

## Die Belanglosigkeit als Methode - aus dem Alltag eines deutschen Computermagazins

### News Summary

Sicher kennen Sie das auch: Gehetzt kommen Sie an einem Presseshop vorbei. Eigentlich wÄ¼rden Sie gern mal wieder ein paar Zeitschriften querlesen, allerdings haben Sie dafÄ¼r keine Zeit. Trotzdem lassen Sie sich hinreiÄ¼en. Schnell ein Blick in die Ecke der monatlich erscheinenden Mags, mit einem Blick Ä¼ber das Angebot streifen, zwei drei interessante Aufmacher gelesen, schnell entschlossen zur Kasse gegangen, gezahlt und zufrieden den abendlichen Lesegenuss schon deutlich vor Augen wieder dem Tagewerk gewidmet.

### News Text

Auf diese Weise hat es vor einigen Tagen auch das "Linux Enterprise Magazin" (wieder einmal) geschafft, meine anfÄ¼ngliche Aufmerksamkeit und sodann auch ein Teil meiner Freizeit zu beanspruchen. Der Aufmacher, der letztendlich meinen Kaufentschluss fÄ¼rderte, titelte unter <i>"Websecurity: Wie Sie Sie Apache besser schÄ¼tzen"</i> sowie <i>"Honeypots als LockvÄ¼gel"</i>. Zugegeben - die Titel jener "Topthemen" sowie die farbliche Aufmachung hÄ¼tten schon hinreichend Warnung sein mÄ¼ssen. Was sich dann jedoch dem geneigten Leser erÄ¼ffnete, war ein wahres Trauerspiel. Der als Topthema angekÄ¼ndigte Apache-Security Artikel entpuppte sich als vierseitiges belangloses GeplÄ¼nkel rund um den Apachen. Von besagten vier Seiten Gesamtumfang benÄ¼tigte der Autor Thomas Kaufmann zunÄ¼chst zwei Seiten, um "Hinweise" zur Installation des Indianers zu geben. Unbestritten - schon beim Kompilieren des Apachen kann das eine oder andere Flag ein Scheunentor Ä¼ffnen. Nur DAS liest man leider bei Herrn Kaufmann nicht. Vielmehr ergÄ¼tzt sich jener an Versionsermittlung, Entpacken des Tarballs, Ermittlung der PID und weiteren "sicherheitsrelevanten" Fragestellungen. Nach dieser "EinfÄ¼hrung" folgen dann die harten Fakten: Man kann die FunktionalitÄ¼t des Apachen doch tatsÄ¼chlich mit Modulen erweitern. Ach?! Zum Beispiel mit mod\_security. Nein! Unbestritten, das Modul mod\_security von Ivan Ristic ist ein sehr ausgereiftes und vor allem leistungsfÄ¼higes Open Source Produkt, um den Apache-Webserver vor einer Vielzahl von Angriffen zu schÄ¼tzen. Nur leider erfÄ¼hrt man dies in den insgesamt zwanzig Zeilen, die der Autor dem Modul insgesamt widmet, nicht. Jener befindet vielmehr, den Leser noch auf die Konfiguration der Standardlogs hinweisen zu mÄ¼ssen.

Wer auf diese Weise jenen "inhaltsreichen" Beitrag mehr oder weniger frustriert hinter sich gelassen hat und nunmehr seine Entspannung 'im' Honeypot sucht, ahnt allerdings noch nicht, dass die Belanglosigkeit und OberflÄ¼chigkeit des soeben Ä¼berwundenen Artikels noch steigerungsfÄ¼hig ist. Allein die Begrifflichkeit des kommenden Beitrags erweckt Neugier: Honeypots - eine sehr wirksame Technologie im Rahmen des Security Auditing - findet man gemeinhin vorrangig in grÄ¼Ä¼eren Netzstrukturen. Die Zielgruppe jenes Beitrag dÄ¼rfte sich damit vorallem aus beruflich interessierten Sicherheitsverantwortlichen sowie engagierten Privatnutzern rekrutieren. Insoweit sollte man gemeinhin einen inhaltlich anspruchsvollen Beitrag zum Thema erwarten dÄ¼rfen. Doch

auch hier versteht es der Autor Sebastian Wolfgarten, einem Studierenden der Wirtschaftsinformatik, den Leser mit offensichtlichen Belanglosigkeiten zu langweilen. Zu Beginn seiner Darstellung vermittelt Wolfgarten dem Leser zunächst sein laienhaftes Verständnis von den einschlägigen Rechtsnormen, die in Wolfgartens lingualer Brillanz mal schnell zu Gesetzen mutieren. Sein Versuch einer rechtlichen Verortung der allgemeinen Problematik untermauert Wolfgarten zugleich mit einer Vielzahl von Adjektiven und Adverbien, um wohl seiner Darstellung einen gesteigerten Bedeutungsgehalt zu geben. Leider erfolglos. Sein gesamter Beitrag erschöpft sich mehr oder weniger in der reflexionsartigen Darstellung einer Systematisierung von Honeypot-Technologien, die in jener Weise wesentlich interessanter in dem Standardwerk

