NACVIEW

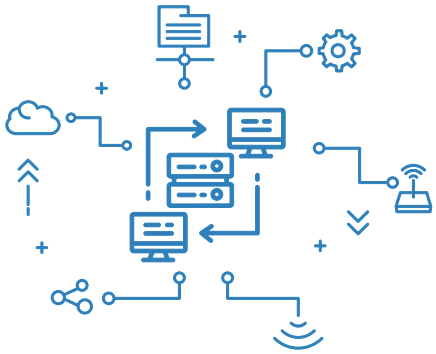
www.nacview.com

DIE GRUNDLAGEN DES MODERNEN MANAGERS

WISSEN SIE, WELCHE UND WIE VIELE GERÄTE SICH IN IHREM NETZWERK BEFINDEN?

Private Telefone von Mitarbeitern, Geräte von Besuchern des Unternehmens, Geräte von Personen, die aus der Ferne arbeiten, IoT-Geräte, nicht konforme Computer, die ein veraltetes Betriebssystem haben oder deren Virenschutzsystem deaktiviert ist. Jedes dieser Geräte, das mit dem Unternehmensnetzwerk verbunden ist, kann eine Bedrohung darstellen. Es braucht nur ein mit Malware infiziertes Gerät, damit sich das Problem auf das gesamte Computernetzwerk ausbreiten kann. Dies kann zu Datenlecks, Diebstahl vertraulicher Informationen oder zur Verschlüsselung von wichtigen Unternehmensdaten führen, was finanzielle und rufschädigende Folgen haben könnte.

Das Netzwerkzugriffskontrollsystem NACVIEW schützt vor unbefugtem Zugriff auf die Infrastruktur vor unbekannten oder potenziell gefährlichen Geräten. Es ermöglicht die vollständige Sichtbarkeit aller mit dem Netzwerk verbundenen Objekte und verwaltet die Gewährung des Zugriffs auf ausgewählte Ressourcen. Dadurch wird das gesamte Unternehmensnetzwerk sicherer, besser koordiniert und effizienter.



In Zeiten des allgegenwärtigen Zugangs zum Internet für verschiedene Gerätetypen, können es sich Unternehmen nicht leisten, die Kontrolle darüber zu verlieren, was und wann eine Verbindung zu ihrem Unternehmensnetzwerk herstellt. Bei den berüchtigtsten böswilligen Angriffen wie WannaCry oder NotPeyta könnten Organisationen mit zentral verwaltetem Netzwerkzugriff das Risiko erheblich reduzieren, indem sie nicht aktualisierte Geräte vom Rest des Netzwerks isolieren würden.

NACVIEW sorgt dafür, dass Ihr Unternehmensnetzwerk besser geschützt und frei von nicht identifizierten Geräten ist.

WARUM ES SICH LOHNT:

VERBESSERUNG DER CYBERSICHERHEIT

Unternehmensressourcen sind verschiedenen Bedrohungen wie Malware, Ransomware und DDoS-Angriffen ausgesetzt. Hacker sind ständig auf der Suche nach Zugang zu sensiblen Daten, die sie im Dark Web verkaufen können. Die NACVIEW-Lösung hilft, diese Bedrohungen zu minimieren, indem sie veraltete oder verdächtige Geräte ausschließt und die Online-Aktivitäten der Nutzer einschränkt.

SICHERER VPN-ZUGANG

Fernarbeit ist zu einem allgemeinen Trend geworden. Dies macht es erforderlich, dass IT-Abteilungen ihren Mitarbeitern den Zugriff auf die Netzressourcen des Unternehmens von außen über VPN ermöglichen. Das Problem bei dieser Lösung ist, dass sie nicht zu 100 % verifiziert werden kann. Ist es wirklich unser Mitarbeiter, der auf das Netzwerk zugreift, oder ist es vielleicht jemand, der das Gerät übernommen oder das Passwort für das VPN gestohlen hat. Daher ist es wichtig, den Fernzugriff mit einem zweiten Authentifizierungsfaktor zu sichern. NACVIEW kann in praktisch jedes VPN-System integriert werden und eine Zwei-Faktor-Authentifizierung mit einer speziellen App für Telefone oder SMS-Einmalpasswörtern durchführen.

BESSERE NUTZUNG ANDERER BESTEHENDER SICHERHEITSSYSTEME

Das NAC-System ist eine zentrale Sicherung, und Protokolle von anderen Systemen wie Virenschutz, Firewalls usw. können dorthin umgeleitet werden. Dadurch ist es möglich, automatisch auf Bedrohungen zu reagieren, die von Systemen Dritter erkannt werden, und potenziell gefährliche oder infizierte Geräte vom internen Netzwerk zu trennen.

WAS SIE SONST NOCH GEWINNEN:

KONTROLLE DER PRIVATEN AUSRÜSTUNG DER BYOD MITARBEITER.

Heutzutage verschwimmt die Unterscheidung zwischen privaten und geschäftlichen Geräten immer mehr. Mehr noch, einige Unternehmen erlauben ihren Mitarbeitern sogar, ihre privaten Geräte für geschäftliche Zwecke zu nutzen, um ihre Produktivität zu steigern und ihre eigenen Kosten zu senken. BYOD muss nicht zwangsläufig zu Lasten der Sicherheit gehen. Eine implementierte Netzwerkzugangskontrolle kann den Zugriff nur auf aktualisierte und gesicherte Geräte erlauben oder Geräte in ein separates VLAN oder Gastnetzwerk umleiten.

KOSTENREDUKTION.

Das System ermöglicht eine schnelle und effiziente Überprüfung der Daten und das Auffinden von Problemen im Netz. So können die Administratoren Probleme effizient diagnostizieren und sofort Gegenmaßnahmen zur Verbesserung der Leistung ergreifen. Darüber hinaus lassen sich dank der Automatisierungsmechanismen viele Aspekte im Voraus planen, so dass das System sie für die Administratoren selbständig ausführen kann. Dazu gehören im Voraus geplante Systembefehle, das automatische Herunterfahren und Einschalten von Wi-Fi-Netzwerken an arbeitsfreien Tagen, damit sie keinen Strom verbrauchen, oder die Weiterleitung von Informationen über Ports, die lange Zeit nicht genutzt wurden, so dass die vorhandenen Geräte optimal genutzt werden können.

KONTROLLIERTER GASTZUGANG.

Heutzutage verschwimmt die Unterscheidung zwischen privaten und geschäftlichen Geräten immer mehr. Mehr noch, einige Unternehmen erlauben ihren Mitarbeitern sogar, ihre privaten Geräte für geschäftliche Zwecke zu nutzen, um ihre Produktivität zu steigern und ihre eigenen Kosten zu senken. BYOD muss nicht zwangsläufig zu Lasten der Sicherheit gehen. Eine implementierte Netzwerkzugangskontrolle kann den Zugriff nur auf aktualisierte und gesicherte Geräte erlauben oder Geräte in ein separates VLAN oder Gastnetzwerk umleiten.

STEIGERUNG DER PRODUKTIVITÄT UND ERGONOMIE.

Mit einer präzisen NACVIEW-Richtlinie erhalten Mitarbeiter, unabhängig davon, wo und wie sie sich mit dem Netzwerk verbinden, immer Zugang zu den ihnen zugewiesenen Teilnetzen und damit zu den Ressourcen und Netzwerkdiensten, die sie benötigen. Wichtig bei der Implementierung eines NAC-Systems ist die Segmentierung des Netzwerks und die Regulierung des Netzwerkverkehrs. Dadurch wird die Bandbreite für jeden Benutzer erhöht.

GERINGERE BETRIEBSKOSTEN.

NACVIEW ist ein von Netzausrüstern unabhängiges System. Daher ist das Unternehmen beim Kauf neuer oder beim Austausch alter Switches nicht von einem einzigen Hersteller preislich abhängig.
Es ist möglich, eine Reihe von Netzgeräteherstellern zu prüfen, so dass jedes Mal die günstigste Option in Bezug auf Sicherheit, Funktionalität und Leistung ausgewählt werden kann.

EINHALTUNG DER SICHERHEITSVORSCHRIFTEN.

NAC ist auch ein wertvolles Instrument, um die Einhaltung relevanter Cybersicherheitsgesetze zu gewährleisten. Netzwerksicherheitsrichtlinien können in DSGVO- oder HIPAA-Compliance-Pläne integriert werden, um den Nachweis zu erbringen, dass die Netzwerke die erforderlichen externen Standards erfüllen.