Bundesamt
für Sicherheit in der
Informationstechnik

Studie „Sicherheitsuntersuchung von Content-Management-Systemen“

Checklisten zur Härtung - TYPO3

Änderungshistorie

Version	Datum	Name	Beschreibung
0.1	11.04.2016	[redacted]	Einarbeitung Checklisten
0.2	26.04.2016	[redacted]	Aktualisierung der Status für die Skriptumsetzung
0.3	26.04.2016	[redacted]	Spezifizierung auf eine TYPO3-Checkliste
0.4	29.04.2016	[redacted]	Review
1.0	29.04.2016	[redacted]	Freigabe
1.1	19.05.2016	[redacted]	Erweiterung um Hinweise für Kompatibilität
2.0	20.05.2016	[redacted]	Freigabe
3.0	22.06.2016	[redacted]	Finalisierung anhand Skriptlösung
4.0	22.07.2016	[redacted]	Fehlerkorrekturen
5.0	12.08.2016	[redacted]	Finalisierung anhand Skriptlösung

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582
E-Mail: bsi-publikationen@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung/Motivation

Ziel der vorliegenden Checkliste ist es, die Umsetzung der Sicherheitsanforderungen für das CMS TYPO3 zu ermöglichen. Diese wurden im Rahmen der Studie „Sicherheitsuntersuchung von Content-Management-Systemen“ [1] erarbeitet.

Die zugehörigen Härtungsskripte sollen die automatische Implementierung der Sicherheitsanforderungen sicherstellen. Allerdings können einige Anforderungen nur manuell umgesetzt werden. Aus diesem Grund ist bei den nachfolgenden Sicherheitsanforderungen vermerkt, welche der Anforderungen durch die Härtungsskripte automatisiert umgesetzt werden können. Eine manuelle Umsetzung ist prinzipiell möglich.

Die Einteilung der zu implementierenden Maßnahmen erfolgt anhand der Komponenten des Gesamtsystems. Die Härtungsmaßnahmen ergeben sich aus internen Sicherheitsempfehlungen der Deutschen Telekom AG [2] bzw. den daraus resultierenden technischen Sicherheitsanforderungen [3], den Dokumenten der BSI-Reihe zur Internet-Sicherheit (ISi-Reihe) [4], den Sicherheitsempfehlungen der CM-Systeme und der Laufzeitumgebungen sowie der Ergebnisse aus dem Test der bereits gehärteten CM-Systeme entsprechend der Studie [1].

2 Content Management Systeme

2.1 TYPO3

Maßnahme	Im Härtungs-skript umgesetzt	Kommandos zur Härtung
Der Standard-Admin-Benutzer sollte gelöscht und stattdessen ein persönlicher Account mit entsprechenden Rollen erstellt werden. Standard-Benutzer fallen oft Angriffen zum Opfer.		Der Standard-Admin-Benutzer wird während der Installation angelegt. Bei der Installation der Introduction-Extension werden außerdem folgende Benutzer mit Standardpasswort angelegt: admin simple_editor advanced_editor Diese Benutzer sollten nach Möglichkeit gelöscht werden.
Das Typo3 „Install Tool“ sollte deaktiviert werden.	x	rm -f /var/www/deb-hardened-typo3/htdocs/typo3conf/ENABLE_INSTALL_TOOL
Der Zugriff auf das „Install Tool“ sollte per IP-Whitelist eingeschränkt werden.	x	Install --> unlock the Install-Tool --> All configuration -->[BE][IPmaskList] = '192.168.1.*'
Der Zugriff auf das Backend darf nur mit SSL gestattet werden.	x	Install --> unlock the Install-Tool --> All configuration -->[BE][lockSSL] = '1'
Es muss sichergestellt sein, dass der Inhalt der Datei LocalConfiguration.php nicht aus dem Netz abrufbar ist.		Sollte PHP-FPM zum Einsatz kommen, so muss sichergestellt sein, dass im Apache alle Dateien mit der Endung php an PHP-FPM übergeben werden. Zusätzlich könnte dem Apache-Benutzer die Leserechte auf alle php-Dateien entzogen werden.
Die Standard-Benutzerrechte sollten nach dem Least-Privilege- Prinzip angepasst werden, so dass Benutzer nur jene Aufgaben durchführen können, die ihnen anvertraut sind. Jedes zusätzliche Recht ermöglicht Missbrauch.		Prüfung der Vergabe der Gruppen zu Benutzern Prüfung der Vergabe von Berechtigungen für Benutzer
Da Fehlerinformationen teilweise auch interne technische Informationen enthalten, sollten alle Debug-Informationen in produktiven Systemen unterbunden werden.	x	Install --> unlock the Install-Tool --> All configuration -->[SYS][displayErrors] = '0' [SYS][errorHandlerErrors] = '0' [SYS][exceptionalErrors] = '0' [SYS][sqlDebug] = '0'
Unterstützt der SMTP-Server TLS, so muss TYPO3 entsprechend konfiguriert werden, den Mail-Versand verschlüsselt durchzuführen.		Install --> unlock the Install-Tool --> All configuration -->[MAIL][transport_smtp_encrypt] = <ssl, sslv2, sslv3 oder tls>
E-Mail-Benachrichtigung bei	x	Install --> unlock the Install-Tool --> All

(fehlerhaften) Anmeldungen am Backend sollte aktiviert werden.		configuration --> [FE][warning_email_addr] = <E-Mail-Adresse> [FE][warning_mode] = 1
Damit Benutzer mit der Berechtigung template-access keine eigenen PHP-Dateien ausführen lassen können, sollte die Option [FE][noPHPscriptInclude] auf 1 gesetzt werden. Dadurch wird verhindert, dass PHP-Skripte aus TypoScripts heraus aufgerufen werden können, wenn sie nicht in speziellen Verzeichnissen liegen.	x	Install --> unlock the Install-Tool --> All configuration --> [FE][noPHPscriptInclude] = '1'
Der Parameter lockIP sollte gesetzt werden, um Session-Hijacking-Angriffe zu verhindern. Hierdurch wird eine Verknüpfung aus Benutzersession und der IP-Adresse des Benutzers hergestellt.		Install --> unlock the Install-Tool --> All configuration --> [FE][lockIP] = 2 [BE][lockIP] = 4
Um Clickjacking-Angriffe zu verhindern, muss der HTTP-Header X-Frame-Option korrekt gesetzt werden. Wenn dies nicht bereits im Apache konfiguriert ist, kann es in TypoScript eingestellt werden.		Siehe https://docs.typo3.org/typo3cms/SecurityGuide/GuidelinesIntegrators/Typoscript/#clickjacking
Viele TYPO3-Extensions werden mit Test- und Dokumentationsdateien installiert. Da diese Dateien auch Informationen wie Versionsnummern enthalten können, wird empfohlen, alle unnötigen Dateien der Extensions zu löschen.		Da die Dateistruktur von Extensions meist einem Schema entsprechen, sollten folgende Dateien gesucht und gelöscht werden: /typo3conf/ext/*/ChangeLog /typo3conf/ext/*/README.md /typo3conf/ext/*/LICENSE.md /typo3conf/ext/*/doc/ /typo3conf/ext/*/Documentation/ /typo3conf/ext/*/.git* /typo3conf/ext/*/.git/ /typo3conf/ext/*/Tests /typo3conf/ext/*/_make /typo3conf/ext/*/phpunit* /typo3conf/ext/*/build.xml /typo3conf/ext/*/CHANGELOG.md
In der Basis-Installation von TYPO3 wird ein "vendor"-Ordner mitgeliefert. In diesem befinden sich viele Test- und Dokumentationsdateien. Teilweise befinden sich in den Test-Dateien auch bekannte Schwachstellen, so dass diese Dateien gelöscht werden sollten.		/vendor/pear/net_url2/docs/ /vendor/pear/http_request2/docs/ /vendor/phpwhois/idna-convert/ example.php /vendor/psr/log/Psr/Log/Test/ /vendor/swiftmailer/swiftmailer/doc/ /vendor/symfony/console/Tests/ /vendor/symfony/finder/Tests/
Damit das Session-Cookie niemals über eine unverschlüsselte Kommunikation übertragen wird, muss das "secure" Attribut für Session-Cookies gesetzt werden. Als Voraussetzung ist es notwendig, SSL/TLS am Webserver	x	Install --> unlock the Install-Tool --> All configuration --> [SYS][cookieSecure] = 1

aktiviert zu haben.		

3 Laufzeitumgebungen

3.1 PHP

Maßnahme	Im Härtungs-skript umgesetzt	Kommandos zur Härtung
Es ist zu prüfen, ob für die eingesetzte PHP-Version noch Hersteller- Support besteht. Siehe http://php.net/supported-versions.php	x	user@host:~$ php -v
Die Darstellung von Fehlermeldungen während der Laufzeit ist zu unterbinden und Fehlermeldungen sollten protokolliert werden.	x	php.ini: display_errors = Off log_errors=On
Die „Register Globals“ Einstellung ist zu deaktivieren. Ab Version 5.4 ist diese Option nicht mehr vorhanden und folglich generell deaktiviert.	x	php.ini: register_globals = Off
Sicherheitskritische PHP-Funktionen sollten deaktiviert werden. Einige der hier deaktivierten PHP-Funktionen könnten für zusätzlich eingesetzte PHP-Bibliotheken benötigt werden und müssten dann manuell ausgetragen werden.	x	php.ini: disable_function = dl, fsocket_open, ini_alter, parse_ini_file, passthru, pcntl_alarm, pcntl_exec, pcntl_fork, pcntl_get_last_error, pcntl_getpriority, pcntl_setpriority, pcntl_signal, pcntl_signal_dispatch, pcntl_sigprocmask, pcntl_sigtimedwait, pcntl_sigwaitinfo, pcntl_strerror, pcntl_wait, pcntl_waitpid, pcntl_wexitstatus, pcntl_wifexited, pcntl_wifsignaled, pcntl_wifstopped, pcntl_wstopsig, pcntl_wtermsig, phpinfo, popen, set_time_limit, show_source
Assert-Funktionen werden für den Produktivbetrieb nicht benötigt und sollten deaktiviert werden.	x	php.ini: assert.active = Off
Der httpOnly-Wert in PHP-Session-Cookies sollte standardmäßig gesetzt werden.	x	php.ini: session.cookie_httponly = 1
Die Entropie der PHP Session-ID sollte erhöht werden (ab PHP 5.0).	x	php.ini: session.hash_function = sha512 session.hash_bits_per_character = 6 session.entropy_length = 64
PHP-Informationen sollten aus dem HTTP-Response Header entfernt werden.	x	php.ini: expose_php = Off
Die Funktion "Force Redirect" sollte	x	php.ini:

aktiviert werden, wenn CGI oder FastCGI verwendet wird. Wenn CGI oder FastCGI nicht eingesetzt wird, muss default aktiviert bleiben.		cgi.force_redirect=On
Es sollte unterbunden werden, dass Inhalt von externen Ressourcen geladen werden kann.	x	php.ini: allow_url_fopen = On Typo3 benötigt die Option allow_url_fopen um z.B. Extensions zu laden. Deshalb muss hier der Wert auf On gesetzt werden.
Es sollte unterbunden werden, dass PHP-Code von externen Ressourcen nachgeladen werden kann.	x	php.ini: allow_url_include = Off
Die Ausführungszeit eines PHP-Skripts sollte zur Reduzierung der Anfälligkeit für Denial of Service-Angriffe begrenzt werden.	x	php.ini: max_execution_time = 240
Um einen Denial of Service-Angriff über Hashtabellen-Kollision zu verhindern, sollte die Anzahl der übergebbaren Parameter beschränkt werden.	x	php.ini: max_input_vars = 1500
Die Interpretation von Rohdaten des POST-Requests sollte nicht generell stattfinden.	x	php.ini: always_populate_raw_post_data = -1
Die maximale Größe von POST-Daten sollte beschränkt werden. Da diese Einstellung auch auf Upload-Requests bezogen wird, sollten die Hersteller-Empfehlungen berücksichtigt werden.	x	php.ini: post_max_size = 12M
Die maximale Größe von Upload-Requests sollte beschränkt werden. Dabei sind die Hersteller-Empfehlungen zu berücksichtigen.	x	php.ini: upload_max_filesize = 10M

4 Web- und Application Server

4.1 Apache Webserver

Da die Dateien der Apache-Konfiguration stark von der Linux-Distribution und der Apache-Version abhängen, können sich die Pfade und Dateinamen unterscheiden, z.B. wird alternativ zu "apache2" oft auch "httpd" verwendet.

Maßnahme	Im Härtungs-skript umgesetzt	Kommandos zur Härtung
Nicht benötigte Apache-Module müssen deaktiviert werden. Aktive Module erhöhen die Komplexität der Installation und damit auch die Angriffsfläche. Die meisten gefunden Schwachstellen im Produkt Apache HTTPd finden sich in Modulen. Schwachstellen in deaktivierten Module sind somit nicht direkt ausnutzbar.	x	root@host:~$ editor /etc/apache2/apache2.conf # Prüfung der LoadModule Direktiven # und/oder root@host:~$ ls /etc/apache2/mods_enabled # Deaktivierung unnötiger Module: root@host:~$ a2dismod <modname> # z.B.: sudo a2dismod autoindex # Insbesondere folgende Module sollten deaktiviert werden: # actions, autoindex, access_compat, suexec, include
Falls mod_suexec nicht verwendet wird, sollten die suexec helper binary entfernt werden.	x	Entfernen/Deinstallieren des apache2-suexec/ apache2-suexec-custom Paketes
Nicht benötigte HTTP-Methoden müssen deaktiviert werden. In den meisten Installationen genügen die Methoden GET und POST. Bei einzelnen Einsatzszenarien können darüber hinaus auch weitere Methoden notwendig sein.	x	root@host:~$ editor /etc/apache2/apache2.conf # Folgende Zeile muss in allen Location, File und Directory-Bereichen vorkommen: AllowMethods GET POST # Zusätzlich muss das Modul allowmethods aktiviert sein sudo a2enmod allowmethods
Informationen über den Webserver in HTTP-Headern müssen auf ein Mindestmaß beschränkt werden.	x	root@host:~$ editor /etc/apache2/conf-enabled/security.conf ServerTokens Prod
Informationen über den Webserver in Fehlerseiten, die durch den Webserver ausgeliefert werden, müssen entfernt werden.	x	root@host:~$ editor /etc/apache2/conf-enabled/security.conf ServerSignature Off
Standardmäßig vorhandene Inhalte müssen entfernt werden.		# Entfernen von default content Inhalten in folgenden Verzeichnissen /opt/apache2/ /var/www/html /usr/lib/cgi-bin/test-cgi root@host:~$ sudo rm <file> root@host:~$ sudo rmdir <directory>

