www.bit-fighter.de
IT-Security | Webdesign | Auditing | Software-Development

Fehler gefunden, und nun?!

Manchmal springt es einen regelrecht an. Ein Fehler, eine Lücke im System. Aber wie geht man mit dieser Situation um? Sollte der Bug gemeldet werden? Gehe ich damit Risiken ein? Dieser Artikel wird Ihnen die Motive und Folgen von ungefragten Sicherheitsüberprüfungen aufzeigen.

Was haben die hier bloß gemacht…

Ist Ihnen auch schon mal ein Produkt begegnet was nur so von Fehlern strotzt? Wie haben Sie reagiert? Haben Sie es dem verantwortlichen Entwickler oder Administrator gemeldet? Oder haben Sie es auf sich beruhen lassen. In diesem Artikel möchte ich Ihnen, mit Hilfe von Praxisbeispielen, diesen innerlichen Konflikt näher bringen.

Meist geschieht es ganz zufällig. Man surft gerade über eine Seite. Ganz normal. Und dann ein Klick, eine falsche Eingabe und es ist passiert.
Ein SQL-Fehler auf dem Bildschirm. Es ist ein SQL-Statement zu erkennen, dass gerade eine SQL-Abfrage machen wollte. Scheinbar wurde dieser Fehler durch eine falsche Angabe einem Textfeld ausgelöst. Dieser Fehler lässt vermuten, dass die Usereingaben nicht ausreichend überprüft werden. Vielleicht ist sogar SQL-Injection möglich.
Und nun beginnt der innere Kampf. Kann man diesen Fehler irgendwie ausnutzen? Sind irgendwelche wichtigen Daten gefährdet? Gibt es noch weitere Fehler? Soll ich das jetzt ausprobieren?

Diese beschriebene Situation kommt tagtäglich auf hunderten von Webseiten vor. Es ist eine Möglichkeit wie Fehler gefunden werden. Per Zufall. Es gibt aber auch die Situation, dass gezielt nach Fehler gesucht wird. Penetrationstests die weder beauftragt noch autorisiert wurden.

Warum sollte man das eigentlich tun?

Die Motive für solche Tests sind sehr vielseitig. Neugier spielt hier aber wohl die Hauptrolle. Wie oben beschrieben stößt man zufällig auf einen Fehler, und kann einfach nicht aufhören es weiter zu probieren. Man ist angestachelt durch den zufälligen Erfolg. Man will dieses unverhoffte Vergnügen ausnutzen, und einfach mal in Ruhe ausprobieren was möglich ist.

Es gibt aber auch Menschen die gezielt Penetrationstests durchführen, auch wenn sie sich bewusst sind das sie über keinerlei Befugnis verfügen. Gründe für solche Tests gibt es viele. Der Klassiker wäre Geld. Viele erhoffen sich einen kleinen ‚finanziellen' Ausgleich für Ihre Mühe. Eine häufig vorkommende Motivation wäre auch der Selbstschutz. Einige versierte

User sind sich der Wichtigkeit ihrer Daten bewusst. Sie prüfen ganz einfach ob ihre Daten sicher aufgehoben sind. Sie möchten sichergehen das für sie und ihre privaten Daten keinerlei Risiko besteht, und das der Betreiber seine Versprechungen auch tatsächlich einhalten kann.

Zum Schluss wäre dann noch der kriminell orientierte Typ zu erwähnen. Er richtet bewusst Schäden an, oder stielt Daten für ein Konkurrenzunternehmen. Diese Motivation ist sicherlich, aus Sicht der Administratoren, die gefährlichste. Wird hier eine Schwachstelle gefunden, sind diese Daten mit sofortiger Wirkung verloren. Eine Informationsmail o.ä. braucht man sich in diesem Fall nicht erhoffen.

Nicht bis ins letzte Detail…

Wenn Sie nicht zu den kriminell motivierten Menschen gehören, dann stellen Sie sich früher oder später die Frage: „Wie weit kann ich gehen?!“

Bei einem gefundenen Fehler wird natürlich der Ehrgeiz geweckt.
Allerdings sollte man sich an diesem Punkt in Selbstbeherrschung üben. Man darf nie vergessen, dass man sich in einem fremden System befindet, und dass es sich nicht um eine erlaubte Prüfung handelt. Somit bewegt man sich in einem Bereich, der Straf- und Zivilrechtlich durchaus bedenklich werden kann.
Unter Umständen gefährden Sie die Stabilität eines produktiven Systems. Daher sollten Sie sich bei jedem Schritt fragen, ob Sie diese Aktion bei dem Betreiber noch rechtfertigen können.

Wenn Sie beispielsweise bei einer Webapplikation festgestellt haben das SQL-Injection möglich ist, ist es dann noch nötig ein ‚DROP’-Statement zu testen?

Nachdem Sie erfolgreich eine Userdatenbank geknackt haben, halten Sie es dann für nötig diese Daten im Internet zu veröffentlichen?

Wohl eher nicht!

Melden oder nicht melden, dass ist hier die Frage.

Nun stellt sich die Frage, wie Sie mit den gewonnenen Informationen umgehen. Eigentlich liegt die Benachrichtigung der Verantwortlichen doch sehr nah.
Zunächst sollte man sich aber über die eigene Erwartungshaltung im Klaren sein. Was möchte ich mit der Mitteilung der Fehler erreichen?

