GDPR

POSSIBLE USES OF CONTROLLING NETWORK ACCESS within the framework of the General Data Protection Regulation

Usually abbreviated as GDPR, this regulation replaces the more than 20-year-old legal framework for data protection.

Until now, that framework consisted of the European Data Protection Directive from 1995 and the national data protection laws based on it, such as the Data Protection Act 1998 (UK).

The GDPR regulates the type of data that must be protected and how this data is handled. It also prescribes specific control mechanisms and sanctions.

WHAT'S IT ABOUT?

Since 2018, the European General Data Protection Regulation is the new basis for data protection.

The regulation will apply to all companies with headquarters and/or a subsidiary in the EU without exceptions. It will furthermore affect companies worldwide that collect data from persons within the EU. In the short and medium term, companies will have to examine their use of personal data in detail and extend the protection of this data where necessary.

GDPR

macmon supports the implementation of the GDPR through monitoring, segmenting and isolating end devices

macmon NAC, the leading German solution for network access control, provides an effective means of meeting various requirements of the GDPR.

The macmon solution turns heterogeneous and complex networks into one intelligent unit, effortlessly enabling efficient monitoring and providing protection against unauthorised access.

This is how macmon guarantees a clear overview and documentation of the local network and access to it, for example. It also logs all attempts at access in full and even recognises when such an attempt occurs at an unusual time.

& EFFICIENT, COMPLETE, LOW-MAINTENANCE

In addition to issuing alerts and preventing unauthorised network access, segmenting networks dynamically is also the most effective and most secure way of preventing unauthorised access to data.

Combining the storage of sensitive data on separate servers (to make it accessible only within defined network segments) with macmon Network Access Control ensures maximum protection.

The network is segmented in connection with an easy-to-administrate end device group. This significantly reduces the scope of end devices to be considered for securely processing particularly sensitive data while simultaneously focussing it on critical devices. A clear web interface also offers an overview of which devices can be and currently are connected.

macmon isolates end devices not in line with the GDPR – because they do not or they no longer meet security requirements – from sensitive areas and moves them to quarantine. This significantly reduces the workload of IT administrators and makes it possible to comply with the processes specified by the GDPR.

> Many companies have now realised that NAC solutions are indispensable.
>
> *- Christian Bücker, CEO macmon secure GmbH -*

Protection from data abuse

Wireless networks (WLANs) are increasingly being used to link all types of different devices. In some cases, company devices even share a network with visitor devices. In hospitals, for example, such networks might even contain sensitive patient data as well.

Even though the necessary technology is available, the required segmentation of WLANs into VLANs is not yet common practice. Its implementation is as simple as it is sensible. Without this segmentation, unmonitored devices, such as those of external service providers, are in the same network as highly sensitive patient data.
The latter is therefore exposed to a significant risk of data abuse. It is important to close this gap with the macmon NAC solution.

Survey by GOV UK:

A recent government study showed only 38% of British firms were aware of the new guidelines surrounding the GDPR.

Among those surveyed, only 27% of them have already made changes to their operations in response to GDPR's introduction, with 49% of those making changes to their cyber security practices.

The above result, includes a total of 1519 business with employees ranging from 2 – 250+.

However, 73% of companies surveyed have not yet taken any specific technological or organisational measures in preparation for the GDPR.

These companies are therefore behind schedule and at risk of implementing the rules in force since May 25, 2018.
Adapting IT systems to the requirements of the GDPR is crucial, but is also seen as the biggest challenge by a fifth of those surveyed.

It is estimated that investments will be required in most cases. According to market researchers, the need for action is especially pressing when it comes to IT security.

The basic requirements here are the secure operation of IT, constantly monitoring it in real time and measures reacting to conspicuous activities in the network by means of a security solution like macmon.

Over half of all companies surveyed plan to invest more in cyber security in the coming months. As far as GOV UK is concerned, this is urgently required in order to use modern technology to efficiently avert security risks and attacks on personal data too. Detecting and combating security breaches is of fundamental importance in this process.

Source of the government study: Gov.UK:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/675620/Cyber_Security_Breaches_Survey_2018_-_Preparations_for_the_new_Data_Protection_Act.pdf

+44 118 978 0077

nac@macmon.eu

www.macmon.eu

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