Die Erstellung von Verzeichnislisten (Indizierung) muss deaktiviert werden.		root@host:~$ editor /etc/apache2/apache2.conf # Es darf in der Options-Direktive nicht "Indexes" vorkommen <Directory /> ... Options None ... </Directory>
Alle Webserverprozesse dürfen nicht mit Systemprivilegien laufen.		root@host:~$ editor /etc/apache2/apache2.conf User ${APACHE_RUN_USER} Group ${APACHE_RUN_GROUP} # Die Platzhalter sind unter /etc/apache2/env definiert. APACHE_RUN_USER darf hierbei nicht 'root' entsprechen, sondern muss ein dedizierter Nutzer sein.
Der Webserver darf nur Dateien ausliefern, die für die Auslieferung bestimmt sind. Es kann durch die Directory-, File*- und Location*-Direktiven bestimmt werden, welche Dateien/Pfade aufgerufen werden dürfen und welche verboten sind. Es sollte explizit definiert werden, welche Dateiendungen erlaubt sind.	x	root@host:~$ editor /etc/apache2/apache2.conf <Directory /> AllowMethods GET POST Require all denied Options None AllowOverride None </Directory> <Directory /var/www/> AllowMethods GET POST Require all granted Options SymLinksIfOwnerMatch AllowOverride None </Directory> <FilesMatch "[^.].*\.(?!(css|html|js|pdf|txt|xml|xsl|gif|ico|jpe?g|png|mp4|mp3|mkv|svg|php))[0-9a-z]{2,4}$"> Require all denied </FilesMatch>
Für die Verschlüsselung mit HTTPS muss das TLS-Protokoll verwendet werden.	x	# In der Konfigurationsdatei für SSL muss folgende Direktive eingestellt werden: SSLProtocol All -SSLv2 -SSLv3 # Bei Bedarf auch -TLSv1, so dass nur TLSv1.1 und TLSv1.2 unterstützt werden.
Es muss eine OpenSSL-Version >= 1.0.1 eingesetzt werden, damit das Protokoll TLSv1.2 unterstützt wird. Regelmäßige Updates von OpenSSL erlauben die Verwendung von neueren und sichereren TLS-Protokollen.		# Prüfung der installierten OpenSSL-Version: root@host:~$ openssl version
Die TLS-Konfiguration darf keine unsicheren Cipher-Suites verwenden.	x	# In der Konfigurationsdatei für SSL muss folgende Direktive eingestellt werden: SSLCipherSuite 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-

		SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA256' # Nähere und immer aktuelle Informationen können unter https://wiki.mozilla.org/Security/Server_Side_TLS eingesehen werden.
Die TLS-Konfiguration muss vorsehen, dass beim Verbindungsaufbau die als am sichersten einzustufenden Cipher-Suites mit oberster Priorität ausgewählt werden.	x	# In der Konfigurationsdatei für SSL muss folgende Direktive eingestellt werden: SSLHonorCipherOrder On
SSL-Komprimierung muss deaktiviert werden.	x	# In der Konfigurationsdatei für SSL muss folgende Direktive eingestellt werden: SSLCompression off
Der Zugriff auf den Webserver und Server-Fehler müssen protokolliert werden.	x	root@host:~$ editor /etc/apache2/apache2.conf LogLevel notice ErrorLog ${APACHE_LOG_DIR}/error.log LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined LogFormat "%h %l %u %t \"%r\" %>s %O" common LogFormat "%{Referer}i -> %U" referer LogFormat "%{User-agent}i" agent
Das unautorisierte Überschreiben der Webserver-Konfiguration muss verhindert werden.	x	root@host:~$ chown -R root:root /etc/apache2/ root@host:~$ chmod -R 644 /etc/apache2/
Verschiedene Instanzen des Apache-Webservers auf einem System müssen jeweils als dedizierter Nutzer ausgeführt werden.		root@host:~$ editor /etc/apache2/apache2.conf User ${APACHE_RUN_USER} Group ${APACHE_RUN_GROUP}
Die Webanwendung muss gegen Clickjacking per X-FRAME-OPTIONS-Header abgesichert werden. Siehe https://de.wikipedia.org/wiki/Clickjacking .	x	root@host:~$ editor /etc/apache2/conf-enabled/security.conf Header set X-Frame-Options: "sameorigin" # Hierfür muss das Modul mod_headers aktiviert sein: root@host:~$ a2enmod headers
Die Funktion "TraceEnabled" muss deaktiviert werden, so dass die HTTP-Methode TRACE nicht unterstützt wird.	x	root@host:~$ editor /etc/apache2/conf-enabled/security.conf TraceEnable Off
Apache kann über die LimitRequestBody Direktive die max. Uploadgröße von Dateien festlegen und dadurch einen	x	root@host:~$ editor /etc/apache2/apache2.conf # Die Direktive LimitRequestBody muss für

zusätzlichen Schutz vor DoS-Attacken bieten.		das entsprechende Upload-Verzeichnis gesetzt werden: <Directory "/usr/local/apache2/uploads"> LimitRequestBody 10485760 </Directory>
Wenn nicht unbedingt benötigt, muss die Unterstützung für "Server Side Includes" deaktiviert werden.		root@host:~$ editor /etc/apache2/apache2.conf # Es darf in der Options-Direktive nicht "Includes" vorkommen <Directory /> Options None # (Nicht '+Includes') </Directory> # Das Modul mod_include muss deaktiviert sein: root@host:~$ a2dismod include
Der Logs-Ordner sollte nur im Besitz und beschreibbar von root sein, so dass keine unbefugten Änderungen möglich sind.	x	root@host:~$ chmod 750 /var/log/apache2 root@host:~$ chmod 640 /var/log/apache2/* root@host:~$ chown -R root:adm /var/log/apache2
Der Apache vhost muss dediziert für die Domain konfiguriert sein. Andernfalls wäre es denkbar, dass eine Anwendung durch den Request-Header 'Host:' angreifbar wäre.		# Für jeden Domain und jeden Port wird eine Datei unter /etc/apache2/sites-available/ angelegt: <VirtualHost <domain-name>:80> -> CMS-Konfiguration <VirtualHost <domain-name>:443> -> CMS-Konfiguration SSL <VirtualHost *:80> -> zeigt auf leeren document root # Anschließend wird jede dieser Sites aktiviert: root@host:~$ a2ensite
Der Standard-vhost sollte entfernt werden.	x	root@host:~$ /etc/apache2/sites-enabled/999-default.conf root@host:~$ /etc/apache2/sites-available/999-default.conf