- Dankbarkeit?
- Respekt/Anerkennung?
- Fehlerbehebung (damit z.B. Kundendaten wieder sicher sind)?
- Geld?

Normalerweise würde man die Fehlerbehebung als Selbstverständlich betrachten. Auch ein Dankeschön würde die Höflichkeit gebieten. Aber die Realität sieht ganz anders aus!
Aus Erfahrung kann man sagen, dass 4 von 5 Administratoren kein liebes Wort übrig haben werden.

Mein Baby fasst keiner an…

Warum reagieren viele Administratoren so aggressiv? Nun, eigentlich ist es fast verständlich. Entwickler investieren oftmals viel Geld und Zeit um ein Projekt auf die Beine zu stellen. Ein Außenstehender kann dies kaum nachvollziehen. Tritt nun die Situation ein, dass ein fremder dieses ‚Baby' anfasst und ungefragt testet, ist das für viele ein rotes Tuch. Oft entsteht dann der Eindruck, dass ein Wildfremder diktiert wie man sein Programm zu entwickeln hat. Sobald diese Situation eintritt, schaltet man auf Durchzug.
Somit ist es wichtig, bei der Meldung, den richtigen Ton zu treffen.

Feedback ist eine Kunst…

Der Entschluss ist gefallen, Sie möchten das Problem melden. Aber nur wie?
In der Regel hat man 3 Möglichkeiten:

1. den Fehler direkt beim Betreiber melden
2. den Fehler veröffentlichen (Bugtraq & Co)
3. die Kombination aus 1. und 2.

Jede Möglichkeit hat ihre Vor- und Nachteile.

Viele Entwickler betrachten ihr Werk als ihr Baby. Sie haben Zeit und Geld investiert um dieses Projekt auf die Beine zu stellen. Und dann kommt ein User daher, der ungefragt dieses Baby analysiert und dann einem auch noch sagen will was man zu tun hat.
Diese Sicht ist doch durchaus menschlich. Daher kann man auch nachvollziehen das die große Dankbarkeit doch eher zur Seltenheit gehört. Hier gilt das Sprichwort „Der Ton macht die Musik!" also besonders. Oftmals reicht es schon aus, die grundlegenden Feedbackregeln einzuhalten:

- Mit dem positiven Anfangen (Ihre Webseite gefällt mir sehr, besonders…)
- keine allgemeinen Sachen (An vielen Stellen habe ich das und das gefunden…)
- genaue Fakten
- nicht unter der Gürtellinie
- Lösungsvorschläge unterbreiten

Des Weiteren ist auch die Art der Formulierung enorm wichtig…

SCHLECHT: „Ich habe mal die Webseite von dir geprüft, und hab viele Fehler gefunden…"
→ das könnte sofort als persönlichen Angriff gewertet werden
BESSER: „Aufgrund von <Grund angeben> habe ich Ihre Webseite überprüft. Dabei bin ich über ein paar Dinge gestolpert die mir ein bisschen Sorgen machen…"

SCHLECHT: „den BUG musst du beheben und zwar so…"
→ Man sollten dem Autor nicht unbedingt die Art und Weise vorschreiben.
BESSER: „Diese Situation könnte man u.a. so entschärfen…"

Wie man sieht, ist es ein schmaler Grad. Selbst wenn man alle Feedbackregeln beherrscht, ist das noch lange keine Garantie für eine positive Reaktion. Man sollte viel mehr auf das schlimmste gefasst sein. Somit gilt als primäres Ziel immer der Eigenschutz! Niemand ist bereit sich, für eine fehlerhafte Applikation, eine Anzeige einzufangen nur weil die

Entwickler sich angegriffen fühlen. Um dieses Risiko zu minimieren, muss man der Mitteilung so viele Informationen wie möglich mitgeben:

D.h.:

- Warum hat man das Produkt geprüft?
- Wie ist man vorgegangen (zur Nachvollziehbarkeit)?
- Was hat man an Informationen zu Gesicht bekommen?
- Wurde die Lücke schon veröffentlicht?
- …

Auch bei diesen Punkten kann man das Risiko einer Strafanzeige nicht ausschließen.

Keine Reaktion ist auch eine Reaktion…

Wenn man eine Lücke gefunden hat, gibt man diese Info an die Entwickler weiter, um ihnen die Möglichkeit zu bieten den Fehler zu beheben, ohne das Schaden entsteht. Das erfordert natürlich Verschwiegenheit.
Wie reagiert man aber wenn man keinerlei Reaktion erhält, oder der Fehler nicht behoben wird?
Sollte auf den Fehler nicht angemessen reagiert werden, muss man sich der Verantwortlichkeit gegenüber den betroffenen Usern bewusst werden! Es kann immer sein das eine andere Person diesen Fehler auch entdeckt, und womöglich keine ehrenhaften Grundsätze hat. Man kann in diesem Fall die Sicherheitslücke öffentlich machen. Im Internet gibt es diverse Seiten, bei denen man Fehler zu allen Applikationen melden kann.
Dadurch zwingt man die Entwickler zur Reaktion.
Dieser Schritt sollte den betroffenen Entwicklern aber unbedingt mitgeteilt werden!

Fazit…

Das Melden von Fehlern ist durchaus ehrenhaft, bietet aber großes Risiko. Nicht jeder kann mit der Kritik umgehen, und es bedarf einer Vielzahl von Kommunikationsregeln, damit das Unterfangen nicht mit einer Anzeige endet.

© by Marco Leypold 2006