D-Grid Integrationsprojekt 2 (DGI-2)

DGI-2 Security

Prozesse zur Behandlung von Sicherheitsvorfällen

Version 1.0, 30.07.2012

D-Grid Integrationsprojekt 2 (DGI-2)

Autoren

Benjamin Henne, Christian Szongott (RRZN, Leibniz Universität Hannover)

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	07.06.2012	C. Szongott	Framework
0.2	28.06.2012	C. Szongott B. Henne	Beschreibung der Hauptprozesse
0.3	24.07.2012	C. Szongott	Kleine Anpassungen
0.4	26.07.2012	B. Henne	Kleine Erweiterungen
0.5	27.07.2012	C. Szongott B. Henne	Einarbeitung von Feedback
0.6	27.07.2012	B. Henne	Überarbeitung der Grafiken
1.0	30.07.2012	B. Henne C. Szongott	Kleine Anpassungen

1 Inhalt

2 Einführung

Das D-Grid ist wie jede andere verteilte Infrastruktur stetigen Angriffen ausgesetzt. Diese Angriffe richten sich häufig gegen die im D-Grid eingesetzte Software und dabei speziell gegen die Komponenten der verwendeten Middleware, welche auf allen Ressourcen der D-Grid-Infrastruktur installiert sind. Schwachstellen in der verwendeten Software werden nicht nur von potentiellen Angreifern entdeckt, sondern auch durch Sicherheitsforscher oder durch Teilnehmer des D-Grids.

Aufbauend auf dem D-Grid Betriebskonzept (Version 2.1 vom 13.01.2012) liefert dieses Dokument einige Handlungsbeschreibungen für den Umgang mit Sicherheitsproblemen, wie Sicherheitsvorfällen oder Schwachstellen in D-Grid Software.

Dieses Dokument soll den Nutzern, Administratoren der Ressourcenbetreiber, als auch den beteilgten CERTs als Orientierung und Leitfaden dienen, wie bei den im folgenden beschriebenen Sicherheitsvorfällen zu verfahren ist.

