D-Grid Integrationsprojekt 2 (DGI-2)

DGI-2 Security

Richtlinie zur Behandlung von Sicherheitsvorfällen im D-Grid

Version 1.0, 25.08.2011

D-Grid Integrationsprojekt 2 (DGI-2)

Autoren

Christopher Kunz (DCSec, Leibniz Universität Hannover)

Tobias Dussa (KIT)

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IG07014F gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Versionsgeschichte

Revision	Datum	Bearbeiter	Anmerkungen
0.1	26.07.11	C.Kunz / DCSec	Übertragung und Anpassung der EGI-Policy „Incident Response Procedure“ gemäß Meilen-steinplan
0.2	28.07.11	T. Dussa / KIT	Ergänzungen und Korrekturen
1.0	25.08.11	C.Kunz / DCSec	Veröffentlichte Version

Inhalt

1 Richtlinie zur Behandlung von Sicherheitsvorfällen im D-Grid

Ein „Sicherheitsvorfall“ ist die Mißachtung einer expliziten oder impliziten Sicherheitsvorschrift (also etwa einer lokalen oder gridweiten Regulierung). Die Regulierungen in dieser Richtlinie (Policy) finden keine Anwendung auf den Informationsfluß von einem Grid-Ressourcenbetreiber zum DFN-CERT oder anderen Stellen, denen er zur Meldung von Sicherheitsvorfällen ohnehin, unabhängig von seiner Mitarbeit im D-Grid, verpflichtet ist.

Diese Richtlinie soll sicherstellen, daß Nachforschungen zu jeglichen sicherheitsrelevanten Vorfällen im D-Grid angestellt werden können und daß alle Ressourcenbetreiber solche Vorfälle unverzüglich und ohne Ausnahme an die entsprechende Stelle melden. Insbesondere sollen Sicherheitsvorfälle mit hoher Priorität behandelt und geeignetes Personal mit der Nachforschung beauftragt werden.

Für eine effiziente und unverzügliche Reaktion auf sicherheitsrelevante Vorfälle ist es unabdingbar, daß alle Ressourcenbetreiber aktuelle Kontaktinformationen des site-weiten Sicherheitsbeauftragten in den entsprechenden Kanälen wie der Datenbank des Grid Operation Center (GOCDB) vorhalten. Die Security Officers von NGI_DE sind als D-Grid-weite Ansprechpartner für Sicherheitsfragen zuständig. Jeder Vorfall soll an die für das D-Grid zuständigen CERTs gemeldet werden, um eine optimale Steuerung der Arbeiten und Nachforschungen zu gewährleisten. Informationen über Sicherheitsvorfälle können, sofern notwendig, auch an Partner-Grids im EGI-Verbund weitergegeben werden, etwa um eine Nachforschung über die Grenzen des nationalen Grid hinaus zu ermöglichen.

Als Teilnehmer am D-Grid erklären Sie sich mit den im Folgenden aufgezählten Regeln zur Behandlung von Sicherheitsvorfällen einverstanden:

1. Wenn Sie auf ein mögliches Sicherheitsproblem bei der Nutzung der lokalen D-Grid-Ressourcen aufmerksam werden, verständigen Sie unverzüglich den Sicherheitsbeauftragten Ihrer Heimatorganisation.
2. Mögliche Sicherheitsprobleme, die das gesamte D-Grid betreffen könnten, sollen unverzüglich an die Mailingliste NGI-DE-CSIRT@LISTSERV.DFN.DE (die DFN-CERT und KIT-CERT umfaßt) gemeldet werden.
3. Sofern Sie für D-Grid-Ressourcen die technische oder administrative Verantwortung innehaben, sollen Sie auf Vorfälle, die Ihnen gemeldet werden, unverzüglich reagieren und diese untersuchen.
4. Ihre Nachforschungen und forensische Untersuchungen sollen Spuren und Beweise eines sicherheitsrelevanten Vorfalls erhalten, nicht zerstören. Sie sollen sich an die industrieüblichen Vorgehensweisen zur forensischen Untersuchung von Computersystemen halten. Die Ergebnisse Ihrer Nachforschungen sollen Sie dem D-Grid-Sicherheitsbeauftragten zukommen lassen.
5. Der Schutz privater Daten soll auch bei der Untersuchung von sicherheitsrelevanten Vorfällen stets erhalten bleiben. Informationen, die im Rahmen der Untersuchung eines Vorfalls von Ihnen zur Verfügung gestellt werden, sollen nicht veröffentlicht werden. Eine Veröffentlichung kann nur mit Zustimmung aller beteiligten Nutzer/Ressourcenbetreiber sowie des Sicherheitskoordinators erfolgen - für jeden Vorfall ist eine separate Genehmigung notwendig. Eine Veröffentlichung von sicherheitsrelevanten Informationen - etwa im Rahmen von „Security Advisories“ - ist nur in Rücksprache mit den Security Officers von NGI-DE beziehungsweise der EGI-IRTF zulässig.

Ein „Security Advisory“ ist ein Hinweis auf aktuelle Sicherheitsprobleme durch eine dazu berufene Stelle. Es kann als Warnung vor einem konkreten Sicherheitsvorfall (Incident) oder auch als vorbeu-

gende Maßnahme, etwa nach Entdeckung einer Sicherheitslücke, herausgegeben werden. Berufene Stellen sind häufig CERTs, Softwarehersteller, Betroffene oder unabhängige Sicherheitsberater.