CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Portsicherheit

Definition Port

- Ein Port oder eine Portnummer ist in Rechnernetzen eine Netzwerkadresse, mit der das Betriebssystem die Datenpakete eines Transportprotokolls zu einem Prozess zuordnet. Zusammen mit der IP-Adresse ermöglicht der Port die Adressierung eines Servers oder Clients. Durch Angabe von Quell- und Zieladresse, jeweils bestehend aus IP-Adresse und Port, ist es möglich, eine bestehende Verbindung eindeutig zu identifizieren.

Allgemeine Bemerkung

- **Ports**, die **nicht** von aktiven Diensten oder Anwendungen **benötigt** werden, stellen **zusätzliche Angriffsfläche** dar und sollten daher stets **geschlossen** werden!

Unsicherer Port: 80 | HTTP

Grundlage des World Wide Web:

- HTTP wird hauptsächlich für die Übertragung von Webseiten (HTML-Dokumenten) vom Server zum Browser verwendet.

Stateless Protocol:

- HTTP speichert keine Informationen über vorherige Anfragen, jede Anfrage wird unabhängig behandelt.

Textbasierte Anfragen und Antworten:

- HTTP-Kommunikation erfolgt in Form von textbasierten Anfragen (Requests) und Antworten (Responses).

Keine Verschlüsselung:

- Daten werden unverschlüsselt übertragen, was sie anfällig für Abhör- und Man-in-the-Middle-Angriffe macht.

Sichere Alternative: 443 | HTTPS

Verschlüsselung:

- HTTPS verschlüsselt die übertragenen Daten, um die Sicherheit der Kommunikation zu erhöhen. Dies schützt vor Abhör- und Man-in-the-Middle-Angriffen.

Verwendung von SSL/TLS:

- HTTPS implementiert SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) Protokolle, um die Kommunikation zu verschlüsseln.

Authentifizierung des Servers:

- HTTPS ermöglicht die Authentifizierung des Servers, um sicherzustellen, dass Nutzer mit dem legitimen Server kommunizieren.

Unsicherer Port: 20&21 | FTP

Datenübertragung zwischen Systemen:

- Das Protokoll wird verwendet, um Dateien zwischen einem Client und einem Server über ein Netzwerk zu übertragen.

Unterstützt Benutzerauthentifizierung:

- FTP erlaubt den Zugriff auf Dateien mittels Benutzername und Passwort, obwohl dies unverschlüsselt geschieht.

Zwei Kommunikationskanäle:

- Es verwendet einen Steuerkanal (für Befehle und Antworten) und einen Datenkanal (für die eigentliche Datenübertragung).

Aktiver und passiver Modus:

- FTP kann im aktiven oder passiven Modus betrieben werden, was die Art der Verbindungsaufnahme zwischen Client und Server bestimmt.

Sichere Alternative: 22 | SFTP

Sichere Datenübertragung:

- SFTP ist eine Erweiterung des Secure Shell-Protokolls (SSH) und wird für die sichere Datenübertragung über ein Netzwerk verwendet.

Verschlüsselte Übertragungen:

- SFTP bietet eine sichere Methode für die Übertragung von Dateien, da alle Daten (inkl. Anmeldeinformationen) verschlüsselt übertragen werden.

Authentifizierung und Autorisierung:

- SFTP ermöglicht verschiedene Authentifizierungsmethoden, einschließlich Passwörter und digitale Schlüssel.

Integritätsprüfung:

- SFTP führt eine Integritätsprüfung der übertragenen Daten durch, um sicherzustellen, dass sie während der Übertragung nicht manipuliert wurden.

Unsicherer Port: 23 | Telnet

Fernzugriff auf Server:

- Telnet ermöglicht es Benutzern, sich aus der Ferne an einem Server anzumelden und diesen zu steuern.

Textbasierte Schnittstelle:

- Benutzer interagieren mit dem Server über eine textbasierte Schnittstelle, oft über die Kommandozeile.