Hinweis: Die folgenden Module müssen aufgrund der getroffenen Härtungsmaßnahmen aktiviert werden:

- headers
- rewrite
- allowmethods

5 Datenbanken

5.1 MySQL

Maßnahme	Im Härtungs-skript umgesetzt	Kommandos zur Härtung
Nicht benötigte (Default-)Datenbanken auf dem Datenbanksystem müssen gelöscht werden.		user@host:~$ mysql -u root -p # Identifizieren der vorhandenen Datenbanken: mysql> SHOW DATABASES; # Wechsel in eine dieser Datenbanken: mysql> USE <database_name>; # Auflistung der Tabellen in dieser Datenbank: mysql> SHOW TABLES; # Löschen einer ganzen Datenbank: mysql> DROP DATABASE <database_name>; # Löschen einer einzelnen Tabelle innerhalb der Datenbank: mysql> DROP TABLE <table_name>;
Nicht benötigte (Default-)Benutzer und (Default-)Rollen müssen gelöscht werden.		user@host:~$ mysql -u root -p # Auflistung aller Benutzer mysql> SELECT user, host FROM mysql.user; # Löschen eines Benutzers mysql> DELETE FROM mysql.user WHERE user='<default user name>';

Erweiterte Privilegien dürfen nur dem Super-User zur Verfügung stehen.		user@host:~$ mysql -u root -p
		mysql> SELECT user, host FROM mysql.user WHERE (Select_priv = 'Y') OR (Insert_priv = 'Y') OR (Update_priv = 'Y') OR (Delete_priv = 'Y') OR (Create_priv = 'Y') OR (Drop_priv = 'Y') OR (File_priv = 'Y') OR (Process_priv = 'Y') OR (Super_priv = 'Y') OR (Shutdown_priv = 'Y') OR (Create_user_priv = 'Y') OR (Grant_priv = 'Y') OR (Repl_slave_priv = 'Y');
		# darf nur root oder debian-sys-maint zurückgeben
		mysql> SELECT user, host FROM mysql.db WHERE db = 'mysql' AND ((Select_priv = 'Y') OR (Insert_priv = 'Y') OR (Update_priv = 'Y') OR (Delete_priv = 'Y') OR (Create_priv = 'Y') OR (Drop_priv = 'Y') OR (Grant_priv = 'Y'));
		# darf nur root oder nichts zurückgeben
		# sollten auch weitere Benutzer zurückgegeben werden, so muss geprüft werden warum diese die erweiterten Privilegien (markiert mit 'Y') besitzen und sie sollten entsprechend angepasst werden.

Die Privilegien SELECT, INSERT, UPDATE, DELETE, CREATE, DROP und ALTER		user@host:~$ mysql -u root -p mysql> SELECT user,host,Db FROM mysql.db

dürfen nur Benutzern gegeben werden, die diese auch für die entsprechenden Datenbanken benötigen.		WHERE Select_priv='Y' OR Insert_priv='Y' OR Update_priv='Y' OR Delete_priv='Y' OR Create_priv='Y' OR Drop_priv='Y' OR Alter_priv='Y'; # Für jeden Eintrag ist zu überprüfen, ob der Benutzer die Rechte für die Datenbanken benötigt.
Es muss sichergestellt sein, dass kein Benutzer mit leerem Benutzernamen existiert.		user@host:~$ mysql -u root -p mysql> SELECT user,host FROM mysql.user WHERE user = ''; # darf nichts zurückgeben.
Es muss sichergestellt sein, dass bei der Benutzer-Authentifizierung keine Wildcards (“%“) im Hostnamen verwendet werden. Durch Wildcards ist es möglich, dass weitaus mehr Clients den Benutzer zur Authentifizierung verwenden können.		user@host:~$ mysql -u root -p mysql> SELECT user, host FROM mysql.user WHERE host = '%'; # darf nichts zurückgeben. # In manchen Fällen ist der Einsatz von Wildcards sinnvoll, der Einsatzzweck sollte jedoch geprüft werden.
Es muss sichergestellt sein, dass ein Login des Super-Users nur an Localhost erfolgen kann.		user@host:~$ mysql -u root -p mysql> SELECT User,Host,Password FROM mysql.user where user='root'; # Nur <hostname>; localhost; 127.0.0.1; ::1 darf zurückgegeben werden
Falls Passwörter als Authentisierungsmerkmal genutzt werden, müssen diese mindestens 8 Zeichen lang sein und drei der folgenden Zeichentypen beinhalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.		# Ab Version 5.6 kann eine Passwort-Policy über das Plugin validate_password eingestellt werden: root@host:~$ editor /etc/mysql/my.cnf # Folgender Inhalt sollte in der my.cnf hinterlegt werden um das Plugin zu aktivieren: [mysqld] plugin_dir = /usr/lib/mysql/plugin plugin-load=validate_password.so validate-password=FORCE_PLUS_PERMANENT # Anschließend muss die Passwort-Policy konfiguriert werden: user@host:~$ mysql -u root -p mysql> SHOW VARIABLES LIKE 'validate_password%'; | validate_password_dictionary_file | | | validate_password_length | 8 | | validate_password_mixed_case_count | 1 | | validate_password_number_count | 1 | | validate_password_policy | MEDIUM | | validate_password_special_char_count | 1 |
Es ist sicherzustellen, dass alle Accounts ein Passwort haben.		user@host:~$ mysql -u root -p mysql> SELECT User,host FROM mysql.user WHERE (plugin IN('mysql_native_password', 'mysql_old_password') AND

		(LENGTH(Password) = 0 OR Password IS NULL)) OR (plugin='sha256_password' AND LENGTH(authentication_string) = 0); # darf nichts zurückgeben.
Zugriffe auf Datenbanksysteme sowie kritische Datenbank-Procedures und Datenbankinhalte müssen geloggt werden.	x	root@host:~$ editor /etc/mysql/my.cnf [mysqld] log-error slow_query_log_file = /var/lib/mysql/slow-query.log slow_query_log = 1 log-raw = OFF # erst seit 5.7 log-warnings = 2
Die Betriebssystemrechte für die Dateien und Verzeichnisse der Datenbank (Programm-, Control-, Trace- und Logdateien) müssen exklusiv dem Betriebssystemkonto des Datenbanksystems zugeordnet werden.		# zum Überprüfen: sudo ls -l <Verzeichnis/Datei> # Identifizieren des Datenverzeichnis: user@host:~$ mysql -u root -p mysql> show variables where variable_name = 'datadir'; root@host:~$ chmod 700 <zurückgegebenes Verzeichnis/Datei> root@host:~$ chown mysql:mysql <zurückgegebenes Verzeichnis/Datei> # Identifizieren der Log-Verzeichnisse und Dateien: user@host:~$ mysql -u root -p mysql> show variables like 'log_bin_basename'; mysql> show variables like 'log_error'; mysql> show variables like 'slow_query_log_file'; mysql> show variables like 'relay_log_basename'; mysql> show variables like 'general_log_file'; root@host:~$ chmod 660 <zurückgegebenes Verzeichnis/Datei> root@host:~$ chown mysql:mysql <zurückgegebenes Verzeichnis/Datei> # Identifizieren der Datei mit dem SSL-Key: user@host:~$ mysql -u root -p mysql> show variables where variable_name = 'ssl_key'; root@host:~$ chmod 400 <zurückgegebenes Verzeichnis/Datei> root@host:~$ chown mysql:mysql <zurückgegebenes Verzeichnis/Datei> # Identifizieren des Plugin-Verzeichnis: user@host:~$ mysql -u root -p mysql> show variables where variable_name = 'plugin_dir' root@host:~$ chmod 755 <zurückgegebenes Verzeichnis/Datei> root@host:~$ chown mysql:mysql <zurückgegebenes Verzeichnis/Datei>

Der Datenbank-Daemon muss mit der Option safe-user-create gestartet werden.	x	root@host:~$ editor /etc/mysql/my.cnf [mysqld] safe-user-create = 1
Die Startoption old-passwords muss deaktiviert werden, um sichere Passwort-Hash-Funktionen zu verwenden.	x	root@host:~$ editor /etc/mysql/my.cnf [mysqld] old-passwords = 0
Die Startoption secure-auth muss verwendet werden, damit keine Accounts mehr verwendet werden können, die noch alte Passwort-Hashes haben.	x	root@host:~$ editor /etc/mysql/my.cnf [mysqld] secure_auth=ON
Sofern nicht benötigt, muss die Symlink-Funktion deaktiviert werden.	x	root@host:~$ editor /etc/mysql/my.cnf [mysqld] skip_symbolic_links=yes
Die Datenbank muss mit der Option local-infile=0 gestartet werden.	x	root@host:~$ editor /etc/mysql/my.cnf [mysqld] local-infile=0
Die Startoption allow-suspicious-udfs muss deaktiviert sein.	x	root@host:~$ editor /etc/mysql/my.cnf [mysqld] allow-suspicious-udfs = false
Die Startoption skip-grant-tables muss deaktiviert sein.	x	root@host:~$ editor /etc/mysql/my.cnf [mysqld] skip-grant-tables = false
Der MySQL-Listener ist an Localhost zu binden (anstelle von skip-networking).	x	root@host:~$ editor /etc/mysql/my.cnf [mysqld] bind-address = 127.0.0.1
Der SQL-Mode NO_AUTO_CREATE_USER muss aktiviert sein.		user@host:~$ mysql -u root -p mysql> SET GLOBAL sql_mode = 'modes + NO_AUTO_CREATE_USER'; SET SESSION sql_mode = 'modes + NO_AUTO_CREATE_USER'; # Wirksamkeit testen: mysql> SELECT @@GLOBAL.sql_mode; SELECT @@SESSION.sql_mode;
Der Datenbank-Dämon muss mit einem dedizierten, nicht-administrativen Unix/Linux-Konto laufen, das auf dem System nur für die MySQL-DB verwendet wird.	x	root@host:~$ editor /etc/mysql/my.cnf [mysqld] user = <mysql-user> # Wirksamkeit testen: user@host:~$ ps -ef | grep "^<mysql-user>.*$" # darf nur den Mysql-Deamon "mysqld" zurückgeben
Standardmäßig loggt Unix alle MySQL-Kommandozeilen-Queries in die .mysql_history Datei im eigenem Home-Verzeichnis. Die History-Datei sollte regelmäßig gelöscht oder gegen /dev/null gelinkt werden. Optional: Betrifft die .bash_history ebenso.		Die Datei ~/.mysql_history darf keine sensiblen Daten/Queries enthalten (optional: ~/.bash_history). Als Softlink Richtung /dev/null: user@host:~$ ln -s /dev/null $HOME/.mysql_history

6 Betriebssysteme

6.1 Linux

Maßnahme	Im Härtungs-skript umgesetzt	Kommandos zur Härtung
Damit während des Boot-Vorgangs die Konfiguration von Grub nicht genutzt werden kann, um direkt in eine Root-Shell zu booten, sollten Teile des Grub-Menüs mit einem Passwort-Schutz versehen werden. Hierfür muss eine Anweisungsdatei für {{update-grub}} unter /etc/grub.d/ angelegt werden, in der ein entsprechendes Passwort gesetzt wird, welches mittels grub-mkpasswd-pbkdf2 erstellt wurde.		# Erstellung eines Passworts mittels grub-mkpasswd-pbkdf2: root@host:~$ grub-mkpasswd-pbkdf2 # Erstellung einer Anweisung für update-grub: root@host:~$ editor /etc/grub.d/01_boot-password # Inhalt der Datei inklusive des Passwort-Hashes aus grub-mkpasswd-pbkdf2: #! /bin/sh cat <<EOF ###################### # Set a boot config protection password ###################### set superusers="root" # The password is: toor -- Generate a new one running grub-mkpasswd-pbkdf2 password_pbkdf2 root grub.pbkdf2.sha512.10000.746EB9982AC[...] # ###################### EOF # Ausführen von update-grub, damit die Änderungen wirksam werden: root@host:~$ update-grub
Viele Dienste und Protokolle öffnen Ports am Server, über die ein Angreifer potentiell ins System eingreifen kann. Aus diesem Grund müssen alle nicht benötigten Dienste und Protokolle deaktiviert werden.		# Prüfung des laufenden Dienste mittels systemctl: root@host:~$ systemctl status <daemon> # Deaktivierung unnötiger Dienste: root@host:~$ systemctl disable xxx.service # Prüfung der offenen Ports: root@host:~$ ss -tulpn root@host:~$ netstat -tulpen
Bei der Installation von Software und Hardware werden oftmals Funktionen aktiviert, die nicht für den Betrieb und die Funktionalität des Systems notwendig sind. Funktionen der Software sind meistens ein fester Bestandteil, der nicht einzeln gelöscht oder deinstalliert werden kann. Solche Funktionen müssen über die Konfiguration oder Einstellungen dauerhaft deaktiviert werden.		
Damit einem Nameserver nicht erlaubt	x	root@host:~$ editor /etc/host.conf

