

Acceptable Use Policy / Allgemeine Benutzungsordnung für Dienste der CMO Internet Dienstleistungen GmbH

Allgemeine Verhaltensvorschriften

Der Kunde der CMO darf die Dienste der CMO nur für erlaubte Zwecke nutzen.

Dem Kunden der CMO ist es insbesondere untersagt, die Dienste der CMO zu missbrauchen, um gesetzeswidrige / illegale, obszöne, drohende / bedrohliche, beleidigende, verleumderische, abscheuliche / verabscheuungswürdige Informationen, Daten oder sonstiges Material zu speichern oder abzulegen oder zu übertragen, zu versenden, zu verteilen oder sonst zu verbreiten oder verbreiten zu lassen sowie zu einem Verhalten zu ermutigen oder aufzufordern, das eine strafbare oder ordnungswidrige Handlung begründet oder sonst anderweitig gegen die öffentliche Sicherheit und Ordnung oder gegen nationales oder internationales Recht verstößt.

Die CMO behält sich das Recht vor, gesetzeswidrige Informationen, Daten oder sonstiges Material unverzüglich und ohne vorherige Ankündigung von Ihren Servern oder sonst aus ihren Diensten zu entfernen.

Der Kunde sichert zu, auch die nachfolgenden „Besonderen Verhaltensvorschriften“ zu beachten.

System- und Netzsicherheit

Der Kunde wird jeden Versuch unterlassen, die Benutzer-Authentifikation bzw. die Sicherheit eines Host, eines Netzes oder Kontos zu umgehen oder umgehen zu können („Hacking“ und „Cracking“). Hierunter fallen u.a. der Zugriff auf nicht für den Kunden bestimmte Daten, Einloggen auf einem Server bzw. einem Konto, für die dem Kunden seitens der CMO keine ausdrückliche Zugangserlaubnis vorliegt, sowie „Probing“ der Sicherheit des CMO-Netzes bzw. anderer Netze (z.B. Betreiben eines SATAN-Scan o.Ä. Tools). Jeder SATAN-Scan oder ähnlicher Netz-Scan wird als aktiver Hacking / Cracking-Versuch betrachtet und zur Anzeige gebracht.

Der Kunde wird jeden Versuch unterlassen, Dienste, die an Nutzer, Hosts und Netze erbracht werden, zu stören oder Dienste einzu-setzen die diese stören könnten („Denial-of-Service“-Angriff). Hierunter fallen u.a. das „Flooding“ von Netzen, vorsätzliche Versuche Dienste zu überlasten und Versuche, auf einem Host einen „Crash“ herbeizuführen.

Der Kunde wird jeden Versuch unterlassen, Programme, Skripts oder Befehle zu verwenden bzw. Messages zu senden, die die Computersitzung eines Nutzers durch irgendwelche Mittel bzw. über das Internet stören oder stören könnten.

Im Falle von Zuwiderhandlungen wird die CMO unverzüglich jede tatsächliche und rechtliche Abwehr- und / oder Ahndungsmaßnahme ergreifen, insbesondere auch den oder die Verursacher auf Unterlassung und Schadensersatz in Anspruch nehmen und gegebenenfalls den oder die Vorgänge zur Kenntnis der zuständigen Strafverfolgungsbehörde bringen.

Die CMO unterstützt darüber hinaus in vollem Umfang jede Untersuchung von Verstößen gegen die System- und Netzsicherheit, auch soweit sie davon nicht unmittelbar betroffen wird, falls die zuständigen Behörden die CMO um ihre Mitwirkung ersuchen.

Unbefugte Konten- oder Computernutzung

Der Kunde wird jeden Versuch unterlassen, ein Internet-Konto oder einen Computer ohne entsprechende Berechtigung durch den Inhaber / Eigentümer zu nutzen. Unter derartige Versuche fallen „Social Engineering“, Passwort-Cracking, Abschannen auf Sicherheitslücken, Denial-of-Service-Angriffe (Ping-Flooding), Abschließen / Beendigung von Packets10 mit unzulässiger Paketgröße, UDP11-Flooding, halboffenes TCP, Connection-Flooding etc) u. Ä.

