Security-Referenzinformationen

Sicherheitsempfehlungen und -benachrichtigungen finden Sie unter http://www.cisco.com/go/psirt sowie weitere Informationen des Product Security Incident Response Team (PSIRT).

Best Practices

Erhöhte Sicherheit auf Cisco Routern

In diesem Dokument werden einige Konfigurationseinstellungen von Cisco vorgestellt, die Netzwerkadministratoren zur Verbesserung der Sicherheit in Erwägung ziehen sollten, ihre Router, insbesondere die Routergrenzen, zu ändern. In diesem Dokument geht es um grundlegende "boilerplate"-Konfigurationselemente, die nahezu universell in IP-Netzwerken anwendbar sind, sowie um einige unerwartete Elemente, von denen Sie sich bewusst sein sollten.

Cisco IOS-KennwortverschlüsselungsFakten

Eine Quelle, die nicht von Cisco stammt, hat ein Programm zur Entschlüsselung von Benutzerkennwörtern (und anderen Kennwörtern) in Cisco Konfigurationsdateien veröffentlicht. Das Programm entschlüsselt keine Kennwörter, die mit dem Befehl **enable secret** festgelegt wurden. Die unerwartete Sorge, die dieses Programm bei Kunden von Cisco hervorgerufen hat, hat uns zu dem Verdacht geführt, dass viele Kunden für mehr Sicherheit auf die Cisco Passwortverschlüsselung angewiesen sind, als sie eigentlich vorgesehen war. In diesem Dokument werden das Sicherheitsmodell für die Passwortverschlüsselung von Cisco und die Sicherheitsbeschränkungen dieser Verschlüsselung erläutert.

SAFE-Entwurf von Cisco
SAFE ist ein umfassendes Sicherheitskonzept, das Unternehmen die sichere Teilnahme am E-Business ermöglicht. SAFE nutzt einen modularen Ansatz, der das Sicherheitsdesign, die Bereitstellung und das Management vereinfacht, wenn Netzwerke wachsen und sich ändern, und optimiert so Netzwerke, die auf Cisco AVVID (Architektur für Sprache, Video und integrierte Daten) basieren.

Strategien zur Abwehr, Verfolgung und Eindämmung von Angriffen

Charakterisierung und Verfolgung von Paketfluten mit Cisco Routern

> Denial of Service (DoS)-Angriffe sind im Internet üblich. Der erste Schritt bei der Reaktion auf einen solchen Angriff besteht darin, herauszufinden, welche Art von Angriff er ist. Viele der häufig verwendeten DoS-Angriffe basieren auf Paketfluten mit hoher Bandbreite oder auf anderen sich wiederholenden Paketströmen. Dieses Dokument bietet Einblicke in das Verständnis und die Nachverfolgung dieser Angriffe.

Strategien zur Bekämpfung des Nimda-Virus

Dieser Index enthält eine umfassende Auflistung aller technischen Tipps und Empfehlungen zur Eindämmung des Nimda-Virus.

[Strategien zur Bekämpfung des Code Red Worm]

Dieser Index enthält eine umfassende Auflistung aller technischen Tipps und Empfehlungen zur Eindämmung des Code Red Wurms.

[Strategien zum Schutz vor DDoS-Angriffen (Distributed Denial of Service)]

Dieses Whitepaper enthält eine technische Beschreibung des Vorfalls eines potenziellen DDoS-Angriffs und Vorschläge für Methoden, wie die Cisco IOS-Software dagegen eingesetzt werden kann.

[Strategien zum Schutz vor Denial-of-Service-Angriffen über UDP-Diagnoseports]

Dieses Whitepaper enthält eine technische Beschreibung des Vorfalls eines potenziellen UDP Diagnostic Port-Angriffs und Vorschläge für Methoden zum Einsatz der Cisco IOS-Software zum Schutz vor diesem Angriff.

[Strategien zum Schutz vor Denial of Service-Angriffen auf TCP SYN]

Dieses Whitepaper enthält eine technische Beschreibung des Vorfalls eines potenziellen TCP-SYN-Angriffs und Vorschläge für Methoden zur Abwehr dieser Angriffe mit der Cisco IOS-Software.

[Die neuesten Denial-of-Service-Angriffe: Beschreibung und Informationen zur Minimierung von Effekten]
Hinweis: Der obige Link verweist auf eine externe Website, die nicht von Cisco Systems, Inc. verwaltet wird.

Sie liefert detaillierte Informationen zu "smurf"-Angriffen, mit Schwerpunkt auf Cisco Routern und wie die Auswirkungen dieser Angriffe reduziert werden können. Einige Informationen sind allgemein gehalten und stehen nicht in Zusammenhang mit dem Hersteller, der eine bestimmte Wahl getroffen hat. Er wurde jedoch mit dem Schwerpunkt eines Cisco Routers geschrieben. Dieses Dokument bestätigt nicht die Auswirkungen von "smurf"-Angriffen auf Geräte anderer Anbieter. Sie enthält jedoch Informationen über verschiedene Anbieter.

Weitere Ressourcen

[Cisco Produkt-Sicherheit - Reaktion auf Vorfälle]

Dieses Dokument beschreibt die Verfahren zur Fehlerberichterstattung und Reaktion auf Vorfälle - insbesondere, was zu tun ist, wenn Sie sich in einem aktiven Sicherheitsangriff befinden oder glauben, angegriffen zu werden, wenn Sie ein Sicherheitsproblem mit einem Cisco Produkt haben, technische Sicherheitsinformationen zu einem Cisco Produkt erhalten möchten oder wenn Sie zusätzliche Fragen zu einem angekündigten Sicherheitsproblem mit einem Cisco Produkt haben. Die Rolle des Cisco Product Security Incident Response Team (PSIRT) bei der Behandlung von Sicherheitsvorfällen wird erläutert.
