Lucca 08 Febbraio 2023

Buongiorno

In merito agli attacchi hacker che si stanno verificando ai sistemi informatici nazionali, dobbiamo mai come ora dare la massima attenzione ai dettami della cyber security. Consideriamo che solo nel nostro Paese nel 2022 abbiamo avuto un aumento del 138% di attacchi informatici.
Spesso e volentieri sia il cittadino che i vari consigli di amministrazione di società pubbliche e private non danno molta importanza a questi eventi fino a quando non capita qualcosa di veramente grave che va a danneggiare da un punto di vista economico gli uni e da un punto di vista di immagine gli altri.
Come sappiamo gli attacchi informatici sono tentativi da parte di individui o gruppi di compromettere la sicurezza di un sistema informatico o di rubare informazioni sensibili “regolamento europeo 2016/679 gdpr”.
Questi attacchi possono assumere molte forme, tra cui phishing, malware, ransomware, intrusioni di rete e molto altro.
Per essere il più chiaro possibile andrò a spiegare cosa si intente per gli attacchi sopra elencati:

Phishing:
è una forma di attacco informatico che mira a ottenere informazioni personali o finanziarie degli utenti tramite l'inganno. Questo viene fatto di solito tramite e-mail fraudolente o siti web contraffatti che sembrano essere di società affidabili, come banche o servizi di e-commerce. Gli utenti sono invitati a inserire informazioni sensibili come nome utente, password o informazioni sulle carte di credito, che vengono quindi utilizzate per il crimine finanziario o l'identità.

Malware:
è una contrazione della parola inglese "malicious software", che significa "software dannoso". Si riferisce a qualsiasi tipo di software progettato per danneggiare, rubare o controllare il sistema informatico senza il consenso dell'utente. I tipi di malware più comuni includono virus, worm, trojan, adware, spyware e ransomware. Questi programmi possono distruggere i dati, rallentare il sistema, rubare informazioni personali o addirittura impedire l'accesso al computer. Il malware può diffondersi attraverso e-mail, siti web compromessi, programmi gratuiti o software scaricato dal web.

Ransomware:
è un tipo di malware che cifra i file sul computer della vittima e ne chiede il riscatto per ottenere la chiave di decifratura. Questo significa che gli utenti non possono più accedere ai propri file e devono pagare una somma di denaro, spesso in criptovaluta, per ottenere la chiave per decifrarli. Se non pagati, gli hacker minacciano di cancellare o pubblicare i file. Il ransomware è una minaccia per la sicurezza informatica e può causare notevoli danni, sia finanziari che alle attività. Per prevenire gli attacchi ransomware, è importante eseguire regolarmente il backup dei dati, tenere il software aggiornato e non aprire e-mail o allegati sospetti.

In baso a quanto detto per prevenire gli attacchi informatici, è importante adottare buone pratiche di sicurezza informatica, come la creazione di password forti, la manutenzione regolare del software cioè fare sempre gli aggiornamenti di sistema così che patch correttive vadano a immunizzare alcune falle del sistema stesso, inoltre è importante utilizzare software di antivirus “non gratuiti” per la diffidenza verso e-mail o link sospetti.
Non meno importante ed essere informati e formati sulle minacce informatiche più recenti su come riconoscerle e prevenirle.

DIEMME INFORMATICA s.r.l.
Sede legale – Via Ceppo di Melo 27, 55014 Marlia Lucca (LU) c.f e p.iva 02115770469
Sede operativa - Via Mattei Enrico 721/E, 55100 Lucca (LU)
Tel.0583491734 – Fax 05831861308 – info@diemmeinformatica.com – www.diemmeinformatica.com
Socio Federprivacy

Di seguito vado ad elencare alcune buone regole di comportamento da adottare sia sul posto di lavoro che per gli affari personali sempre in merito alla sicurezza informatica di cui sopra;

Per quanto riguarda la posta:

- Tutta la corrispondenza di lavoro deve essere inviata da un indirizzo e-mail ufficiale della azienda/scuola
- Evitare di utilizzare account personali per il flusso di lavoro
- Salva i messaggi personali in una cartella designata
- Organizza la tua e-mail e file per progetto o tipo di lavoro
- Evitare di aprire gli allegati da una fonte non attendibile es: miur@ministerio.org
- Evitare di fare clic sui collegamenti in un'e-mail da una fonte non attendibile
- Evitare di fornire l'ID utente e la password o altre informazioni riservate in un'e-mail o in una risposta a un'e-mail
- Riconoscere e prevenire le truffe di phishing via e-mail.

Per quanto riguarda la tua postazione di lavoro:

- Blocca il tuo computer quando non sei presente;
- Disconnettersi o spegnere quando si torna a casa;
- Scollegare il computer dalla rete wireless quando si utilizza una rete cablata;
- Patch e aggiorna il tuo sistema operativo;
- Installa e aggiorna il tuo antivirus e anti-malware con le ultime definizioni di sicurezza;
- Crea un ID utente univoco quando condividi un computer con altri;
- Abilita il blocco popup nel browser;
- Informati dettagliatamente (ad es. chiedendo informazioni al CED) prima di installare o scaricare software sul tuo computer;
- Metti in sicurezza la postazione del tuo ufficio quando esci.

Questo sono solamente alcuni piccoli accorgimenti semplici e fattibili da tutti.

Ringraziandovi per l'attenzione
DPO Dott. Gabriele Mencarini