Im Falle von Zuwiderhandlungen wird die CMO unverzüglich jede tatsächliche und rechtliche Abwehr- und / oder Ahndungsmaßnahme ergreifen, insbesondere auch den oder die Verursacher auf Unterlassung und Schadensersatz in Anspruch nehmen und gegebenenfalls den oder die Vorgänge zur Kenntnis der zuständigen Strafverfolgungsbehörde bringen.

Die CMO unterstützt darüber hinaus in vollem Umfang jede Untersuchung von Verstößen gegen die System- und Netzsicherheit, auch soweit sie davon nicht unmittelbar betroffen wird, falls die zuständigen Behörden die CMO um ihre Mitwirkung ersuchen.

e-Mail-Mißbrauch

Der Kunde wird jeden Versuch unterlassen, eMails gegen den erklärten oder mutmaßlichen Willen an Dritte Personen zu senden.

Der Kunde wird insbesondere jeden Versuch unterlassen, einen anderen durch die Zusendung oder sonstige Verwendung einer eMail zu schikanieren, zu belästigen, zu beleidigen oder sonst zu stören. Dies gilt unabhängig von der Form, Sprache, Häufigkeit oder Größe der eMail.

Unter vorstehende Verstöße fällt insbesondere auch der Versand von nicht verlangten, großen eMail-Messages („junk mail“ oder „spam“), sowie der Versand kommerzieller Werbung, informativer Ankündigungen, politischer Schriften etc. Der Kunde darf derartiges Material nur an Empfänger senden, die dieses ausdrücklich und nachweisbar verlangt haben. Unter vorstehende Verstöße fallen auch der Versand von Kettenbriefen sowie „Mailbombing“¹².

Der Kunde wird zudem jeden Versuch unterlassen, Informationen in eMail-Headers zu fälschen

Der Kunde wird auch jeden Versuch unterlassen, Konten und Dienste der CMO zur Sammlung von Antworten auf Messages zu nutzen, die von einem anderen Internet Service Provider verschickt wurden, wenn die entsprechenden Messages gegen die vorliegende Acceptable Use Policy oder die Acceptable Use Policy des anderen Providers verstößen. Diese Regeln gelten auch für andere Distributionsmedien auf Internet-Basis.

Im Falle von Zuwiderhandlungen wird die CMO unverzüglich jede tatsächliche und rechtliche Abwehr- und / oder Ahndungsmaßnahme ergreifen, insbesondere auch den oder die Verursacher auf Unterlassung und Schadensersatz in Anspruch nehmen und gegebenenfalls den oder die Vorgänge zur Kenntnis der zuständigen Strafverfolgungsbehörde bringen.

Die CMO unterstützt darüber hinaus in vollem Umfang jede Untersuchung von Verstößen gegen die System- und Netzsicherheit, auch soweit sie davon nicht unmittelbar betroffen wird, falls die zuständigen Behörden die CMO um ihre Mitwirkung ersuchen.

Wichtiger Hinweis: Elektronische Mail passiert von Ihrer Quelle bis zur Destination zahlreiche Internet Mail-Server. Der Schutz der Privatsphäre wird bei den einzelnen Mail-Servern, auch bei denen der CMO, in der Regel nicht garantiert. Ein auf den absoluten Schutz der Privatsphäre bedachter Kunde sollte daher ein Verschlüsselungssystem verwenden, um die entsprechenden Messages für alle, die sich nicht im Besitz des richtigen Schlüssels befinden, unlesbar zu machen. Die CMO legt großen Wert auf den Schutz der Privatsphäre ihrer Kunden und prüft eMails ihrer Kunden nur, wenn dies unter Beachtung der im Verkehr erforderlichen Sorgfalt notwendig erscheint – z.B. im Falle der Fehlersuche/-beseitigung bei der eMail-Zustellung oder wenn die CMO aufgrund gesetzlicher oder behördlicher Maßnahmen hierzu verpflichtet ist.