Unverschlüsselte Datenübertragung:

- Sowohl die Anmeldeinformationen als auch die übertragenen Daten sind unverschlüsselt und daher unsicher.

Einfaches Protokoll:

- Telnet ist für seine Einfachheit bekannt, bietet aber aufgrund des Fehlens von Verschlüsselung und modernen Sicherheitsfunktionen nur eine geringe Sicherheit.

Sichere Alternative: 22 | SSH

Sichere Fernsteuerung:

- SSH ist ein Protokoll für sichere Netzwerkdienste über ein ungesichertes Netzwerk, am häufigsten für Fernzugriff auf Server und für sichere Datenübertragungen (z.B. mit SFTP).

Verschlüsselte Sitzungen:

- SSH verschlüsselt die gesamte Sitzung, einschließlich Anmeldeinformationen und übertragener Daten, um die Sicherheit zu gewährleisten.

Sichere Alternative: 22 | SSH

Schlüsselbasierte Authentifizierung:

- SSH unterstützt die schlüsselbasierte Authentifizierung, bei der digitale Schlüssel für eine sichere Anmeldung ohne Passworteingabe verwendet werden.

Tunneling und Port-Weiterleitung:

- SSH ermöglicht das Tunneling von Netzwerkverbindungen und kann verwendet werden, um andere Netzwerkdienste sicher über einen verschlüsselten Kanal zu leiten.

Unsicherer Port: 25 | SMTP

E-Mail-Übertragung:

- SMTP wird zum Senden von E-Mails von einem Mail-Server zum anderen oder zum Endbenutzer verwendet.

Textbasiertes Protokoll:

- SMTP verwendet ein textbasiertes Format für die Übertragung von Nachrichten.

Unverschlüsselte Übertragung:

- Standardmäßig werden Nachrichten ohne Verschlüsselung übertragen, was sie anfällig für Abhörangriffe macht.

Einfache Authentifizierung:

- SMTP unterstützt Authentifizierung, aber ohne Verschlüsselung sind die Anmeldeinformationen ungeschützt.

Sichere Alternative: 465 | SMTPS

SSL/TLS-Verschlüsselung:

- Stellt von Beginn an eine sichere Verbindung mittels SSL/TLS her.

Verbesserte Sicherheit:

- Schützt die Übertragung von E-Mails vor Abhör- und Man-in-the-Middle-Angriffen.

Kompatibilität:

- Nicht alle E-Mail-Server unterstützen SMTPS, daher ist die Verbreitung begrenzt.

Sichere Alternative: 587 | StartTSL mit SMTP

Nachträgliche Verschlüsselung:

- Beginnt als unverschlüsselte Verbindung und wechselt dann zu einer verschlüsselten Verbindung.

Flexibilität:

- Ermöglicht die Nutzung von Verschlüsselung auf Servern, die sowohl verschlüsselte als auch unverschlüsselte Verbindungen unterstützen.

Weit verbreitet:

- Viele E-Mail-Server und -Clients unterstützen StartTLS.

Unsicherer Port: 53 | DNS

Namensauflösung im Internet:

- DNS übersetzt Domainnamen in IP-Adressen, was für das Routing im Internet unerlässlich ist.

Unverschlüsselt und unauthentifiziert:

- Standard-DNS ist unverschlüsselt und bietet keine Authentifizierung, was es anfällig für Angriffe wie DNS-Spoofing macht.

Hierarchisches System:

- DNS verwendet eine hierarchische Struktur mit verschiedenen Ebenen von Namen-Servern.

Wichtig für das Internet-Routing:

- DNS ist entscheidend für das Funktionieren des Internets, da es die Benutzung von leicht merkbaren Domainnamen ermöglicht.

Sichere Alternative: 443 | DNS-over-HTTPS (DoH)

Verschlüsselt DNS-Anfragen:

- Verwendet HTTPS, um DNS-Anfragen zu verschlüsseln und zu sichern.

