

# Ist Ihre Acceptable Use Policy (AUP) den sozialen Medien gewachsen?

## Zusammenfassung

Dieses Dokument richtet sich an Entscheidungsträger in der IT, im Personalwesen und Führungspersonen mit Verantwortung für Acceptable Use Policies (AUPs) für E-Mail und Web in einem Unternehmen. Es soll einen Leitfaden darstellen, wie eine AUP aktualisiert werden muss, um der steigenden Beliebtheit und Nutzung sozialer Medien im geschäftlichen Umfeld Rechnung zu tragen. Es identifiziert einige der Probleme, die mit der Erstellung und Verwaltung einer AUP zusammen hängen, insbesondere in Verbindung mit neuen Web-2.0-Technologien, und zeigt, dass eine erfolgreiche AUP mehr ist, als eine einfache Liste mit Ge- und Verboten.

## Inhalt

Einführung: Was ist eine Acceptable Use Policy (AUP)? .....	1
Warum Sie eine Acceptable Use Policy benötigen .....	2
Erstellung und Entwicklung einer AUP .....	2
Warum sich Unternehmen Gedanken über soziale Medien machen sollten .....	3
Wie Sie Ihre AUP auf soziale Medien einstellen .....	6
Fazit .....	6
Referenzen .....	7
M86-Lösungen zur Umsetzung von AUPs .....	7
Web-Sicherheit .....	7
E-Mail-Sicherheit .....	7
Über M86 Security .....	8

## Einführung: Was ist eine Acceptable Use Policy?

Fast alle Unternehmen sind auf die Informationstechnologie angewiesen, um ihr Geschäft zu betreiben. Die meisten Angestellten im Büro nutzen einen Computer, und viele haben einen eigenen Dienst-Laptop oder -PC zur Verfügung, der auch für private Zwecke genutzt wird. E-Mail und Web stellen unabdingbare Werkzeuge dar, die es den Angestellten ermöglichen, ihre Arbeit schnell und effizient durchzuführen. Allerdings kann diese Technologie auch missbraucht werden.

Bereits seit Jahren geben Arbeitgeber ihrem Personal Richtlinien zur angemessenen Nutzung von Telefonen am Arbeitsplatz vor. Die meisten Unternehmen nutzen einen pragmatischen Ansatz und erlauben eine angemessene private Nutzung der Telefone, ausgenommen beispielsweise lange oder internationale Gespräche. Andere haben klare Regeln festgelegt, die keinerlei private Nutzung erlauben. Mit der steigenden Nutzung von E-Mails und Web am Arbeitsplatz wurden diese Regelungen oft auf alle Bereiche der Informationstechnologie ausgedehnt und wurden so zu einer Acceptable Use Policy (AUP).

Diese AUPs waren die ersten Gründe für inhaltsorientierte Funktionalitäten in Sicherheitslösungen für E-Mails. Sie erlaubten den Unternehmen die einheitliche und technisch unterstützte Durchsetzung der Richtlinien. Diese Sicherheitslösungen für E-Mail können genutzt werden, um die Anwender zu schulen, indem diese informiert werden, dass eine Handlung außerhalb der AUP der Organisation lag. Anwender, welche die Medien regelmäßig missbrauchen, rücken ins Blickfeld von IT-Sicherheit und Personalabteilung, die Disziplinarmaßnahmen verhängen können. Diese inhaltsbasierten Funktionen werden nun auch genutzt, um andere Richtlinien durchzusetzen, beispielsweise Compliance und Richtlinien zur Unternehmensführung in den Bereichen E-Mail und Web. Einige Firmen haben eine Richtlinie zur „Durchführung des Geschäftsbetriebs“ (Business Conduct Guideline), an deren Prinzipien sich die Internet-AUP orientieren sollte.

