Austausch- und Kommunikationsplattform forum.ms.de des Schulamtes für die Stadt Münster

Datenschutzerklärung

Quelle: https://iserv.eu/doc/privacy; angepasst

Verantwortung für die Datenverarbeitung

Verantwortlich für die Datenverarbeitung in forum.ms.de (IServ) ist:

Schulamt für die Stadt Münster
Friedrich-Ebert-Straße 110
48153 Münster

Die Kontaktdaten der zuständigen behördlichen Datenschutzbeauftragten:

Jörg Falke
dsb@muenster.org

Ifeanyi Klare
dsb-klare@stadt-muenster.de

Zuständige Aufsichtsbehörde ist:

Die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW Postfach 20 04 44
40102 Düsseldorf
Tel.: 0211/38424-0

E-Mail: poststelle@ldi.nrw.de

Allgemeine Definitionen

Zweckbestimmung

IServ ist eine pädagogische die für forum.ms.de schulübergreifend eingesetzt wird und folgende Komponenten beinhaltet:

- Schulorganisation: Hierzu gehören z.B. Kalender, Adressbuch, Dateiserver, Infobildschirm
- Gruppen- und Benutzerverwaltung samt der zugehörigen Rechte- und Berechtigungsverwaltung
- Kommunikation per E-Mail, Chat, Foren, News

Rechtsgrundlage

Die personenbezogene Verarbeitung von Daten der Nutzerinnen/Nutzer ist insofern zulässig, soweit der Betroffene hierin eingewilligt hat (Siehe Nutzerordnung).

Art der gespeicherten Daten

Zu jeder Nutzerin/jedem Nutzer werden folgende Daten gespeichert:

- Vorname
- Nachname
- Spitzname (Sofern von Benutzer selbst eingegeben)
- farbliche Darstellungen (von Benutzer selbst festgelegt)
- Account im Format vorname.nachname
- Passwort als Prüfsumme
- interne E-Mail-Adresse (Account@forum.ms.de)
- das persönliche Verzeichnis samt dort vom Benutzer abgelegter Dateien wie Bilder, Dokumente, Videos und andere
- Termine
- Datum der Erstellung des Benutzers
- Zeitstempel
- Letzter Login
- Gruppenmitgliedschaften
- persönliche Einstellungen
- Inhalte der Kommunikation aus E-Mail, Chat, Foren, usw.
- IP-Adresse
- Informationen zu http und smtp Anfragen, Raumbuchungen, Klausurplänen (Falls aktiviert)
- Druckaufträge und Druckguthaben (Falls aktiviert)

Sämtliche Anmeldeversuche am Server werden mit IP-Adresse und Zeitstempel protokolliert.

Kreis der Betroffenen

Jede Nutzerin/jeder Nutzer des Servers der einen Account besitzt.

Regelmäßig übermittelte Daten

Es erfolgt grundsätzlich keine Datenübermittlung, weder innerhalb noch außerhalb der Mitgliedstaaten der Europäischen Union.

Zugriffsberechtigung

Alle Nutzerinnen/Nutzer des Servers entsprechend der schulindividuell erteilten Gruppenberechtigungen (siehe Rechte-, Rollenkonzept).

Verfahrensbeschreibung

In diesem Dokument werden die folgenden Arten von Daten unterschieden:

- Auf persönliche Daten hat nur die Nutzerin/der Nutzer selbst Zugriff.
- Auf gruppenbezogene Daten haben alle Mitglieder der jeweiligen Gruppe Zugriff. Die genauen Zugriffsrechte sind konfigurierbar (siehe Rechte, Rollenkonzept).
- Öffentliche Daten werden von ausgewählten Nutzerinnen/Nutzern erstellt (siehe Rechte, Rollenkonzept) und sind für ausgewählte Gruppen oder alle Nutzerinnen/Nutzer lesbar.
- Logs protokollieren Änderungen an Daten oder Zugriffe.

Beim IServ Portalserver gelten folgende systemweite Standards:

- Maßnahmen zur Berichtigung:
    - Persönliche Daten können jederzeit von der Nutzerin/dem Nutzer selbst geändert werden.
    - Gruppenbezogene Daten können von Gruppenmitgliedern geändert werden.
    - Öffentliche Daten können nur von ausgewählten Nutzerinnen/Nutzern (siehe Rechte, Rollenkonzept) bearbeitet werden.
    - Logs können nicht geändert werden.
- Maßnahmen zur Löschung:
    - Nutzerinnen/Nutzer können alle Daten löschen, auf die sie Schreibzugriff haben.
    - Logs werden automatisch nach 6 Monaten gelöscht.
    - Gelöschte Nutzerinnen/Nutzer und Gruppen werden sicherheitshalber noch für 90 Tage gespeichert und danach endgültig gelöscht.
    - Eine Löschung erfolgt im Dateisystem und in der Datenbank.
    - Unabhängig davon können Daten noch für maximal 6 Monate auf dem Backupserver vorgehalten werden.
- Maßnahmen zur Sperrung:
    - Die Daten gelöschter Nutzerinnen/Nutzer und Gruppen werden bis zu ihrer endgültigen Löschung gesperrt.
- Verfahren zur Übermittlung:
    - Daten oder Logs werden nicht automatisiert an Dritte übertragen.
    - In einigen Modulen können Links auf externe Quellen hinterlegt werden. Greift eine Nutzerin/ein Nutzer auf diese zu, sieht der externe Anbieter IP-Adresse und Browser der Nutzerin/des Nutzers, nicht jedoch seine Benutzerkennung.

Für einzelne Module werden mitunter abweichende Regelungen benötigt, die im Folgenden beschrieben sind.

Adressbuch

Jede Nutzerin/jeder Nutzer besitzt einen Eintrag im öffentlichen Adressbuch des Servers, der seinen Vor- und Nachnamen enthält. Dieser kann nach eigenem Ermessen um weitere Daten ergänzt werden. Nutzerinnen/Nutzer können ihren Eintrag im gemeinsamen Adressbuch sperren, damit sie von anderen Nutzerinnen/Nutzern nicht mehr gesehen werden.

Anmeldung

Erfolgreiche und fehlgeschlagene Anmeldungen am Server werden protokolliert.

App

Der IServ Portalserver informiert IServ über das Vorhandensein und den Gelesen-Status von Benachrichtigungen. IServ informiert die App mittels der Benachrichtigungsdienste von Apple respektive Google darüber. Wurde eine Benachrichtigung gelesen, meldet die App dies direkt an den jeweiligen IServ Portalserver zurück. Die Betreiber der Benachrichtigungsdienste sehen nur die Identifikationsnummer einer Benachrichtigung und eine pseudonymisierte Kennung des Accounts, die Inhalte werden direkt zwischen der App und dem jeweiligen IServ Portalserver ausgetauscht.

Darüber hinaus bieten Smartphones vielfältige Funktionen, die personenbezogene Daten mit anderen Apps oder den Herstellern wie Apple und Google teilen, z. B. Cloud-Backups. Diese werden vom Nutzer selbst konfiguriert und liegen außerhalb des Wirkungskreises des Serverbetreibers.

E-Mail

E-Mails werden beim Löschen zunächst in den Ordner „Papierkorb“ verschoben und dort nach 7 Tagen automatisch endgültig gelöscht. Die Nutzerin/der Nutzer kann E-Mails im Ordner „Papierkorb“ auch sofort manuell endgültig löschen.

Von der Nutzerin/dem Nutzer versendete E-Mails werden an die jeweiligen Zielserver übermittelt, die nicht den Datenschutzrichtlinien von IServ unterliegen. Nutzerinnen/Nutzer können auf Wunsch ihre eigenen E-Mails automatisch an eine externe E-Mail-Adresse umleiten. Bei der Einrichtung wird ein entsprechender Datenschutzhinweis angezeigt.