3 Behandlung von Sicherheitsvorfällen

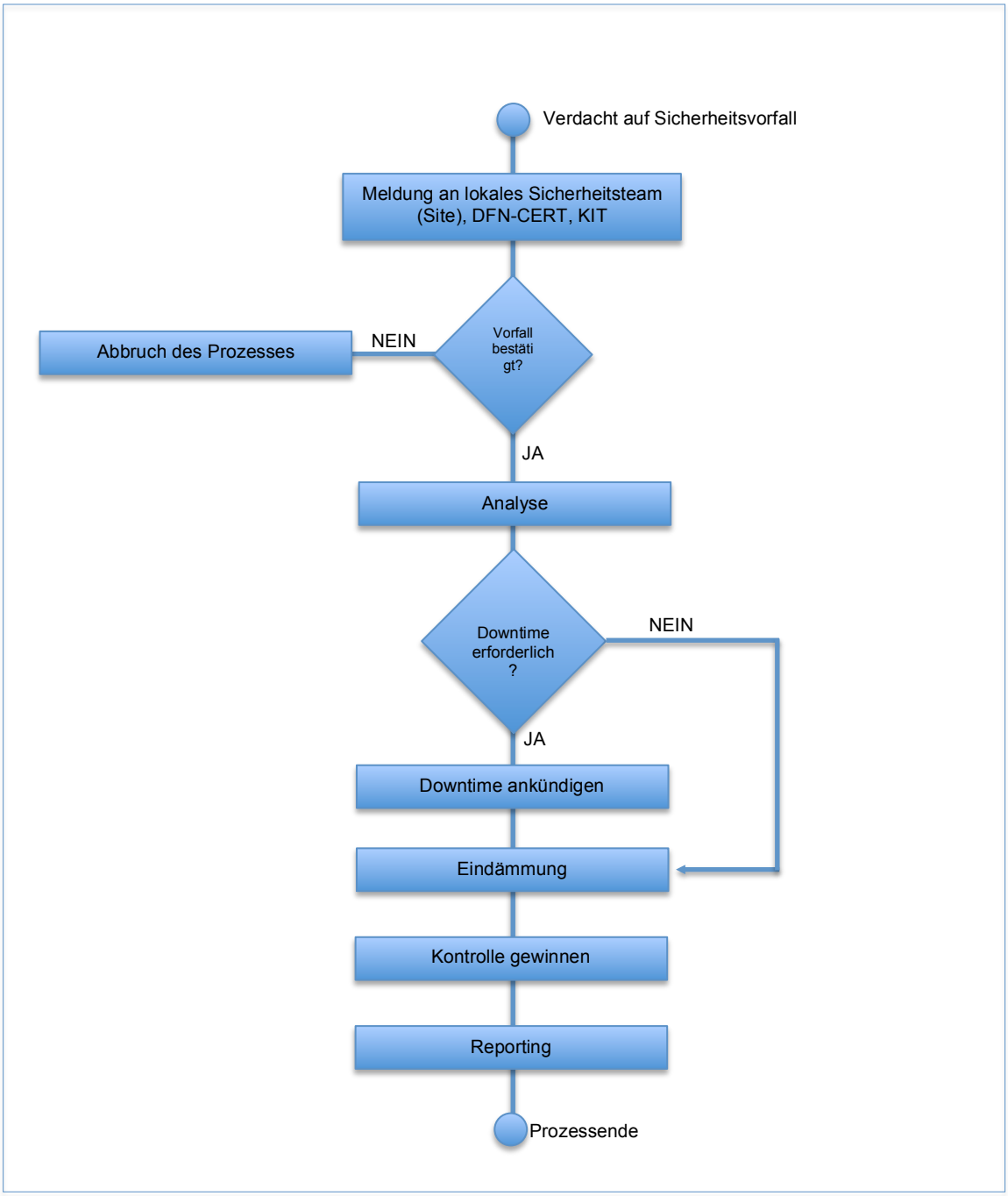
3.1 Ziel

Diese Vorgehensbeschreibung zeigt, wie mit auftretenden Sicherheitsvorfällen im Rahmen des D-Grids verfahren werden soll.

3.2 Beteiligte Personen

- Entdecker des vermuteten Vorfalls: Er meldet den Vorfall mit allen beobachteten Details
- Lokales Sicherheitsteam: Sicherheitsteam der Grid-Site (Universität/andere Einrichtung)
- DFN-CERT und KIT-CERT übernehmen den weiteren Ablauf

3.3 Ablauf



Entdeckung/Meldung

Liegt ein Verdacht auf einen Vorfall vor, so wird dies an das lokale Sicherheitsteam der eigenen Einrichtung sowie an das DFN-CERT / KIT-CERT gemeldet. Hierzu müssen alle Nutzer wissen, wie diese Einrichtungen im Ernstfall zu erreichen sind. Kontaktemailadressen und Telefonnummern sollten an zentraler Stelle verzeichnet sein (Siehe hierzu den Abschnitt Meldung auf Seite 10).

Die minimalen Angaben einer solchen Meldung sind:

- Datum und Zeitpunkt des Vorfalls (mit Zeitzone)
- Quell-IP, Ports und Protokolle
- Ziel-IP, Ports und Protokolle

Diese Minimalanforderung sind der „CSIRT Description for DFN-CERT“ entnommen.

Bestätigung

Bei einem Verdacht auf einen Vorfall wird geprüft, ob wirklich ein Vorfall vorliegt. In manchen Fällen ist dieses eindeutig. Ist dies nicht der Fall, so muss das verdächtige System genauer überprüft werden. Dabei können folgende Informationen eine Hilfestellung bieten:

- http://www.dfn-cert.de/informationen/themen/incident-response-informationen/nachsehen-linux.html
- http://www.dfn-cert.de/informationen/themen/incident-response-informationen/nachsehen-windows.html

Analyse

Ist der Verdacht bestätigt, wird mit der Analyse des Vorfalls begonnen. Dabei sind u.a. folgende Fragen zu klären:

- Wann und wo ist der Vorfall passiert?
- Was genau ist passiert?
- Wer ist beteiligt und wer ist der Angreifer?
- Wie ging er vor? Welche Schwachstelle wurde ausgenutzt?
- Welcher Schaden ist bisher entstanden? Welcher weitere Schaden droht?

Außerdem wird festgelegt, wie im Weiteren vorgegangen werden soll, welche Maßnahmen voraussichtlich zu tätigen sind und wer in diese Maßnahmen miteinzubeziehen ist.