Einige grundlegende Filterfunktionen können als Teil einer AUP eingesetzt werden, darunter:

- Filter für unangemessene Sprache
- Analyse unangemessener Bilder
- Gefährliche Dateitypen
- Unangemessene Websites
- Übermäßige nicht geschäftsrelevante Web-Aktivitäten
- Übermäßige nicht geschäftsrelevante Nutzung von E-Mails

## Warum Sie eine Acceptable Use Policy benötigen

Es gibt drei Hauptgründe für ein Unternehmen, eine AUP für die Nutzung von Web und E-Mail im Unternehmen zu entwickeln:

1. Sicheres Arbeitsumfeld
2. Produktivität der Angestellten
3. Internetsicherheit

Alle drei Bereiche haben Einfluss auf das Unternehmen und die Mitarbeiter und sollten sinnvoll zusammenarbeiten, um zu gewährleisten, dass die Angestellten ihre Tätigkeiten sicher und produktiv ausführen können.



Organisationen sind dafür verantwortlich, ihren Angestellten ein sicheres Arbeitsumfeld zur Verfügung zu stellen, und verschiedene Länder und Rechtsprechungen gehen von verschiedenen Graden der Umsetzung aus. Als Teil dieses Arbeitsumfeldes sollten die Angestellten vor unangemessenem Material geschützt sein, sei es ein Witz per E-Mail oder Bilder auf dem Computer eines anderen Angestellten. Belästigte Angestellte ziehen oft ihren Arbeitgeber zur Verantwortung, auch wenn die Tat von anderen Angestellten ausging. Ein Beispiel für den Ernst dieses Themas ist die Entschädigung von 982.000 US-\$, die ein ehemaliger Angestellter der Stadt Morristown, NJ, erhielt, nachdem er das Opfer fortgesetzter sexueller Belästigung durch einen anderen Angestellten, der derartige Bilder auf einem Arbeitsplatzcomputer zeigte, war. ([http://www.nj.com/news/index.ssf/2009/03/former\\_morristown\\_employee\\_rec.html](http://www.nj.com/news/index.ssf/2009/03/former_morristown_employee_rec.html))

Die Produktivität der Angestellten kann beeinträchtigt werden, wenn unkontrollierter Zugriff auf Internetressourcen wie Sportseiten, Videostreaming, persönliche Webmail und Interneteinkäufe erlaubt ist. Die Einordnung dieser Seiten in zwei Kategorien, „arbeitsbezogen“ und „nicht arbeitsbezogen“ hilft Unternehmen bei der Beobachtung der Nutzung. Aber erst die Möglichkeit, die Nutzung nach Tageszeit einzuschränken oder die Zeit für nicht arbeitsbezogene Tätigkeiten zu begrenzen, ermöglicht die Durchsetzung der AUP. Ein Beispiel wäre, nicht arbeitsbezogene Internetnutzung vor und nach der Arbeitszeit sowie während der Mittagspause zu erlauben. Eine Einschränkung des Zugriffs auf nicht arbeitsbezogene Websites hält die Angestellten bei der Arbeit und vermeidet Ablenkungen.

Auch wenn die Internetsicherheit in erster Linie für die Firmen wichtig ist, sind auch die Angestellten betroffen. Sie können durch Identitätsdiebstahl und andere Kompromittierungen geschädigt werden, die sich aus Internet- bzw. Web-basierten Angriffen ergeben. Die Errichtung effektiver Schutzbarrieren ist einfacher, wenn das Unternehmen den Zugriff auf Inhalte genau kontrollieren kann. Muss beispielsweise ein Angestellter, ausgenommen IT-Personal, Zugriff auf ausführbare Dateien haben? Benötigt irgendein Angestellter außerhalb der Marketingabteilung Zugriff auf Videostreaming und Bilddateien? Durch die strikte Zugriffskontrolle je nach Angestelltem und Dateityp für E-Mail und Web können Sie die Angriffsfläche für Ihr Unternehmen klein halten.

Eine weitere hilfreiche Maßnahme ist eine Zugriffsbeschränkung für bekannte legitime, aber oft durch Schadcode infizierte Seiten, die nicht arbeitsrelevant sind. Das Unterbinden möglichst vieler nicht geschäftsrelevanter E-Mails an die Angestellten reduziert die Wahrscheinlichkeit, dass das System eines Angestellten infiziert wird.

