Whitepaper

Bring Your Own Device

Netzwerksicherheit trotz fremder Systeme

Wie können Sie sicherstellen, dass Ihre Netzwerkressourcen geschützt bleiben, obwohl Mitarbeitern und Externen wie Wartungsfirmen oder Consultants gestattet wird, mit ihren eigenen Devices im Netzwerk zu arbeiten?

Der Begriff „Bring Your Own Device" ist aktuell in allen Medien vertreten und scheint auch in nahezu jedem Unternehmen eine Rolle zu spielen. Doch was genau bedeutet dieses „Schlagwort" und warum sollte man sich damit befassen? Wie der Begriff bereits impliziert, geht es dabei um Geräte, die von Mitarbeitern wie Externen mitgebracht werden - in der Regel werden damit in erster Linie Mobile Devices wie Smartphones und Tablets, aber auch Laptops bezeichnet. Die Verwaltung und Absicherung dieser Geräte stellt die IT-Abteilungen häufig vor eine große Herausforderung. Inzwischen gibt es unzählige Mobile Device Management Lösungen (MDM) am Markt, die versprechen, dieser Anforderung Herr zu werden. Doch was ist mit den Geräten, die Mitarbeitern oder Externen gehören und auf denen keine Firmensoftware installiert werden darf oder kann?

Zu diesem Thema begegnen uns in den Unternehmen immer wieder ähnliche Ausgangsszenarien:

- Keine Übersicht über die angeschlossenen Geräte
- Keine Möglichkeit, automatisiert Gastzugänge bereit zu stellen
- Immer höhere Anforderungen, bestimmte Ressourcen nutzbar zu machen
- Keinen Schutz vor Netzwerkangriffen wie z.B. ARP-Spoofing
- Keine Übersicht der Aktivitäten von zugelassenen Geräten
- Hoher Aufwand beim Patchen der vielen LAN-Ports
- Kein Schutz vor einmal zugelassenen Geräten

Lösungsansatz

Ein pragmatischer und leicht nutzbarer Lösungsansatz ist der Einsatz der Netzwerkzugangsschutz-Lösung macmon. Mit macmon erhalten Sie die Möglichkeit, die öffentlichen und die nicht öffentlichen Bereiche der Netzwerke strikt voneinander zu trennen. Die erste „Line of Defence" verhindert den Zugang unbekannter Geräte. Geräte die am Netzwerkverkehr teilnehmen dürfen, müssen sich über Ihre MAC-Adresse, einen „Fingerprint" oder ein Zertifikat ausweisen. Die zweite „Line of Defence" schützt vor Angriffen auf Netzwerkkomponenten und vor Adressmanipulationen und verhindert so Lauschangriffe auf den Datenverkehr oder die internen Ressourcen.

Neue Geräte, die ans Netz angeschlossen werden, erkennt und lokalisiert macmon sofort. Sollte das Gerät unbekannt sein, alarmiert macmon und leitet, bei entsprechender Konfiguration, automatisch Gegenmaßnahmen ein. Die Einführung einer Zugangsüberwachung ist einfach und schnell installiert und kann mit wenig Aufwand betrieben werden.

Bei fremden oder unautorisierten Geräten bietet macmon zudem eine dynamische Möglichkeit Netzwerkanschlüsse einem „Gäste-Netz" zuzuordnen, welches z.B. nur Zugang zum Internet oder einem Konferenzserver hat. Das verfügbare Gästeportal mit optionaler Selbstregistrierung und der V-LAN Manager reduzieren den Administrations-aufwand und geben Ihnen gleichzeitig einen stets aktuellen Netzwerküberblick. Die Gültigkeitsdauer eines „Gäste-Tickets" als auch die Dauer des Aufenthaltes, genutzte Anschlüsse, verwendete V-LANs, etc. werden vollständig protokolliert. Auf diesem Wege decken wir bereits den größten Teil der zuvor genannten Anforderungen ab und das unabhängig von den eingesetzten manage-

baren Switchen. Doch was ist mit der Gefahr, die von zugelassenen, aber nicht sicher betriebenen Geräten ausgeht?

So sind beispielsweise Universitäten mit dieser Thematik bereits seit vielen Jahren konfrontiert – die Studenten bringen eigene Devices mit und benötigen Zugang zum Campus-Netzwerk. Dort wurden dementsprechend die Server bestmöglich gesichert. Da dies aber im Unternehmensnetzwerk und vor allem nachträglich nicht so ohne weiteres umsetzbar ist, muss eine alternative Möglichkeit gefunden werden.

Hier kommt die Segmentierung des Netzwerks durch macmon zur Hilfe. Ein positiver Nebeneffekt bei der Einführung von V-LANs sind fest vorgegebene Datenrouten. Mit diesen leicht definierbaren Verbindungen ist die Kombination mit einem Intrusion Prevention System (IPS) auf einfache Weise möglich. Alle Kommunikationswege, die von unsicheren Systemen genutzten werden, können so abgesichert werden. In der Regel sind IPS Systeme sogar in der Lage, Informationen über Angriffe gezielt weiter zu geben. Durch eine Kopplung des IPS Systems mit macmon, können so angreifende oder schädliche Systeme automatisiert wieder vom Netzwerk getrennt werden.

macmon secure gmbh

macmon secure ist ein deutscher Software-Hersteller spezialisiert auf Netzwerk-Sicherheit. Die eigen entwickelte, herstellerunabhängige und modulare NAC-Lösung macmon schützt das Netzwerk vor unautorisierten, nicht sicheren Geräten und internen Angriffen. Kunden profitieren vom Security-Know How, planbaren Kosten und einem sehr hohem Sicherheitsniveau der Software bei einfachem Handling und Betrieb, dem Einsatz intelligenter Technologien, der Kopplung von macmon mit anderen führenden Security-Produkten und der ständigen Erweiterung des Funktionsprofils entsprechend der neuesten Entwicklungen und Standards. macmon secure beschäftigt etwa 20 Mitarbeiter in Deutschland. Zum Kundenstamm gehören europaweit mehr als 300 Unternehmen unterschiedlicher Branchen u. a. Bundesministerien, Volkswagen, Müller Milch, ZF, RWE Power, SWR, Vivantes, ZIVIT, KfW Kreditanstalt für Wiederaufbau, Sparkassen und Volksbanken. Firmensitz der macmon secure gmbh ist Berlin. macmon secure ist Mitglied bei BITKOM und der Trusted Computing Group.

Kontakt
Christian Bücker, Geschäftsführung
Nicole Wetzel, Vertriebsleitung
Charlottenstraße 16, D-10117 Berlin
Tel. +49 30 2325777-0
vertrieb@macmon.eu
www.macmon.eu