Downtime

In der Regel sollte ein System für weitere Analysen und die spätere Wiederherstellung des Systems vom Netz genommen werden. Die betroffenen Grid-Komponenten erfahren entsprechend eine Downtime. Diese muss in den entsprechenden Informationsdiensten oder Ticketsystemen angekündigt werden.

Eindämmung

Eine abschließende Lösung ist oft nicht sofort möglich, da die Systeme in Betrieb sind und beispielsweise komplexe Grid-Jobs nicht abgebrochen werden sollen. Hier kann folglich Kontakt mit den Ausführenden der Jobs aufgenommen werden. Meist ist es im Interesse der Nutzer und daher ist abzuwägen, ob laufende Jobs abgebrochen werden sollen, um direkt mit einer Eindämmung zu beginnen. Auf diese Weise könnten Nutzerdaten nicht weiter geschädigt/ungewollt verbreitet werden.

Eindämmungsmaßnahmen teilen sich in Maßnahmen, die das System betreffen, wie

- Entfernen gehosteter Daten (Malware, Warez),

- Sperren kompromittierter lokaler Accounts, Auschluss aus *gridmap-file*s und (X)UUDBs, in letzter Instanz widerrufen von Grid-Zertifikaten falls diese betroffen sein könnten
- Abschalten angegriffener / gefährdeter Dienste, Systeme
- Oberflächliches Säubern des Systems mit Virenscannern, Anti-Spyware und Ähnlichem,
- Entfernen erkannter Hintertüren im System

und in Maßnahmen, die das Netzwerk betreffen, wie

- System komplett vom Netz nehmen,
- Beschränken des betroffenen Systems auf ein Quarantänenetz,
- Sperren bestimmter Dienste oder Protokolle,
- Einsetzen eines Rate Limit für bestimmte IP-Adressen oder Protokolle,
- Sperren ausgewählter eigener IP-Adressen.

Kontrolle gewinnen

Wurde der Vorfall grundsätzlich eingedämmt, muss im Weiteren festgelegt werden, wie wieder volle Kontrolle über das System gewonnen werden kann. Je nach Vorfall bedeutet dies oft eine Neuinstallation aller betroffenen Systeme, um sichergehen zu können, dass alle potentielle Schadsoftware vollständig entfernt worden ist.

Eine Neuinstallation wird möglichst in einer entsprechend geschützten Umgebung (idealerweise offline) durchgeführt, so dass der vorherige Angreifer nicht direkt wieder (z. B. über eine alte Schwachstelle) in das System einbrechen kann. Alle Sicherheitsupdates müssen gemacht werden und außerdem sollte eine möglichst starke Härtung des Systems vorgenommen werden, um in Zukunft die Zahl möglicher Angriffspunkte gering zu halten.

Reporting

Wurde das Sicherheitsproblem gelöst, das System wieder in Betrieb genommen und eine eventuelle Downtime-Meldung revidiert, sollte der Sicherheitsvorfall nachbereitet werden. Es ist festzuhalten, was funktioniert hat, was nicht und was im eigenen Handeln noch verbesserungswürdig ist. Die gewonnen Erkenntnisse sind zuletzt in existierende Notfallpläne einzuarbeiten, um für den nächsten Vorfall besser gewappnet zu sein.

4 Behandlung von Sicherheitsschwachstellen

4.1 Ziel

Diese Vorgehensbeschreibung zeigt, wie mit identifizierten Sicherheitsschwachstellen im Rahmen des D-Grids verfahren werden soll.

