Sicherung von Netz, Systemen, Anwendungen (Security)

Übersicht über den Dienst

Durch eine Reihe von Maßnahmen werden das Netz, die Betriebssysteme und die Anwendungen am Fachbereich vor Angriffen und Störungen geschützt.

Erbringer: FB3-Technik
Scope: FB3, Gäste des FB3
Kunden: Basisdienst für alle FB3-Mitglieder

Bedarfsniveau: Hohes Bedarfsniveau
Priorität: Höchste Priorität
Status: Konsolidierungsphase Betriebsphase

Technische Unterstruktur

- Patch-Management: regelmäßiges, automatisiertes oder manuelles Installieren von sicherheitsrelevanten (und anderen) Betriebssystem- und Anwendungs-Patches
- Anbieten von Anti-Viren-Software für alle relevanten Betriebssystemplattformen
- Mitgliedschaft aller Techniker in der DFN-CERT-Mailingliste
- Information der Techniker und (in Einzelfällen) der Nutzer bei bekanntgewordenen Sicherheitsproblemen; Bekanntmachung von Informationen zu entsprechenden Schutzmaßnahmen
- Einbeziehen von sicherheitsrelevanten Verhaltensregeln in die IT-Policy des FB3
- Anbieten von sicheren Anwendungen und Netzprotokollen (z.B. SSH); Deaktivierung von unsicheren Anwendungen bzw. Protokollen
- Webanwendung zur Verwaltung persönlicher SSH-Schlüssel
- Anbieten von Maßnahmen zur Spam-Abwehr (SpamAssassin)
- Virenerkennung in E-Mails
- Automatisierte End-of-Life Erkennung für die Betriebssysteme

Beziehungen zu anderen Diensten

- Kommunikation mit Nutzern [kommunikation-mit-nutzern.html] (Bekanntmachen von Problemen und Maßnahmen)
- Mail-Dienst [mail.html] (Spam-Abwehr und Virenerkennung)
- Definition von Policies

Absehbare Entwicklungen

- Anheben des allgemeinen Sicherheitsniveaus; Schaffung von verbindlichen Vorgaben
- Sicherheitserwägungen müssen zukünftig stärker und frühzeitig in alle Planungsprozesse einfließen

Sicherung von Netz, Systemen, Anwendungen (Security)

- Einrichtung eines CERT bzw. eines festen Anlaufpunktes für Sicherheitsprobleme
- Einführung einer zentralen Firewall
- Einführung von zentraler Intrusion Detection
- Schaffung von Mechanismen zum automatisierten Löschen inaktiver Benutzeraccounts (nicht-triviale Aufgabe)

Aufwand für den Dienst

Beteiligte Personen		
Bereich	**Mitarbeiter**	**Zeit/Mitarbeiter**
zentrale, dezentrale Technik	mehrere Techniker	ca. 3d/a
Zeitliche Gliederung		
mehrmals pro Woche	einige Minuten	einfache Tätigkeiten
mehrmals pro Monat	einige Stunden	anspruchsvollere Tätigkeiten
einmal pro Jahr	einen Tag	Experten-Tätigkeiten

Autor: Oliver Laumann
Stand: $Id: security.xml,v 1.7 2012/01/26 12:24:51 net Exp $
URL: http://www.informatik.uni-bremen.de/t/info/dienste/security.html