

Bericht über die Forumsentführung

Vorabversion

Verfasst vom

IT-Team der Piratenpartei Deutschland: <https://wiki.piratenpartei.de/IT>

betrifft den Vorfall vom 13.02.2010

Andreas Gockel
Christoph Löhr
Sebastian Mohr
Rüdiger Pretzlaff
Jan Marten Simons
Hanno Wagner

Inhaltsverzeichnis

Executive Summary.....	1
Ausgangssituation.....	1
Aktionen der AG Forum	2
Motivation.....	2
Vorbereitungen.....	2
Entführung.....	2
Sicherheitslücken des neuen Servers.....	3
Aktionen der IT.....	3
Technischer Rückumzug.....	3
Stellungnahmen im Forum.....	4
Aktueller Zustand des Forums.....	4
Administration.....	4
Jürgen Neuwirth.....	4
Dominique Schramm.....	4
Arvid Dörwald.....	5
Vorschlag Neustrukturierung Forum.....	5
Abschließende Anmerkungen aus der IT.....	5
Referenzen.....	6

Executive Summary

Das Forum wurde in der Nacht von Freitag auf Samstag von der Bundes-IT-Infrastruktur entwendet. Das Forum wurde nach Verhandlungen seitens der IT am Samstag wieder zurückgeholt. In den anschließenden Ermittlungen wurde Jürgen Neuwirth, mit Beihilfe von Dominique Schramm, als ausführende Person festgestellt. Jedoch wurde die gesamte Aktion von der AG Forum getragen, namentlich stellten sich Jürgen Neuwirth (I need Money, June), Arvid Doerwald (Arvid), Kyra Anisimov (Kyra), Dominique Schramm (NetAndroid), André Reichelt (AndreR), Thomas Gaul (ThomasG), Monika Belz (Miriam) und Marco König (Sensemann) hinter die Aktion.

Ausgangssituation

Das Forum der Piratenpartei ist eines der ältesten Kommunikationsmedien die die Partei hat. Es lief seit der Gründung der Piratenpartei auf der Hardware, die explizit von der Piratenpartei gemietet wurde; die Daten waren immer unter der Kontrolle der Piratenpartei bzw. von deren IT.

Innerhalb des Forums hat die IT keine weitergehenden Rechte; das Forum wird von den Administratoren und Moderatoren selbst verwaltet.

Einige Forenadministratoren (Jürgen Neuwirth und Dominique Schramm) hatten für die Erfüllung ihrer Aufgaben Shellzugriff auf diesem Rechner (erstellen neuer Indizes).

Arvid Dörwald wurde als stellvertretender Administrator geführt. Im Forum waren zwar Administrationsrechte nicht sichtbar, aber er schien sie zu haben[1]. Shellzugriff auf den Rechner hatte er allerdings nicht.

Die IT hat regelmäßig Backups des Forums gemacht - einerseits Datenbankdumps, andererseits Backups der Forensoftware. Das Forum liegt auf einem VServer, welcher hochverfügbar erstellt wurde. Es ist geplant, das Forum (wie jeden anderen Dienst, den die IT anbietet) auf eine eigene KVM-Instanz zu ziehen, da sich diese als für uns verlässlicher herausgestellt haben.

Aktionen der AG Forum

Motivation

Die hier getroffenen Aussagen sind die Interpretation der Situation, die die IT vorgefunden hat. Die AG Forum kann dies anders sehen!

Die Administratoren und Moderatoren der AG Forum waren seit Mitte 2009 in Aufregung und Sorge, da zu dem Zeitpunkt laut Ihrer Sicht nicht klar genug geäußert wurde, dass das Forum weiterhin bestehen bleibt. Es gab zwar eine Vorstandsempfehlung, das Forum zu schließen, allerdings wurde dieser Beschluß zwei Wochen später aufgehoben. Sie leben in permanenter Unsicherheit und Furcht, dass das Forum geschlossen wird. Gegenteilige Aussagen wurden ignoriert (*FIXME*: Protokoll BuVo wo das drinsteht laut Jens?), Protokolle wurden fehlinterpretiert.

Allerdings wurde auch nie bei den entsprechenden Gruppen (BuVo, IT) nachgefragt, sondern sich auf die eigene Interpretation verlassen. Aus Ihrer Sicht war seit Juni 2009 das Forum von einer Löschung bedroht, sie agieren in permanenter Angst vor dieser Situation.

Vorbereitungen

Innerhalb der AG Forum gab es Diskussionen, wie man mit der Situation umgeht, was Jürgen und Arvid in ihren Erklärungen unabhängig voneinander bestätigen. Es entstand der generelle Plan, das Forum umzuziehen, bevor die Löschung akut wird. Dafür wurden Spenden in der AG Forum gesammelt (siehe Punkt 7 von Arvid, 3. und 4. Absatz von Jürgen), um einen eigenen Server bei einem alternativen Anbieter anzumieten, und um eine eigene Domain zu registrieren. Diese Domain sollte möglichst ähnlich wie der jetzige Name sein (forum.piratenpartei.de). Es wurde frühzeitig die Domain „forum-piratenpartei.de“ registriert (letzte Änderung am 09.02.2010).

Auf dem angemieteten Server wurde von Dominique Schramm in einer Aussage gegenüber Sebi, Chrit und Rince, ein LAMP (Linux, Apache, MySQL, PHP)-System auf Basis von Debian Lenny installiert, wobei ein privater Debian-Mirror als Grundlage diente.

Diese Vorbereitungen und Pläne wurden unseres Wissens nur innerhalb der AG Forum besprochen, weder die Benutzer des Forums noch die IT wurden in die Planung einbezogen.

Entführung

Nachdem Hardware und Software fertiggestellt waren, wurde der Umzug durchgeführt. Dafür wurde durch Jürgen Neuwirth ein Dump der Datenbank auf Shellebene erstellt, ebenso wie ein Archiv der Forumsdateien.

Diese Daten wurden unverschlüsselt in den öffentlich verfügbaren Teil des Foren-Webservers gelegt. Von dort konnten diese Daten von jeder Person heruntergeladen werden, die zufällig in dieses Verzeichnis schaute; eine Authentisierung via Username+Passwort gab es nicht.

Nachdem die Daten via sicherer Verbindung (https) heruntergeladen wurden, wurden von Jürgen Neuwirth auf den Servern der IT die entsprechenden Daten gelöscht - das Forum wurde per „rm“ gelöscht, die Forums-Datenbank wurde ebenfalls geleert.

Als letzter Schritt wurde via .htaccess-Datei eine Umleitung eingebaut, die jeden Besucher, der auf „http://forum.piratenpartei.de/“ oder „https://forum.piratenpartei.de/“ wollte, auf „http://forum-piratenpartei.de/“ schickte.

Innerhalb des Forums gab es auf dem neuen Server personelle Veränderungen; Arvid Dörwald wurde offiziell zum Administrator ernannt; er war somit nicht mehr Ersatzadministrator.

Sicherheitslücken des neuen Servers

Der neue Server des Forums hat aus Sicht der IT einen Sicherheitsstandard, der nicht dem unseren entspricht:

- Der Root-Zugriff ist von überall aus möglich gewesen, es gab eine Passwort-Authentisierung, keine ausschließliche Authentisierung durch SSH-Keys
- Auf allen virtuellen Maschinen wurde zudem das selbe Paßwort benutzt
- Es gab kein Backup-Konzept für die Daten, beim Ausfall des RAID-Systems wären sämtliche Daten verloren gewesen
- Es gab keine Failoverlösung bzw. Ersatzhardware, falls dieser Rechner ausfiel
- Der virtuelle Server mit den MySQL-Daten war von außen erreichbar via ssh.
- Das Forum lief nun ausschließlich über unverschlüsselte Verbindungen - einen https-Zugriff, wie ihn die IT bereitgestellt hat, gab es nicht.

Aktionen der IT

Uns wurde der Umzug erst bekannt, als wir am Samstag morgen um 09:48 eine Mail bekamen mit dem Hinweis, dass das Forum nun unter einer neuen Domain laufen würde; gepaart mit der Frage, ob dies mit uns abgesprochen war.

Wir haben diese Aussage überprüft und festgestellt, was geschehen ist (siehe „Entführung“).

Unser nächstes Ziel war, die Wiederherstellung des vorigen Zustands (Forum auf Hardware der IT), lückenlose Aufklärung und der Versuch, die Aussenwirkung der Partei zu wahren.

Dafür haben wir versucht alle uns bekannten Administratoren (Arvid Dörwald, Dominique Schramm, Jürgen Neuwirth) telefonisch zu erreichen und in einer Telefonkonferenz zu klären, was geschehen ist. Es wurde bei diesen Gesprächen bereits auf die rechtlichen Probleme hingewiesen, die aus dieser Migration resultierten.

Im Zuge dieser Telefonkonferenzen konnte herausgearbeitet werden, wer welchen Schritt bei der Migration gemacht hat; der IT wurden die Zugangsdaten zu dem neuen Server gegeben, um eine Rück-Migration in die Wege zu leiten.

Technischer Rückumzug

Ziel der Migration war nicht nur eine Rück-Migration der Daten, sondern auch eine forensische Untersuchung, ob und was genau an den Daten verändert wurde und die Sicherstellung, dass auf dem Gastrechner keine Daten der Piratenpartei wiederhergestellt werden können.

Dafür wurden erst die Datenbank und das Forum gesichtet, um einen Überblick über den Ist-Zustand zu verschaffen.

Um einen konsistenten Zustand zu migrieren wurde der Webserver heruntergefahren und ein Datenbank-Dump erstellt. Dieser wurde via verschlüsselter und authentisierter Verbindung (scp) auf die eigene Hardware übertragen.

Die Daten und die Forenapplikation wurden auf der IT-eigenen Hardware eingespielt und überprüft. Erst hiernach wurde das Forum wieder freigegeben für alle Forenbenutzer.

Die gesamten Daten der virtuellen Instanz wurden zusätzlich für weitere Untersuchungen gesichert.

Um eine unbeabsichtigte Weitergabe der Daten zu verhindern, wurden auf der (IT-externen) Gastmaschine alle Festplatten mehrfach überschrieben (wipe); die Konfiguration der Festplattensysteme und das Betriebssystem wurden gelöscht.

Stellungnahmen im Forum

Im Forum ist Samstag morgen eine Stellungnahme von Arvid zu lesen, in der die Akteure darlegen, warum aus Ihrer Sicht diese Migration notwendig war[3]. Innerhalb der darauf sich entwickelnden Diskussion wird klar, dass die Benutzer nicht glücklich über diesen Umgang mit der Basis sind[3a][3c][3d][3e]; sie wundern sich auch über den neuen Status von Arvid[3b].

Nach der Rück-Migration gibt es eine weitere Stellungnahme (diesmal von Jürgen Neuwirth), in der er seine Sicht darstellt[4]. Diese aus unserer Sicht einseitige Darstellung (auch, weil sie im Unterforum „Ankündigungen der AG“ erschien) erregte die Aufmerksamkeit diverser Blogs und anderer Medien (FIXMBR[5], Fefe[6], Spiegel Online[7]).

Mit ThomasG wurde Samstag abend noch vereinbart, eine gemeinsame Telefonkonferenz der AG Forum und der IT zu machen, geplant wurde Sonntag abend ab 19 Uhr, zusammen mit einem Moderator.

Diese Telefonkonferenz fand auch statt[8], die IT wollte hauptsächlich eine De-Eskalierung der Situation erreichen um eine Situation zu bekommen, in der eine sachliche Diskussion möglich wäre.

Aktueller Zustand des Forums

Das Forum läuft wieder auf der IT-Hardware und ist ins Sicherungskonzept mit eingebunden. Damit ist eine Hochverfügbarkeit, ein regelmäßiges Backup der Daten und auch die Erreichbarkeit des Forums via verschlüsselter und authentisierter Verbindung (https) gegeben.

Administration

Die Administration des Forums wurde nach einer weiteren Eskalation der Situation (Administratoren des Forums waren in der Lage, Datenbankdumps via Web-Interface der Forensoftware zu erstellen und zu bekommen) verändert.[9]

Aktuell haben nur zwei Mitglieder der IT auf dem Forum Administrationsrechte; alle anderen Administratoren sind aus Sicherheitsgründen zu normalen Benutzern „zurückgestuft“ worden.

Jürgen Neuwirth

Seine Administrationsrechte auf Forums- und Shellebene wurden entzogen, da er den Dump erstellt hatte, welcher auf den externen Gast-Rechner übertragen wurde. Er hat diesen auch auf den Webserver gelegt, da er der einzige eingeloggte User mit Zugriffsrechten zum fraglichen Zeitpunkt war[b1]. Er hatte die Möglichkeit, via Webinterface Dumps zu erstellen, hat diese allerdings wahrscheinlich nicht genutzt.

Dominique Schramm

Seine Administrationsrechte auf Forumsebene und Shellebene wurden ebenfalls entzogen. Er hat sein Amt nach dem Rück-Umzug (und der entsprechenden Rückfragen) niedergelegt und um Löschung aus der Admingruppe gebeten.

Er hat über den offiziellen Piratenpartei-Twitteraccount Falschmeldungen gegen Mitglieder der IT versandt, welches zu einer weiteren Eskalation der Situation führte. Auch dieses wurde in der Blogosphäre kommentiert.[10]

Arvid Dörwald

Arvid hat das erste Statement der Administration nach dem Umzug veröffentlicht und scheint aus unserer Sicht eine der treibenden Kräfte hinter der Migration zu sein. Er hat seine Administrations-Tätigkeit nach der Telefonkonferenz am Sonntag abend temporär bis zum 22.02.2010 niedergelegt.

Auf dem neuen Server war er nicht mehr nur Moderator sondern Administrator auf dem Forum; dies war vorher nicht der Fall. Auch ihm wurden alle Administrations-Rechte entzogen.

Vorschlag Neustrukturierung Forum

Nachdem ein Teil der Forumsadministration einen Nachbarschaftsstreit gleicht, ist unser Vorschlag, dass die Rolle der Administratoren und Moderatoren neu definiert wird und eine Regelung zur Löschung oder Änderung von Postings getroffen wird.

Unserer Meinung nach sollte es eine strikte Trennung der technischen Administration des Forums und der inhaltlichen Moderation der Beiträge geben.

Die technische Administration des Forums sollte von Mitgliedern der IT durchgeführt werden, welche aber im Forum selbst keinerlei weitergehenden Rechte haben.

Die inhaltliche Moderation des Forums erfolgt durch „Globale Moderatoren“, die auf allen Unterforen gleichen Rechte haben.

Diese Moderatoren sollten bei Streits neutral sein, keine Posts ändern, sondern höchstens rechtlich problematische Postings in einen gesperrten Bereich verschieben und den Poster bitten, das Posting neu zu formulieren.

Abschließende Anmerkungen aus der IT

Während der gesamten Situation war für uns nicht zu erkennen, dass die Mitwirkenden bereit waren, die Problematik vor und mit der Migration lückenlos aufzuklären. Für uns ist bisher nicht zu erkennen, dass Jürgen Neuwirth und Arvid Dörwald ihre Fehler einsehen oder akzeptieren, dass sie überzogen gehandelt haben. Stattdessen wird seitens Arvid Dörwalds gegen die IT oder den Bundesvorstand gewettert (vorgegangen/polemisch geschrieben)[11], was auch an alle Forennutzer per E-Mail geschickt wurde. Es gibt im Forum auch Falschaussagen der Beiden. Es ist bisher keine Bereitschaft zu erkennen, dass diese Aktion weder gut für die Partei noch für das Forum war. Ihre Argumentation „Wir haben es für die Partei und die Mitglieder des Forums getan“ lässt sich weder beweisen noch wurde vorher versucht, die Meinung der Nutzer des Forums zu befragen. Stattdessen wird versucht durch ihre Darstellung und Angriffe gegen die IT von ihren eigenen Fehlern abzulenken.

Es blieben einige Fragen offen, wie die Migration von den Servern der Piratenpartei weg durchgeführt wurde. Auf die Frage ob der Zugriff auf den erstellten Datenbankdump in irgendeiner Form geschützt war, konnte er nicht sofort antworten; erst als jemand anderes das Stichwort „.htaccess-Datei“ einwarf hat er sich darauf berufen. Diese Datei wurde allerdings erst später gebraucht, um die Umleitung auf die neue Foren-Seite zu erstellen, ob damit auch der Zugriff auf den Dump geschützt wurde können wir nicht beurteilen.

Wie bereits gezeigt ist Jürgen Neuwirth der einzige Administrator mit Shellzugriff auf den Forums-Server, der zum Tatzeitpunkt eingeloggt war. Er war damit der einzige Forenadministrator, der diesen Dump auf Shellebene durchführen konnte. Nur mit seiner Hilfe konnte das Forum so schnell umziehen.

Das die IT so schnell und stark reagiert hat, lag einerseits daran, dass es vor dieser Migration keine Kommunikation seitens der AG Forum gab - weder wurde um Unterstützung gebeten, noch wurde angefragt, warum das Forum im Migrationsplan nicht erwähnt wurde. Stattdessen wurden wir mit den Tatsachen konfrontiert, dass (Nutzer-)Daten unrechtmäßig von den Servern der IT kopiert und auf diesen Servern gelöscht wurden. Dieser Zustand sollte so schnell wie möglich aufgelöst werden. Ob den Unterzeichnern der entsprechenden Erklärung[12] die rechtliche Problematik bewusst ist, ist uns nicht bekannt, ebensowenig wie das im Forum veröffentlichte gemeinsame Schuldeingeständnis eines der Unterzeichner[13].