[Honeypot: Tracking Hackers](http://www.amazon.com/exec/obidos/ASIN/0321108957/ref%3Dnosim/honeypots-20/102-735-4182-2582533 "Honeypot: Tracking Hackers") von Lance Spitzner zu finden ist. Natürlich verweist auch Wolfgarten in einer Endnote auf Spitzner - allerdings eben nur auf eine Website, die schon seit einiger Zeit keinen Inhalt mehr bietet, sondern vielmehr mit einem Domainkaufangebot im Netz präsent ist. Quellenarbeit scheint also nicht das Fachgebiet des Autors zu sein. Alles in allem hat man den Eindruck, jener Beitrag wurde vom Autor irgendwann zwischen zwei Lehrveranstaltungen zu Papier gebracht, wobei die Primärintention jener Zeilen wohl irgendwo zwischen Selbstdarstellung und Seitenfüllerei ansiedelt. Andererseits - vielleicht ist der Maßstab für die hier geäußerte Kritik ja nur etwas einseitig gewählt - vielleicht sollte man bei der Beurteilung einfach in Betracht ziehen, dass es sich beim Autor um einen Studierenden handelt, dem noch die hinreichende Erfahrung fehlt und der die Erwähnung der eigenen Person in jenem Blatt als die vorrangige Pflicht ansieht.

Unverzeihlich ist dagegen, dass die Herausgeber jener Ansammlung von Belanglosigkeiten sich letztendlich auch noch dazu entschlossen, besagtem Studenten das Editorial der gegenständlichen Ausgabe "anzuvertrauen". Hier läuft Letztbenannter nunmehr auch zur eigentlichen Hochform auf. Die einführenden Weisheiten über die verschiedenen Facetten und die Bedeutung der IT-Sicherheit in der Informationsgesellschaft lesen sich wie der Prolog eines Security Auditing Berichts. Sodann folgen Erfahrungen und Erkenntnisse aus dem mehrjährigen "Berufsalltag" bei einer international tätigen Wirtschaftsprüfungsgesellschaft, deren Namen man i. erfährt, wenn man sich einige Seiten später den vorbenannten Honeypot-Beitrag in quasi masochistischer Art und Weise einverleibt. Das Editorial schließt mit dem mehrdeutigen, augenscheinlich menschliche Weisheit transportierenden 

>"Ja ja, Theorie und Praxis"</div>Wie wahr, wie wahr! Auch wenn der Autor bei verschiedenen Veranstaltungen zum Thema "Honeypots" omnipräsent erscheint und sich darüber hinaus auch als Buchautor versucht, sind eben jene Umstände noch kein Garant für qualitativ hochwertige Beiträge in einem Computermagazin.

Fazit dieses kleinen "Ratix": Ich habe selten ein "Fachmagazin" gelesen, in dem Anspruch und Wirklichkeit so weit auseinanderklaffen. Es scheint wohl eine unumkehrbare Entwicklung innerhalb jener Sparte von Presseerzeugnissen zu sein, möglichst schnell Seitenfüllerei zu betreiben und dabei den Anspruch an Qualität als das unumgänglichste Kriterium der Veröffentlichungsfähigkeit zu betrachten. Das dabei vorbenannte Computermagazin kein Einzelfall ist, belegt leider auch ein Verlagserzeugnis des Branchenprimus: War zu einem früheren Zeitpunkt die c't noch ein wirklich lesenswertes Produkt des Heise-Verlages, so hat auch jenes Fachmagazin in letzter Zeit leider den Weg hin zum Boulevardmagazin eingeschlagen. Allerdings bietet der Heise-Verlag mit der iX zumindest noch eine lesenswerte Alternative zur c't - was dagegen für den Software & Support Verlag, dem Herausgeber des Linux Enterprise Magazins, leider nicht gilt. Deren Portfolio scheint nach einem kurzen Überblick ähnlich

positioniert zu sein, wie besagtes Linux Enterprise Magazin.

weiterführende Links

[Leitseite smartnuts.com](#)

[Urteilsdatenbank smartnuts.com](#)

www.smartnuts.com