Diese drei Bereiche sind die Hauptgründe für die Entwicklung und Durchsetzung von AUPs; sie beeinflussen sich allerdings manchmal gegenseitig. Deshalb muss ein Unternehmen diese Richtlinien priorisieren. Es ist wichtig zu wissen, dass es nicht die eine, ideale Richtlinie für alle Organisationen gibt. Fangen Sie mit einer Grundstruktur an und passen Sie die AUP dann nach den Bedürfnissen Ihres Unternehmens an.

## Erstellung und Entwicklung einer AUP

Jedes Unternehmen benötigt seine eigene, angepasste AUP, um die Ideale und Standards ihres Betriebs umzusetzen. Sie sollten mindestens die folgenden Punkte in Betracht ziehen:

1. Erlauben Sie eine begrenzte private Nutzung von Web und E-Mail.
2. Umreißen Sie unter Berücksichtigung der Unternehmenskultur, was akzeptabel ist und was nicht.
3. Bleiben Sie konsistent mit der bisherigen Handhabung.
4. Identifizieren Sie alle E-Mails mit Name oder E-Mail-Adresse; vermeiden Sie falsche Absender.
5. Informieren Sie die Mitarbeiter über Urheberrechtsfragen in Zusammenhang mit E-Mails und Internet-Dokumenten.
6. Informieren Sie die Mitarbeiter über akzeptables Verhalten innerhalb und außerhalb der Geschäftszeiten, wenn es dabei Unterschiede gibt (die klar in der Richtlinie hinterlegt sein müssen).
7. Behalten Sie sich das Recht vor, alle Nachrichten und Dateien im Unternehmensnetzwerk zu überwachen.

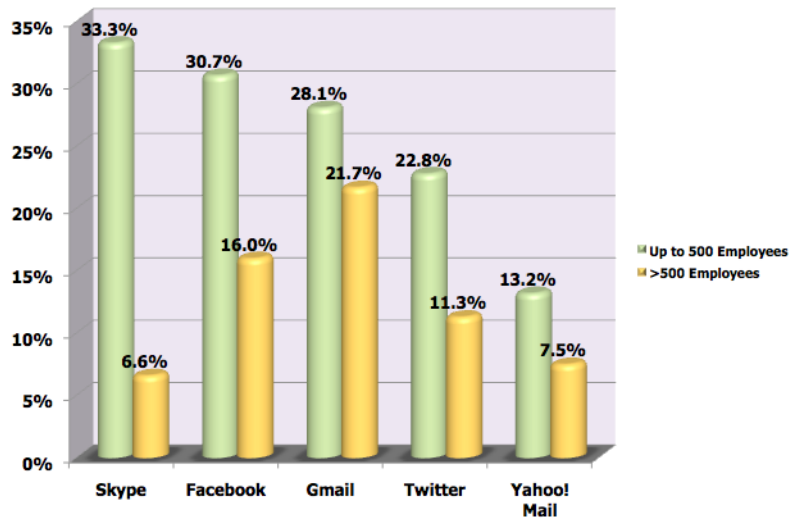
Viele Websites bieten Vorlagen und Ideen für AUPs an. Suchen Sie nach Seiten, die in einer ähnlichen juristischen Zuständigkeit liegen wie Sie, und erwägen Sie mehrere AUPs, wenn Sie Ihr Personal weltweit verteilt haben, um die Unterschiede in örtlichen Gesetzen und Gebräuchen abzubilden. M86 Security bietet ein White Paper und weitere Materialien zur Erstellung von AUPs unter [www.m86security.com](http://www.m86security.com) an.

## Warum Sie sich Gedanken über soziale Medien machen sollten

Soziale Medien verbreiten sich schneller als erwartet. Sie werden zum neuen de-facto-Standard, um mit persönlichen Bekannten in Kontakt zu bleiben und auch immer mehr zum Medium für berufliche Netzwerke. Anwender verbringen jeden Tag mehr Zeit mit sozialen Medien, auch am Arbeitsplatz, und kommunizieren über diese neuen Sites – üblicherweise unbehelligt von Überwachung und Sicherheitsrichtlinien. Deshalb müssen Unternehmen auch die Aktivitäten in sozialen Medien in ihren AUPs erfassen. Das einfache Verbot des Zugriffs schneidet die Anwender ab und schränkt auch ihre arbeitsbezogenen Aktivitäten ein.

Dieses Diagramm zeigt, wie häufig die neuen Kommunikationsformen in unterschiedlichen Unternehmen eingesetzt werden. Viele Firmen nutzen soziale Medien als Teil ihrer Kommunikationskanäle, geben Nachrichten über Twitter weiter oder unterhalten ein Unternehmensprofil auf Facebook und ähnlichen Sites.

Nutzung verschiedener Web-2.0-Werkzeuge aus „The Benefits and Risks of Web 2.0“, einem White Paper von Ostermann Research



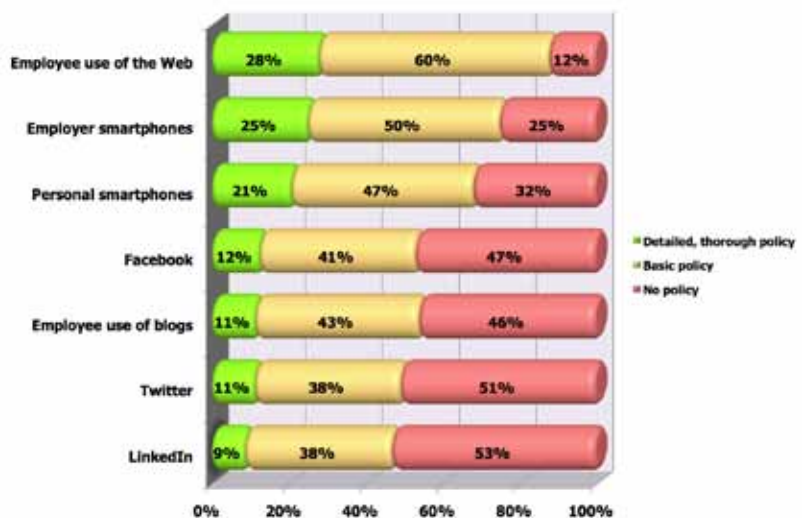
Daten aus Industrie und Forschungen zeigen, dass die Anwender das Web und Web-2.0-Tools verstärkt nutzen. Einige Beispiele:

- Im April 2010 wurden 110 Mrd. Minuten auf Blog-Seiten und in sozialen Netzwerken verbracht. Der typische Besucher verbrachte im Vergleich zum Vorjahr<sup>1</sup> zwei Drittel mehr Zeit auf diesen Seiten.
- Im April 2010 zogen Blog-Seiten und soziale Netzwerke im Vergleich zum Vorjahr 24% mehr Online-Anwender an.
- Es gibt zur Zeit 190 Mio. Anwender auf Twitter<sup>3</sup>, 519 Mio. Anwender auf Facebook<sup>4</sup>, 65 Mio. Anwender auf LinkedIn<sup>5</sup> und 115 Mio. Anwender auf Friendster<sup>6</sup>.

Obwohl soziale Netzwerke den Ruf einfacher Anwendungen haben, gibt es für soziale Netzwerke und verwandte Tools eine Reihe nützlicher Geschäftsanwendungen. Beispielsweise erhalten einige über diese Tools aktuelle Nachrichten von vertrauenswürdigen Kollegen, zeigen Fachwissen gegenüber Kunden und Interessenten, versenden Marketingnachrichten oder kündigen zukünftige Webinare und Messeteilnahmen an.

Diese Werkzeuge können Anwender in ihrer Produktivität steigern, indem sie schnelleren Zugriff auf Informationen ermöglichen, die Entscheidungsfindung beschleunigen und Unternehmen einen direkten Wettbewerbsvorteil bieten. Das folgende Diagramm zeigt, wo die meisten Unternehmen Richtlinien für die Nutzung dieser neuen Technologien festlegen.

Aktuelle Richtlinien zur Nutzung verschiedener Kommunikationsmittel in Organisationen aus „The Benefits and Risks of Web 2.0“, einem White Paper von Ostermann Research



1. Quelle: The Nielsen Company, April 2010 (<http://is.gd/cR9GP>)  
 2. Quelle: The Nielsen Company, April 2010 (<http://is.gd/cR9GP>)  
 3. <http://is.gd/cRaJQ4>  
 4. <http://is.gd/cRaUd>  
 5. <http://is.gd/cRaYw>  
 6. <http://is.gd/cRaYw>

Warum sollten Sie sich die Arbeit machen, eine Richtlinie für neue Kommunikationstechnologien wie soziale Medien zu definieren? Diese Frage geht zurück auf die ursprünglichen Gründe für die Entwicklung von AUPs – sicheres Arbeitsumfeld, Produktivität der Angestellten und Internetsicherheit. Da die Kommunikation über soziale Medien interaktiv ist, sich ihrer niemand entziehen kann und in Echtzeit stattfindet, kann die Nutzung dieser Tools ohne Kontrolle und Überwachung zu Haftungsrisiken für das Unternehmen führen und dessen Ruf gefährden.

E-Mails werden heute in den meisten Firmen gut geschützt und kontrolliert. Noch wichtiger ist, dass die Angestellten dies wissen und deshalb der Missbrauch zurück geht. Soziale Medien allerdings nutzen keine E-Mails zur Kommunikation. Vielmehr werden Webprotokolle wie HTTP und HTTPS eingesetzt, die weniger geschützt und kontrolliert sind. Die meisten Unternehmen haben eine grundlegende URL-Filterung, um sicher zu stellen, dass die Anwender keine pornografischen Websites aufsuchen. In der Vergangenheit gab es auch Unternehmen, die den Zugriff auf soziale Medien völlig blockiert haben. Dies hat sich aber geändert, da diese Sites heute als wertvolle geschäftliche Ressource genutzt werden können.

Da das Web weniger streng kontrolliert wird, ist die Gefahr höher, dass Angestellte unangebrachtes Material verbreiten oder andere Angestellten drangsalieren (die Site selbst unterliegt nicht der Unternehmensrichtlinie). Hier kommt die gut definierte AUP zum Tragen – die Firma besitzt die Infrastruktur, die zum Zugriff auf die Site genutzt wird und hat somit das Recht zu bestimmen, wie diese Infrastruktur genutzt wird. Die Angestellten bei der Sache zu halten ist heute schwieriger, da sie einerseits das Facebook-Profil des Unternehmens bearbeiten, aber auch Zeit auf der eigenen Facebook-Seite verbringen. Über 95% aller Malware-Infektionen entstammen dem Web, so dass gute Schutz- und Kontrollmechanismen entscheidend sind.

Ein abschließender Punkt zum Ruf eines Unternehmens: Es braucht Jahre, um einen guten Ruf aufzubauen, aber nur Sekunden, ihn zu zerstören. Die Presse hat bereits über Angestellte berichtet, die auf Facebook oder Twitter über ihre Vorgesetzten, Mitarbeiter und sogar Kunden herzogen. Hier ein Beispiel:

Im Januar 2009 nutzte ein Angestellter der PR-Agentur Ketchum Twitter, um einige wenig schmeichelhafte Kommentare über die Stadt Memphis abzulassen, kurz bevor eine Präsentation bei der weltweiten Kommunikationsabteilung von FedEx stattfand, dem größten Arbeitgeber in Memphis. Ein Angestellter von FedEx entdeckte den Tweet, antwortete dem Absender und informierte das obere Management von FedEx, die Leitung der Kommunikationsabteilung bei FedEx und die Verantwortlichen bei Ketchum.

Ein leitender Angestellter von FedEx antwortete folgendermaßen: „... alle Teilnehmer der heutigen Veranstaltung, einschließlich derjenigen die heute früh mit Ihnen im Vortragsaal waren, haben gerade ihr erstes Gehalt des Jahres 2009 mit einer Kürzung von 5% erhalten ... viele meiner Mitstreiter stellen genauso wie ich die Investition in Ketchum in Frage, um das Eröffnungsvideo für die heutige Veranstaltung zu produzieren, eine Arbeit, die genauso gut von internen, preisgekrönten Kräften mit jahrzehntelanger Erfahrung in der Fernsehproduktion hätte erbracht werden können.“

<http://shankman.com/be-careful-what-you-post/>

Unternehmen sollten verstehen, wie soziale Medien genutzt und mit einbezogen werden können, bevor sie in Geschäftsprozesse eingebunden werden. Diese Lektion musste die konservative Partei in Großbritannien lernen, als sie eine Website online stellte, welche die Beziehung zwischen dem amtierenden Premierminister, Gordon Brown, und einer großen britischen Gewerkschaft offen legen sollte. Die Konservativen erhofften sich, dass Besucher auf dieser Seite soziale Medien nutzen würden, um die Information weiter zu verbreiten. Durch einen fehlenden Sicherheitsmechanismus auf der Seite konnten Hacker aber die Besucher einfach auf andere Websites umleiten, darunter auch pornografische Websites<sup>7</sup>.

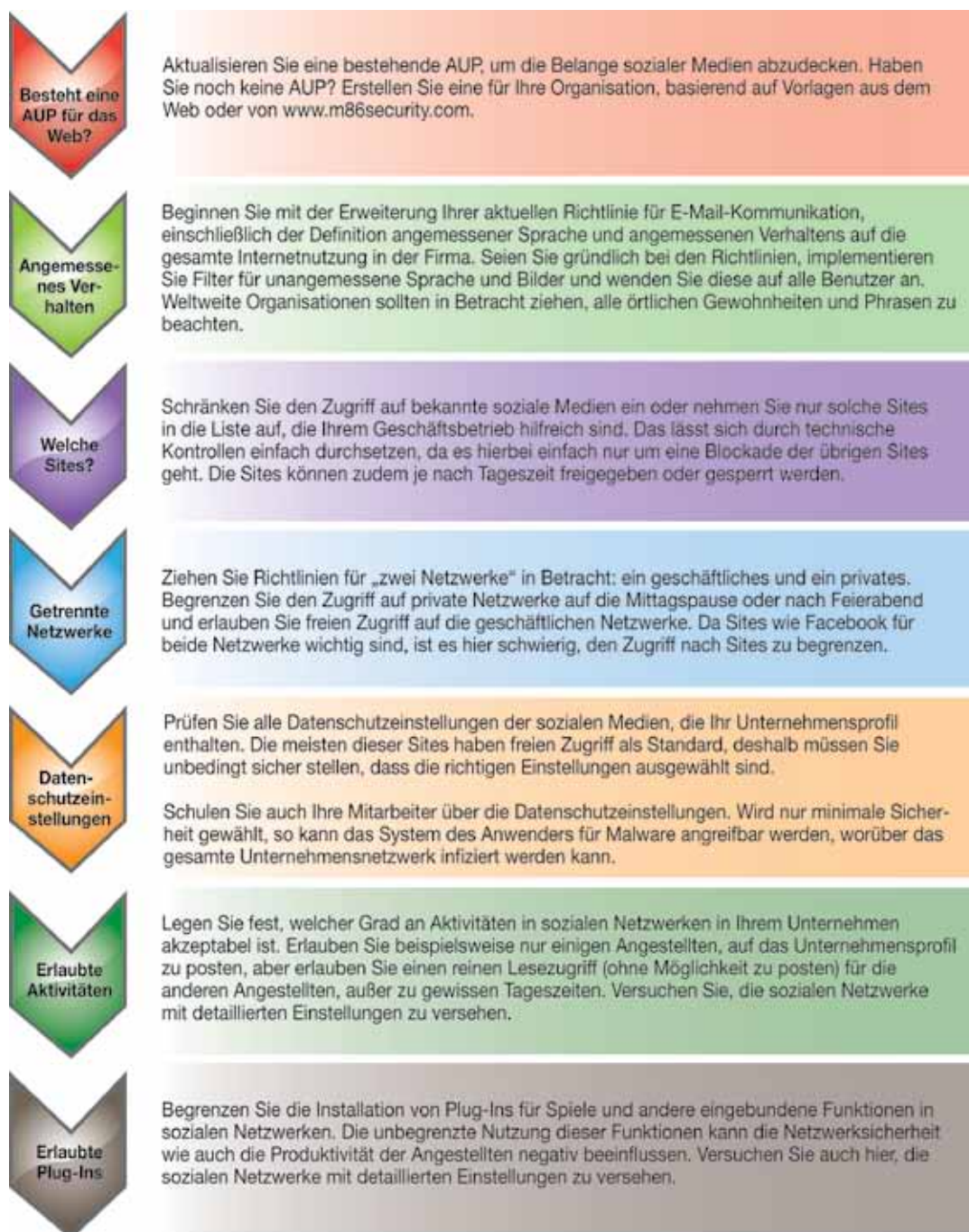
Eines der Hauptprobleme bei der Kommunikation über soziale Netzwerke ist, dass sie für alle offen sind und durch Suchmaschinen indiziert werden. Das bedeutet, dass Konversationen oder Tweets in den Suchergebnissen aller auftauchen, was anderen ermöglicht, sie zu sehen. Das kann zumindest beschämende, aber auch juristische Folgen haben.

---

7. <http://www.telegraph.co.uk/technology/twitter/7499228/Conservatives-embarrassed-as-hackers-exploit-loophole-on-anti-union-website.html>

## Wie Sie Ihre AUP auf soziale Medien einstellen

Das folgende Diagramm zeigt, wie Sie Ihre AUP erweitern können, um den Gebrauch sozialer Medien abzudecken



Diese Schritte stellen sicher, dass Sie eine möglichst effektive AUP erstellen, und helfen Ihnen, die Möglichkeit des Zugriffs Ihrer Angestellten und die Arten von Inhalten genau nach Wunsch zu definieren.

## Fazit

Dieses Dokument hat sich mit der Wichtigkeit und der Nutzung von AUPs für E-Mails und Web beschäftigt. Für viele Unternehmen sind AUPs besonders nützlich, wenn sie diese mit technischen Lösungen für Internetsicherheit durchsetzen. Die richtige Erweiterung Ihrer AUP auf soziale Medien ist entscheidend. Sie riskieren andernfalls Schaden für das Unternehmensimage, juristische Folgen und/oder Malware-Angriffe. Bei der Erweiterung Ihrer AUP auf soziale Medien sollten Sie sich an die Leitlinienempfehlungen und Beispiele zur technischen Durchsetzung in diesem Dokument halten.

## Referenzen

1. Source: The Nielsen Company, April 2010 (<http://is.gd/cR9GP>)
2. Source: The Nielsen Company, April 2010 (<http://is.gd/cR9GP>)
3. <http://is.gd/cRaJQ4> <http://is.gd/cRaUd>
4. <http://is.gd/cRaYw>
5. <http://is.gd/cRaYw> Source: The Nielsen Company, April 2010 (<http://is.gd/cR9GP>)

## M86-Lösungen zur Umsetzung von AUPs

Die Entwicklung einer AUP ist nur der erste Schritt bei der Verwaltung und Regulierung der sozialen Medien im Unternehmen. AUPs werden effektiver, wenn Organisationen diese für alle Anwender konsistent technisch umsetzen. M86 Security bietet innovative Lösungen, die alle Sicherheitsfragen im Internet adressieren, die Produktivität der Anwender sicher stellen und die von Firmen geforderte Überwachung und Berichterstattung bieten.

### Web-Sicherheit

**M86 Secure Web Gateway (SWG)** – Appliance- und SaaS-basierte Lösung, die maximale Sicherheit für Unternehmen gegenüber den verwundbarsten Kanälen im Web, HTTP und HTTPS, bietet. Kombiniert pro-aktive Malware-Erkennung mit URL-Filterung, Virenschutz, Caching und DLP-Kontrollen zur effektivsten Web-Sicherheits- und Produktivitätslösung auf dem Markt. Das SWG umfasst detaillierte Einstellungen für soziale Medien, mit der Unternehmen die Kontrolle über soziale Medien behalten.

**M86 WebMarshal** – Softwarebasierte Web-Gateway-Lösung, die verbesserte Funktionalitäten zur Produktivitätssicherung und Richtlinienumsetzung bietet. Sie geht über reine URL-Filterung hinaus, um umfassende Zugriffskontrollen für das Web, einen umfassenden Schutz vor Gefahren (URL-Filter, Viren- und Malware-Schutz) und Schutz vor Datenlecks in einer einzigen, richtlinienbasierten, einfach zu verwaltenden und hoch skalierbaren Lösung zu vereinen.