wird, Hostnamen falsch aufzulösen (spoofen), wird die Einstellung des Resolvers so angepasst, dass eine Validierung des Hostnames durchgeführt wird. Dies schützt vor Hostname-Spoofing.		# Inhalt der Datei (Wesentlich ist "nospoof on"): order hosts, bind multi on nospoof on spoofalert on
Der Linux-Kernel kann zum Schutz vor Auswirkungen von Buffer-Overflows angewiesen werden, die Speicherstruktur von Programmen zufällig zu gestalten.	x	root@host:~$ echo 'kernel.randomize_va_space = 2' >> /etc/sysctl.d/99-hardened.conf root@host:~$ sysctl --system
Falls vorhanden, muss die Funktion für „rp_filter“ (Reverse Path Filter) bzw. eine entsprechende Funktion des verwendeten Derivates gesetzt sein. Diese Einstellung bewirkt, dass eingehende Netzwerk-Pakete gefiltert werden, für deren Quell-Adresse keine Rückroute bekannt ist.	x	root@host:~$ echo 'net.ipv4.conf.all.rp_filter = 1' >> /etc/sysctl.d/99-hardened.conf root@host:~$ sysctl --system
ARP-Pakete sollen nur von den Interfaces mit der korrekten Adresse beantwortet werden. Referenz: http://wiki.openvz.org/Multiple_network_interfaces_and_ARP_flux	x	root@host:~$ echo 'net.ipv4.conf.all.arp_filter = 1' >> /etc/sysctl.d/99-hardened.conf root@host:~$ echo 'net.ipv4.conf.default.arp_filter = 1' >> /etc/sysctl.d/99-hardened.conf root@host:~$ echo 'net.ipv4.conf.all.arp_ignore = 1' >> /etc/sysctl.d/99-hardened.conf root@host:~$ echo 'net.ipv4.conf.default.arp_ignore = 1' >> /etc/sysctl.d/99-hardened.conf root@host:~$ echo 'net.ipv4.conf.all.arp_announce = 2' >> /etc/sysctl.d/99-hardened.conf root@host:~$ echo 'net.ipv4.conf.default.arp_announce = 2' >> /etc/sysctl.d/99-hardened.conf root@host:~$ sysctl --system
Die IPv4- und IPv6-Adressen aller Schnittstellen eines Servers müssen statisch konfiguriert werden.	x	root@host:~$ editor /etc/network/interfaces: # Je Interface (hier eth0) muss eine statische IP-Adresse vergeben werden: iface eth0 inet static address 10.0.2.15/24 gateway 10.0.2.1 # Jedes umkonfigurierte Interface muss neu gestartet werden: ip addr flush dev eth0 && ifdown -a && ifup -a
Die Verarbeitung von ICMPv4- und ICMPv6-Paketen, die für den Betrieb nicht benötigt werden, muss deaktiviert werden.	x	root@host:~$ echo 'net.ipv4.icmp_echo_ignore_broadcasts = 1' >> /etc/sysctl.d/99-hardened.conf root@host:~$ echo 'net.ipv4.icmp_ignore_bogus_error_responses = 1' >> /etc/sysctl.d/99-hardened.conf root@host:~$ sysctl --system

IP-Pakete mit nicht benötigten Optionen oder Erweiterung-Headern dürfen nicht bearbeitet werden. Bestimmte Optionen und Erweiterungen von Paketen könnten ausgenutzt werden, um einen Denial-of-Service-Angriff durchzuführen.	x	# Siehe Firewall-Maßnahmen.
Auf dem System gespeicherte Passwörter müssen vor unbefugtem Zugriff geschützt gespeichert werden. Grundsätzlich sollten nur Passwort-Hashes (bcrypt, scrypt) statt Passwörtern gespeichert werden. Dateien, die Hashes von Passwörtern enthalten, müssen vor unbefugtem Zugriff geschützt werden.	x	# Prüfung, dass Passworte nicht in der /etc/passwd hinterlegt sind: root@host:~$ cat /etc/passwd # Einschränkung des Zugriffs auf die /etc/shadow: root@host:~$ chown root:shadow /etc/shadow root@host:~$ chmod 640 /etc/shadow # Suche nach Dateien mit potentiellen enthaltenen Passworten: root@host:~$ find -P / -nowarn -exec grep "passw" {} --print \; 2>/dev/null
Sicherheitsrelevante Ereignisse müssen abhängig vom Verwendungszweck des Systems mit genauem Zeitstempel und einer eindeutigen Systembezeichnung protokolliert werden.	x	# Falls rsyslog als Log-Daemon verwendet wird: root@host:~$ echo 'auth,authpriv.* /var/log/auth.log' >>/etc/rsyslog.conf root@host:~$ echo '$ActionFileDefaultTemplate RSYSLOG_SyslogProtocol23Format' >>/etc/rsyslog.conf
Der Schutz vor SYN-Flood Attacken muss aktiviert werden.	x	root@host:~$ echo 'net.ipv4.tcp_syncookies = 1' >> /etc/sysctl.d/99-hardened.conf root@host:~$ sysctl --system

6.2 SSH

Maßnahme	Im Härtungs-skript umgesetzt	Kommandos zur Härtung
Secure Shell (SSH) muss der einzige Dienst sein, der eine Fernwartung/Remote-Anmeldung mit privilegierten Rechten ermöglicht.	x	root@host:~$ update-rc.d telnet disable root@host:~$ update-rc.d rsh disable
Es muss ausschließlich die Protokollversion SSH-2 eingesetzt werden.	x	root@host:~$ editor /etc/ssh/sshd_config # Einstellung in der sshd_config Datei, dass nur Protokoll 2 verwendet wird, was üblicherweise Standard ist: Protocol 2
Der SSH-Serverdienst muss als Stand-Alone-Daemon ausgeführt werden.	x	root@host:~$ echo 'SSHD_OPTS=' > /etc/default/ssh root@host:~$ update-rc.d xinetd disable
Es müssen starke Krypto-Algorithmen verwendet werden.	x	root@host:~$ editor /etc/ssh/sshd_config # Folgende Einstellung zu den Direktiven Cipher, MAC und KexAlgorithms sollten

		gesetzt werden: Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr MACs hmac-sha2-512,hmac-sha2-256,hmac-ripemd160 KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
TCP/IP-Port-Weiterleitungen („Port Forwarding“) müssen kontrolliert eingesetzt oder deaktiviert werden.	x	root@host:~$ editor /etc/ssh/sshd_config GatewayPorts no # Standardwert
Gateway-Ports dürfen nicht aktiviert werden.	x	root@host:~$ editor /etc/ssh/sshd_config GatewayPorts no # Standardwert
X11-Weiterleitungen müssen kontrolliert eingesetzt oder deaktiviert werden.	x	root@host:~$ editor /etc/ssh/sshd_config X11Forwarding no # Falls X11Forwarding notwendig sein sollte, so sollte es an das Loopback Interface gebunden werden: X11UseLocalhost yes
SSH-„Agent Forwarding“ muss serverseitig deaktiviert werden.	x	root@host:~$ editor /etc/ssh/sshd_config AllowAgentForwarding no
Tunnel Devices dürfen nicht benutzt werden.	x	root@host:~$ editor /etc/ssh/sshd_config PermitTunnel no # Standardwert
Es muss unterbunden werden, dass der Root-Account direkt über SSH angemeldet werden kann. Vorab muss geprüft werden, dass es einen alternativen Nutzer gibt, da sonst eine Aussperrung erfolgt.	x	root@host:~$ editor /etc/ssh/sshd_config PermitRootLogin no
SSH-Logins müssen aufgezeichnet werden.	x	root@host:~$ editor /etc/ssh/sshd_config SyslogFacility AUTH #Standardwert LogLevel VERBOSE
Host-basierte Authentifizierung (via rhosts/shosts) darf nicht verwendet werden.	x	root@host:~$ editor /etc/ssh/sshd_config IgnoreRhosts yes # Standardwert RhostsRSAAuthentication no # Standardwert HostbasedAuthentication no # Standardwert IgnoreUserKnownHosts yes
Ein leeres Passwortfeld darf nicht akzeptiert werden und es sollte der Zeitpunkt der letzten Anmeldung angezeigt werden.	x	root@host:~$ editor /etc/ssh/sshd_config PrintLastLog yes #Standardwert PermitEmptyPasswords no #Standardwert
Administrative Dienste müssen an genau eine Schnittstelle gebunden werden. Wenn der Server an mehreren Netzen erreichbar ist, ist es sinnvoll, administrative und fachliche Netze zu	x	root@host:~$ editor /etc/ssh/sshd_config # Der SSH-Dienst sollte bei Verwendung mehrerer Netze auf die IP-Adresse des administrativen Netzes gebunden sein, so dass er nicht im fachlichen Netz erreichbar ist.