Foren

Nutzerinnen/Nutzer können nur eigene Forenbeiträge ändern und löschen. Administratorinnen/Administratoren können einzelne Beiträge, bestimmte Themen oder ganze Foren löschen. Beim Löschen einer Nutzerin/eines Nutzers wird der Autorenname aus all seinen Forenbeiträgen gelöscht. Der Inhalt der Forenbeiträge bleibt jedoch bei schulöffentlichen Foren dauerhaft und bei gruppenbezogenen über die Lebenszeit der jeweiligen Gruppe erhalten.

Kalender

Keine Abweichungen.

Messenger

Nutzerinnen/Nutzer können über die Oberfläche nur auf Nachrichten aus Räumen zugreifen, in denen sie Mitglied sind. Bei Betreten eines Raumes erhalten Nutzerinnen/Nutzer keinen Zugriff auf frühere Nachrichten im Raum. Nutzerinnen/Nutzer mit dem Recht „Meldungen ansehen“ erhalten die Ausschnitte der gemeldeten Konversationen unabhängig davon, ob sie Mitglied im betroffenen Raum sind.

Von bearbeiteten Nachrichten werden auch sämtliche älteren Fassungen zu Dokumentationszwecken gespeichert. Ebenso bleiben von der Nutzerin/dem Nutzer gelöschte Nachrichten im System gespeichert und werden nur ausgeblendet. Einmal gelesene Nachrichten bleiben auch dann erhalten, wenn die Absender-Nutzerin/der Absender-Nutzer gelöscht wurde. Gelöschte Räume und Räume ohne Mitglieder werden nach spätestens 24 Stunden endgültig vom Server gelöscht.

News

Die Administratorin/der Administrator kann optional einzelne News-Kategorien als RSS-Feed im Internet veröffentlichen.

Office

Das Modul Office bietet die Möglichkeit bei der gemeinsamen Bearbeitung von Dokumenten die Funktion Änderungen nachverfolgen zu aktivieren. Dabei werden die Änderungen, die Nutzerinnen/Nutzer an einem Dokument durchführen, mit ihrem vollen Vor- und Nachnamen verknüpft. Bei der Löschung des Benutzerkontos bleiben diese Informationen im Dokument erhalten, da die Informationen nicht sicher automatisiert aus den Dokumenten entfernt werden können und ein Interesse der anderen Nutzerinnen/Nutzer, welche das Dokument bearbeiten, besteht, den Ursprung von Änderungen nachvollziehen zu können.

Texte

Über den Bearbeitungsverlauf sind alte Versionen der Texte verfügbar. Dies hat zur Folge, dass im Inhalt des Textes gelöschte Informationen weiterhin abrufbar sind. Hierbei sind Änderungen einzelnen Nutzerinnen/Nutzern zugeordnet. Diese Zuordnung bleibt auch nach dem Löschen einer bearbeitenden Nutzerin/eines bearbeitenden Nutzers bestehen, wird aber anonymisiert. Der Bearbeitungsverlauf kann nur gelöscht werden, indem der Text selbst von berechtigten Nutzerinnen/Nutzern gelöscht wird. Nicht alle Nutzerinnen/Nutzer mit dem Recht einen Text zu bearbeiten, können diesen Text auch vollständig löschen.

Umfragen

Die Datenspeicherung erfolgt so, dass nicht zugeordnet werden kann, welche Nutzerin/welcher Nutzer welche Antworten gegeben hat. Die Teilnehmerliste wird automatisch 30 Tage nach Ende der Umfrage gelöscht. Die Ergebnisse einer Umfrage können als CSV-Datei exportiert werden, nicht jedoch die Namen der Teilnehmerin/des Teilnehmers.

Videokonferenzen

Zusätzlich zur Datenverarbeitung auf dem IServ werden die eigentlichen Videokonferenzen auf durch die IServ GmbH betriebenen Servern durchgeführt. Die Server werden bei vertraglichen Partnern der IServ GmbH in Deutschland angemietet. Eine detaillierte Liste der Vertragspartner befindet sich im AV-Vertrag.

