CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

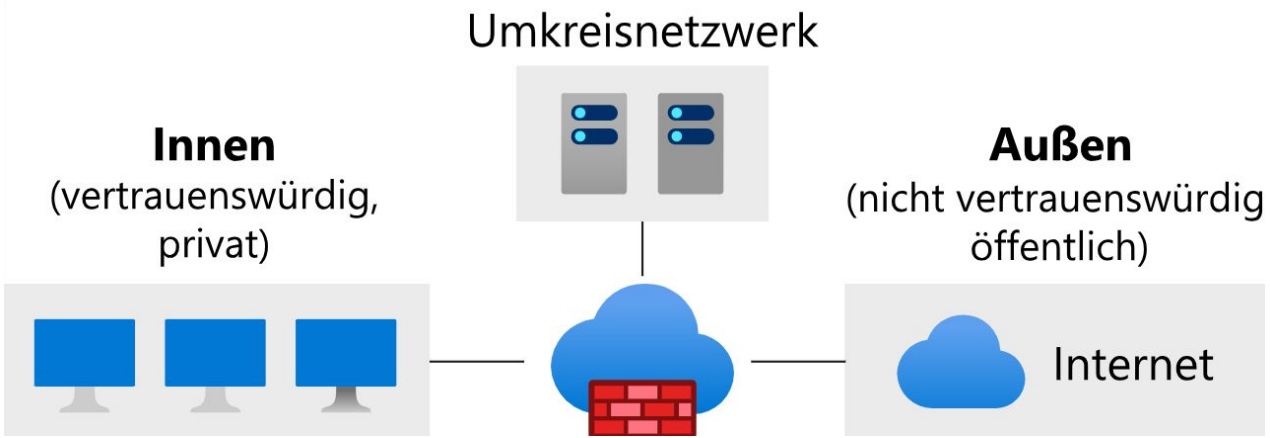
CloudCommand GmbH chr.schumacher@gmx.tm

Netzwerk-sicherheits-zonen

Was sind Netzwerksicherheitszonen?

- Eine Netzwerksicherheitszone ist ein Netzwerksegment, für das spezifische Sicherheitsrichtlinien gelten und das oft durch Firewalls von anderen Netzwerksegmenten abgetrennt ist. Es gibt drei verschiedene Arten von Sicherheitszonen.

Vertrauenswürdige oder private Zonen



Vertrauenswürdige oder private Zonen

- Eine vertrauenswürdige oder private Zone enthält die Ressourcen und Geräte, die niemals für eine Person außerhalb Ihrer Organisation zugänglich sein sollten. Dazu gehören beispielsweise Drucker, von internen Benutzern verwendete Arbeitsstationen und interne Server. In dieser Art von Zone werden Geräte mit privaten IP-Adressen konfiguriert.

Öffentliche Zonen

- Eine öffentliche Zone enthält alles außerhalb der Organisation. Eine solche Zone ist Teil des Internets oder eines anderen Netzwerks, und unterliegt nicht der Kontrolle durch Ihre Organisation.

Richtlinien für die Zonenfilterung

Richtlinien für die Zonenfilterung regeln, wie Datenverkehr zwischen verschiedenen Zonen weitergeleitet wird. Zu diesen Richtlinien gehören u. a. folgende Arten:

- **Von einem internen an ein externes Netzwerk gesendeter Datenverkehr und von einem internen Netzwerk an ein Umkreisnetzwerk gesendeter Datenverkehr:** Dieser Filtertyp überprüft den gesamten Datenverkehr, der aus dem internen Netzwerk an das Umkreisnetzwerk weitergeleitet wird. Beispielsweise müssen Ihre internen Mitarbeiter*innen auf eine öffentliche Website zugreifen. Der Datenverkehr wird untersucht, um festzustellen, ob die Website vertrauenswürdig ist.

Richtlinien für die Zonenfilterung

- **Von einem externen an ein internes Netzwerk gesendeter Datenverkehr:** Bei diesem Filtertyp wird Datenverkehr blockiert, der von außerhalb in Ihr Netzwerk weitergeleitet werden soll. Es wird nur Datenverkehr weitergeleitet, der eine direkte Reaktion auf eine Anforderung aus der inneren Zone darstellt. Ein interner Mitarbeiter könnte beispielsweise eine Webseite von einem Server anfordern. In diesem Fall würde die Antwort zugelassen werden, wenn es sich um eine vertrauenswürdige Quelle handelt, damit der Benutzer die Website verwenden kann.

Richtlinien für die Zonenfilterung

- **Von einem externen Netzwerk an ein Umkreisnetzwerk gesendeter Datenverkehr:** Bei diesem Filtertyp wird der gesamte Datenverkehr überprüft, der von außerhalb in das Umkreisnetzwerk weitergeleitet wird. Der Datenverkehr wird entweder zugelassen oder nicht zugelassen. Zu der Art von Datenverkehr, der möglicherweise weitergeleitet wird, gehören E-Mails und HTTPS-Datenverkehr.

Richtlinien für die Zonenfilterung

- Filter für die **Kommunikation zwischen einem Umkreisnetzwerk und außerhalb.** Dieser Filtertyp untersucht Datenverkehr, der vom Umkreisnetzwerk stammt und Ihr Netzwerk verlässt. Der Datenverkehr darf das Netzwerk basierend auf den Firewallregeln und der Ressource bzw. dem Client, die/der die Anforderung gestartet hat, verlassen. Angenommen ein E-Mail-Server im Umkreisnetzwerk muss sich mit einem anderen Server außerhalb des Netzwerks synchronisieren. In diesem Fall legen Sie mithilfe von Firewallregeln fest, was geschehen soll.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm