Leibniz-Rechenzentrum München

Mein Rechner ist geknackt: Was tun?*

Petra Eilfeld**

29.9.2003

Inhaltsverzeichnis

*http://www.lrz-muenchen.de/services/security/angriff/

**http://www.lrz-muenchen.de/persons/petra_eilfeld.html

Hacker-Angriffe treten zunehmend häufiger auf und werden zugleich wirkungsvoller, da frei verfügbare Hacker-Tools immer effektiver und leichter zu bedienen werden und damit auch von Personen mit minimalem Know-How ("Script-Kiddies") angewendet werden können. Parallel dazu nimmt die Zahl und "Mächtigkeit" der Viren und Würmer ebenfalls kontinuierlich zu. Als Folge davon ist die Sicherheits-Problematik inzwischen schon so bedeutend, dass sie sowohl in der aktuellen Tages- und Wochen-Presse als auch im Fernsehen diskutiert wird.

Das Leibniz-Rechenzentrum[1] *(LRZ) möchte Sie deshalb mit dieser Schrift informieren, was Sie im Falle eines* **erfolgreichen Angriffs** *selbst tun können. Noch besser wäre es jedoch, sich schon im Vorfeld auf Angriffe vorzubereiten.*

Achtung!
Diese Schrift **behandelt nicht die Vermeidung** *von erfolgreichen Angriffen, was natürlich in jedem Fall vorzuziehen wäre. In diesem Zusammenhang verweisen wir auf das Informations-Angebot*[2] *des LRZ und speziell auf die Schrift*

Wie mache ich meinen Rechner sicherer ? – Ein paar 'Bauernregeln[3]

1 Motivation

 1

Da Sie dieses Dokument gerade lesen, müssen Sie sehr wahrscheinlich nicht mehr davon überzeugt werden, dass Security[4] wichtig ist; sehr wahrscheinlich trifft im Augenblick (mindestens) eines der folgenden Motive für Sie zu:

- Ihr Rechner ist gerade das Ziel eines Angriffs (bzw. Sie befürchten dies):
  Dann wissen Sie spätestens jetzt, dass es sinnvoll gewesen wäre, sich schon früher mit dem Thema "Sicherheit" zu befassen.

- Sie wollen sich informieren, wie Sie sich auf den Worst-Case vorbereiten können:
  Wenn Sie nicht schon Sicherheits-bewußt wären, würden Sie wohl kaum dieses Dokument ohne konkreten Anlass lesen.

Möglicherweise versuchen Sie aber auch Kolleg(inn)en, Vorgesetzte etc. von der Wichtigkeit der System-Sicherheit zu überzeugen. Dann finden Sie im Dokument "Warum ist Security wichtig ?[5]" einige Argumente dafür. Dort werden folgende Fragen näher behandelt:

- Was auch Ihnen passieren könnte ![6]
- Warum ist System- und Netz-Sicherheit so wichtig ?[7]
- Warum haben Hacker oft besonders leichtes Spiel ?[8]
- Warum ist die Anzahl der Angriffe so angestiegen ?[9]

[1] `http://www.lrz-muenchen.de/`
[2] `http://www.lrz-muenchen.de/services/security/`
[3] `http://www.lrz-muenchen.de/services/security/sec-thumbrules/`
[4] `http://www.lrz-muenchen.de/services/security/motivation/#begriff`
[5] `http://www.lrz-muenchen.de/services/security/motivation/`
[6] `http://www.lrz-muenchen.de/services/security/motivation/#bsp`
[7] `http://www.lrz-muenchen.de/services/security/motivation/#motivation`
[8] `http://www.lrz-muenchen.de/services/security/motivation/#leichtes-spiel`
[9] `http://www.lrz-muenchen.de/services/security/motivation/#angriffe`

- Begriffs-Bildung: Was ist der Unterschied zwischen "Sicherheit" und "Security" ?[10]
- Welche Sicherheits-Dienste bietet das LRZ ?[11]

2 Vorbereitungen auf einen Angriff

 2

Schon im Vorfeld sollten Sie einige Vorbereitungen auf einen Angriff treffen:

- Einige Aktionen können Sie *prinzipiell* nur durchführen, solange Ihr Rechner noch "sauber" ist.

- Ein geknackter Rechner bedeutet viel weniger Stress für Sie, wenn Sie dann schon genau wissen, was Sie in diesem Fall zu tun haben.

Wie sollten Sie sich also am besten vorbereiten ?

- Sorgen Sie *kontiniuerlich* für einen jeweils **aktuellen Backup** Ihrer Daten!

  Ist der eigene Rechner geknackt, ist es nämlich oft am einfachsten, den Rechner neu zu installieren. Dies setzt aber eine funktionierende Datensicherung voraus.

 3

- Wenn Sie sich schon intensiver mit dem Thema "Security" beschäftigt haben, sollten Sie sich folgende Frage stellen:

  ≫*Habe ich ausreichend Zeit und Selbst-Disziplin, um einen* **regelmäßigen Integritäts-Check** *meines Rechners durchzuführen?*≪

  Mit Integritäts-Checkern[12] will man erkennen, ob Dateien (Inhalt und/oder Eigenschaften) verändert wurden. Diese Tools kosten zwar Aufwand, sind aber eine wertvolle Warn-Einrichtung. Außerdem ersparen sie nach einem Angriff auch manchmal eine Neu-Installation, da man ja erkennen kann, was genau vom Angreifer im eigenen Rechner verändert wurde. Im Ideal-Fall reichen dann folgende Teil-Schritte aus:

  - Entfernen der "Hinterlassenschaften" des Angreifers (z.B. eine "Hintertür").
  - Evtl. Nach-Installation von System-Komponenten aus dem Backup, die der Angreifer verändert oder gelöscht hat.
  - Einspielen der aktuellen Security-Patches (auch bekannt als "Security-Hot-Fixes" oder "Security-Updates"). Eigentlich hätte dies schon vorsorglich erfolgen sollen (dann wäre der Einbruch bzw. die Viren-/Wurm-Infektion auch möglicherweise verhindert worden).

- Entwerfen Sie **Richtlinien**[13] (Policy) dafür, wie Ihre Reaktion auf einen Angriff aussehen soll.

- Entwickeln Sie ein *detailliertes* Konzept[14] ("Kochrezept"), wie nach einem Angriff der Produktions-Betrieb wiederhergestellt wird.

3 Richtlinien für die Behandlung eines Angriffs

 4

Die (möglichst knappen) **Richtlinien (Policy)** für die Behandlung eines Angriffs beschreiben nur die *prinzipiellen* Regeln, Vorgehensweisen etc. Da die Policy eine größere Tragweite haben kann, sollte sie zumindest von der/vom Vorgesetzten abgesegnet werden; noch besser ist es, wenn die Policy vom Lehrstuhl, dem Institut etc. verabschiedet wird.

Aus diesem Grunde sollte die Policy relativ lange gültig sein können und nicht häufig an technische und/oder organisatorische Änderungen angepasst werden müssen. Sie erreichen dies dadurch, dass Sie in die Policy explizit keine technischen und/oder organisatorischen Details mit aufnehmen; derartige Informationen sind dann Bestandteil eines Vorgehens-Konzepts.

Beim Erarbeiten einer Policy sollten Sie sich u.a. mit folgenden Fragen auseinandersetzen:

- Natürlich interessiert es Sie wahrscheinlich, was genau der Angreifer auf Ihrem Rechner gemacht hat. Doch: *Wieviel Aufwand ist Ihnen eine derartige Analyse wert?*

  Ziehen Sie dabei in Betracht, dass selbst erfahrene Spezialisten mit den entsprechenden Analyse-Tools für eine *ausführliche* Analyse eines *einzigen* Rechners 3 - 10 Arbeitstage veranschlagen.

- *Sollen Beweise für die Aktivitäten des Angreifers gesichert werden?*
  Evtl. sogar Gerichts-verwertbar?

  Auch die Beweis-Sicherung kann sehr aufwändig sein; dies gilt besonders dann, wenn die Beweise für ein evtl. folgendes Strafverfahren brauchbar sein sollen/müssen.

- *Soll der Angreifer ermittelt werden?*
  Wieviel Aufwand darf eine derartige Ermittlung kosten?

  Erfahrungsgemäß ist die Ermittlung des Angreifers ohne die Einschaltung von Spezialisten und/oder Strafverfolgungsbehörden praktisch aussichtslos bzw. nur durch einen glücklichen Zufall möglich. Ihnen sollte jedoch klar sein, dass eine Ermittlung einen sehr großen Aufwand kostet und deshalb nur in extrem schweren Fällen vertretbar ist.

- *Wer soll/muss nach einem Angriff informiert werden?*
  - Kolleg(inn)en?
  - Vorgesetzte?
  - Eigene Benutzer(innen)?
  - LRZ?
  - DFN-CERT[15]?
  - Strafverfolgungsbehörden?