Usenet-Vorschriften

Wichtiger Hinweis: Die CMO gibt die eingespeisten News in der Regel ungeprüft weiter, kontrolliert den Inhalt der dem Kunden zur Verfügung stehenden Newsgroup nicht, und haftet nicht für den Inhalt der geposteten Nachrichten in den USENETS; dies gilt auch in den Fällen, in denen es sich beim Autor um einen Kunden der CMO handelt.

Das Posting durch den Kunden in einer USENET Newsgroup muss den schriftlich niedergelegten Charters bzw.

den FAQs (Frequently Asked Questions) der entsprechenden Newsgroup entsprechen. Der Kunde darf nur in denjenigen Newsgroups Anzeigen posten, deren Charters / FAQs dies ausdrücklich gestatten. Der Poster ist für die Bestimmung der Etikette einer bestimmten Newsgroup vor dem entsprechenden Posten verantwortlich.

Der Kunde darf dieselbe oder ähnliche Message in keiner großen Anzahl von Newsgroups posten (Übermäßiges Cross-Posting oder Mehrfach-Posting, auch als „USENET-Spam“ bekannt.)

Der Kunde darf keine Kettenbriefe posten.

Der Kunde darf keine Binärdatei in einer Newsgroup posten, die für den entsprechenden Zweck nicht speziell benannt wurde. Kunden dürfen Posts, bei denen es sich nicht um ihre eigene handelt, nicht löschen, stornieren, aufheben oder sonst außer Kraft setzen, es sei denn, sie sind offizielle Newsgroup Moderatoren in Wahrnehmung ihrer Aufgaben.

Der Kunde darf Header-Informationen nicht fälschen. Darunter fällt auch der Versuch, den Genehmigungsprozess für das Posten in eine moderierte Newsgroup zu umgehen.

Der Kunde darf keine eMails für Adressen verlangen bzw. veranlassen, bei denen es sich nicht um das Konto bzw. den Dienst des Kunden bei der CMO handelt in der Absicht, Antworten in schikanöser oder sonst wie störender Weise zu provozieren oder zu sammeln, nachdem der Dienst bei der CMO gekündigt wurde.

Im Falle von Zuwiderhandlungen wird die CMO unverzüglich jede tatsächliche und rechtliche Abwehr- und / oder Ahndungsmaßnahme ergreifen, insbesondere auch den oder die Verursacher auf Unterlassung und Schadensersatz in Anspruch nehmen und gegebenenfalls den oder die Vorgänge zur Kenntnis der zuständigen Strafverfolgungsbehörde bringen.

Die CMO unterstützt darüber hinaus in vollem Umfang jede Untersuchung von Verstößen gegen die System- und Netzsicherheit, auch soweit sie davon nicht unmittelbar betroffen wird, falls die zuständigen Behörden die CMO um ihre Mitwirkung ersuchen.

- ¹ Illegales Eindringen von Computerbenutzern in fremde Computersysteme
- ² Versuch, sich Zugang zu Computersystemen ohne entsprechende Berechtigung zu verschaffen
- ³ Beobachtung / Protokollierung
- ⁴ Security Analysis Tool for Auditing Networks
- ⁵ Angriff zum Erreichen eines „Verweigern von Leistungen“ auf dem angegriffenen System
- ⁶ „Überfluten“ (z.B. mit e-Mails, Pings etc.)
- ⁷ Absturz
- ⁸ Trickreiches Verleihen von Personen zur Preisgabe ihres Passworts
- ⁹ „Überfluten“ durch Pingen
- ¹⁰ Datenpakete
- ¹¹ User Datagram Protocol = Transportprotokoll im Internet
- ¹² „Überschwemmen“ eines Nutzers bzw. Standorts mit sehr großen bzw. vielen e-Mails.