An die Server der IServ GmbH werden Klarnamen der Teilnehmer, IP-Adressen, Browserkennungen, Berechtigungen, Videokonferenz-Raum-Einstellungen wie beispielsweise der Raumname und die Adresse sowie eine eindeutige Identifikationsnummer des IServs übermittelt. Auf dem Videokonferenz-Server haben die Nutzerin/der Nutzer die Möglichkeit, Daten in Form von Beteiligungen am virtuellen Whiteboard, Chat-Nachrichten, hochgeladenen Präsentationen und Notizen einzugeben. Außerdem fallen Metadaten wie Dauer der Videokonferenz und Zeitstempel zu Ereignissen wie dem Beitritt oder dem Verlassen einer Konferenz an.

Diese Daten werden frühestens zum Ende der Videokonferenz und spätestens nach Ablauf von sieben Tagen gelöscht. Sicherungskopien dieser Daten werden nicht angelegt.

Audio- und Videoübertragungen werden grundsätzlich nur durchgeleitet, aber nicht gespeichert.

Die IServ GmbH wertet angefallene Daten zusätzlich zur Bereitstellung des Dienstes ausschließlich zu diagnostischen und in anonymisiert Form zu statistischen Zwecken aus. Eine Weitergabe von personenbezogenen Daten an Dritte findet nicht statt.

Technische und organisatorische Maßnahmen

Die für dieses Verfahren eingesetzte Technik ist in die Netzwerkinfrastruktur der citeq eingebunden. Bei der citeq werden technische und organisatorische Maßnahmen getroffen um die Datensicherheit und den Datenschutz sicherzustellen. Sie orientieren sich an den sechs Datensicherheits- und Datenschutz-Schutzzielen, die nachfolgend mit den für dieses Verfahren wichtigsten Maßnahmen aufgeführt werden.

Verfügbarkeit

Innerhalb einer bestimmten Zeit ist sichergestellt, dass auf die Daten zugegriffen werden kann:

- IServ läuft im Dauerbetrieb 24/7. Es gibt keine zeitlichen Zugriffsbeschränkungen
- Es erfolgt eine tägliche Datensicherung. Diese erfolgt auf einem separaten Backupserver im Netzwerk der citeq und kann von dort wiederhergestellt werden.

Vertraulichkeit

Es können nur Personen auf die entsprechenden Daten zugreifen, die auch die Berechtigung dafür haben:

- Es gelten die allgemeinen Zutritts, Zugangs- und Zugriffsregelungen der citeq.
- Durch eine dokumentierte Berechtigungsvergabe wird sichergestellt, dass nur berechtigte Personen auf die Datenbestände zugreifen können. Der Server ist über einen DSL-Anschluss erreichbar und beinhaltet eine Firewall. Die Anmeldung erfolgt ausschließlich durch Benutzeraccount und Passwort

Integrität

Innerhalb einer bestimmten Zeit ist sichergestellt, dass die Daten nicht verändert wurden:

- Auf Server und Backupserver haben nur die Systemadministratoren der citeq bzw. die Fernwartungsauftragsdatennehmer Zugriff. Sie stellen sicher, dass das Betriebssystem regelmäßig aktualisiert wird (Schutz vor Veränderung der Daten durch Angriffe oder unberechtigten Zugriff).
- Innerhalb des Verfahrens haben nur die fachliche Administration dieses Verfahrens und die Personen, die die Datenpflege betreiben, Zugriff auf die Datenbestände (Schutz vor Veränderung durch unberechtigten Zugriff).

Transparenz

Die automatisierte Verarbeitung von Daten kann mit zumutbarem Aufwand geplant, nachvollzogen, überprüft und bewertet werden:

- Die Dokumentation des IServ-Portalservers mit Weboberfläche, des Benutzerbereiches und der Administratoren, die Beschreibung der Module, die Einbindung der Windowsrechner sowie die Installation und Konfiguration ist unter https://iserv.eu/doc/ einzusehen.

