CIRCOLARE 20/01 del 14.1.2020

Attacchi Ransomware e Sicurezza Informatica

Gentile cliente,
negli ultimi mesi abbiamo riscontrato un aumento sensibile di attacchi informatici di tipo Ransomware, ossia attacchi che rendono inaccessibili **tutti** i dati aziendali con l'obiettivo di richiedere un riscatto per sbloccare l'accesso ai dati.

Molti attacchi informatici verso grandi imprese e multinazionali non vengono resi noti, per evitare ulteriori possibili attacchi ed un evidente danno d'immagine. Ciò nonostante, nelle ultime settimane si sono intensificate le notizie che parlano di infezioni da ransomware:

1. https://www.cybersecurity360.it/news/unicredit-accesso-non-autorizzato-a-3-milioni-di-dati-ecco-i-rischi-e-come-proteggersi/
2. https://www.pmi.it/tecnologia/software-e-web/318251/consulenti-del-lavoro-allarme-pec-infette.html
3. https://www.zdnet.com/article/ransomware-attack-hits-major-us-data-center-provider/
4. https://www.tomshw.it/altro/attacco-ransomware-contro-lospedale-fatebenefratelli-di-erba-35mila-radiografie-inaccessibili/

Vi invitiamo a prestare la **massima attenzione** alle mail e ai siti Web a cui accedete perché una disattenzione potrebbe causare seri danni alla Vostra Azienda.
Di seguito riteniamo opportuno fornirvi alcuni suggerimenti:

1. In generale, **non aprite** e-mail "dubbie" di persone che non conoscete, né tantomeno cliccate sui link contenuti
2. Verificate bene l'indirizzo e-mail del mittente (non solo il nome visualizzato, ma anche l'indirizzo) per essere sicuri che sia corretto: spesso il nome visualizzato come mittente è corretto, ma l'indirizzo è palesemente **fasullo**
3. Verificate il testo della mail, spesso le e-mail di phishing contengono **errori** di ortografia o di grammatica
4. Istituti di credito, Poste, PayPal, corrieri ed eventuali altri servizi/siti a cui siete iscritti **non chiedono mai** i dati di accesso via mail o via telefono
5. **Non credete** alle e-mail allarmanti: "Il tuo conto verrà disabilitato se…" oppure "Ho installato un software sul tuo PC che mi permette di spiarti dalla webcam..."
6. **Non credete** alle "offerte irrinunciabili" o alle mail di comunicazione di vincite
7. **Verificate** l'indirizzo web riportato nel link: passandoci sopra con il mouse senza cliccare diventa visibile il **link** (questo riporta al nostro sito) e si può facilmente capire se è fasullo.

Se avete il dubbio di aver aperto una mail o un allegato o di aver visitato un sito Web non corretto vi consigliamo di spegnere il PC e avvisare immediatamente i vostri riferimenti IT. Il danno spesso non è immediatamente visibile, ma una rilevazione rapida permette di eliminare o ridurre al minimo i problemi causati da Ransomware.

► Per fare un check-up sui livelli di sicurezza dei vostri dati, prendete contatto con SET Group scrivendo a commerciale@setgroup.com.

La Divisione IT Security

SET srl
Via Marosticana 279, 36031 Dueville (VI) ITALY
Cod. Fisc. / P. IVA / Reg. Impr. VI 01957980244
REA VI n° 196653 | pec@pecsetgroup.com
Cap. Sociale Euro 103.480,00 int. versato

Filiali
Verona | Padova | Treviso | Venezia | Pordenone
Contatti
Tel. +39 0444 594044 | Fax +39 0444 593878
info@setgroup.com | [Skype] Set_group