Informazione Regolamentata n. 0524-5-2020	Data/Ora Ricezione 25 Marzo 2020 15:12:19	MTA - Star

Societa'	:	IT WAY
Identificativo Informazione Regolamentata	:	129510
Nome utilizzatore	:	ITWAYN02 - Passatempi
Tipologia	:	REGEM
Data/Ora Ricezione	:	25 Marzo 2020 15:12:19
Data/Ora Inizio Diffusione presunta	:	25 Marzo 2020 15:15:24
Oggetto	:	Itway difende le reti internet.

Testo del comunicato

Vedi allegato.

Comunicato Stampa

ITWAY CONTINUA AD ASSICURARE IL FUNZIONAMENTO DELL'ATTIVITA' DI CYBER SECURITY A DIFESA DELLE RETI INTERNET AZIENDALI E DELLO SMART WORKING

- **Il virus corre sul web, crescono del 15% le attività di contagio in rete con 50 milioni di attacchi informatici al giorno**
- **Potenziate le difese sulla rete attraverso una task force operativa 24/7**
- **Itway vigila su oltre 50.000 posti di lavoro digitali**

Ravenna, 25 marzo 2020 –**Itway S.p.A.**, società quotata al segmento MTA di Borsa Italiana, attiva nel settore dell'IT, Cyber Security ed AI, comunica che le sue attività rientrano tra i servizi ritenuti essenziali indicate nel Decreto emesso dalla Presidenza del Consiglio in tema di "***Misure urgenti di contenimento del contagio sull'intero territorio nazionale***" in vigore dal 23 marzo 2020, che non si possono bloccare poiché comprese nella lista dei servizi considerati essenziali, e rientrante tra i codici ATECO, **J dal 58 al 63** - (**Itway: 62.02**) per i servizi di *"consulenza nel settore delle tecnologie dell'informatica"*, in deroga all'obbligo di sospensione delle attività come richiesto dagli stessi provvedimenti governativi.

Itway continua ad assicurare l'operatività nella sicurezza delle reti informatiche attraverso la sua controllata, la struttura specialistica di Cyber Security' **Be Innova'** che gestisce il '***Network Operation Center'*** ed il '***Security Operation Center'*** (N+SOC) di Trento. Si tratta di una di squadra d'assalto e di difesa attiva su vari turni 24/7, creata già da fine febbraio, che garantisce la sicurezza delle reti Internet. Sono stati attivati in modalità operativa diversi Gruppi che in logica di business continuity, uniscono la presenza fisica al Centro N+SOC con altri Gruppi in modalità di lavoro *agile* H24 per scongiurare le minacce che, soprattutto in questo periodo di aumento delle modalità di lavoro in smart working, navigano attraverso la rete Internet contenendo all'interno delle email potenti virus, malware, che dal proprio PC di casa possono arrivare fino alla rete aziendale. I malware sono in azione e trovano ancor più terreno fertile con le nuove modalità di lavoro richieste dalle misure di contenimento del contagio sull'intero territorio nazionale. L'allarme è già scattato tra gli esperti di cyber security di tutto il mondo poiché si stanno evidenziando decine di siti ed app che usano parole chiave come: "coronavirus" "pandemia" "virus" etc. per attirare ignari navigatori della rete e scatenare il contagio che dal proprio PC può arrivare alla rete aziendale e vice versa.

Gli attacchi informatici mondiali al secondo sono circa 600 suddivisi nella varie tipologie di attacco (Deny Access, Web & Mail Virus, Intrusion detection, Antispam, Phishing, Bot, Vulnerability) con circa 50 milioni/giorno di attacchi per un totale annuo di circa 18 miliardi attacchi in costante crescita.

