

Memorandum of Understanding

Zweck des Memorandums

Dieses Memorandum of Understanding (MOU) dient dazu, die Verwendung von erweiterten Rechten (root, privileged users, Admins) auf trash.net zu klären und zu regeln. Nicht zuletzt geht es auch darum, unseren Benutzern zu zeigen, dass wir ihr Vertrauen verdienen. Wir Besitzer (Frauen sind immer auch eingeschlossen) erweiterter Rechte haben uns auf diese Verhaltensweisen geeinigt und bestätigen mit unserer Unterschrift, dass wir uns daran halten werden. Dieses MOU ist von uns Betroffenen selbst geschrieben und kann von uns jederzeit an neue Situationen angepasst werden.

Begriffsklärung: Mit 'Admins' sind jeweils alle Benutzer mit erweiterten Rechten gemeint.

Ziele der Admins

Wir Admins sind darum besorgt, auf trash.net einen möglichst guten und stabilen Dienst anzubieten. Wenn möglich erweitern wir den Umfang der angebotenen Dienste oder verbessern diese. Ziel ist es, den Usern mit den zur Verfügung stehenden Mitteln und Geräten möglichst viel zu bieten. Wir leisten Freiwilligenarbeit und wertschätzen gegenseitig die aufgewendete Zeit und Einsatzbereitschaft.

Aufgaben der Admins

Jeder Admin kümmert sich selbständig um den ihm überlassenen Bereich. Er hält aber auch immer die Augen offen nach (potentiellen) Problemen in Bereichen, für die er nicht direkt zuständig ist, und informiert den betreffenden Admin bzw. behebt das Problem gleich selbst. Selbstverständlich helfen und unterstützen sich die Admins gegenseitig wo nötig und möglich.

Verwendung von Accounts mit erweiterten Rechten

Erweiterte Rechte werden auf die speziellen *4ta Accounts vergeben und nicht auf normale User Accounts.

Anleitungen zur Bedienung, zu Konzepten und zum Troubleshooting werden in der System-Dokumentation im trash.net Wiki dokumentiert. Änderungen an Services, Konfiguration oder Installation/Update/De-Installation von Software wird auf der jeweiligen VM im /etc/LOG mit Datum und Person dokumentiert.

Diese Änderungen sowie deren Dokumentation im /etc/LOG werden mit etckeeper getrackt und müssen mit einem kurzen Kommentar eingchecked werden.

Logins als User mit erweiterten Rechten werden mit einer durchgehend verschlüsselten ssh-Verbindung (via access1/access2 vom Client zum Server) gemacht. Die Verwendung von ssh erst ab einer Zwischenstation wird vermieden, wenn es nicht absolut unumgänglich ist, augenblicklich über die erweiterten Rechte zu verfügen, und keine andere Möglichkeit besteht.

Um uns vor Fehlern mit möglicherweise schweren Folgen zu schützen, loggen wir uns nur dann als Admins ein, wenn wir diese erweiterten Rechte effektiv brauchen. Wenn die

entsprechende Aufgabe erledigt ist, loggen wir uns sofort wieder aus und arbeiten unter unserem normalen Login weiter.

Generell werden alle Arbeiten, Scripts usw. mit so wenig Rechten wie möglich durchgeführt.

Die privaten Dateien (Homedirs, Mailspool, Queues von at- und cron-jobs, usw.) der User sowie Daten der Benutzer von Dienstleistungen, die trash.net anbietet (zum Beispiel Bier-Server), sind tabu. Die einzigen Ausnahmen sind begründete Verdachte auf Tätigkeiten, die in den Benutzungsregeln ausdrücklich untersagt sind. Die Daten eines Benutzers werden nur mit Vorstands-Beschluss untersucht. Es werden nur die relevanten Dateien eingesehen; Mail nur, wenn es absolut unumgänglich ist, und in diesem Fall auch nur die für den konkreten Fall relevanten. Sämtliche unternommenen Schritte werden detailliert im /etc/LOG der jeweiligen VM eingetragen, und der betroffene Benutzer wird darüber informiert, dass seine Dateien und evtl. sein Mail angeschaut wurden.

Logs, in denen das Verhalten von Benutzern gespeichert wird, werden nur ausgewertet, wenn dies in einem konkreten Fall zur Fehlerbehebung direkt notwendig ist. Solche Datensammlungen werden so klein wie möglich gehalten, alte Daten so bald wie möglich gelöscht.

Alles, was mit erweiterten Rechten gemacht wird, darf von anderen Admins angeschaut werden (z.B. was in den Homedirs der *4ta Accounts liegt) und kann auch protokolliert werden (z.B. Shell-History). Die privaten Homedirs der Admins sind jedoch wie alle anderen Homedirs tabu.

Die zusätzlichen Rechte, die wir Admins haben, verwenden wir dazu, trash.net für die Benutzer attraktiver zu machen. Wir geben uns selbst keine Privilegien damit; solche können nur vom Sysadmin bzw. vom Vorstand verteilt werden.

Verwendung des root-Passwortes

Das root Passwort und andere zentrale Passworte werden in einer KeePass Datenbank aufbewahrt. Diese wird über die trash-cloud zu allen Techstaff Mitgliedern repliziert. So ist eine maximale Verfügbarkeit bei gleichzeitiger Synchronisation sichergestellt.

Verwendung der E-Mail-Adresse <root@trash.net>

Die Adresse <root@trash.net> wird für externe Kommunikation nur in Absprache mit dem Sysadmin verwendet. Die PGP-Keys von root@trash.net werden besonders sorgfältig gehütet und verwendet. Andere Keys werden nur mit diesem Key unterschrieben, wenn sie die dafür definierten Bedingungen erfüllen.

Verhalten in Notfällen

Für Notfälle (System down, Angriff auf System, Spamversand usw.) existieren spezielle Planungen. Jeder Admin leitet alle entsprechenden Schritte ein, sobald er Kenntnis von einer solchen Situation erlangt. Die anderen Admins werden so schnell wie möglich informiert. Details über Missbräuche von trash.net werden ebenfalls im /etc/LOG der jeweiligen VM dokumentiert,

Streitigkeiten

Im Falle von Uneinigkeiten hat der Sysadmin das letzte Wort. Er hört sich die Vorschläge der anderen Admins an, aber als Verantwortlicher für die Maschine muss er nicht darauf

eingehen, sondern macht das, was er für richtig hält und informiert die anderen Admins über die getätigten Aktionen.

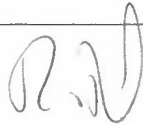




Wegnahme erweiterter Rechte

Der Sysadmin und/oder der Vorstand können die erweiterten Rechte einer Person jederzeit ohne Begründung widerrufen. Der so seines Amtes enthobene Admin wahrt Stillschweigen über systemspezifische Information (zum Beispiel Sicherheitslücken usw.)

Weitergeben des root-Passwortes oder Erteilung erweiterter Rechte

Das root-Passwort oder andere erweiterte Rechte werden nur vom Sysadmin vergeben.

Die folgenden Personen verpflichten sich für die Amtsdauer 2019-2020 zur Einhaltung des MOU:

Name	Datum	Funktion	Unterschrift
Roman Fischer	12.4.19	Präsident	
René Jacquemai	12.4.2019	Kassier	
Othmar Truniger	12.4.2019	Sysadmin	
Frank David	12.4.2019	Vorstand	F. David
Lukas Balle	17.4.2019	Vorstand	
Thomas Bader	21.5.2019	techstaff	
Bent Schneider	21.5.2019	techstaff	B. Schneider