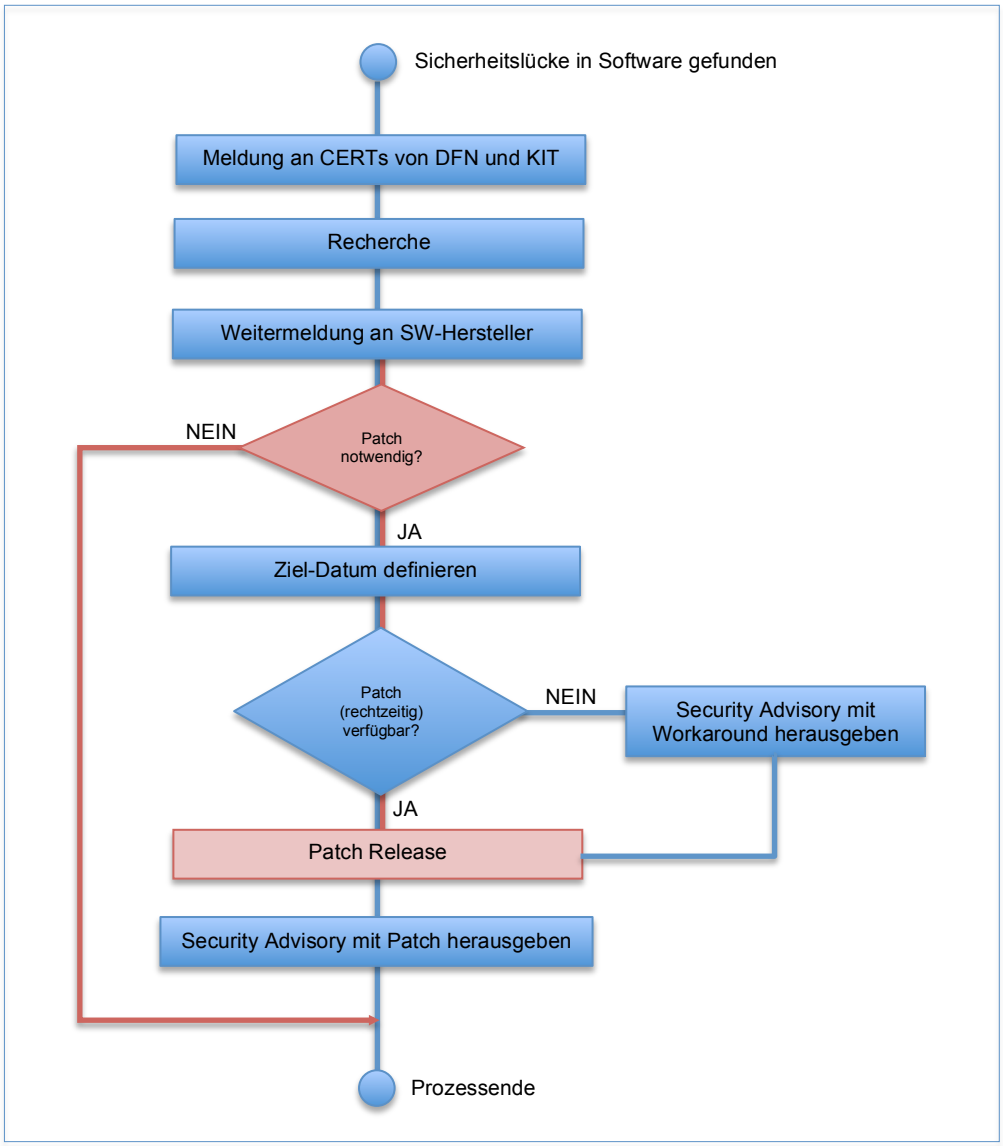
4.2 Beteiligte Personen

- Entdecker der Sicherheitsschwachstelle: Er meldet den Vorfall mit allen beobachteten Details
- DFN-CERT und KIT-CERT übernehmen den weiteren Ablauf

- Software-Hersteller bewertet die Schwachstelle und stellt Patches zur Verfügung

4.3 Ablauf

Gemäß dem Meilensteinbericht „Richtlinie zur Meldung und Bearbeitung von Sicherheitsproblemen bei Software im D-Grid“ wird bei einer Sicherheitslücke in D-Grid Software wie folgt verfahren.
Findet ein D-Grid-Anwender oder ein Site-Administrator eine relevante Sicherheitslücke in einer im D-Grid eingesetzten Software, so tritt folgender Arbeitsablauf in Kraft.



Meldung

Das Sicherheitsproblem wird an die Mailadresse NGI-DE-CSIRT@LISTSERV.DFN.DE gemeldet. Diese Funktionsadresse ist ein Verteiler an die CERTs von KIT und DFN, so dass die im D-Grid-Kontext relevanten Stellen in jedem Fall informiert werden.
Ebenso kann die Hotline des DFN-CERTs (+49 40 808077 590) genutzt werden, welche Administratoren auch bei Grid-spezifischen Sicherheitsfragen und Problemen beratend zur Seite steht.

