Parasol Island

Arbeitsanweisung
zur Durchführung von Patches

Dateiname:	03_11_PSL_ISMS_Patchplan_v00.10_pN
Dokumentenebene:	03_Arbeitsanweisungen
Erstellt von:	Philip Hansen
Version:	00.10
Status:	Freigegeben
Letzte Aktualisierung am/von:	10.11.2017 | Peter Norenkemper
Exportiert am:	10.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	10.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	12.7

Version	Datum	Autor	Änderung
00.01	30.08.2017	Philip Hansen	Erstellung
00.02	21.09.2017	Justus Heinser	Anpassungen
00.10	10.11.2017	Peter Norenkemper	Finalisierung

Parasol Island

Inhaltsverzeichnis

Parasol Island

1. Ziel des Patchplans

Der Patchplan soll die Anforderungen der Change Management Richtlinie konkret planen.
Er soll Checklisten für die Nutzer von IT-Systemen und besonders den Administrator bieten, um Sicherheitslücken schnellstmöglich zu schließen. Gleichzeitig ist es erforderlich, den laufenden Betrieb nicht übermäßig zu stören oder gar zu gefährden.
Daher ist es notwendig, Patches vorher zu planen und Absprache mit allen Abteilungen zu halten.
Bei Gefahr im Verzug gilt die Regel Sicherheit vor Verfügbarkeit, was bedeuten kann, dass Systeme zugunsten der Sicherheit zeitweise aus dem Betriebsablauf entfernt werden müssen, um Sicherheitslücken zu schließen.
Administratoren und Informationssicherheitsbeauftragter haben die Pflicht, sich durchgehend über mögliche Sicherheitslücken zu Informieren, um gegebenenfalls außerplanmäßige Updates zu veranlassen.

2. Definitionen

Server sind für den Dauerbetrieb bestimmt, sie werden allerdings nicht vom Benutzer selbst gesteuert. Durch die zentralisierte Datenspeicherung entsteht ein großes Risiko, welches regelmäßig auf das kleinstmögliche Niveau gebracht werden muss.
Workstations sind Arbeitsrechner, welche vom Benutzer gesteuert werden. Auf ihnen liegen keine Daten und die Zugriffsrechte sind eingeschränkt. Allerdings kann das Fehlverhalten von Nutzern hohe Risiken mit sich bringen, weshalb hier vor allem Sicherheitsschulungen für die Nutzer durchgeführt werden müssen. Durch die direkte Internetnutzung besteht zudem ein stark erhöhtes Risiko durch Schadsoftware.
Lokale Administratorrechte sind nur eingeschränkt zu vergeben und die Rechner sind stichprobenartig vom Administrator oder ISB zu kontrollieren.
Die Nutzer haben den Administrator in seiner Tätigkeit zu unterstützen, indem sie Updates selber durchführen, sofern ihnen das möglich ist. oder den Administrator informieren, sobald sicherheitsrelevante Software geupdatet werden kann.
Renderblades sind leistungsstarke Maschinen zum Verarbeiten von Daten. Sie werden nicht durch den Nutzer selbst gesteuert und auf ihnen liegen keine Daten, weshalb das Risiko kleiner ist als bei Servern.
Peripherie sind alle Geräte, welche zwar an unsere IT-Systeme angeschlossen sind, jedoch durch ihren Komplexitätsgrad und ihre Funktionsweise nur ein geringes Risiko darstellen. (z.B. Drucker, Switches, Telefone)

3. Auflistung der zu patchenden Systeme

Name	Typ	Risoko
Domaincontroller	Server	Hoch
Fileserver	Server	Hoch
Linux-Server	Server	Hoch
Windows-Server	Server	Hoch
Windows Workstations	Workstation	Hoch
Mac Workstations	Workstation	Hoch
Mobilgeräte	Workstation	Hoch
Drucker	Peripherie	Gering
Switches	Peripherie	Gering
WLAN AccessPoints	Peripherie	Gering

4. Zu patchende Software auf Server

Da die Server untereinander vernetzt sind, ist das Schließen von Sicherheitslücken nur so effektiv wie die schwächste Komponente, woraus folgt, dass alle Server mit höchster Priorität zu patchen sind. Besondere Aufmerksamkeit erfordern:

- Betriebssystem
- Antivirus Software

Updates werden automatisch vom System heruntergeladen und installiert, müssen jedoch manuell neu gestartet werden.

Jedoch mindestens einmal im Monat sind die Server auf den Bedarf eines Neustartes zu kontrollieren und nach Absprache durchzuführen.
Dafür ist die erste Woche eines Monates festzuhalten. Es ist Rücksprache mit allen Abteilungsleitern zu halten um Rechenoperationen von zeitkritischen Projekten nicht zu gefährden. Bei Auffälligkeiten oder Bekanntwerden einer akuten Gefährdungslage ist ein Neustart sofort durchzuführen.

5. Patches auf Workstations

Updates des Virenscanners und des Betriebssystems werden automatisch installiert Besonders durch Internetnutzung ist eine erhöhte Gefährdung durch Schadsoftware anzunehmen und Virenscanner sind bei sofortigen Erscheinen von Patches zu aktualisieren.
Der erforderliche Neustart sollte wenn möglich unverzüglich ausgeführt werden, jedoch spätestens am Ende des Arbeitstages.
Mailclients, Browser, Java und Flashupdates sowie andere Software, die direkt mit dem Internet benutzt wird, sind ebenso kritisch, werden jedoch nicht zentral verwaltet und erfordern daher eine Kontrolle an der Workstation selbst. Der Nutzer hat trotz automatischer Updates regelmäßig zu kontrollieren, dass seine Software nicht veraltet ist.

6. Patches von Peripherie

Peripherie ist nur selten Angriffsziel von Schadsoftware, das Risiko ist jedoch nicht auszuschließen. Daher ist eine regelmäßige Kontrolle auf neue Firmware-Updates erforderlich.
Einmal jährlich sollten Peripheriegeräte kontrolliert werden und wenn möglich Updates durchgeführt werden. Der Zeitpunkt ist so zu wählen, dass ein Ausfall des Systems kurzzeitig vertretbar ist. Bei den meisten Geräten empfiehlt sich, wenn möglich ein Backup der Settings oder ein vorheriges zu notieren.

7. Patches von Grafiksoftware

Die Gefahren von Sicherheitslücken in Grafiksoftware sind als sehr gering einzuschätzen, weshalb Updates nicht automatisch bezogen werden.
Die Gefahr von Inkompatibilität bei neueren Versionen ist hier relevanter, so dass diese Softwarepakete oder damit verbundene Plug-Ins nur nach vorheriger Planung, möglichst ohne Zeitdruck durchgeführt werden.

8. Kontrolle über ESET

Der Administrator kann zentral die Aktualität des Betriebssystems und der Virenscanner über ESET kontrollieren und Updates sowie Neustarts ausführen. Dies betrifft Server und Workstations gleichermaßen.

9. Firewall

Die Firewall aktualisiert sich bei Erscheinen von Patches automatisch, eine Einschränkung des Betriebsablaufes ist hierdurch nicht zu erwarten. Allerdings ist die Lizenz einmal jährlich rechtzeitig zu erneuern. Geschieht das nicht, werden keine neuen Updates geladen.

10. Übersicht

Typ	Patches	Häufigkeit
Server	● Betriebssystem ● Virenscanner	● Automatische Installation ● Neustart bei Gelegenheit, aber mindestens 1x monatlich. ● Wöchentliche Kontrolle
Renderblades	● Betriebssystem ● Virenscanner	● Automatische Installation ● Neustart bei Gelegenheit.
	● Royal Render ● Grafiksoftware	● nach vorheriger Planung ● zentralisiert
Workstation	● Betriebssystem ● Virenscanner	● Automatische Installation ● Neustart unverzüglich nach Aufforderung, wenn möglich
	● Browser ● Mailclient ● Java ● Flash	● Automatische Installation ● Neustart unverzüglich nach Aufforderung, wenn möglich ●
	● Grafiksoftware ● Royal Render	● nach vorheriger Planung
Peripherie	● Firmware	● Nach Bedarf, mindestens jährlich