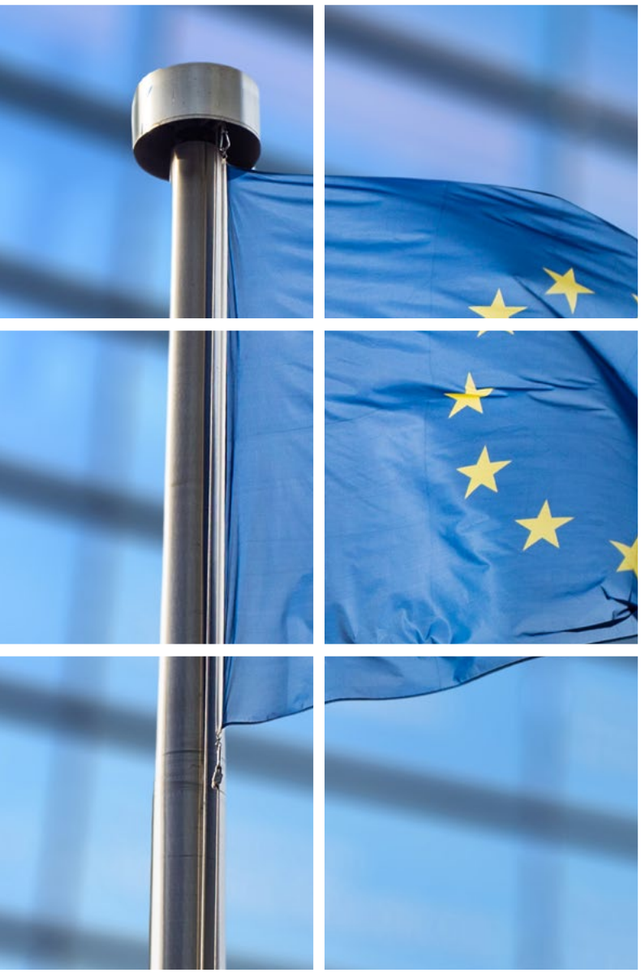
macmon
nac intelligent einfach

DSGVO

EINSATZMÖGLICHKEITEN VON NETZWERKZUGANGSKONTROLLE

im Rahmen der Datenschutzgrundverordnung



WORUM GEHT ES?

Sie wird kurz „DSGVO“ oder aus dem englischen „General Data Protection Regulation“ („GDPR“) genannt. Die DSGVO löst den mehr als 20 Jahre alten Rechtsrahmen des Datenschutzes ab.

Das waren bisher die EU-Datenschutzverordnung aus dem Jahre 1995 und die darauf basierenden nationalen Datenschutzgesetze, in Deutschland handelt es sich dabei um das BDSG.

Die DSGVO regelt die Art der zu schützenden Daten und den Umgang damit. Außerdem werden konkrete Kontrollmechanismen und Sanktionen vorgeschrieben.

Die Europäische Datenschutzgrundverordnung ist ab 2018 die neue Grundlage für den Datenschutz.

Die Verordnung richtet sich ausnahmslos an alle Unternehmen mit Sitz und/oder Niederlassung in der EU. Darüber hinaus sind außerdem weltweit Unternehmen betroffen, die Daten von Personen erheben, die sich in der EU aufhalten. Kurz und mittelfristig werden Unternehmen ihren Umgang mit personenbezogenen Daten im Detail prüfen müssen und gegebenenfalls den Schutz dieser Daten ausbauen.

DSGVO

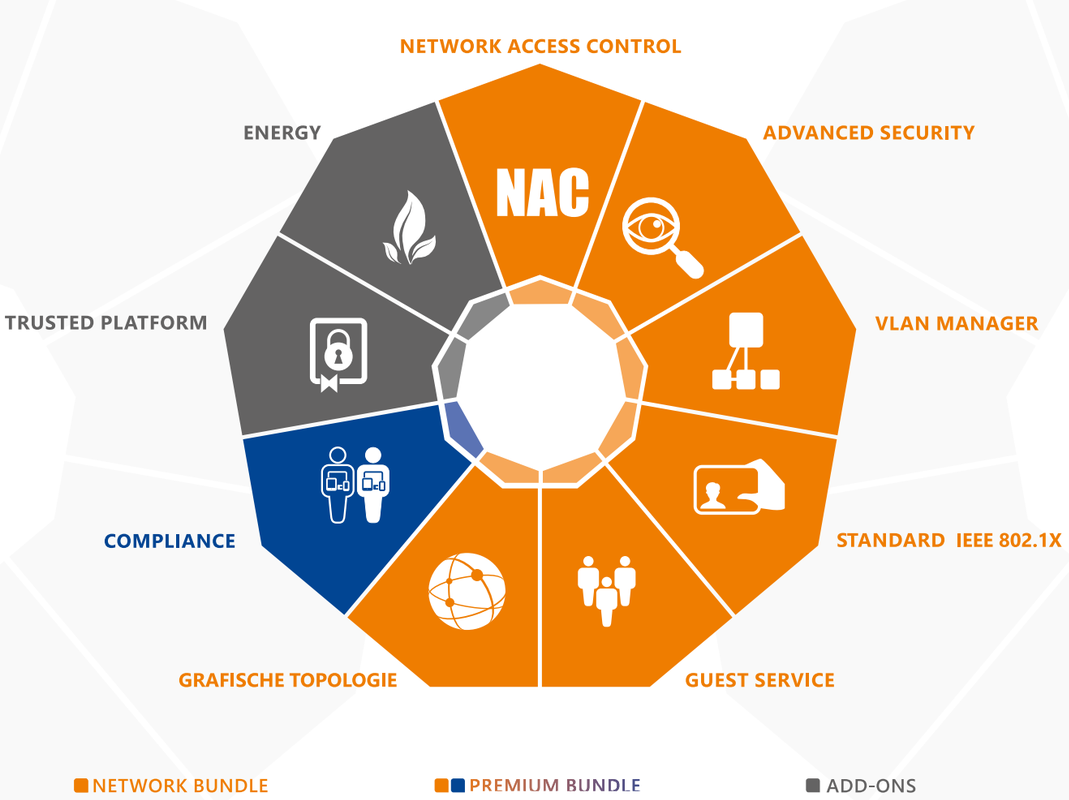
DEUTSCHER HERSTELLER

macmon unterstützt die Umsetzung der DSGVO durch Übersicht, Segmentierung und Isolierung von Endgeräten

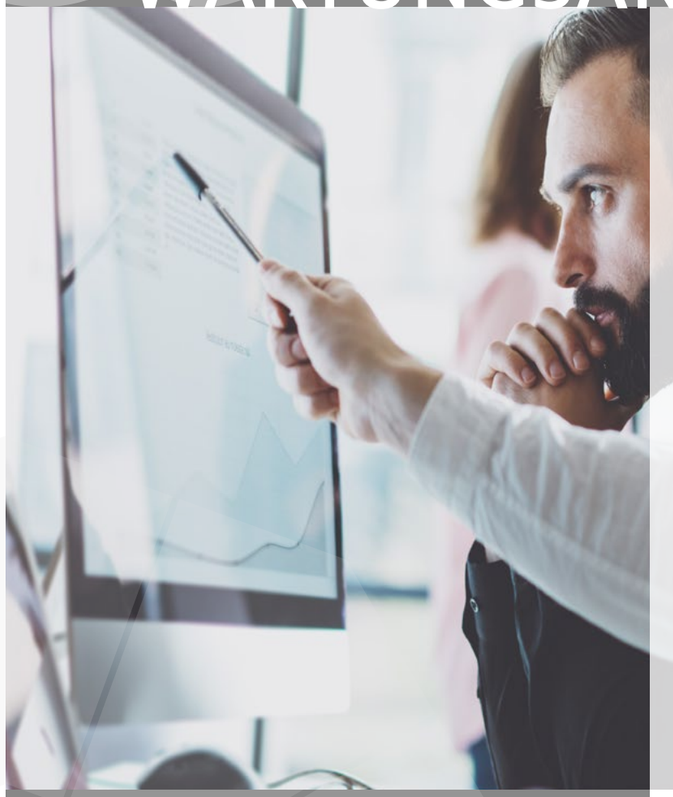
macmon NAC, die führende deutsche Lösung für Netzwerkzugangskontrolle, bietet die Möglichkeit verschiedene Anforderungen der DSGVO effektiv zu unterstützen.

Das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierte macmon macht aus heterogenen und komplexen Netzwerken eine intelligente Einheit und ermöglicht bei minimalem Aufwand die effiziente Überwachung und den Schutz vor unbefugten Zugriffen.

So gewährleistet macmon beispielsweise eine eindeutige Übersicht und Dokumentation des lokalen Netzwerkes und dessen Zugänge. Außerdem protokolliert es lückenlos alle Zugangsversuche und erkennt auch, wenn ein solcher zu einer ungewöhnlichen Uhrzeit stattfindet.



& EFFIZIENT, LÜCKENLOS, WARTUNGSARM



Neben der Alarmierung und der Verhinderung von unerwünschten Netzwerkzugriffen, stellt die dynamische Segmentierung von Netzwerken den effektivsten und sichersten Weg dar, um unbefugten Zugriff auf Daten zu verhindern.

Die Haltung der sensiblen Daten auf separaten Servern - um diese nur innerhalb definierter Netzwerksegmente erreichbar zu machen - sorgt in Verbindung mit macmon Network Access Control für größtmöglichen Schutz.

Die Segmentierung des Netzwerkes erfolgt in Verbindung mit einfach zu administrierenden Endgerätegruppen. Dadurch wird der Scope der für die gesicherte Verarbeitung besonders schützenswerter Daten zu betrachtenden Endgeräte erheblich reduziert und gleichzeitig auf die entscheidenden Geräte fokussiert. Eine übersichtliche Weboberfläche gibt dazu einen Überblick darüber, welche Geräte eine Verbindung erhalten können und aktuell erhalten.

Endgeräte, die nicht DSGVO-konform sind, weil sie den Sicherheitsanforderungen nicht oder nicht mehr entsprechen, isoliert macmon von sensiblen Bereichen und verschiebt sie in die Quarantäne. Das reduziert die Arbeitsbelastung von IT-Administratoren erheblich und ermöglicht die Einhaltung von in der DSGVO geforderten Prozessen.

> Viele Unternehmen haben jetzt die Unverzichtbarkeit einer NAC-Lösung erkannt.
>
> *- Christian Bücker, GF macmon secure GmbH -*

Schutz vor Datenmissbrauch

In kabellosen Netzwerken (WLAN) sind immer häufiger Geräte unterschiedlichster Art vereint. Teilweise findet man sogar Unternehmensgeräte gemeinsam mit Besuchergeräten vor. In Krankenhäusern beispielsweise befinden sich unter Umständen in einem solchen Netzwerk sogar gleichzeitig sensible Daten von Patienten.

Die erforderliche Segmentierung von WLANs in VLANs gehört jedoch noch nicht zur gängigen Praxis, obwohl die dafür nötige Technologie bereit steht. Ihre Umsetzung ist gleichermaßen einfach wie sinnvoll. Ohne diese Trennung sind unkontrollierte Geräte, beispielsweise von externen Dienstleistern, im gleichen Netzwerk wie hochsensible Patientendaten.
Letztere sind somit einer erheblichen Gefährdung durch Datenmissbrauch ausgesetzt. Diese Lücke gilt es mit der macmon NAC-Lösung zu schließen.

KONTROLLE

IDC-Umfrage ergibt:

44 Prozent der befragten Unternehmen sind nicht ausreichend auf die DSGVO vorbereitet

Überraschend erscheinen die Ergebnisse einer aktuellen Umfrage der IDC unter 251 Unternehmen und Organisationen in Deutschland mit mehr als 20 Mitarbeitern.

Bei dieser gaben immerhin 15 Prozent an, ihre Firma sei bereits vollständig „compliant", weitere 41 Prozent haben bereits vereinzelte Maßnahmen umgesetzt.

44 Prozent der befragten Unternehmen erklärten jedoch, dass sie noch keine konkreten technologischen oder organisatorischen Maßnahmen zur Vorbereitung auf die DSGVO getroffen haben.

Diese Unternehmen sind damit in Verzug und laufen Gefahr, nicht alle relevanten Maßnahmen bis zum 25. Mai 2018 noch umsetzen zu können. Der Anpassung der IT-Systeme an die Anforderungen der DSGVO kommt eine zentrale Rolle zu, gleichzeitig wird sie von jedem Fünften als größte Herausforderung empfunden.

Nach IDC-Einschätzungen sind Investitionen in den meisten Fällen erforderlich. Marktforscher sehen einen besonderen Handlungsbedarf in der IT-Security.

Grundlegende Anforderungen sind hier der sichere Betrieb der IT, ihre permanente Überwachung in Echtzeit und Maßnahmen als Reaktion auf Auffälligkeiten im Netzwerk durch eine Sicherheitslösung wie macmon.

Fast die Hälfte der befragten Unternehmen planen in den kommenden Monaten verstärkt in Cyber Security zu investieren. Aus IDC-Sicht ist dies auch dringend notwendig, um Sicherheitsrisiken und Angriffe auf personenbezogene Daten mit moderner Technologie effizient abzuwehren. Dem Aufspüren und Bekämpfen von Sicherheitsverletzungen kommt dabei eine zentrale Bedeutung zu.
Quelle der IDC-Untersuchung: Computerwoche.de

KONTAKT

+49 30 2325 777-0

nac@macmon.eu

www.macmon.eu

macmon
nac intelligent einfach

macmon secure GmbH
Alte Jakobstraße 79-80
10179 Berlin
Telefon +49 30 2325 777-0
nac@macmon.eu
www.macmon.eu