  Welche Informationen sollen dabei jeweils weitergegeben werden?
  Erhalten alle die gleichen Informationen oder wird nach Empfänger-Gruppe unterschieden?

[10] `http://www.lrz-muenchen.de/services/security/motivation/#begriff`
[11] `http://www.lrz-muenchen.de/services/security/lrz-dienste/`
[12] `http://www.lrz-muenchen.de/services/security/links/#integrity`
[13] siehe  4 auf Seite 4
[14] siehe  5 auf Seite 7
[15] `http://www.lrz-muenchen.de/services/security/dfn-cert/`

- *Wie soll der Produktions-Betrieb beim geknackten Rechner wiederhergestellt werden?*

  Es gibt dabei folgende prinzipielle Vorgehensweisen:

  – Sie versuchen, auf dem Rechner die Spuren des Angreifers zu beseitigen.
  Dies kann jedoch sehr aufwändig sein. Außerdem stellt sich dann sofort folgende Frage:

  ≫*Kann ich mir sicher sein, dass ich nicht eine vom Angreifer eingebaute Hintertür, Zeitbombe etc. bei der Säuberung übersehe?*≪

  Diese Frage können Sie i.a. nur dann guten Gewissens mit "Ja" beantworten, wenn Sie

  * einen *"sauberen" identischen* Vergleichs-Rechner besitzen.
  * regelmäßig einen Integritäts-Check[16] bei Ihrem Rechner durchgeführt haben.

  – Sie installieren den Rechner ohne grosses Nachdenken einfach neu und spielen danach die *aktuellen Security-Patches* für Ihr Betriebssystem, Ihre Spezial-Anwendungen, Ihre Benutzerdaten etc. ein.

  Bei geeigneter Vorbereitung kostet diese Vorgehensweise oft viel weniger Aufwand als die vorhergehende Variante.

  Selbst wenn man weiß, was genau der Angreifer mit dem eigenen Rechner gemacht hat, bleibt einem dennoch oft nur die Neu-Installation:
  Durch den Vorfall hat man nämlich z.B. herausgefunden, dass das Betriebssystem des eigenen Rechners schon so alt ist, dass der Hersteller es nicht mehr unterstützt und deshalb auch keine Security-Patches mehr dafür bereitstellt.

  Außerdem ist ein *standardisiertes Verfahren*, mit dem Rechner einfach neu installiert werden können, auch bei der normalen Systemverwaltung sehr hilfreich und kann dort viel Arbeit einsparen.

- *Welche weitergehenden Aktionen sind noch erforderlich?*

  Weitere Aktionen sind i.a. nur dann notwendig, wenn Ihr Rechner von mehreren Personen genutzt wird oder wenn der Rechner zu einer Gruppe von Rechnern gehört, die vom selben Personen-Kreis genutzt wird (z.B. alle Rechner eines Lehrstuhls oder die Rechner in einem Pool):

  – Auf jeden Fall sollten *alle Benutzer(innen)* des geknackten Rechners *so schnell wie möglich sämtliche Passwörter* ändern.
  Der Angreifer hätte ja alle eingegebenen Passwörter mitprotokollieren können.

  Ist der geknackte Rechner in ein lokales Netz eingebunden, so sollten auch alle Benutzer(innen) in diesem Verbund ihre sämtlichen Passwörter ändern.
  Der Angreifer hätte ja einen sogenannten Sniffer installieren können, mit dem man alle Passwörter abhören kann, die im Klartext übers Netz gehen (heutzutage leider noch viel zu oft der Fall).

  – Gibt es in der Arbeits-Gruppe, im Rechner-Pool etc. noch weitere Rechner, die ähnlich wie der geknackte Rechner ausgestattet sind, sollten Sie auch auf diesen Rechnern die aktuellen Security-Patches einspielen; diese Rechner haben nämlich sehr wahrscheinlich die gleichen Sicherheits-Lücken wie der geknackte.

[16] siehe ☜ 3 auf Seite 3

– Sie sollten jedoch noch einen Schritt weiter gehen und *prinzipiell alle* Rechner ihrer Arbeits-Gruppe, des Rechner-Pools etc. auf verdächtige Spuren oder Vorkommnisse hin näher untersuchen.
Selbst wenn die anderen Rechner eine ganz andere Betriebssystem-Version oder sogar -Variante besitzen, kann der Angreifer sie z.B. schon mit Hilfe von abgehörten Passwörtern ebenfalls geknackt haben.

