Informazione Regolamentata n. 0524-4-2020	Data/Ora Ricezione 25 Marzo 2020 15:14:49	MTA - Star

Societa'	:	IT WAY
Identificativo Informazione Regolamentata	:	129509
Nome utilizzatore	:	ITWAYN02 - Passatempi
Tipologia	:	REGEM
Data/Ora Ricezione	:	25 Marzo 2020 15:14:49
Data/Ora Inizio Diffusione presunta	:	25 Marzo 2020 15:15:20
Oggetto	:	Itway continues to ensure internet networks.

Testo del comunicato

Vedi allegato.

Press Release

ITWAY CONTINUES TO ENSURE THE FULL OPERABILITY OF CYBER SECURITY ACTIVITIES TO DEFEND CORPORATE AND SMART WORKERS INTERNET NETWORKS

- **The virus runs on the web, contagious activities on the net grow by 15% with 50 million cyber-attacks per day**
- **Enhanced network defenses through a 24/7 operational task force**
- **Itway oversees more than 50,000 workplaces**

Ravenna, 25 March 2020 –**Itway S.p.A.**, a company listed on the MTA segment of the Italian Stock Exchange, active in the IT, Cyber Security and AI sectors, announces that its activities are among the services considered essential in the Decree issued by the Presidency of the Council on the subject of "**Urgent Measures to contrast national infection** " and to be included in the list of services considered essential within the ATECO codes, **J 58 to 63** - (**Itway: 62.02**) referring to the so called services of " consultancy in the IT technology sector" in derogation from the obligation to suspend activities as required by the same government measures.

Itway continues to ensure the operation of the security of computer networks through its subsidiary, the specialist Cyber Security' **Be Innova'** facility that manages the **'Network Operation Center'** and the **'Security Operation Center'** (N-SOC) in Trento. It is an active assault and defense team on several rounds 24/7, created as early as the end of February, which guarantees the security of Internet networks

Several groups have been activated in operational mode, combining the physical presence at the N-SOC Center with other Groups in agile H24 work mode to ward off threats that, especially in this period of increased number of people in smart working mode, surf through the Internet containing within the emails powerful viruses, malware, which from employee home PC can go as far as the corporate network. Malware are in action and find even more fertile ground with the new ways of working required by measures to contain infection throughout the country. The alarm has already been raised among cyber security experts around the world as dozens of sites and apps that use keywords such as: "coronavirus" "pandemia" "virus" etc. are being highlighted to attract unsuspecting network surfers and trigger the contagion that from the PC can get to the corporate network and vice versa.The world's cyberattacks per second are about 600 divided into the various types of attack (Deny Access, Web & Mail Virus, Intrusion detection, Antispam, Phishing, Bot, Vulnerability) with about 50 million/day of attacks for an annual total of about 18 billion attacks constantly growing.

"To date, Itway 'watches' over 50,000 digital jobs, employees and professionals who have adopted smart working from home." says the ***President and CEO of Itway G. Andrea Farina****. "Working from home isn't always safe and your PC needs to be protected like business facilities. You have to equip yourself with seats with security systems verified by the cyber security department of the company and if the company is an SME, and does not have an internal, or adequate, cyber security system, you need to rely on specialized facilities equipped with SOC ". "In times of Coronavirus"* ***continues Andrea Farina****" dozens of pirated emails from so-called senders such as the Higher Institute of Health and/or Civil Protection whose object is*

'coronavirus'. Before opening emails these must be checked, they must be cleaned up, as does our NSOC Specialist Task Force. 'Pirate' emails represent a kind of picklock to get into the company's servers, infecting computer systems and stealing data. Our reorganization of the work, following the COVID-19 pandemic, was adopted to enable the operation of all our specialists by providing continuity in monitoring and enhancing cyber security services even in the presence of a worst case scenario, which is the worst-case scenario for businesses". "*Among the customers we serve there are Local Governments, public transport companies, but also hospitals and large private companies", **continues Andrea Farina**, "the ongoing health emergency requires each of us to do our job with responsibility, respecting the recommendations of the health and government authorities and taking all measures to protect public health, its employees, customers and suppliers. No one can be exempted from this emergency and we also do it by 'protecting' the computers and computer networks of companies as well as the PCs of so many workers. In this period, the internet is certainly overloaded and this can lead to slowdowns in connections. We are talking about critical infrastructures that need to be protected. It is a kind of virtual treasure that can no longer be dispensed with and without which we would all go into crisis. And it is a duty and a responsibility for all of us to take care of our data, protect it and operate at the maximum security*."

In addition to the activity detected by the N-SOC of Itway, there are various sources that confirm a general growth trend of about 15% of the malicious cyber-hacking activities that take advantage of the ongoing health crisis. The pursuit of smart working has meant that, in the emergency of ensuring operational, security aspects have been neglected, often using unsafe Virtual Private Network (VPN) systems, obsolete PCs and often private, unsecured and up-to-date PCs, connected to VPNs with corporate networks. This brings a risk of infection, with viruses, at a very high rate.

The analogy with human life in these days is as narrow as it is representative of the pervasiveness of cybersecurity in the existence of people, companies and institutions.
The main threats that such as Cybersecurity Business Units are detected at the moment, are represented by:

- Cyber attacks – based on the exploitation of vulnerabilities of digital devices in use,
- Phishing & Smishing,
- Account take over.

To ensure and protect the safety of its employees and the continuity of service to customers, Itway has taken all necessary steps to allow the work activities of its staff to continue in Smart Working mode, with the exception of those whose presence is strictly necessary in the operational units of the H24 crisis and for those it has adopted the best protection of health in accordance with the rules imposed.

****

This press release is available at the Company Headquarters, on the Company's website at www.itway.com the Italian Stock Exchange, and at the 1info storage mechanism at www.1info.it

****

Founded in Ravenna on July 4, 1996, Itway S.p.A. is the head of an IT group working in the IT industry to design, manufacture and deploy technologies and solutions in the cybersecurity, artificial intelligence (AI) cloud computing and big data industry. For more than 25 years, the group has been the benchmark for Digital Transformation solutions and services. Itway has been listed on the Italian Stock Exchange since 2001.

CONTACTS:

ITWAY SpA

Tel. +39 0544 288711

investor.relations@itway.com

POLYTEMS HIR SRL

Tel. +39 06.69923324

Bianca Fersini +39 336742488

b.fersini@polytemshir.it

Silvia Marongiu + 39 3371464491

s.marongiu@polytemshir.it

Fine Comunicato n.0524-4	Numero di Pagine: 5