Intervenierbarkeit

Die Daten verarbeitende Stelle kann nachweisen, dass sie den Betrieb ihrer informationstechnischen Systeme steuernd beherrscht:

- Der bei der citeq ansässige Systemadministrator kann sämtliche Einlogmöglichkeiten für Teilnehmer und Fernwartungsauftragsdatennehmer jederzeit von jedem Ort sperren.
- Die zuständigen Systemadministratoren sind in der Verwendung des Verfahrens geschult.

Nicht-Verkettbarkeit

Es kann sichergestellt werden, dass Daten nur zu dem Zweck automatisiert verarbeitet werden, zu dem sie erhoben wurden:

- Die Anwendung wird auf einem dedizierten Server betrieben, der nur zu diesem Zweck betrieben wird.

Protokolle

Logdateien

Die im Folgenden beschriebenen Logdateien sind nur der Nutzerin/dem Nutzer *root* in der Systemkonsole zugänglich, nicht jedoch der Administratorin/ dem Administrator über die Weboberfläche. Die Daten dürfen ausschließlich zur Fehleranalyse und nach Absprache mit dem Schulamt für die Stadt Münster zur Aufklärung von Missbrauchsfällen verwendet werden, nicht jedoch für routinemäßige Kontrollen.

Legende

PD: Diese Datei kann personenbezogene Daten wie z. B. IP-Adressen oder Benutzernamen enthalten.

DB: Diese Datei speichert keine zeitliche Abfolge von Ereignissen, sondern Schlüssel-Wert-Paare. Beispielweise speichert /var/log/lastlog für jeden Systembenutzer den Zeitpunkt des letzten erfolgreichen Logins. Dieser gespeicherte Wert wird bei jedem Login aktualisiert. Solche Logdateien haben keine begrenzte Speicherdauer, sondern können nur insgesamt gelöscht werden.

Apache

Apache ist der Webserver, der die Weboberfläche von IServ ausliefert.

Verzeichnis: /var/log/apache2

Dateiname	PD	Speicherdauer	Beschreibung
access.log	ja	7 Tage	Zugriffe (IP-Adresse, Benutzer, Zeitstempel, Anfrage, Status-Code, Größe, Referrer, Browser)
error.log	ja	7 Tage	Fehler (Zeitstempel, Schweregrad, IP, Meldung)
other_vhosts_access.log	ja	7 Tage	Zugriffe auf andere Ports oder Hostnames

APT

APT ist die Debian-Paketverwaltung, die zum Herunterladen und Installieren von IServ-Modulen und IServ-Updates verwendet wird.

Verzeichnis: /var/log/apt

Dateiname	PD	Speicherdauer	Beschreibung
history.log	nein	12 Monate	Aktivitätsprotokoll
term.log	nein	12 Monate	Bildschirmausgabe

Chat

Das Chat-Modul von IServ.

Verzeichnis: /var/lib/iserv/chat

Dateiname	PD	Speicherdauer	Beschreibung
group/*	ja	7 Tage	Gruppenräume
public/*	ja	7 Tage	Öffentliche Räume

Etherpad

Etherpad ist der Backend-Server des Texte-Moduls.

Verzeichnis: /var/log/etherpad-lite

Dateiname	PD	Speicherdauer	Beschreibung
etherpad-lite.log	nein	7 Tage	Warnungen und Fehler

Exim

Exim ist der MTA von IServ, der für den Empfang und Versand von E-Mails verantwortlich ist.

Verzeichnis: /var/log/exim4

Dateiname	PD	Speicherdauer	Beschreibung
mainlog	ja	7 Tage	Zugestellte E-Mails (Zeitstempel, Absender, Empfänger, IP-Adresse, Protokoll)
paniclog	ja	7 Tage	Schwerwiegende Fehler (Zeitstempel, Meldung)
rejectlog	ja	7 Tage	Abgewiesene E-Mails (Zeitstempel, Absender, IP-Adresse, Fehlermeldung)

iservupd

iservupd ist das Updateprogramm von IServ, das jede Nacht automatisch Updates herunterlädt und installiert.

Verzeichnis: /var/log/iservupd

Dateiname	PD	Speicherdauer	Beschreibung
log.*	nein	30 Tage	Programmausgabe

Let's Encrypt

Let's Encrypt ist eine X.509-Zertifizierungsstelle, über die IServ sich selber vollautomatisch kostenlose SSL-Zertifikate erstellen kann.

Verzeichnis: /var/log/letsencrypt

Dateiname	PD	Speicherdauer	Beschreibung
letsencrypt.log	nein	10 Aufrufe	Programmausgabe

PostgreSQL

PostgreSQL ist der Datenbankserver, der vor allem von der Weboberfläche zum Speichern von Daten verwendet wird.

Verzeichnis: /var/log/postgresql

Dateiname	PD	Speicherdauer	Beschreibung
postgresql-*-main.log	ja	7 Tage	Warnungen und Fehler

ProFTPd

ProFTPd ist der FTP-Server von IServ.

Verzeichnis: /var/log/proftpd

Dateiname	PD	Speicherdauer	Beschreibung
controls.log	nein	7 Tage	mod_ctrls-Log
proftpd.log	ja	7 Tage	Logins (Zeitstempel, IP-Adresse, Benutzer)
tls.log	nein	7 Tage	Zugriffe per SSL
write.log	ja	7 Tage	Schreibzugriffe (IP-Adresse, Benutzer, Zeitstempel, Datei, Status-Code, Größe)
xferlog	ja	7 Tage	Datenübertragungen
xferreport	ja	7 Tage	Datenübertragungen

System

Verzeichnis: /var/log

Dateiname	PD	Speicherdauer	Beschreibung
alternatives.log	nein	4 Wochen	Paketverwaltung (update-alternatives)
apcupsd.events	nein	4 Wochen	USV
aptitude	nein	12 Monate	Paketverwaltung (aptitude)
auth.log	ja	7 Tage	Anmeldungen am System (lokal, SSH, cron)
btmp	ja	4 Wochen	Fehlgeschlagene Logins an der Systemkonsole
daemon.log	ja	7 Tage	Systemdienste (u. a. atftpd, dhcpd, iserv, named, ntpd, pptpd, smbd)
debug	ja	7 Tage	Kernel: Debug-Meldungen
dpkg.log	nein	12 Monate	Paketverwaltung (dpkg)
fail2ban.log	ja	7 Tage	Firewall (fail2ban)
fontconfig.log	nein	–	Schrift-Cache. Wird nicht rotiert, aber bei Updates vom fontconfig-Paket überschrieben.
iservbackup	nein	1000 Zeilen	Backup-Status
journal/*/system.journal	ja	7 Tage	Alle Meldungen, die auch in /var/log/*.log landen
kern.log	nein	7 Tage	Kernel: Meldungen
lastlog	ja	DB	Letzte Logins an der Systemkonsole

mail.log	ja	7 Tage	Mailserver (Cyrus)
monit.log	nein	4 Wochen	Monitoring der Systemdienste (monit)
rkhunter.log	nein	7 Tage	Rootkit-Scanner (rkhunter)
slapd.log	ja	7 Tage	Verbindungsaufbauten und fehlgeschlagene Authentifizierungsversuche mit IP-Adresse
syslog	ja	7 Tage	Systemdienste (u. a. atftpd, cron, cyrus, dhcpd, iserv, kernel, named, sessauthd, smbd`, ``spamd)
user.log	ja	7 Tage	Systemdienste (u. a. iserv, regdns, sessauthd)
wtmp	ja	4 Wochen	Letzte Logins an der Systemkonsole

Verzeichnis: /var/lib/iserv/log

Dateiname	PD	Speicherdauer	Beschreibung
auth.log	ja	7 Tage	Anmeldungen am System (lokal, SSH, cron)

ulogd

ulogd protokolliert geroutete TCP-SYN-Pakete mit Zielport 25 (SMTP) oder Zielport 443 (HTTPS) im PCAP-Format, damit bei Warnmeldungen vom Internetanbieter nachvollzogen werden kann, welcher Client Spam versendet haben könnte (SMTP) oder mit einem Virus infiziert sein könnte, wenn dieser mit einem Command-and-Control-Server Kontakt aufgenommen hat (HTTPS).