Wie könnte nun eine Policy für die Behandlung eines Angriffs aussehen ?
Hier ein Beispiel, wie es in ähnlicher Form auch beim LRZ verwendet wird:

Primäres Ziel nach einem Angriff ist die *schnelle und dauerhafte Wiederherstellung des Produktions-Betriebs* mit einem *möglichst geringen* Aufwand. Dies hat im *Normalfall* u.a. folgende Konsequenzen (Ausnahmen siehe unten):

- Bei der Analyse des Vorfalls soll vorwiegend herausgefunden werden, durch welche Sicherheits-Lücke der Angreifer eindringen konnte und welche Informationen, Rechte etc. der Angreifer erhalten hat. Für diese Tätigkeit sollen aber nur wenige Stunden aufgewendet werden.
- Beweise sollen nur in dem Umfang gesichert werden, wie es mit geringem Aufwand möglich ist. Dabei wird wegen des andernfalls extrem hohen Aufwands bewusst darauf verzichtet, dass die Sicherstellung Gerichts-verwertbar ist.
- Es wird darauf verzichtet, den Angreifer zu ermitteln und Spezialisten oder Strafverfolgungsbehörden einzuschalten.
- Der Produktions-Betrieb soll mit *demjenigen standardisierten* Verfahren wiederhergestellt werden, mit dem normalerweise die eigenen Rechner neu installiert werden.
- Bei allen ähnlich konfigurierten Rechnern müssen evtl. fehlende Security-Patches eingespielt werden.
Alle Rechner müssen auf verdächtige Spuren etc. näher untersucht werden.

Ausnahmen werden nur in folgenden Fällen gemacht:

- Der Vorfall ist besonders schwerwiegend.
- Die Identität des Angreifers kann ohne großen Aufwand ermittelt werden.
- Es gibt (eindeutige) Hinweise, dass der Angreifer aus dem unmittelbaren lokalen Umfeld kommt.

Folgende Punkte sollen ebenfalls berücksichtigt werden:

- Zumindest der unmittelbare Vorgesetzte muss von dem Vorfall verständigt werden; dieser entscheidet dann über Maßnahmen, die über den Standard-Ablauf hinausgehen.
- Alle durch den Vorfall potentiell betroffenen Benutzer sollen verständigt und intensiv gedrängt werden, sämtliche Passwörter zu ändern.
- Das LRZ erhält eine kurze Mitteilung über den Vorfall; das DFN-CERT wird dann informiert, wenn von dem Vorfall auch andere Organisationen außerhalb des Münchner Wissenschafts-Netzes betroffen sind oder wenn das LRZ dazu explizit rät.

- Der Vorgehensplan für die Reaktion auf Angriffe soll alle relevanten technischen und organisatorischen Details enthalten und regelmäßig aktualisiert werden (mindestens 1-mal pro Jahr; besser noch kontinuierlich parallel zu relevanten Änderungen in der Rechner-Landschaft).

4 Pragmatisches Konzept für die Behandlung eines Angriffs

 5

Wie kann man nun (konkret) nach einem Sicherheits-Problem bzw. einem Angriff den Produktions-Betrieb wiederherstellen ? Hier einige pragmatische Hinweise, was Sie aus Sicht des LRZ auf jeden Fall tun sollten und was keinen großen Zusatzaufwand kostet:

- Nehmen Sie den verdächtigen bzw. geknackten Rechner so schnell wie möglich vom Daten-Netz. Dadurch wird verhindert, dass ein Angreifer ungehindert andere Benutzer und/oder Rechner schädigen kann.

- Sammeln Sie alle Informationen, die bei der Diagnose helfen könnten (seltsame Meldungen, Log-Dateien, verdächtige Dateien etc.), und machen Sie sich auch Notizen über Ihre Beobachtungen.

  Vergessen Sie dabei nicht, die gesammelten Dateien etc. so aufzubewahren, dass diese durch die wahrscheinlich erforderliche Neu-Installation nicht gelöscht werden.

  Sollten Sie den Rechner intensiver nach Einbruchs-Spuren untersuchen wollen, hilft Ihnen dabei möglicherweise auch der Artikel "Intruder Detection Checklist[17]" des "CERT Coordination Center[18]".

- Verständigen Sie Ihre(n) Vorgesetzte(n) von dem Vorfall.