trennen, so dass z.B. SSH ausschließlich aus dem administrativen Netz erreichbar ist.		ListenAddress $IPADDRESS # IP-Adresse des administrativen Netzwerkes (0.0.0.0 = alle Interfaces)
Administrative Dienste müssen an einen definierten Port gebunden werden.	x	root@host:~$ editor /etc/ssh/sshd_config Port 22 #Standardwert
Falls IPv4 und IPv6 nicht gleichzeitig verwendet werden, sollte das zu nutzende Protokoll angegeben werden.	x	root@host:~$ editor /etc/ssh/sshd_config # Angabe, ob IPv4 ("inet") oder IPv6 ("inet6") unterstützt wird. AddressFamily inet
Pluggable Authentication Modules (PAM) sollte nur verwendet werden, falls unbedingt erforderlich. Die Hinweise in der manpage für sshd_config sind zu beachten.	x	root@host:~$ editor /etc/ssh/sshd_config # Angabe, ob PAM genutzt ("yes") oder nicht verwendet wird ("no"). UsePAM no
Die Nutzung des SSH-Dienstes muss auf Gruppen (bzw. Benutzer) beschränkt werden.		root@host:~$ editor /etc/ssh/sshd_config # Angabe von erlaubten Benutzern in der Form user1[@host] mit Trennung durch Leerzeichen: AllowUsers $USERS # Angabe von erlaubten Benutzergruppen mit Trennung durch Leerzeichen: AllowGroups $GROUPS

6.3 Benutzer und Rechte

Maßnahme	Im Härtungs-skript umgesetzt	Kommandos zur Härtung
Alle Prozesse müssen mit den minimal zur Funktion des Prozesses notwendigen Rechten gestartet werden. Insbesondere sollten Prozesse nach Möglichkeit nicht unter dem Benutzer root betrieben werden. Eine Wiederverwendung von Laufzeitbenutzern für mehrere Prozesse sollte vermieden werden, so dass z.B. der Apache httpd und der Tomcat Server nicht mit demselben Benutzer betrieben werden.		
Konfigurationsdateien, die von Prozessen mit Root-Rechten ausgelesen werden können, sowie ausführbare Dateien, die mit Root-Rechten aufgerufen werden (beispielsweise über cron-, Init-Skripte usw.), und die Verzeichnisse, in denen sich diese befinden, müssen mittels Dateisystem-Berechtigungen derart geschützt sein, dass sie nur mit Root-Rechten veränderbar sind.		

Bei der Erstellung von Dateien müssen die Dateiberechtigungen so gesetzt sein, dass das Verändern nur dem Ersteller der Datei bzw. der entsprechenden Gruppe möglich ist.	x	# In hardening.sh in '/etc/profile.d/': umask 0022
Die Mount Points für Dateisysteme, die von Benutzern ohne root-Rechte gemountet werden können, müssen mit der Option „nodev“ und „nosuid“ versehen werden.		# Suchen in /etc/fstab nach Einträgen mit der user-Option und Hinzufügen von nodev und nosuid.
Konten müssen gegen unautorisierte Nutzung durch Verwendung mindestens eines Authentisierungsmerkmals geschützt werden.		# Prüfung der /etc/shadow auf Benutzer ohne Passwort: gawk -i inplace -v INPLACE_SUFFIX=.bak 'BEGIN{FS=OFS=":"} $2==""{$2="!"} {print $0}' /etc/shadow
Die Berechtigungen von Konten und Anwendungen müssen auf ein für deren Aufgaben notwendiges Minimum reduziert werden.		
Vordefinierte Konten müssen deaktiviert werden.		
Accounts (außer Root), die für die Administration bestimmter Dienste eingerichtet werden (beispielsweise ein Account für die Wartung der Datenbank oder des Webservers), müssen so eingerichtet werden, dass damit ausschließlich diejenigen Arbeiten durchgeführt werden können, die für diese Rolle notwendig sind (Prinzip der minimalen Rechte – Least Privilege).		
Jeder System-Account muss eine eindeutige UID aufweisen.		# Prüfung in der /etc/passwd.

Die PATH-Umgebungsvariable aller Accounts darf nicht den Pfad „.“ (aktuelles Verzeichnis) enthalten.	x	# Prüfung, ob in der PATH-Umgebungsvariable ein . enthalten ist:
		# In hardening.sh in '/etc/profile.d/'
		PATH=$(echo -n ${PATH} | awk 'BEGIN{ORS=RS=":"} $0!="."{print $0}')
		export PATH

Vordefinierte Authentisierungsmerkmale müssen geändert werden. Oft werden Software-Komponenten mit einem vordefinierten Passwort installiert. Diese Standard-Passwörter müssen geändert werden, da diese ansonsten zur Authentifizierung von Angreifern genutzt werden können.		
Falls Passwörter als Authentisierungsmerkmal genutzt		# Die Konfiguration einer Passwort-Richtlinie für Betriebssystemnutzer kann in folgenden

werden, müssen diese mindestens 8 Zeichen lang sein und drei der folgenden Zeichentypen beinhalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.		Dateien vorgenommen werden: /etc/login.defs /etc/security/pwquality.conf
Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss ein Schutz gegen Wörterbuch- und Brute-Force-Angriffe vorhanden sein, der das Erraten von Passwörtern stark erschwert.		# Es kann das Paket fail2ban verwendet werden, um Accounts zu sperren, welche mehrmals mit einem falschen Passwort authentifiziert werden sollten.
Falls Passwörter als Authentisierungsmerkmal genutzt werden, darf deren Darstellung nicht im Klartext erfolgen.		root@host:~$ editor /etc/pam.d/common-password # insbesondere die Direktive obscure bewirkt das Ausblenden von Passworten: password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512
Die Identifizierung von Benutzern an Systemaccounts (root, oracle, wlsadmin,...) muss eindeutig sein und darf nur nach einer individuellen, starken Authentifizierung erfolgen. Es dürfen keine gemeinsamen Passwörter für die Remoteanmeldung verwendet werden.		

