen

Erste Schritte

- Verstehen des Updateverwaltungsprozesse
- Kenntnis der verfügbaren Tools
- Auswählen der richtigen Tools für Ihre Bedürfnisse
- **Wissen, wo ich die neusten Informationen finde**



IT VISION
2010

Ohne Plan keine Chance im Chaos

Planen und Bewerten

- Bestandsaufnahme / Ermitteln vorhandener Computerressourcen
- Bewerten der Sicherheitsbedrohung und der Sicherheitsrisiken
- Bewerten der vorhanden Infrastruktur zur Softwareverteilung



Ohne Plan keine Chance im Chaos

Planen und Bewerten

- Bestandsaufnahme / Ermitteln vorhandener Computerressourcen
- Bewerten der Sicherheitsbedrohung und der Sicherheitsrisiken
- Bewerten der vorhanden Infrastruktur zur Softwareverteilung



Ohne Plan keine Chance im Chaos

Planen und Bewerten

- Bestandsaufnahme / Ermitteln vorhandener Computerressourcen
- **Bewerten der Sicherheitsbedrohung und der Sicherheitsrisiken**
- Bewerten der vorhanden Infrastruktur zur Softwareverteilung



Ohne Plan keine Chance im Chaos

Planen und Bewerten

- Bestandsaufnahme / Ermitteln vorhandener Computerressourcen
- Bewerten der Sicherheitsbedrohung und der Sicherheitsrisiken
- **Bewerten der vorhanden Infrastruktur zur Softwareverteilung**



Vertrauen ist gut, Kontrolle ist besser

Identifizieren

- Zuverlässiges Erkennen neuer Softwareupdates
- Feststellen, ob Softwareupdates für die Produktionsumgebung relevant sind
- Beziehen der Quelldateien des Softwareupdates
- Überprüfen der Sicherheit und Installierbarkeit der Updates
- Bestimmen, ob das Software Update als normale Änderung oder als Notfallmaßnahme gelten soll



Vertrauen ist gut, Kontrolle ist besser

Identifizieren

- **Zuverlässiges Erkennen neuer Softwareupdates**
- Feststellen, ob Softwareupdates für die Produktionsumgebung relevant sind
- Beziehen der Quelldateien des Softwareupdates
- Überprüfen der Sicherheit und Installierbarkeit der Updates
- Bestimmen, ob das Software Update als normale Änderung oder als Notfallmaßnahme gelten soll



Vertrauen ist gut, Kontrolle ist besser

Identifizieren

- Zuverlässiges Erkennen neuer Softwareupdates
- **Feststellen, ob Softwareupdates für die Produktionsumgebung relevant sind**
- Beziehen der Quelldateien des Softwareupdates
- Überprüfen der Sicherheit und Installierbarkeit der Updates
- Bestimmen, ob das Software Update als normale Änderung oder als Notfallmaßnahme gelten soll



Vertrauen ist gut, Kontrolle ist besser

Identifizieren

- Zuverlässiges Erkennen neuer Softwareupdates
- Feststellen, ob Softwareupdates für die Produktionsumgebung relevant sind
- **Beziehen der Quelldateien des Softwareupdates**
- Überprüfen der Sicherheit und Installierbarkeit der Updates
- Bestimmen, ob das Software Update als normale Änderung oder als Notfallmaßnahme gelten soll



Vertrauen ist gut, Kontrolle ist besser

Identifizieren

- Zuverlässiges Erkennen neuer Softwareupdates
- Feststellen, ob Softwareupdates für die Produktionsumgebung relevant sind
- Beziehen der Quelldateien des Softwareupdates
- **Überprüfen der Sicherheit und Installierbarkeit der Updates**
- Bestimmen, ob das Software Update als normale Änderung oder als Notfallmaßnahme gelten soll



Vertrauen ist gut, Kontrolle ist besser

Identifizieren

- Zuverlässiges Erkennen neuer Softwareupdates
- Feststellen, ob Softwareupdates für die Produktionsumgebung relevant sind
- Beziehen der Quelldateien des Softwareupdates
- Überprüfen der Sicherheit und Installierbarkeit der Updates
- **Bestimmen, ob das Software Update als normale Änderung oder als Notfallmaßnahme gelten soll**



Prüfe, mit wem du dich binden willst

Evaluieren und Prüfen

- Bestimmen geeigneter Maßnahmen
- Planen der Veröffentlichung des Softwareupdates
- Erstellen der Veröffentlichungsversion
- Durchführen eines Testes auf Akzeptanz der Version



Prioritätenlevel

Priorität	Empfohlener Zeitrahmen	Min. empfohlener Zeitrahmen
Emergency	Innerhalb von 24 Stunden	Innerhalb von 2 Wochen
High	Innerhalb eines Monats	Innerhalb von 2 Monaten
Medium	Je nach Verfügbarkeit, eines neuen Service Pack oder Update, dass ein Update für diese Sicherheitsanfälligkeit innerhalb von 4 Monaten umfasst	Ausrollen des Softwareupdates innerhalb von 6 Monaten
Low	Je nach Verfügbarkeit, eines neuen Service Pack oder Update, dass ein Update für diese Sicherheitsanfälligkeit innerhalb von 1 Jahr umfasst	Innerhalb eines Jahres, oder nicht installieren



Prüfe, mit wem du dich binden willst

Evaluieren und Prüfen

- Bestimmen geeigneter Maßnahmen
- Planen der Veröffentlichung des Softwareupdates
- Erstellen der Veröffentlichungsversion
- Durchführen eines Testes auf Akzeptanz der Version



Prüfe, mit wem du dich binden willst

Evaluieren und Prüfen

- Bestimmen geeigneter Maßnahmen
- Planen der Veröffentlichung des Softwareupdates
- **Erstellen der Veröffentlichungsversion**
- Durchführen eines Testes auf Akzeptanz der Version



Prüfe, mit wem du dich binden willst

Evaluieren und Prüfen

- Bestimmen geeigneter Maßnahmen
- Planen der Veröffentlichung des Softwareupdates
- Erstellen der Veröffentlichungsversion
- Durchführen eines Testes auf Akzeptanz der Version



Allzeit bereit!

Bereitstellen

- **Vorbereiten der Bereitstellung**
- Bereitstellen des Softwareupdates auf den Zielcomputer
- Überprüfen nach der Implementierung



Allzeit bereit!

Bereitstellen

- Vorbereiten der Bereitstellung
- Bereitstellen des Softwareupdates auf den Zielcomputer
- Überprüfen nach der Implementierung



Allzeit bereit!

Bereitstellen

- Vorbereiten der Bereitstellung
- Bereitstellen des Softwareupdates auf den Zielcomputer
- Überprüfen nach der Implementierung



Mehr ist das eigentlich nicht

Wenn Sie alles Richtig gemacht haben, landet kein Ball bei Ihnen im Netz.



Linkliste

- <http://technet.microsoft.com/de-de/updatesmanagement/bb245843.aspx>
- <http://www.microsoft.com/security>
- <http://www.microsoft.com/germany/technet/sicherheit/bulletins/revsbwp.msp#E1F>
- <http://www.microsoft.com/technet/security/bulletin/revsbwp.msp>



Ihr Kontakt



PC-Ware Information Technologies AG

Blochstraße 1

04329 Leipzig

phone: +49 341 25 68 000

fax: +49 341 25 68 999

web: www.it-superstar.de