A2

**Anfrage zur Schließung von firewallinfo.de**
Von: chefredaktion@muenchnernotizen.info <Chefredaktion muenchnernotizen>
An: presse@hosteurope.de
Datum: Mon, 14 Aug 2006 12:40:01 +0200

sehr geehrte damen und herren der presseabteilung!

im zusammenhang mit recherchen zu umfassenden hackerangriffen in deutschland und österreich sind wir auf einen sachverhalt gekommen zu dem wir sie um stellungnahme ersuchen:

.) wie zahlreiche andere internetpräsenzen war auch firewallinfo.de von hackerangriffen, einer fundamentalistisch orientierter gruppe offensichtlich türkischen ursprungs betroffen. firewallinfo.de wurde mit einem contentmanagementsystem aktuellster version auf php-basis betrieben (version 1.0.10 joomla). nachdem es sich bei den betreibern aus fachlicher sicht, betreffend die internetsicherheit, um sehr sachkundige personen handelt und uns auch die schriftlichen aussagen betreffend der ordnungsgemäßen administration vorliegen, gehen wir davon aus, daß alle sicherheitsstandards striktest von dieser seite her eingehalten wurden, die mit der seitenpflege in zusammenhang stehen. ebenso ist bekannt, das gerade betreiber solch einschlägiger webportale durch den contentbezogenen inhalt gerne ziel von hackerangeriffen darstellen und umsomehr darauf bedacht sind, keinerlei lücken in ihren systemen solchen angriffen aussetzbar zu machen.

wie aus der logik resultierend, bedürfen cms auf php-basis entsprechende rechte um einen ordnungsgemäßen interaktiven ablauf zu gewährleisten. diese vorgaben werden durch die programmierer des programmes erlassen. im gegenständlichen fall wurden in anbetracht der durch kriminelle energien verursachten hackerversuche der vergangenen wochen zusätzlich die rechte noch weiter eingeschränkt um solchen versuchen zusätzlich entgegen zu wirken.

die betreiber von firewallinfo.de haben beispielsweise auf den servern, der von ihnen gehosteten website in ordnern scripte wie z.b. die "C99shell" vorgefunden mit denen spam und phishing-mails versand werden können. dies ist grundsätzlich nur möglich, wenn die von ihnen betriebenen server nicht mit notwendigen sicherheitsstandards abgeschirmt wurden.

um den angriffen im erweiterten umfang entgegenzuwirken gingen die administratoren sogar so weit, daß sie die eigenen rechte so weit einschränkten, daß diese für eigenen administraiven handlungen, die normal ohne entsprechenden eingriff durchgeführt werden können, selbst rechteanpassungen vornahmen. trotz umfassender datensicherung durch die betreiber und löschung der "feindscripte" hat ihr unternehmen am heutigen tag zum zweiten mal die gesamte internetpräsenz vom netz genommen.

aus dem uns vorliegenden sachverhalt und den zusätzlichen erhebungen bei anderen webhostern ergibt sich für uns folgender sachstand:

ihr unternehmen ist offensichtlich nicht in der lage die eigenen server vor kriminellen handlungen abzusichern, bei denen das cms auf php-basis betrieben wird. von anderen unternehmen erhielten wir die aussagen, daß ggf. der kunde informiert werden würde und ein etwaig vorhandenes script, daß ein sicherheitsrisiko darstellen würde, für sich einzeln gesperrt wird. ihre vorgangsweise erweckt den anschein 08/15 internetpräsenzen administrativ abwickeln zu können, jedoch notwendige übliche und gängige sicherheitsstandards im gegenständlichen fall bei cms auf php-basis nicht zu erbringen - obwohl php doch auch bereits den standard zuzuordnen ist.

das verschulden im gegenständlichen fall dem endkunden in die schuhe zu schieben und zusätzlich sich von diesem durch stillegung der webpräsenz zu verabschieden und nicht für die eigene verantwortlichkeit einzutreten stellt zumindest für uns ein novum dar.

in erwartung ihrer geschätzten schriftlichen stellungnahme verbleibe ich

mit freundlichen grüssen
walter egon glöckel

Chefredaktion muenchnernotizen
Magazin für Deutschland, Österreich und Schweiz seit 2000

Walter Egon Gloeckel

Unterschrift nicht bestätigt

Digital unterschrieben von Walter Egon Gloeckel
DN: cn=Walter Egon Gloeckel, o=Nachrichtenmagazin DER GLOECKEL (ISSN 1992-0318), ou=Chefredaktion, c=AT
Datum: 2007.06.23 23:18:39 +02'00'
Ursache: Dokument ist zertifiziert.
Speicherort: Hainburg