6.4 Firewall

Maßnahme	Im Härtungs-skript umgesetzt	Kommandos zur Härtung
Die Erreichbarkeit von Diensten muss eingeschränkt werden. Es ist jedoch die Einhaltung von RFC 1122 zu beachten, insbesondere beim Filtern bzw. Zulassen von ICMP Paketen. Falls sich Dienste nicht durch Konfiguration auf die minimal erforderlichen Schnittstellen (z.B. auf localhost) beschränken lassen, muss ein lokaler Paketfilter die Erreichbarkeit reglementieren.	x	# Einstellungen der iptables-Firewall müssen gezielt nach Einsatzzweck vorgenommen werden. Es wird empfohlen, die INPUT und OUTPUT Chains generell zu verwerfen (DROP) und mit einem Whitelist-Ansatz einzelne Ports/Protokolle freizugeben (ACCEPT): root@host:~$ iptables -P INPUT DROP root@host:~$ iptables -P OUTPUT DROP root@host:~$ iptables -P FORWARD DROP # Weiterführend müssen alle ein- und ausgehenden Protokolle und Ports mit ACCEPT definiert werden. # Nach einem Test der Auswirkungen muss iptables persistiert werden, damit es nach einem Neustart weiterhin sicher konfiguriert ist.

6.4.1 Beispiel für eine iptables-Konfiguration

Die IP-Adressen müssen angepasst werden. Eventuell sind weitere Freischaltungen notwendig.

```
# Generated by iptables-save v1.4.21
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -m conntrack --ctstate INVALID -j DROP
-A INPUT -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -m conntrack --ctstate NEW -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -m conntrack --ctstate NEW -j ACCEPT
-A INPUT -s x.x.x.x/32 -p udp -m udp --sport 53 -m comment --comment "first DNS" -j ACCEPT
-A INPUT -s x.x.x.x/32 -p udp -m udp --sport 53 -m comment --comment "second DNS" -j ACCEPT
-A INPUT -p icmp --icmp-type destination-unreachable -j ACCEPT
-A INPUT -p icmp --icmp-type source-quench -j ACCEPT
-A INPUT -p icmp --icmp-type time-exceeded -j ACCEPT
-A INPUT -p icmp --icmp-type parameter-problem -j ACCEPT
-A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -m conntrack --ctstate INVALID -j DROP
-A OUTPUT -d 192.168.x.x/32 -p tcp -m tcp --dport 8080 -m comment --comment "proxy" -j ACCEPT
-A OUTPUT -d x.x.x.x/32 -p udp -m udp --dport 53 -m comment --comment "first DNS" -j ACCEPT
-A OUTPUT -d x.x.x.x/32 -p udp -m udp --dport 53 -m comment --comment "second DNS" -j ACCEPT
-A OUTPUT -d 192.168.x.x/32 -p tcp -m tcp --dport 25 -m comment --comment "mail" -j ACCEPT
-A OUTPUT -s 192.168.x.x/32 -p tcp -m tcp --dport 443 -m conntrack --ctstate NEW -j ACCEPT
-A OUTPUT -p icmp --icmp-type destination-unreachable -j ACCEPT
-A OUTPUT -p icmp --icmp-type source-quench -j ACCEPT
-A OUTPUT -p icmp --icmp-type time-exceeded -j ACCEPT
-A OUTPUT -p icmp --icmp-type parameter-problem -j ACCEPT
-A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
COMMIT
```

Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik, Studie „Sicherheitsuntersuchung von Content-Management-Systemen“, Stand 01.04.2016.

[2] Deutsche Telekom AG, Privacy and Security Assessment Verfahren, http://www.telekom.com/psa, Stand 28.04.2016.

[3] Deutsche Telekom AG, Technische Sicherheitsanforderungen, http://www.telekom.com/static/-/155996/21/technische-sicherheitsanforderungen-si, Stand 28.04.2016.

[4] Bundesamt für Sicherheit in der Informationstechnik, BSI-Standards zur Internet-Sicherheit (Isi-Reihe), https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Isi-Reihe/Isi-Reihe_node.html, Stand 29.10.2015.

Stichwort- und Abkürzungsverzeichnis

Begriff	Beschreibung
BSI-Standards zur Internet-Sicherheit (ISi)	Standard zur Information von Behörden und Unternehmen zur Absicherung von Web-Angeboten
Cascading Style Sheets (CSS)	Computersprache für die Gestaltung digitaler, vorwiegend Web-basierter Dokumente
Common Gateway Interface (CGI)	Standard für den Datenaustausch zwischen einem Webserver und dritter Software
Content-Management-System (CMS)	Software zur Erstellung und Pflege von Webinhalten
Datenbank (DB)	System zur elektronischen Datenverwaltung
Denial of Service (DDoS)	Angriff zur Einschränkung der Verfügbarkeit einer Anwendung oder eines Dienstes
End of Life (EOL)	Bezeichnung für nicht mehr produzierte bzw. nicht mehr lieferbare Produkte
Extensible Markup Language (XML)	Auszeichnungssprache zur Darstellung hierarchisch strukturierter Daten in Form von Textdateien
Hypertext Markup Language (HTML)	Textbasierte Auszeichnungssprache zur Strukturierung digitaler Dokumente
Internet Adresse (IP)	Adresse in Computernetzen
Pluggable Authentication Modules (PAM)	Authentifizierungsframework für Anwendungen und Dienste eines Linux-Systems
Secure Shell (SSH)	Bezeichnet sowohl ein Netzwerkprotokoll als auch entsprechende Programme, mit deren Hilfe man auf eine sichere Art und Weise eine verschlüsselte Netzwerkverbindung mit einem entfernten Gerät herstellen kann
Structured Query Language (SQL)	Datenbanksprache zur Definition von Datenstrukturen in relationalen Datenbanken sowie zum Bearbeiten und Abfragen von darauf basierenden Datenbeständen

Erläuterungen zu Kommando-Syntax:

In den Spalten „Kommandos zur Härtung“ werden teilweise Präfixes verwendet, um anzudeuten, in welchem Kontext der Befehl ausgeführt werden muss. Diese Präfixes und weitere Syntax-Elemente sollen an dieser Stelle beschrieben werden:

Präfix / Syntax	**Beispiel**	**Bedeutung**
root@host:~$	root@host:~$ chmod 644 /pfad/datei	Ein Shell-Befehl, ausgeführt mit Root-Rechten. Alternativ zu dem Root-Nutzer kann hier auch sudo verwendet werden.
user@host:~$	user@host:~$ ps -ef | grep root	Ein Shell-Befehl, ausgeführt ohne spezielle Rechte.
mysql>	mysql> SELECT * from mysql.user;	Ein MySQL-Befehl. Kann entweder in der Kommandozeile oder in einem MySQL-Client verwendet werden.
<datei>:	php.ini:	Hier wird auf den Inhalt einer Datei verwiesen. Ist kein absoluter Pfad zu der Datei angegeben, so ist davon auszugehen, dass die Datei an keinem festen Ort im Dateisystem zu finden ist. Der absolute Pfad der Datei ist abhängig vom Zielsystem.
#	# Prüfung der LoadModule Direktiven	Zeilen, welche mit einem # beginnen, sind Kommentare innerhalb einer Reihe von Anweisungen. Sie dienen lediglich der Dokumentation der Anweisungen.