Die Problemmeldung sollte mindestens folgende Informationen enthalten:
- Genaue Versionsbezeichnung der betroffenen Software
- Systemumgebung (Betriebssystemart und -version)
- Schritte, die zur Entdeckung der Sicherheitslücke geführt haben
- Wenn möglich, Anleitung zur Reproduktion der Sicherheitslücke („Proof of Concept“-Exploit)
- Eigene Einschätzung der Gefährlichkeit
- Kontaktinformationen des Meldenden

Recherche und Weitermeldung

Sobald eine Meldung über die Funktionsadresse NGI-DE-CSIRT@LISTSERV.DFN.DE erfolgt ist, wird die Bearbeitung von den beteiligten CERTs übernommen. Diese ermitteln zunächst die zuständigen Entwickler und melden die gefundene Sicherheitslücke an diese weiter. Die Validierung der Sicherheitslücke in einer Testumgebung gehört nicht zu den Aufgaben des CERT.

Aktionen des Software-Herstellers

Der Software-Hersteller prüft, ob die gemeldete Lücke existiert und sorgt für eine Schließung dieser, entweder durch Hinweise oder notwendige Software-Patches.

Ziel-Datum

Die CERTs beurteilen die Lücke auf ihre Gefährlichkeit und Risiken hin. Entsprechend der Einordnung kann festgelegt werden, wie schnell eine Schließung der Lücke notwendig ist.

Security Advisory oder Workaround

Nach Behebung des Problems wird - koordiniert durch die CERTs in Absprache mit dem Softwarehersteller - ein Security Advisory verfasst und auf dem DFN-CERT Portal (https://portal.cert.dfn.de/adv/) veröffentlicht. Sollte ein Softwarehersteller nicht gewillt oder in der Lage sein, das Problem zu beheben, oder sollte sich das Problem nicht ohne Weiteres/rechtzeitig lösen lassen, so wird ein entsprechender Workaround erarbeitet und veröffentlicht. Veröffentlicht der Software-Hersteller später einen entsprechenden Software-Patch, so wird das Advisory entsprechend aktualisiert.

5 Behandlung kritischer Schwachstellen

Ein Prozess zur Behebung kritischer Sicherheitslücken wie er im EGI existiert (Operational Security Procedures: Critical Vulnerability Handling), kann im D-Grid nicht durchgesetzt werden. Das DFN-CERT gibt Security Advisories heraus, die Site-Betreibern als Informationen bereit stehen.
Die Betreiber sind angehalten sich über neue Sicherheitslücken zu informieren. Es gibt im D-Grid jedoch keinen Weg, um eine Site, die kritische Sicherheitsupdates nicht einspielt, im weiteren Betrieb einzuschränken. So ist es beispielsweise im D-Grid nicht vorgesehen eine Site aus den entsprechenden Informationssystemen (als verfügbare Ressource) zu entfernen, bis vorhandene Lücken geschlossen worden sind.

6 Fazit

In diesem Dokument werden Prozesse dargestellt, die es Ressourcenanbietern, CERTs und entsprechenden Software-Herstellern ermöglicht, auf Sicherheitsprobleme adäquat und schnell zu reagieren. Neben einem Prozess zur Behandlung von Sicherheitsvorfällen wird ebenfalls ein Prozess zur Behandlung und Beseitigung von Sicherheitsschwachstellen dargestellt. Im Rahmen dieses Dokuments werden die an den Prozessen beteiligten Personen/Institutionen definiert und es wird aufgezeigt, wie sich die enge Zusammenarbeit innerhalb der Prozesse darstellt.

Alle an den Prozessen beteiligten Partner verfolgen zwei Hauptziele:

- Minimierung der Auswirkungen eines Sicherheitsvorfalls
- Reduzierung des Risikos von Sicherheitsvorfällen durch die Beseitigung von sicherheitskritischen Software-Schwachstellen

7 Referenzen

[1] B. Henne, C. Kunz, C. Szongott: Richtlinie zur Meldung und Bearbeitung von Sicherheitsproblemen bei Software im D-Grid, Meilensteinbericht M12 DGI-2 Phase 2

[2] DGI-2: Betriebskonzept für die D-Grid Infrastruktur, Version 2.1 Draft, 13.01.2012, http://www.d-grid.de/fileadmin/user_upload/documents/Kern-D-Grid/Betriebskonzept/D-Grid-Betriebskonzept.pdf

[3] CSIRT Description for DFN-CERT (RFC 2350), 20.01.2012, http://www.dfn-cert.de./en/rfc2350.html