Schutz der Privatsphäre:

- Verhindert das Abfangen und Manipulieren von DNS-Anfragen.

Integration in Web-Browser:

- Wird zunehmend in Web-Browsern integriert für verbesserte Sicherheit.

Unsicherer Port: 110 | POP3

E-Mail-Empfang:

- POP3 wird verwendet, um E-Mails von einem Server auf den lokalen Computer des Benutzers zu übertragen.

Einfaches Protokoll:

- POP3 ist ein einfaches Protokoll mit limitierten Funktionen im Vergleich zu moderneren E-Mail-Protokollen.

Unverschlüsselte Übertragung:

- In seiner Standardkonfiguration erfolgt die Übertragung von E-Mails unverschlüsselt.

Download und Löschung von E-Mails:

- POP3 lädt E-Mails herunter und löscht sie in der Regel vom Server, was unterschiedlich zu IMAP ist, das die E-Mails auf dem Server belässt.

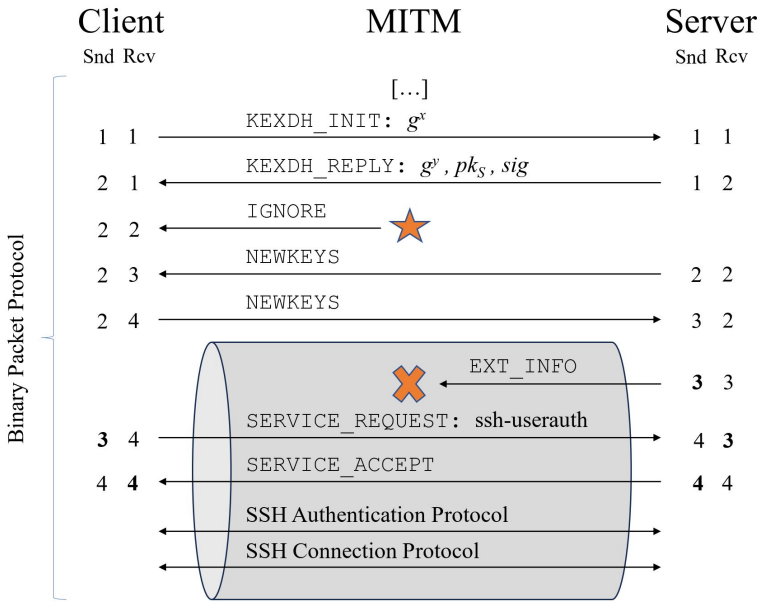
Weitere unsichere Ports, Protokolle und Alternativen

Unsicherer Port & Protokoll		Sichere Alternative	
143	IMAP	993	IMAPS
161	SNMP	161	SNMPv3
139	NetBIOS	445	SMB over TCP
389	LDAP	636	LDAPS
514	Syslog	6514	Syslog over TLS
513	Rlogin	22	SSH
514	RSH	22	SSH
3389	RDP	3389	RDP over SSL/TLS

Aktuelles Beispiel: Terrapin SSH-Attacke

"Indem ein Angreifer die Sequenznummern während des Handshakes sorgfältig anpasst, kann er eine beliebige Anzahl von Nachrichten, die zu Beginn des sicheren Kanals vom Client oder Server gesendet werden, entfernen, ohne dass der Client oder der Server es bemerken." heißt es in der Mitteilung, die von den Forschern veröffentlicht wurde. "Der Angriff kann in der Praxis durchgeführt werden, was einem Angreifer ermöglicht, die Sicherheit der Verbindung zu verschlechtern, indem er die Erweiterungsverhandlungsnachricht (RFC8308) aus dem Transkript abschneidet. Die Trunkierung kann dazu führen, dass weniger sichere Client-Authentifizierungsalgorithmen verwendet werden und bestimmte Gegenmaßnahmen gegen Angriffe auf die Tastenanschlagszeit in OpenSSH 9.5 deaktiviert werden."

Aktuelles Beispiel: Terrapin SSH-Attacke



CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm