Konzept zum Virenschutz- und Patchmanagement (VPM-Konzept) vom 01.06.2005 (MittVw Seite 80)

1. Zielsetzung

Dieses Konzept konkretisiert für die Administratorinnen und Administratoren die Anwendung der geltenden Richtlinien, insbesondere der PC-Richtlinie, der Freigaberichtlinie und einer zukünftigen Netzwerk-Richtlinie in Bezug auf die Handhabung von Virenschutz und Patchmanagement auf Windows Betriebssystemen. Soweit dezentral andere Betriebssysteme eingesetzt werden, sind vergleichbare Maßnahmen zu treffen, um die Sicherheit der zu verarbeitenden Daten zu gewährleisten.

2. Virenschutzmanagement

2.1 Virenschutzprogramm

Als Virenschutzprogramm für PC-Clients und Server ist das in der geltenden IuK-Architektur-Richtlinie aufgeführte Programm einzusetzen. Dabei ist sicherzustellen, dass das Programm stets aktiviert ist. Für die Verteilung und Aktualisierung des Programms ist der zentrale ePO-Dienst (electronic Policy Orchestrator) bei Dataport zu nutzen. Dieser Dienst ermöglicht eine Erfolgskontrolle der Installationen.

2.2 Virensignaturen

Bei Bekanntgabe einer neuen Virensignatur durch den Hersteller des Virenschutzprogramms ist unter Nutzung des bei Dataport installierten zentralen ePO-Dienstes sicherzustellen, dass diese unverzüglich eingespielt wird. Dataport informiert durch die Viren Task Force über neue Viren und Signaturupdates.

3. Virenschutzmanagement

3.1 Allgemeines

Ausgelieferte Korrekturen (Patches), die Fehler in eingesetzten Programmen beheben, sind unverzüglich zu installieren.
Jede Behörde kann die Informationen über derartige Korrekturen direkt vom Softwarehersteller beziehen. Zusätzlich werden sie von Dataport im FHHIntranet und ggf. auch per Mail zur Verfügung gestellt. Die Dringlichkeit einer Installation wird vom Softwarehersteller klassifiziert. Dataport stellt im FHHIntranet eine eigene Bewertung zur Verfügung, die den IuK-Leitern in den Behörden per Mail zur Kenntnis gegeben wird. Aus der Bewertung durch Dataport ergibt sich die Dringlichkeit der Installation.

Die Bewertungsstufen sind:

Kritisch	**Es besteht die Möglichkeit einer akuten Gefährdung des FHH-Netzes. Der Patch ist umgehend zu installieren**
Wichtig	Eine Gefährdung des FHH-Netzes ist prinzipiell möglich. Der Patch ist im Rahmen geregelter Changes zu installieren
Normal	Eine Gefährdung des FHH-Netzes ist unwahrscheinlich. Der Patch ist mit der nächsten Sammlung von Patches (Service Pack) zu installieren
Nicht relevant	Eine Gefährdung des FHH-Netzes besteht nicht, da das betroffene Produkt nicht im Einsatz ist. Der Patch braucht nicht installiert zu werden

3.2 Technische Umsetzung

Die Auslieferung und ggf. Installation von Patches auf vernetzten Rechnern wird über den Software Update Service (SUS) von Dataport vorgenommen. Hierdurch kann der Umsetzungserfolg verifiziert werden. Alle Rechner, die zum Zeitpunkt der Installation von Patches nicht in Betrieb oder nicht mit dem Netz verbunden waren, müssen bei Inbetriebnahme oder Verbindung zum Netz mit dem Patch versorgt werden. Ebenso ist zu gewährleisten, dass neu installierte Rechner nur mit dem aktuellen Stand der Patches in das Netz eingebunden werden.

4. Informationsaustausch

4.1 Bericht an die für Grundsatzangelegenheiten der IuK-Technik zuständigen Stelle

Nach Anforderung der für Grundsatzangelegenheiten der IuK-Technik zuständigen Stelle berichtet Dataport den Patch-Stand der PC-Clients und Server, die über den Software Update Service von Dataport angeschlossen sind.

Soweit PC-Clients und Server über einen dezentralen SUS angeschlossen sind, müssen die betreibenden IuK-Stellen sicherstellen, dass auf Anforderung die für Grundsatzangelegenheiten der IuK-Technik zuständige Stelle jederzeit über den Patch-Stand dieser PC-Clients und Server informiert werden kann.

4.2 Unterrichtung von Dataport

Die Behörden informieren Dataport über ggf. auftretende Probleme mit installierten Patches. Darüber hinaus werden mit der Viren Task Force bei Dataport Informationen über den Umgang mit dem eingesetzten Virenschutzprogramm und auftretenden Viren ausgetauscht. Probleme mit der eingesetzten Programmversion, mit neuen Signaturupdates oder dem Auftreten von Viren werden ebenfalls von den Behörden an das Funktionspostfach Virenschutz@dataport.de von Dataport gemeldet.

4.3 Information der IuK-Stellen

Dataport veröffentlicht die Informationen zum Virenschutz und Patchmanagement zusammen mit den eigenen Erfahrungen und Lösungstipps der Softwarehersteller im Intranet. Darüber hinaus steht Dataport im engen Kontakt mit dem Hersteller, und bietet spezielle Problemlösungen für Standardsoftware an.

5. Fristen

5.1 Elektronic Policy Orchestrator

Die IuK-Stellen, die an das Active Directory angeschlossen sind, müssen sich bis zum 31. August 2005 an den ePO-Dienst bei Dataport angeschlossen haben. Die anderen IuK-Stellen müssen sich zügig in Absprache mit Dataport an das ActiveDirectory und den ePO-Dienst anschließen.

5.2 Software Update Service

Sobald der SUS bei Dataport für die Behörden installiert ist, wird die für Grundsatzangelegenheiten der IuK-Technik zuständige Stelle in Abstimmung mit den IuK-Stellen den Termin festlegen, bis zu dem sich die IuK-Stellen, die keinen dezentralen SUS betreiben, angeschlossen haben müssen. Für ESARI-Rechner ist der zentrale SUS Leistungsbestandteil.