Referenzen

- [1]: http://wiki.piratenpartei.de/index.php?title=AG_Forum&diff=360378&oldid=359896
- [2]: http://wiki.piratenpartei.de/index.php?title=AG_Forum&diff=next&oldid=535504
- [3]: <http://forum.piratenpartei.de/viewtopic.php?f=1&t=17252#p219620>
- [3a]: <http://forum.piratenpartei.de/viewtopic.php?f=1&t=17252#p219665>
- [3b]: <http://forum.piratenpartei.de/viewtopic.php?f=1&t=17252#p219658>
- [3c]: <http://forum.piratenpartei.de/viewtopic.php?f=1&t=17252#p219670>
- [3d]: <http://forum.piratenpartei.de/viewtopic.php?f=1&t=17252&start=15#p219719>
- [3e]: <http://forum.piratenpartei.de/viewtopic.php?f=1&t=17252&start=15#p219721>
- [4]: <http://forum.piratenpartei.de/viewtopic.php?f=133&t=17283>
- [5]: <http://www.fixmbr.de/wie-die-piratenpartei-mit-den-daten-ihrer-forennutzer-umgeht/>
- [6]: <http://blog.fefe.de/?ts=b5869765>
- [7]: <http://www.spiegel.de/netzwelt/web/0,1518,677884,00.html>
- [8]: <http://forum.piratenpad.de/fotos>
- [9]: E-Mail von Jamasi an die Aktiven-Mailingliste:

--- 8< --- 8< --- 8< ---

Da wir (IT) befürchten müssen, daß der bisherige Administrator des Forums (Jürgen N.) aktuell noch einen Daten-Dump des Forums über die eingebaute Funktionalität der Forensoftware anzufertigen plant, bevor wir auch dort seinen Zugriff sperren können, haben wir zum Schutz der Nutzerdaten als Notfallmaßnahme das Forum vorerst abgeschaltet. Nachdem wir dem entsprechenden Account die Rechte entzogen haben, werden wir das Forum wieder online schalten.

Wir bitten die Unannehmlichkeiten zu entschuldigen, aber nach den schlechten Erfahrungen am Wochenende sehen wir uns leider zu dieser Maßnahme genötigt.

Gruß,

Jan (jamasi)

Bundes-IT // Technikpirat im Bundesvorstand

--- 8< --- 8< --- 8< ---

- [10]: <http://www.fixmbr.de/piratenpartei-jeder-gegen-jeden/>
- [11]: <http://forum.piratenpartei.de/viewtopic.php?f=133&t=17384>
- [12]: <https://forum.piratenpartei.de/viewtopic.php?t=17386>
- [13]: <https://forum.piratenpartei.de/viewtopic.php?f=1&t=17386&start=15#p221760>

```
[b1]:root@rackham-d:/# last | grep juergen | grep " 1[23] "  
juergen pts/20          pd9e426a3.dip0.t Sat Feb 13 11:46 - 14:23 (02:37)  
juergen pts/4          pd9e418db.dip0.t Sat Feb 13 01:30 - 01:49 (00:18)  
juergen pts/4          pd9e418db.dip0.t Sat Feb 13 00:52 - 01:07 (00:15)  
juergen pts/20          pd9e418db.dip0.t Sat Feb 13 00:09 - 01:08 (00:59)  
juergen pts/10          pd9e418db.dip0.t Sat Feb 13 00:07 - 01:02 (00:55)  
juergen pts/10          pd9e418db.dip0.t Fri Feb 12 19:38 - 20:02 (00:23)  
juergen pts/10          pd9e418db.dip0.t Fri Feb 12 19:21 - 19:37 (00:15)  
juergen pts/10          pd9e418db.dip0.t Fri Feb 12 14:33 - 14:33 (00:00)  
juergen pts/10          pd9e418db.dip0.t Fri Feb 12 11:09 - 12:02 (00:53)  
juergen pts/4          pd9e418db.dip0.t Fri Feb 12 10:26 - 11:27 (01:01)  
juergen pts/22          pd9e41224.dip0.t Fri Feb 12 00:09 - 00:36 (00:26)  
root@rackham-d:/# last | grep netandroid
```