DATASINT S.R.L.
34123 TRIESTE - Viale della Terza Armata 14/b
Tel. 040.308309 - email info@datasint.it

Circolare del 5 ottobre 2017

Oggetto: nuova ondata di email fraudolente CHE CRIPTANO TUTTI I FILES!

Nuova ondata di email fraudolente CHE CRIPTANO TUTTI I FILES!
In genere contengono allegato .zip o .jar o .exe eseguibile che va automaticamente in esecuzione qualora venisse aperto!!!
Cripta TUTTI I FILES DEL COMPUTER E DELLA RETE!!!
L'antivirus in genere non riesce a riconoscerlo come virus.
Rinnoviamo l' invito alla MASSIMA CAUTELA NELL' APERTURA DELLE EMAIL!

In questo ultimo periodo si stanno intensificando le email contenenti virus di tipo "RANSOMWARE" ovvero che cifrano i files di dati presenti nel computer e nella rete aziendale e chiedono il riscatto per decrittarli: NON ESISTE RIMEDIO che pagare o ripristinare da un backup precedente.

Per questo motivo, invitiamo TUTTI alla MASSIMA CAUTELA nell'apertura delle email specialmente se contenenti files ALLEGATI.

Nella malaugurata eventualità che apriate l'allegato e vedete che non succede nulla, ovvero non si visualizza alcunchè, SPEGNETE IMMEDIATAMENTE IL PC!!!! Ci impiega del tempo per cifrare tutto, e lo fa SENZA CHE CE SE NE ACCORGA. Vi avvisa solo a cifratura avvenuta (quando non si può più fare nulla).

Qui di seguito alcune regole di base per non cadere nei tranelli:

1. Chiunque vi scriva, sia banca, corriere espresso o azienda elettricità/gas o azienda in genere DEVE SEMPRE METTERE NEL TESTO IL VOSTRO NOME E/O LA VOSTRA AZIENDA, e non solo l' indirizzo email. Le email che non contengono NEL TESTO il vostro nome o la vostra ragione sociale, ma hanno allegati o link (ovvero un rimando) a siti esterni sono SICURAMENTE VIRUS!!!!!
2. I corrieri espresso nè ENI, nè ENEL o aziende di servizi MANDANO email con allegati né chiedono di andare sul loro sito se non vi siete registrati!!!!! (se siete registrati andateci NON attraverso il link che vi propongono).
3. Se ricevete una email da un corriere e non aspettate da quel corriere qualcosa, è un virus o simile. I CORRIERI NON MANDANO MAI EMAIL SENZA SPECIFICARE IL VOSTRO INDIRIZZO/NOME/DITTA.
4. Alle volte non vi è un allegato ma solo un link (ovvero un rimando) ad un sito esterno: questa è una cosa ESTREMAMENTE PERICOLOSA! ricordatevi di verificare che il link punti effettivamente a quanto detto: per esempio se viene da Unicredit, l'indirizzo DEVE iniziare per https://www.unicreditbanca.it/qualcosa, comunque DEVE essere il sito UFFICIALE.
5. Se avete dubbi NON aprite l'allegato e/o NON cliccate sul link: chiedete PRIMA conferma a chi ve la dovrebbe aver inviata.
6. Ultimamente si sono appropriati di rubriche email e quindi potrebbero arrivare anche da persone conosciute: prestare SEMPRE MOLTA ATTENZIONE e non cliccare su eventuali link presenti nelle email che arrivano da amici/colleghi, se non sono accompagnate da parole che indicano che è stata scritta da chi conoscete; se vi è solo il link e nient'altro, è PROBABILE UN TENTATIVO DI VIRUS o peggio[1].
7. Non confidate nell'antivirus in quanto alle volte i RAMSONWARE riescono a "saltarlo": l'antivirus è come l'ABS delle automobili, entra in funzione in caso di necessità, ma non fa miracoli!
8. NON USARE MAI LA POSTA ELETTRONICA SENZA PRESTARE ATTENZIONE: USATE SEMPRE LA MASSIMA CAUTELA!
9. ANCHE LA Posta Certificata NON e' immune da questo tipo di attacchi!

[1] Definizione di "peggio": virus che vi cripta tutti i documenti che trova (anche sul server) e poi dovete PAGARE per poterli decrittare: NON ESISTE RIMEDIO!!!!