Verzeichnis: /var/log/ulogd

Dateiname	PD	Speicherdauer	Beschreibung
default.pcap	ja	7 Tage	Default-Log für Pakete, die ulogd nicht zuordnen kann
https.pcap	ja	7 Tage	HTTPS-Pakete
smtp.pcap	ja	7 Tage	SMTP-Pakete

Weboberfläche

Verzeichnis: /var/log/php

Dateiname	PD	Speicherdauer	Beschreibung
*****	ja	7 Tage	IServ 2-Fehlerberichte (Zeitstempel, Speicherinhalt des Programms beim Abbruch)
web/dev.log	ja	7 Tage	IServ 3-Fehlerberichte (Testbetrieb)
web/prod.log	ja	7 Tage	IServ 3-Fehlerberichte (Produktivbetrieb)

Datenbank

Zusätzlich zu den Logdateien im Dateisystem werden von IServ auch Datenbanktabellen zur Protokollierung eingesetzt. Diese Tabellen sind teilweise über die Weboberfläche durchsuchbar oder werden maschinell zu administrativen Zwecken ausgewertet. Außerdem sind die Tabellen dem Benutzer *root* über die Systemkonsole zugänglich.

Sitzungen

Die Benutzer-Sitzungen von Diensten wie dem SMB-Server, dem FTP-Server, dem E-Mail-Server und der Weboberfläche werden in folgenden Tabellen protokolliert.

Tabellennamen	PD	Speicherdauer	Beschreibung
session_log	ja	6 Monate	Erfolgreiche An- und Abmeldungen (Zeitstempel, Benutzername, Dienst, Protokoll, IP-Adresse, Port, Prozess-ID, Sitzungs-ID, Ressource, verwendete Verschlüsselung, kontextabhängige Informationen)
session_fail	ja	6 Monate	Fehlgeschlagene Anmeldungen (Zeitstempel, Benutzername, Dienst, Protokoll, IP-Adresse, Port, Ressource, verwendete Verschlüsselung)

Dateioperationen

Dateioperationen, also das Anlegen, Ändern, Entfernen und Verschieben von Dateien wird in folgenden Tabellen dienstübergreifend protokolliert.

Tabellennamen	PD	Speicherdauer	Beschreibung
file_log	ja	6 Monate	Dateioperationen (Zeitstempel, IP-Adresse, Dienst, Benutzername, Gruppen und Benutzer-Homeverzeichnisse, durchgeführte Aktion, Dateityp, Quell- und Zieldateipfad)
file_log_err	ja	6 Monate	Dateioperationen mit Abweichungen vom Standardschema (Zeitstempel, IP-Adresse, Dienst, Benutzername, Gruppen und Benutzer-Homeverzeichnisse, durchgeführte Aktion, Dateityp, Quell- und Zieldateipfad)
file_log_rnfr	ja	6 Monate	FTP-RNFR-Befehle bis RNTO-Befehl folgt, dann in *file_log* übertragen (Zeitstempel, IP-Adresse, Dienst, Benutzername, Gruppen und Benutzer-Homeverzeichnisse, durchgeführte Aktion, Dateityp, Quell- und Zieldateipfad)

Sonstige Protokolle

Für weitere Ereignisse, wie z. B. das Anlegen einer Nutzerin/eines Nutzers, werden Protokolleinträge in die folgende Tabelle geschrieben.

Tabellennamen	PD	Speicherdauer	Beschreibung
log	ja	2 Jahre (Login-Ereignisse werden nur 6 Monate gespeichert)	Erfolgreiche An- und Abmeldungen (Zeitstempel, Benutzername, Anzeigename des Benutzers, Gruppenname, IP-Adresse, Modul, kontextabhängige Informationen)