**M86 Web Filter** – Appliance-basierte Lösung, welche die Nutzung des Web durch Angestellte kontrolliert und protokolliert, mit besonderem Augenmerk auf die Produktivität. Die Appliance kann kontrollieren, welche Websites die Anwender besuchen, nach welchen Begriffen sie suchen und detaillierte forensische Berichte erstellen. Der Web-Filter wird genutzt, um sicher zu stellen, dass die Anwender ihren Job machen und um sie vor den Gefahren des Web zu schützen.

### E-Mail-Sicherheit

**M86 MailMarshal SMTP** – Eine Sicherheitsprodukt für E-Mail, die Schutz vor Gefahren in E-Mails, Inhaltssicherheit, Richtlinienumsetzung, Compliance und Schutz vor Datenlecks in einer hoch skalierbaren, flexiblen und einfach zu verwaltenden Lösung vereint. M86 MailMarshal arbeitet als E-Mail-Gateway und nutzt eine konkurrenzlos gründliche Spamschutz-Engine, die alle ein- und ausgehenden E-Mails an der Netzwerkgrenze filtert.

**M86 MailMarshal Exchange** – Eine der wenigen Lösungen auf dem Markt, die externe und interne, von Anwender zu Anwender innerhalb der Firma verschickte E-Mails filtert und verwaltet. Sie überwacht und kontrolliert die Inhalte bürointerner E-Mails, die innerhalb der Organisation versendet werden, um ein sicheres, produktives Arbeitsumfeld und Compliance mit Acceptable Use Policies zu gewährleisten.

**M86 MailMarshal E-Mail Encryption Solutions** – Diese Lösungen bieten alle Möglichkeiten zur Verschlüsselung von E-Mails, die Unternehmen bei der Business-to-Business (B2B)- oder Business-to-Consumer (B2C)-Kommunikation benötigen. Die Lösungen können automatisch über Richtlinien eingesetzt werden, die in den MailMarshal-Produkten hinterlegt werden und gewährleisten, dass das Unternehmen sicher mit seinen Kunden und Geschäftspartnern kommunizieren kann.

## Über M86 Security

M86 Security ist ein globaler Spezialist für die Gefahrenabwehr in Echtzeit und der Branchenführer für Secure Web Gateways. Die Lösungen des Unternehmens für Web- und E-Mail-Sicherheit, angeboten als Appliances, Software oder Software as a Service (SaaS), schützen über 24.000 Kunden mit über 17 Millionen Anwendern weltweit. Die Produkte von M86 nutzen eine patentierte Code-Analyse in Echtzeit und verhaltensbasierte Technologien zur Erkennung von Malware sowie ständig aktualisierte Daten der M86 Security Labs. Netzwerke werden so gegen weiterentwickelte Gefahren geschützt, die Vertraulichkeit sensibler Informationen gewährleistet und die Compliance garantiert. Das Unternehmen hat seinen Sitz in Orange, Kalifornien, eine internationale Niederlassung in London und Entwicklungszentren in Kalifornien, Israel und Neuseeland. Weitere Informationen zu M86 Security finden Sie unter [www.m86security.com](http://www.m86security.com).

### ERST TESTEN, DANN KAUFEN

M86 bietet Ihnen die Lösungen zum kostenfreien Test und zur Evaluierung. Bitte kontaktieren Sie uns dazu direkt oder gehen Sie auf [www.m86security.com/downloads](http://www.m86security.com/downloads)



**Central Europe**  
Alte Landstrasse 27  
85521 Ottobrunn b. München  
Deutschland

Tel.: +49 (0)89 673597-0  
Fax: +49 (0)89 673597-50

**International Headquarters**  
Renaissance 2200  
Basing View, Basingstoke  
Hampshire RG21 4EQ  
United Kingdom  
Phone: +44 (0) 1256 848080  
Fax: +44 (0) 1256 848060

**Corporate Headquarters**  
828 West Taft Avenue  
Orange, CA 92865  
United States

Phone: +1 (714) 282-6111  
Fax: +1 (714) 282-6116

Version 08/26/10