- Schicken Sie bitte per E-Mail[19] eine kurze Zusammenfassung des Vorfalls dem LRZ an folgende Adresse:

  `security@lrz.de`

  Wir können Ihnen wegen fehlender Person-Power zu unserem Bedauern sehr wahrscheinlich nicht direkt helfen, sind aber aus folgenden Gründen an Ihren Erkenntnissen interessiert:

  - Wir sammeln derartige Informationen, um großflächige Angriffe erkennen und dann eine evtl. erforderliche Koordination der Reaktionen übernehmen zu können.

  - Zum Glück stellt sich manchmal heraus, dass ein vermeintlicher Angriff durch ein falsch konfiguriertes Administrations-Tool verursacht wurde. Eine "großflächigere Sichtweise" hilft i.a. dabei, dies erkennen zu können.

  - Einige Angriffe können nur durch die Einbeziehung von Netz-Komponenten (v.a. die Router) näher untersucht bzw. auch einfach abgestellt werden.

  Wir wollen Sie hier ausdrücklich zu *übervorsichtigem* Verhalten ermutigen. Lieber drei Fehl-Alarme zu viel als ein übersehener Einbruch!

[17] `http://www.cert.org/tech_tips/intruder_detection_checklist.html`
[18] `http://www.cert.org/`
[19] `mailto:security@lrz.de?subject=[Vorfall]`

- Sollten Sie Hinweise haben, dass der Angriff von einem Rechner aus dem *M*ünchner *W*issenschafts-*N*etz (MWN) ausging. Schicken Sie bitte eine entsprechende Hinweis-E-Mail[20] an folgende Adresse:

  `abuse@lrz.de`

  Wir nehmen diese E-Mail entgegen und leiten sie an die zuständigen Ansprechpartner(innen) im MWN weiter. Erfahrungsgemäß ist der Rechner, von dem der Angriff ausging, selbst geknackt und die/der Besitzer(in) ist für einen entsprechenden Hinweis sehr dankbar.

  Sie können natürlich auch die Benachrichtung an `security@lrz.de` gleichzeitig mit einer Kopie an `abuse@lrz.de` schicken. Bedenken Sie dann aber bitte dabei, dass die/der Besitzer(in) des anderen MWN-Rechners die selbe Information erhält wie das LRZ.

- Sollten Sie sich nicht sicher sein, ob es sich überhaupt um ein Security-Problem handelt oder sollte eine ganz *akute Notfall-Situation* eingetreten sein, kontaktieren Sie bitte die LRZ-Hotline[21]

  Tel. 089 / 289-28800 oder E-Mail[22] an "`hotline@lrz.de`"

  oder nutzen[23] Sie das Online-Problem-Management[24].

- Installieren Sie den geknackten Rechner mit einer *möglichst aktuellen* Betriebssystem-Version neu. Spielen Sie danach noch alle relevanten Security-Patches für diese Betriebssystem-Version ein.

  Erst dann sollten Sie den Rechner wieder an das Daten-Netz anschließen.

- Installieren Sie nun die noch erforderliche Spezial-/ Anwender-/ Open-Source-SW und restaurieren Sie danach bei Bedarf die Benutzer-Daten.

- Informieren Sie *alle* Benutzer, die auf dem geknackten Rechner oder im gleichen Segment des lokalen Netzes arbeiten dürfen, und raten sie diesen dringend, *sämtliche* Passwörter *so schnell wie möglich* zu ändern.

- Untersuchen Sie *alle* Rechner in Ihrem Einflußbereich auf verdächtige Spuren oder Vorkommnisse.

- Sollten Sie noch andere Rechner mit nicht mehr unterstützten Betriebssystem-Versionen besitzen, so sollten Sie auf diesen Rechnern unbedingt einen Betriebssystem-Upgrade durchführen.

- Auf *allen* Rechnern sollten Sie evtl. noch fehlende Security-Patches einspielen.

- Beobachten Sie Ihre Rechner in der nächsten Zeit *besonders aufmerksam*.
  Unabhängig davon ist es immer eine gute Idee, *regelmäßig* ein wachsames Auge auf den/die eigenen Rechner zu haben.

[20] `mailto:abuse@lrz.de`
[21] `http://www.lrz-muenchen.de/services/beratung/hotline/`
[22] `mailto:hotline@lrz.de`
[23] `http://arweb.lrz-muenchen.de/ars-bin/arweb`
[24] `http://www.lrz-muenchen.de/fragen/arweb-info/`