THE PENTEST EXPERTS.

In diesem Newsletter erwarten Sie folgende Inhalte:

Sehr geehrte Kunden,
liebe Geschäftspartner,
Freunde und Bekannte,

„50 Milliarden Euro Schaden – Da muss man doch was machen!“ Bundesinnenminister Hans-Peter Friedrich schätzt, dass die deutsche Wirtschaft durch Wirtschaftsspionage einen jährlichen Schaden in Höhe der oben genannten Summe erleidet. Aus diesem Grund haben der *Bundesverband der Deutschen Industrie* (BDI), der *Deutsche Industrie- und Handelskammertag* (DIHK) und das Bundesinnenministerium am 28.08.13 eine gemeinsame Erklärung unterschrieben, deren Ziel es ist, in Ergänzung zur *Cyber-Sicherheitsstrategie für Deutschland* nun auch eine *Nationale Strategie für den Wirtschaftsschutz* zu entwickeln. BDI-Präsident Grillo schwärmt von dieser Strategie als „einem Meilenstein“, der „einzigartig in Europa“ sei.

Ich freue mich, dass das Thema Computersicherheit in den Vordergrund gerückt wird und ins öffentliche Bewusstsein dringt. Die beiden Strategien jedoch verfehlen ihren Sinn, weil ihr Wirkungskreis, da auf Deutschland beschränkt, völlig unpassend ist. Bei der Bekämpfung anderer Arten von Kriminalität wie Drogenschmuggel oder Korruption machen nationale Konzepte ja durchaus Sinn, weil in jedem Land eine andere Gesetzesgrundlage existiert und nationale Grenzen hervorragend geeignet sind, Kontrollen durchzuführen. Wer bei Cyberspionage im World Wide Web allerdings in nationalen Grenzen denkt, geht das Problem auf falsche Weise an:

a) Räumliche Entfernungen spielen im Cyberspace keine Rolle: New York ist von Frankfurt im Netz genauso weit entfernt wie Berlin. Landesgrenzen sind aus Sicht der IT nicht vorhanden. Daher kann die Wirksamkeit einer nationalen Strategie nur unzureichend greifen, denn eine Abgrenzung, gera de auf Deutschland bezogen, suggeriert, dass Cyber-Angriffe gleichermaßen „an der Grenze“ gestoppt werden könnten wie Rauschgifttransporte.

b) Staaten sind in der Lage, Gesetze zu erlassen. Doch solche Gesetze sind im Cyberspace nutzlos – wie will man beispielsweise staatliche oder nicht-staatliche Hacker aus China verurteilen? Im Internet sind Täter nicht identifizierbar und so einer Strafverfolgung gar nicht zugänglich.

Wenn die Behörden und die Politik im Rahmen nationaler Grenzen denken, dann zeigt dies, dass das Internet für sie in der Tat „Neuland“ ist. Auf alle Fälle muss Wirtschaftsspionage mit einer Schadensbilanz von 50 Milliarden Euro der Kampf angesagt werden. Hierbei dürfen sich Unternehmen aber keinesfalls auf die Regierung verlassen, sondern sie sollten Eigeninitiative ergreifen. Eine hervorragende Maßnahme besteht darin, die eigene IT unter die Lupe zu nehmen und sich zu fragen, wie ihre Sicherheit verbessert werden könnte. Einen Quick Win erzielen Sie, indem Sie uns beauftragen, Ihre IT einem Penetrationstest zu unterziehen. Wir analysieren diese tiefgreifend, zeigen Schwachstellen auf und geben Ihnen Hilfeleistung, diese zu beheben. Einen langfristigen Nutzen werden Sie haben, wenn Sie Wege finden, die beim Penetrationstest gefundenen Lücken dauerhaft zu vermeiden. Ich stehe Ihnen jederzeit für eine individuelle Beratung zur Verfügung und freue mich auf Ihren Anruf unter meiner Durchwahl: 07071-407856-15.

Herzliche Grüße,
Ihr Sebastian Schreiber

Aktuelle Events

24.-26.09.13	Tägl. LH[1] auf der Landesmesse Stuttgart: IT+Business
27.09.13	Vortrag auf dem Seminar „Sicheres Mobile Computing“ in Frankfurt/Main
08.-10.10.13	Tägl. LH[1] und versch. Präsentationen auf der it-sa 2013 in Nürnberg
22.10.13	LH[1] auf dem Tag der IT-Sicherheit, IHK Südl. Oberrhein Lahr

[1] Live Hacking

Detaillierte Informationen zu diesen Veranstaltungen finden Sie auf unserer Homepage www.syss.de.

Aktuelle Schulungen

Web-App:
25. - 26.09.13
20. - 21.11.13

Exploits:
01. - 02.10.13

Incident Response:
15. - 17.10.13

IT-Security I:
21. - 22.10.13
25. - 26.11.13

IT-Security II:
23. - 24.10.13
27. - 28.11.13

IT-Forensik:
05. - 07.11.13

Mobile Device:
12. - 13.11.13

PenTests:
15.11.13

IT-Recht:
29.11.13

Windows-Angriffe:
03. - 04.12.13

IPv6:
06.12.13

Bei Teilnahmewunsch oder Fragen wenden Sie sich bitte an info@syss.de.

Sollten Sie den Newsletter nicht beziehen wollen, dann teilen Sie uns dies bitte unter newsletter@syss.de mit, wir werden Sie dann umgehend aus dem Verteiler entfernen.

Impressum:
SySS GmbH · Wohlboldstraße 8 · 72072 Tübingen · Tel. +49 (0)7071 407856-0 · E-Mail: info@syss.de · http://www.syss.de · Geschäftsführer: Diplom-Inform. Sebastian Schreiber
Verantwortlich für Inhalt: Marcus Bauer

THE PENTEST EXPERTS.

SySS entdeckt schwere Sicherheitslücke in TYPO3

von Sebastian Nerz

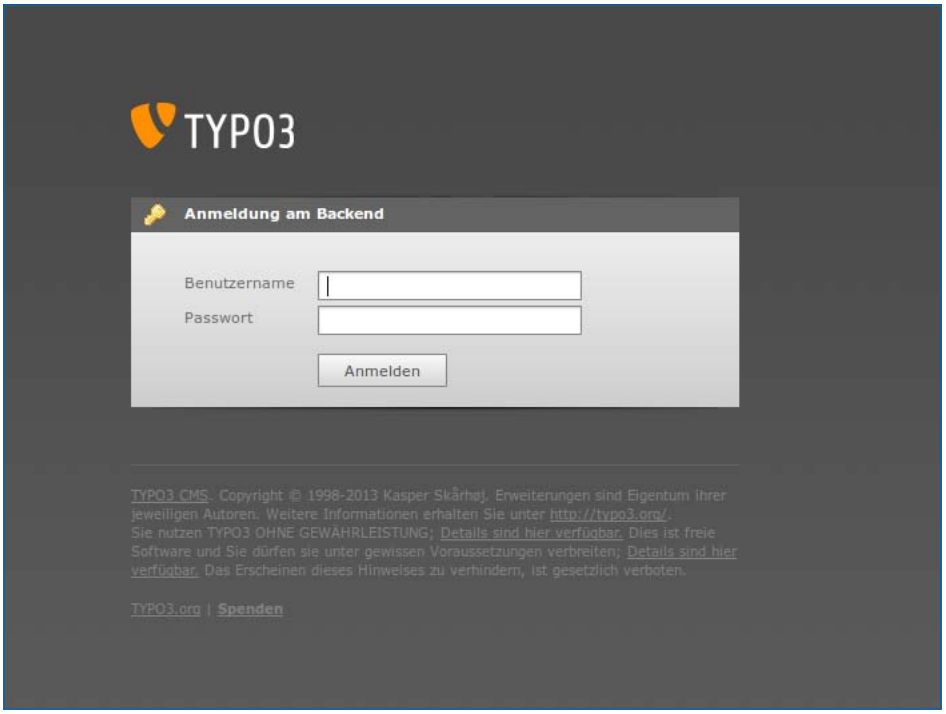
TYPO3 ist ein weitverbreitetes Open Source Web Content Management System, welches besonders im deutschsprachigen Raum eingesetzt wird. Dabei bewegt sich die Größenordnung beim Einsatz zwischen kleinen ehrenamtlichen Projekten, die eine mehr oder weniger statische Webseite und einfache Newsletterfunktionen unterhalten, und Webseiten von Behörden, Krankenhäusern, großen Unternehmen oder internationalen Konzernen, die TYPO3 als grobe Basis oder Framework einsetzen, ihre eigene Funktionalität aber vor allem durch eigene Module aufbauen.

So unterschiedlich diese Anforderungen und Umsetzungen auch sind, in einem Bereich sind sie völlig einig: Das Backend ist TYPO3, es stellt eine Abstraktion über die Datenbanksysteme (MySQL, PostgreSQL, Oracle, etc.), die Programmiersprache (PHP beziehungsweise TYPOscript) und das Betriebssystem (auf welchem auch immer PHP betrieben wird) zur Verfügung, managt Benutzer und bietet eine Struktur für Inhalte und Zugriffe an. Entsprechend kritisch sind Sicherheitslücken im Kern des TYPO3-Systems. Module mögen ein oder zwei Webseiten betreffen (oder auch ein oder zweihunderttausend), aber sie betreffen nicht alle. Ein Problem im Kern ist dagegen für alle Webseiten relevant, völlig egal, wie groß oder klein sie sind.

Dieser Kern (Core) des TYPO3-Systems ist mittlerweile innerhalb von ein paar Jahren gewachsen, gewartet und regelmäßig überprüft worden. Allerdings wurde beim Versionswechsel von TYPO3 4.7 auf TYPO3 6 einiges umgestellt, so dass sich auch neue Fehler eingeschlichen haben.

TYPO3 verwendet mittlerweile ein relativ elaboriertes System zur Rechteverwaltung. So wird beispielsweise zwischen Frontend-Benutzern, die Kommentare einreichen können oder die anderweitig für Nutzer der Webseite gedacht sind, und Backend-Benutzern unterschieden. Letztere sind zum Beispiel für die Administration der Seite verantwortlich, aber auch zum Einpflegen von Inhalten, der Erstellung von News oder Ähnlichem. So muss jeder Webseitenautor oder -mitarbeiter schlussendlich einen Backend-Benutzer zugewiesen bekommen. Dessen Rechte wiederum können relativ flexibel eingestellt werden. Der Zugriff auf den Dateimanager kann beispielsweise auf bestimmte Ordner beschränkt oder komplett untersagt werden.

Dieses Rechtesystem ist soweit in TYPO3 auch korrekt umgesetzt – sofern Benutzer sich an die vorgegebenen Wege halten und keine direkten Zugriffe auf Funktionen oder URL nehmen. Der Zugriff auf den Dateimanager wird entsprechend eingeschränkt. Allerdings hat die SySS GmbH hier Ende Mai ein anderes kritisches Sicherheitsproblem gefunden. Eine jegliche tatsächliche Dateioperation (Hochladen, Anlegen, Umbenennen, Bearbeiten) wird per AJAX-Aufruf an untergeordnete URL weitergegeben, sie erfolgt nicht direkt im Dateimanager. Bei diesen Aufrufen wird zwar kontrolliert, ob ein gültiger Backend-Benutzer eingeloggt ist, aber nicht, ob er die notwendigen Berechtigungen hat. Gleichzeitig verbietet TYPO3 bestimmte Dateioperationen. So können beispielsweise aus Sicherheitsgründen normalerweise keine PHP-Dateien hochgeladen werden. Es ist jedoch möglich, Dateien nach *.php* umzubenennen, solche Dateien anzulegen oder zu bearbeiten.



Anmeldeoberfläche am TYPO3-Backend

THE PENTEST EXPERTS.

Betroffen sind hiervon mindestens die TYPO3-Versionen ab 6.0. Ein erster Patch vom 30.07.2013 behebt zumindest einen Teil der schwerwiegenden Probleme, der Patch vom 04.09.2013 schließt dann die noch vorhandenen Lücken.

In der Praxis bedeutet dies, dass ein Angreifer nach dem Login ins Backend beliebige Dateien anzeigen, erstellen oder bearbeiten kann, unabhängig davon, welche Berechtigungen er hat. Mit einem Zugriff auf

[Host]/[Pfad]/typo3/file_edit.php?target=0:/typo3conf/LocalConfiguration.php

beispielsweise wird die Konfiguration des TYPO3-Systems angezeigt, inklusive der Zugangsdaten zur Datenbank. Alternativ ließe sich natürlich durch Zugriff auf beispielsweise

/typo3/tce_file.php

mit dem Parameter

„file[editfile][0][target]=0:/index.php"

die TYPO3 *index.php* bearbeiten und dort eine Backdoor einbauen, die es gestatten würde, beispielsweise eine PHP-Webshell auf den betroffenen Server zu laden und so beliebigen PHP-Code auszuführen. Sofern nicht spezifische und leider ungewöhnliche Maßnahmen zur Einschränkung der PHP-Installation vorgenommen wurden, ließen sich damit auch beliebige Shell-Befehle auf dem Server ausführen und der Server könnte im Extremfall komplett übernommen werden.

Alternativ könnte ein Angreifer über solche Wege auch Dateien nach *.htaccess* umbenennen und auf diese Weise weitere interpretierte Dateitypen hinzufügen. TYPO3 verbietet hier zwar interessanterweise die Bearbeitung, nicht aber das Anlegen oder das Umbenennen nach *.htaccess*.

Was schafft Abhilfe? Die SySS GmbH hat den Fehler am 24. Mai 2013 gefunden und an das TYPO3-Security-Team weitergeleitet. Der Eingang wurde uns am 27. Mai auch bestätigt und ein erstes Update wurde dann am 30.07. veröffentlicht. Damit wurde zumindest die Erstellung beziehungsweise die Bearbeitung von PHP-Dateien verhindert. Das zweite Update wurde am 04.09. veröffentlicht und behebt dann auch die noch offenen Fehler. Weiterhin ist es möglich, beliebige andere Dateien anzulegen und Konfigurationen auszulesen. Wir haben uns dennoch zu dieser Veröffentlichung entschlossen, da diese Lücke unter bestimmten Umständen weiterhin eine vollständige Übernahme betroffener TYPO3-Systeme erlaubt, ganz egal, welche Rechte ein Backend-Benutzer hat.

Betroffene Kunden sollten das aktuelle Update schnell einspielen, da es sich tatsächlich um ein größeres Sicherheitsrisiko handelt. Zusätzlich empfehlen wir, dass der Zugriff auf PHP-Dateien durch die TYPO3-Editoren verboten werden sollte. Dies ist möglich, indem die Datei

typo3conf/LocalConfiguration.php

angepasst wird. Der array ‚SYS' muss um eine Zeile ergänzt werden:

`textfile_ext´ => `txt,html,htm,css,js,sql,xml,csv´

Gegebenenfalls müssen weitere Formate ergänzt werden, wenn zusätzliche Dateitypen bearbeitet werden sollen. Damit lassen sich zwar weiterhin leere Dateien anlegen, aber zumindest das Auslesen von Konfigurationsdateien ist nicht mehr ganz so einfach.

Allgemein empfiehlt die SySS zusätzlich allen Kunden, die TYPO3 einsetzen, den Zugriff auf das TYPO3-Backend einzuschränken und diesen nur noch vertrauenswürdigen Administratoren zu ermöglichen, denn der Fehler zeigt wieder einmal, dass Zugriffe auf CMS-Systeme nur entsprechend geschulten und vertrauenswürdigen Mitarbeitern gegeben werden sollten. Es kommt leider viel zu häufig vor, dass Rechtesysteme umgangen werden können oder Fehler in einem CMS eine größere Sicherheitslücke öffnen.

Zum Abschluss möchten wir betonen, dass solche Fehler sich klassischerweise kaum oder gar nicht durch eine Firewall, Web Application Firewall oder Ähnliches beheben lassen. Die Firewall kennt üblicherweise ja beispielsweise Benutzerberechtigungen nicht. Gefiltert werden könnten maximal Zugriffe auf bestimmte Dateitypen, wobei solche Filter fehleranfällig und beinahe immer unvollständig sind.