MEDIA RELEASE

Think you're ready for GDPR compliance, but are your networks really secure?

Fontech's study reports over half of companies are open to risks due to the use of shared passwords to protect corporate networks

17 MAY 2018. MADRID. - The 25th of May is fast approaching, which is the deadline for GDPR enforcement. This is the most important change in data privacy regulation in 20 years which has come about in order to better protect and empower EU citizens data privacy. At an organizational level, it will have a dramatic impact on the way in which companies collect data, as well as what they do with that data.

But while we're all focusing on GDPR compliance, wouldn't it be a good moment to consider the overall security of our networks?

Ensuring GDPR password compliance

According to a study conducted by Fontech, the technology arm of Fon and leader in WiFi software solutions, over 50% of participants reported to use a shared password to connect to their workplace WiFi network. In the context of GDPR, the Data Controller of every business is obligated to ensure sufficient security in order to protect data, and the use of shared passwords may open them up to risks as they are far less secure than personalized passwords for each employee.

The threat is real

Cyber incidents targeting businesses nearly doubled from 82,000 in 2016 to 159,700 in 2017, driven by ransomware and new attack methods. And since the majority of cyberattacks are never reported, the actual number of incidents in 2017 could in fact be over 350,000 according to Online Trust Alliance, 2018. As these figures unfortunately show, enterprise networks are under threat.

What's even more frightening is that many of the attacks are not reported, because network administrators are not even aware that they have happened. This is largely due to the fact that they don't have real time visibility over who and what devices are connected to the enterprise network, and certainly don't have any sort of warning system in place in the case of any unusual activity.

Ensuring that no one unauthorized can access corporate networks, and therefore companies' information, seems like a sensible first step in data protection. Businesses should invest in a solution that gives administrators real-time control over who and what devices are connecting to their enterprise networks.

"Enterprise solutions in the market allow administrators to grant users access on an individual basis, and access can be limited at certain hours to avoid security breaches, for example during the night or at weekends. If any unauthorized devices try to connect to the WiFi network within these hours, they'll be blocked from doing so", according to Alex Puregger, Fon's CEO.

Taking the headache out of offering guest WiFi

The internet is so central to many of our day-to-day work tasks that visitors expect to be granted access to enterprise networks. According to Fontech's survey, over 70% of participants reported that their workplaces offer guest WiFi access. Managing the access of these individuals on an ad hoc basis can put a significant burden on IT teams. To ease the workload, many companies offer generic guest

WiFi access, protected by just one password that is openly shared with anyone that needs temporary access to the network. Again, this opens the company up to many risks.

Investing in a solution that enables administrators to offer Guest WiFi in a secure but simple way is a must for businesses in order to ensure external consultants, clients, and other visitors can easily access the network, but with controlled and limited access. Some of the solutions available in the market can be integrated with the employee's calendar, enabling them to automatically grant access to any guest included on the attendee list without having to do anything else.

Now is the time to take control

Next week GDPR will come into force and will apply to any company that processes the data of citizens residing in the European Union, regardless of their location. In the case of a breach of GDPR, companies could be fined up to 4% of annual global turnover or €20 Million (whichever is greater). In addition to the potential financial implications of a breach, the impact on a company's brand and reputation would be hugely damaging, something that has been unequivocally proven by a multitude of scandals that have been in the news in recent years.

About Fontech

Fontech, the technology arm of Fon, makes managing and operating WiFi smart and simple for operators and enterprises. Our portfolio of software-based solutions and team of experts empower our clients to deliver carrier-grade WiFi services in a secure, scalable, and uniquely flexible way, enabling an exceptional WiFi experience for their customers. We are the trusted WiFi software provider to top-tier global telcos and enterprises such as the Deutsche Telekom Group, SoftBank, Telstra, and Vodafone Group. More information at fontech.com

Fon is the global WiFi network. We pioneered residential WiFi sharing over a decade ago and, together with leading telcos, we've built the world's largest WiFi community of over 21 million hotspots. We are experts in keeping people seamlessly connected by aggregating residential and prime public WiFi footprints, as well as facilitating interconnection between WiFi networks. Our global clients include AT&T, British Telecom, Eurona, KPN, Proximus, Travel Club, and Virgin Mobile. Discover more at fon.com

Press Contact
Fon
Clare Bourke
clare.bourke@fon.com