BEST PRACTICES:

AUPs

Geltende Anwendungsrichtlinien

Als Cybersicherheitsexperte ist es einfach, sich auf die Sicherheitskontrollen zu konzentrieren, die Ihre Unternehmensinfrastruktur aktiv schützen, die Daten sichern und gleichzeitig das Risiko durch bösartige Akteur*innen, Bedrohungen und zahlreiche Angriffe mindern. Aber es gibt noch weitere Schlüsselelemente für die Sicherheit Ihres Unternehmens. Ein Paradebeispiel dafür sind die Nutzungsbedingungen (Acceptable Use Policies, AUPs).

jamf

Was ist ein AUP?

Eine Acceptable Use Policy (AUP) ist ein Regelwerk, das von der Geschäftsleitung oder dem Management einer Organisation festgelegt wird und bestimmt, wie Geräte, Software, Daten, Dienste und Ressourcen von den Nutzer*innen dieser Ressourcen zu behandeln sind. AUPs schränken ausdrücklich ein, was die Beteiligten tun können und was sie nicht tun dürfen.

Warum sind sie wichtig?

AUPs sind aus mehreren Gründen notwendig. Es handelt sich dabei vor allem um Leitlinien, die von Organisationen aus allen Branchen weltweit umgesetzt werden:

- Erwartungen an das Verhalten der Endbenutzer*innen festlegen
- Einholung einer Bestätigung, dass die Nutzer*innen die Regeln kennen, verstehen und ihnen zustimmen
- Beschränkung der Nutzung von Hardware, Software, Netzwerken und Websites
- Angleichung der Nutzungsrichtlinien an den Rahmen für die Informationssicherheit zum Schutz der Daten

Viele Organisationen verlangen von den Nutzer*innen ihrer Ressourcen die Unterzeichnung einer AUP, um das Risiko einer rechtlichen Haftung**lich zu verringern. Wenn Endbenutzer*innen und Mitarbeiter*innen über ihre Rechte und Erwartungen bei der Nutzung von Unternehmensressourcen informiert werden, ist es einfacher, die Benutzer*innen aufzuklären und ihnen die Konsequenzen bei Nichteinhaltung der Richtlinien zu vermitteln.**

Entdecken Sie:

1. Was die Acceptable Use Policy bedeutet
2. Warum sie ein wesentlicher Bestandteil Ihrer Sicherheitsmaßnahmen sind
3. Wie Sie Best Practices anwenden, um eine AUP mit Ihrer bestehenden Datenverwaltungsstrategie abzustimmen und Ihren Defense-in-Depth-Plan zu stärken.

Bewährte Verfahren zur Erstellung und Durchsetzung von AUPs

1. **Bewertung.** Bewerten Sie die Ausgangssituation Ihrer Organisation. Überlegen Sie, wie die Benutzer*innen mit den Ressourcen interagieren sollen, wie der Zugriff mit ihren Rollen zusammenhängt und wie dies den geschäftlichen Anforderungen entspricht.

2. **Identifizieren.** Es kann sein, dass Ihre AUP für mehr als nur organisatorische Geräte gilt. Es ist wichtig, die Geräte und Benutzer*innen zu identifizieren, die in den Geltungsbereich Ihrer Richtlinie fallen. Überlegen Sie, ob persönliche Geräte, wie BYOD und vom Benutzer/von der Benutzerin registrierte Geräte, einbezogen werden sollten. Mit dieser Bestimmung können IT-Administrator*innen die richtige Konfiguration implementieren, um den Zugriff auf ihr sicheres Netzwerk auf der Grundlage von Bestandsverwaltungsdatensegmenten zu erlauben oder zu verweigern.

3. **Angleichen.** AUPs sollten sich an Rahmenwerken für die Informationssicherheit orientieren, wie dem Center for Information Security (CIS). Durch die Angleichung der Verwaltungs- und Sicherheitskontrollen sind AUPs kein eigenständiges Dokument. Sie sind Teil einer ganzheitlichen Strategie, die Sie einen Schritt näher an die Tiefenverteidigung mit Abdeckung mehrerer Sicherheitsebenen bringt.

4. **Umfunktionieren.** Sie müssen nicht mit einer leeren Seite beginnen. Recherchieren Sie und nutzen Sie die verfügbaren Ressourcen, die Ihnen bei der Erstellung einer AUP helfen, die auf die Bedürfnisse Ihres Unternehmens zugeschnitten ist. Von Ressourcen, die spezifische Formulierungen für spezielle Anforderungen bereitstellen, bis hin zu umfassenderen Vorlagen, die von vertrauenswürdigen Organisationen auf der Grundlage von Fachgebieten der Informationssicherheit entwickelt wurden, wie z. B. das Verzeichnis der Sicherheitsrichtlinienvorlagen des SANS Institute oder die CIS-Vorlage für die akzeptable Nutzung von Informationstechnologie-Ressourcen.

5. **Durchsetzen.** Jegliche Aktivitäten, die als schädlich erachtet werden, gegen lokale, staatliche, bundesstaatliche oder regionale Gesetze verstoßen, andere Nutzer*innen negativ beeinflussen oder Schaden verursachen – unabhängig von der Absicht – müssen in Ihrer AUP behandelt werden. Denken Sie daran, dass es wichtig ist, die Gerichtsbarkeit anzugeben, für die die AUP gilt. Dies kann die rechtliche Belastung verringern, wenn es zu einem Vorfall kommt, der rechtliche Schritte erfordert. Indem sie spezifisch angeben, für wen die AUP gilt und in welcher Region sie effektiv durchsetzbar ist, können Organisationen, die an mehreren Orten tätig sind, den verschiedenen Graden der rechtlichen Haftung Rechnung tragen, die geoabhängig ist.

jamf

www.jamf.com/de/

Wir unterstützen Sie gerne. Erfahren Sie mehr über die Sicherung Ihres Arbeitsplatzes mit Jamf Trusted Access.