Sicherheit im internen Netzwerk

Netzwerksegmentierung und Port-Authentifizierung

Schutzmaßnahmen für eine erhöhte IT-Security sowie zur Einhaltung von Gesetzen und Richtlinien lassen sich durch eine klare Trennung von Netzwerken, Daten und Prozessen leichter realisieren.

Durch mobile Arbeitsplätze und die Nutzung privater Geräte (BYOD) verschwimmen die Netzwerkgrenzen in Unternehmen zusehends, weshalb eine Absicherung der IT-Infrastruktur für Administratoren immer komplexer wird. Dabei heißt es dann häufig: Je mehr ein Netzwerk segmentiert wird, desto sicherer wird es auch. Wichtig dabei ist aber nicht unbedingt, wie hoch die Anzahl an kleinen Segmenten ist, sondern viel mehr, dass die Unterteilung des Unternehmensnetzwerkes auch in sinnvollen Abschnitten erfolgt. Nur mithilfe einer schlüssigen, gut geplanten Netzwerksegmentierung können auch wirklich bessere Erkennungs- und Abwehrmechanismen realisiert werden. Wir beraten Sie gerne dabei, wie Sie mit Netzwerksicherheit Ihr IT-Sicherheitskonzept ideal ergänzen.

Der Baustein für Ihr IT-Sicherheitskonzept

Zur Umsetzung eines sicheren, internen Netzwerkes bieten wir Ihnen stets eine individuelle und kompetente Beratung, Lösungskonzeption und Implementierung.

Für eine ausreichende Sicherheit im internen Netzwerk empfehlen wir Ihnen als Baustein für Ihr IT-Sicherheitskonzept aufbauend auf Firewall und Managed Switches:

- Netzwerksegmentierung
- Port-Authentifizierung
- Network Access Control

Sicherheit und Kontrolle

- Sensible Bereiche (wie z. B. vertrauliche Informationen) können nur von speziellen Benutzern oder Geräten eingesehen werden.
- Vereinfachtes Ereignis-Monitoring: Schnellere Identifikation und Isolierung von Malware oder Ransomware.

Hohes Schutzniveau für unternehmenskritische Daten und Bereiche.

Verhinderung einer Schatten-IT

- Durch die Verwendung einer Next Generation Firewall und Authentifizierung am Switchport können nur bekannte bzw. berechtigte Nutzer, Endgeräte und Anwendungen im internen Netzwerk verwendet werden.
- Dynamische Einrichtung von Ausnahmen für Arbeitsgruppen.

Nur bekannte und berechtigte Geräte können im Netzwerk verwendet werden.

Verringerung des Administrationsaufwands

- Schnelle und unkomplizierte Zuordnung von Geräten und Benutzern.
- Mitarbeiter (BYOD), Gäste und Geräte erhalten automatisch den ihnen zugewiesenen, gesicherten Zugang zum Netzwerk.

Zentrales, zeit- und kostensparendes Regelwerk für dynamische Bürokonzepte.

> Mit dem Sicherheitskonzept von BASYS haben wir die Gewissheit, dass sich in unserem Netzwerk ausschließlich erlaubte Datenströme bewegen. Das ist gerade für unsere Produktion von entscheidender Bedeutung. Die IT-Sicherheit ist mit dem Konzept auf ein völlig neues Niveau gehoben worden. Insbesondere die Verhinderung der sogenannten Schatten-IT begeistern uns.
>
> IT-Leiter eines weltweit führenden mittelständischen Produktionsunternehmens

© 2023 | www.basys-bremen.de

Sicherheit im internen Netzwerk

Zusammenfassung der Lösung

Komfort
- Automatische, regelbasierte Zuordnung von Geräten und Benutzern verringert den Administrationsaufwand.

Sicherheit
- Im internen Netzwerk können nur bekannte bzw. berechtigte Nutzer, Endgeräte und Anwendungen verwendet werden.
- Segmentierung und regelbasierte Authentifizierung schützt unternehmenskritische Daten und Bereiche vor unbefugtem Zugriff.

Kontrolle
- Überwachung der Verbindung aller Endgeräte, die im Unternehmensnetzwerk verwendet werden.
- Malware oder Ransomware können in Netzwerk-Segmenten schneller identifiziert und isoliert werden, sodass eine Verbreitung einfacher eingedämmt werden kann.
- Überprüfung von Endgeräten auf Aktualität, bevor Sie Zugriff auf das Netzwerk bekommen.

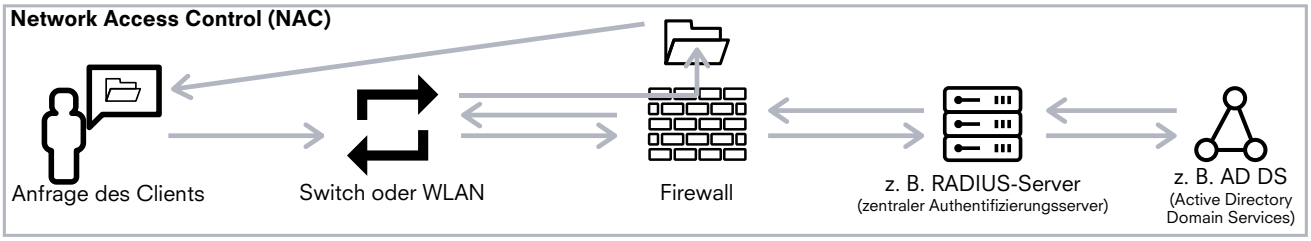
Unser Versprechen an Sie

Wir bieten Ihnen die optimale Unterstützung, mithilfe von Netzwerksicherheit Ihr gesamtes IT-Sicherheitsmanagement zu optimieren.

Unsere IT-Consultants und System-spezialisten entwickeln gemeinsam mit Ihnen das für Sie optimal passende Service-Angebot.

Ein Angebot zum Einstieg

- Die Preisgestaltung ist flexibel und richtet sich nach Ihrer individuellen Umgebung und den von Ihnen gebuchten Leistungspaketen.



Konkrete Vorteile / gewünschte Ergebnisse
- Schlüssige, gut geplante Netzwerksegmentierung für eine jederzeit sichere Arbeitsumgebung
- Sinnvolle Ergänzung Ihres IT-Sicherheitskonzeptes für einen Zuwachs an Kontrolle, Sicherheit und Komfort
- Vertrauensvolle Zusammenarbeit, persönliche Betreuung und regionale Nähe

Warum BASYS?
BASYS liebt und dient dem Mittelstand seit über 30 Jahren. Unsere IT-Berater analysieren Ihre Bedürfnisse und besprechen im Anschluss mit Ihnen die richtigen Schritte. Mit uns bekommen Sie die sichere Netzwerkumgebung, die perfekt zu Ihrem Unternehmen passt. Dies haben wir bereits in zahlreichen Branchen unter Beweis gestellt, auch in sensiblen Bereichen wie etwa Banken & Versicherungen sowie dem Gesundheitswesen.

© 2023 | www.basys-bremen.de

BASYS Bartsch EDV-Systeme GmbH
Hermine-Seelhoff-Straße 1-2
28357 Bremen

T: +49 421 43 420 0
F: +49 421 43 420 333
info@basys-bremen.de

Geschäftsführer:
Olaf Brandt,
Mike Wagner

Amtsgericht Bremen
HRB 11898
VAT-ID DE114401047

NORD/LB
IBAN:DE67 2505 0000 1050 1560 02
BIC: NOLADE2HXXX