CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Arten von Systemhärtung

Betriebssystemhärtung

Dies beinhaltet die Sicherung des Betriebssystems durch dessen Konfiguration zur Minimierung von Schwachstellen. Es umfasst Maßnahmen wie das Deaktivieren unnötiger Dienste, Schließen ungenutzter Ports, Aktivieren von Sicherheitsfunktionen wie Firewalls und Intrusion Detection Systemen, Durchsetzen starker Passwortrichtlinien und regelmäßiges Anwenden von Sicherheitspatches und Updates.

Anwendungshärtung

Die Anwendungshärtung konzentriert sich auf die Sicherung einzelner Softwareanwendungen, die auf dem System laufen. Sie beinhaltet Maßnahmen wie das Entfernen oder Deaktivieren unnötiger Funktionen und Funktionalitäten, Anwenden anwendungsspezifischer Sicherheitspatches und Updates, Verwenden sicherer Programmierpraktiken und Aktivieren von anwendungsebenen Zugangskontrollen und Authentifizierungsmechanismen.

Netzwerkhärtung

Die Netzwerkhärtung zielt darauf ab, die Netzwerkinfrastruktur und Kommunikationskanäle zu sichern. Sie beinhaltet Maßnahmen wie das Konfigurieren von Firewalls, Implementieren von Intrusion Prevention Systemen (IPS) und Intrusion Detection Systemen (IDS), Aktivieren von Verschlüsselungsprotokollen wie SSL/TLS, Segmentieren des Netzwerks zur Reduzierung der Auswirkungen eines Bruchs und Implementieren von Netzwerkzugangskontrollen.

Benutzerkhärtung

Die Benutzerkontenhärtung konzentriert sich auf die Sicherung von Benutzerkonten und deren Privilegien. Sie umfasst Maßnahmen wie das Durchsetzen starker Passwortrichtlinien, Implementieren von Multi-Faktor-Authentifizierung (MFA), Einschränken der Benutzerprivilegien auf das Notwendige, regelmäßiges Überprüfen und Deaktivieren ungenutzter Konten und Überwachen von Benutzeraktivitäten auf verdächtiges Verhalten.

Patch-Management

Das regelmäßige Anwenden von Sicherheitspatches und Updates ist entscheidend für die Systemhärtung. Patch-Management beinhaltet das Überwachen und Installieren von Softwareupdates, einschließlich Betriebssystempatches, Firmware-Updates und Anwendungspatches. Dies hilft, bekannte Schwachstellen anzugehen und das System vor Ausnutzung zu schützen.

Systemüberwachung und -protokollierung

Die Implementierung robuster Überwachungs- und Protokollierungsmechanismen ist wesentlich für die Systemhärtung. Sie beinhaltet das Einrichten von Sicherheitsereignisprotokollierung, Überwachen von Systemprotokollen auf verdächtige Aktivitäten, Implementieren von Intrusion Detection Systemen und Durchführen regelmäßiger Sicherheitsaudits und -überprüfungen, um potenzielle Bedrohungen rechtzeitig zu identifizieren und darauf zu reagieren.

Sicheres Konfigurationsmanagement

Sicheres Konfigurationsmanagement beinhaltet das Festlegen und Aufrechterhalten sicherer Konfigurationen für verschiedene Systemkomponenten, wie Hardware, Betriebssysteme und Softwareanwendungen. Es umfasst Maßnahmen wie das Deaktivieren unnötiger Dienste und Protokolle, Konfigurieren von Zugangskontrollen, Aktivieren von Verschlüsselung und Implementieren sicherer Kommunikationsprotokolle.

Sicherheitsbewusstsein und -schulung

Die Systemhärtung beinhaltet auch das Schulen von Nutzern und Administratoren über Sicherheitsbestpraktiken und potenzielle Bedrohungen. Das Durchführen von Sicherheitsbewusstseinsprogrammen und Schulungssitzungen hilft, das Bewusstsein für Sicherheitsrisiken, Phishing-Angriffe, Social Engineering und andere häufige Angriffsvektoren zu schärfen. Es ermöglicht Nutzern, informierte Entscheidungen zu treffen und sichere Praktiken zu befolgen.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm