Linee guida per riconoscere e prevenire l'insediamento dei virus all'interno dei sistemi informatici

Consapevolezza, la prima fase della sicurezza.

Cari Colleghi,

In questa terza Newsletter, vogliamo affrontare un tema che è particolarmente avverso a chi lavora con i dati e con i sistemi informatici: **i virus e le loro conseguenze.**
Esistono diversi tipi di virus informatici, tra cui worm, trojan, spyware, keylogger e ransomware. Ognuno di questi virus ha delle caratteristiche specifiche dannose per i nostri sistemi, è dunque necessario **saperli riconoscere** per prevenire danni sia al proprio PC ma anche a tutti i server e database a cui sono collegati.

Quali sono i virus e come riconoscerli?

Per riconoscere un virus informatico, è importante prestare attenzione ai segnali di allarme, come rallentamenti del sistema, popup sospetti o messaggi di errore. Qui di seguito elenchiamo alcune caratteristiche specifiche dei virus che potreste incontrare:

Virus: I virus sono programmi dannosi che si replicano e diffondono da un sistema all'altro. Possono causare danni come **la cancellazione di file** o la corruzione dei dati, e diffondersi attraverso diversi canali, come allegati di posta elettronica, file scaricati da Internet o dispositivi di archiviazione esterni infetti.

Worm: I worm sono programmi dannosi che si diffondono attraverso una rete, sfruttando le vulnerabilità del sistema. Possono causare **la saturazione della rete** o la cancellazione di file, diffondersi rapidamente attraverso una rete e possono causare danni a molte macchine in poco tempo.

Trojan: I trojan si presentano solitamente come programmi legittimi ma che in realtà contengono codice dannoso. I trojan portano conseguenze negative come il furto di dati o **la creazione di backdoor** per accedere al sistema e possono diffondersi attraverso diversi canali come e-mail di phishing, siti web dannosi o applicazioni scaricate da fonti non attendibili.

Spyware: Gli spyware raccolgono informazioni sul sistema e sulle attività dell'utente senza il suo consenso. Questi virus arrecano molti danni come la riduzione delle prestazioni o **la violazione della riservatezza dei file** e possono diffondersi attraverso siti web o applicazioni malevole.

Keylogger: I keylogger sono programmi dannosi che registrano le attività dell'utente sul computer, inclusi i tasti premuti sulla tastiera. Possono essere utilizzati per **rubare informazioni sensibili** come password, numeri di carta di credito e altre informazioni personali. Una volta installati, registrano silenziosamente tutte le attività dell'utente e inviano le informazioni a un server remoto.

Ransomware: I ransomware, come già detto nelle Newsletter precedenti, sono particolarmente pericolosi perché **criptano i file del sistema** rendendoli inaccessibili all'utente. Il ripristino dell'accesso ai dati avviene tramite segnalazione alla Polizia Postale che sarà incaricata di individuare **i criminali informatici responsabili dell'attacco**.

Come ci proteggiamo?

Conoscere i diversi tipi di virus informatici ci può aiutare a capire come proteggere le nostre informazioni aziendali ed a evitare di diventare vittima di attacchi informatici come il phishing o lo spamming. Di uguale importanza è **sapere come proteggere il proprio sistema e le proprie informazioni** personali al fine prevenire danni finanziari e proteggere la riservatezza delle informazioni. Per evitare di contrarre virus informatici, è importante **adottare alcune buone pratiche**, come utilizzare software antivirus, aggiornarli frequentemente, installare le patch di sicurezza del nostro sistema operativo ed evitare di cliccare su link sospetti o scaricare file da fonti non attendibili. Dunque, riportiamo di seguito alcuni consigli da seguire per ridurre l'insediamento degli attacchi informatici:

Verificate che il **software antivirus installato sul PC sia sempre aggiornato**. Un antivirus aggiornato può proteggere da diversi tipi di virus informatici, come virus, worm e trojan.

Installate sempre gli aggiornamenti di sicurezza del sistema operativo. **Gli aggiornamenti** del sistema operativo spesso includono patch di sicurezza che **coprono le vulnerabilità del sistema** e possono proteggerti da eventuali minacce. È di fondamentale importanza controllare che questi aggiornamenti siano installati perché, spesso, l'aggiornamento automatico non riesce a scaricare correttamente i file di installazione.

Evitate di cliccare su link sospetti o di scaricare file da fonti non attendibili. I link sospetti possono portarvi su **siti web dannosi che possono infettare i sistemi**. Scaricare file da fonti non attendibili può essere pericoloso, poiché questi file potrebbero contenere virus informatici.

Fate attenzione ai messaggi di posta elettronica sospetti o che provengono da mittenti sconosciuti. I messaggi di posta elettronica sospetti **possono contenere virus informatici** o link a siti web dannosi.

Utilizzate una connessione sicura. Quando siete su Internet, **assicuratevi di utilizzare una connessione sicura**, ovvero utilizzare una connessione crittografata, come una connessione HTTPS, che protegge i dati durante la navigazione.

Fate regolarmente il backup dei dati su un dispositivo esterno o su un servizio di cloud. In questo modo, se il sistema viene infettato da un virus informatico, potranno essere recuperati tutti i dati che, purtroppo, dovranno essere cancellati tramite i ripristini totali.

Una considerazione obbligatoria da fare è che nella protezione dei sistemi da virus e minacce informatiche **non esiste il cosiddetto "rischio 0".**
Rendere il rischio accettabile e gestibile è possibile tramite una maggiore **conoscenza delle minacce** e tramite **comportamenti virtuosi** che mitigano il rischio.

Saluti,
Settore "Infrastrutture Digitali e Sicurezza",
Responsabile Protezione Dati,
Ufficio Privacy Regione Calabria.