"*Ad oggi Itway 'vigila' su oltre 50mila posti di lavoro digitali, di dipendenti e professionisti che hanno adottato lo smart working da casa".* **Commenta il Presidente e AD di Itway *G. Andrea Farina***. "*Lavorare da casa non è sempre sicuro ed il proprio PC deve essere protetto al pari delle strutture aziendali. Bisogna dotarsi di postazioni con sistemi di sicurezza verificati dal dipartimento di cyber security dell'azienda e se l'azienda è una PMI, e non possiede un sistema di cyber security interno, o adeguato, è necessario*

appoggiarsi a strutture specialistiche dotate di SOC". "*In tempi di Coronavirus"* **prosegue Andrea Farina"** *si stanno ricevendo decine di email pirata provenienti da sedicenti mittenti quali l'Istituto Superiore di Sanità e/o la Protezione Civile il cui oggetto è 'coronavirus'. Prima di aprire le email queste vanno controllate, devono essere bonificate, come fa la nostra Task Force specialistica del NSOC. Le email 'pirata' rappresentano una sorta di grimaldello per entrare nei server dell'azienda, infettando i sistemi informatici e rubando i dati. La nostra riorganizzazione del lavoro, a seguito della pandemia COVID-19, è stata adottata per consentire l'operatività di tutti i nostri specialisti fornendo continuità nel monitoraggio e potenziando i servizi di cyber security anche in presenza di un* ***worst case scenario****, ovvero lo scenario peggiore per le aziende*". "*Tra i clienti che serviamo figurano Pubbliche Amministrazioni Locali, società di trasporto pubblico, ma anche ospedali e grandi aziende private",* **continua Andrea Farina***, "l'emergenza sanitaria in corso, impone ad ognuno di noi di fare la propria parte con responsabilità, rispettando le indicazioni delle autorità sanitarie e di governo ed adottando ogni accorgimento a tutela della salute pubblica, dei propri dipendenti, clienti e fornitori. Nessuno si può chiamare fuori da questa emergenza e noi lo facciamo anche '****proteggendo****' i computer e le reti informatiche delle aziende così come i PC di tanti lavoratori. In questo periodo, la rete internet è certamente sovraccarica e ciò può portare a rallentamenti nelle connessioni. Parliamo di infrastrutture critiche che vanno protette. E' una sorta di tesoro virtuale di cui non si può più fare a meno e senza il quale andremmo tutti in crisi. Ed è un dovere ed una responsabilità per tutti noi prenderci cura dei nostri dati, proteggerli ed operare nel massimo della sicurezza*".

Oltre all'attività rilevata dal N+SOC di Itway, sono varie le fonti che confermano un trend generale di crescita del 15% circa delle attività malevole di hackeraggio-sciacallaggio informatico che approfittano della crisi sanitaria in corso. La rincorsa allo *smart working* ha fatto sì che, nell'emergenza di garantire l'operatività, si siano trascurati gli aspetti di sicurezza, utilizzando spesso sistemi VPN (Virtual Private Network) poco sicuri, PC obsoleti e spesso PC privati, non protetti e aggiornati, collegati in VPN con le reti aziendali. Questo comporta un rischio di contagio, con virus, a catena molto elevato.

L'analogia con i fatti umani di questi giorni è tanto stretta quanto rappresentativa della pervasività della sicurezza informatica nell'esistenza di persone, aziende ed istituzioni.

Le principali minacce che come Business Unit Cybersecurity si rilevano in questo momento, sono rappresentate da:

- Cyber attacks – basati sullo sfruttamento delle vulnerabilità dei dispositivi digitali in uso,
- Phishing & Smishing,
- Account take over.

Per garantire e tutelare la sicurezza dei propri dipendenti e la continuità del servizio reso ai clienti, Itway ha adottato tutte le misure necessarie per consentire la prosecuzione delle attività lavorative del proprio personale in modalità Smart Working, ad eccezione di coloro la cui presenza è strettamente necessaria nelle unità operative di crisi H24, per i quali ha adottato la migliore tutela della salute nel rispetto delle regole imposte.

****

Il presente comunicato è disponibile presso la Sede della Società, sul sito internet della Società all'indirizzo www.itway.com la Borsa Italiana, e presso il meccanismo di stoccaggio 1info all'indirizzo www.1info.it

****

Fondata a Ravenna il 4 luglio 1996, Itway S.p.A. è a capo di un gruppo che opera nel settore dell'IT per la progettazione, produzione e distribuzione di tecnologie e soluzioni nel comparto della cybersecurity, artificial intelligence (AI) cloud computing e big data. Il gruppo, da oltre 25 anni rappresenta il punto di riferimento nell'ambito delle soluzioni e servizi della Digital Transformation. Dal 2001 Itway è quotata alla Borsa Italiana.

CONTATTI:

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.0524-5	Numero di Pagine: 5